DOI: 10.62829/VNHN.371.46.51.

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ THEO PHÁP LUẬT CỦA MỘT SỐ QUỐC GIA VÀ ĐỀ XUẤT CHO VIỆT NAM

✍TS. Hoàng Đình Thăng

● **TÓM TẮT:** *Trong thời đại chuyển đổi số, giao dịch điện tử ngày càng phổ biến và đã trở thành nền tảng quan trọng của hoạt động thương mại, dịch vụ công và quản trị xã hội. Cùng với đó, đặc tính phi vật chất, dễ sao chép, truyền tải nhanh và xuyên biên giới của dữ liệu điện tử đã đặt ra nhiều rủi ro về an toàn thông tin, như lộ lọt dữ liệu, giả mạo giao dịch, tấn công mạng, xâm phạm quyền riêng tư, tranh chấp chữ ký điện tử… Vì vậy, nhiều quốc gia đã ban hành các quy định pháp luật để bảo vệ các bên tham gia giao dịch điện tử, đảm bảo an toàn thông tin. Trong bài viết này, chúng ta sẽ khảo sát pháp luật đảm bảo an toàn thông tin trong giao dịch điện tử ở một số quốc gia (trong đó có Việt Nam). Từ đó rút ra bài học kinh nghiệm và đề xuất giải pháp hoàn thiện pháp luật, củng cố hạ tầng kỹ thuật, tăng cường thực thi và nâng cao nhận thức xã hội, nhằm xây dựng một môi trường giao dịch điện tử an toàn, tin cậy và hội nhập đối với Việt Nam.*

● ***Từ khóa:*** *An toàn thông tin; Giao dịch điện tử, Định danh điện tử; Chữ ký điện tử; Bảo vệ dữ liệu cá nhân; So sánh pháp luật; Việt Nam.*

● **ABSTRACT:** *In the digital transformation era, electronic transactions have become increasingly common and serve as an essential foundation for commercial activities, public services, and social governance. Along with this, the intangible nature of electronic data - its ease of duplication, rapid transmission, and cross-border circulation has given rise to numerous information security risks, such as data breaches, transaction forgery, cyberattacks, privacy violations, and disputes over electronic signatures. Therefore, many countries have enacted legal regulations to protect parties involved in electronic transactions and to ensure information security. This article examines the legal frameworks for ensuring information security in electronic transactions in several countries (including Vietnam). From this, it draws lessons and proposes solutions to improve legislation, strengthen technical infrastructure, enhance enforcement, and raise public awareness, with a view to building a safe, reliable, and internationally integrated electronic transaction environment for Vietnam.*

● ***Keywords:*** *N Information security; Electronic transactions; Digital identity; Electronic signature; Personal data protection; Comparative law; Vietnam.*

Ngày nhận bài: 05/9/2025 Ngày bình duyệt: 23/9/2025 Ngày duyệt đăng: 26/9/2025

Sự phát triển mạnh mẽ của công nghệ thông tin và truyền thông đã tạo ra những thay đổi căn bản trong đời sống kinh tế – xã hội. Trong đó, giao dịch điện tử nổi lên như một phương thức giao dịch chủ yếu, thay thế dần các giao dịch truyền thống. Từ thương mại điện tử, dịch vụ tài chính trực tuyến, đến chính phủ điện tử và các ứng dụng số trong y tế, giáo dục, giao dịch điện tử đang trở thành động lực trung tâm thúc đẩy kinh tế số, đổi mới sáng tạo và hội nhập quốc tế.

Trong lĩnh vực pháp luật, nhiều quốc gia và tổ chức quốc tế đã ban hành các văn kiện quan trọng nhằm điều chỉnh hoạt động giao dịch điện tử và bảo vệ an toàn thông tin. Tại Việt Nam, khung pháp lý về giao dịch điện tử đã được hình thành với Luật Giao dịch điện tử năm 2005 (vừa được sửa đổi năm 2023), Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018 và các văn bản hướng dẫn thi hành. Đây là nền tảng quan trọng để thúc đẩy kinh tế số và bảo đảm an toàn thông tin. Tuy vậy, hệ thống pháp luật hiện hành vẫn còn tồn tại một số bất cập như: quy định chồng chéo giữa các luật, thiếu hướng dẫn chi tiết cho các giao dịch xuyên biên giới, năng lực thực thi còn hạn chế, chế tài chưa đủ sức răn đe, trong khi nhận thức của cộng đồng về bảo mật thông tin chưa cao. Điều đó khiến Việt Nam đối diện nguy cơ gia tăng tội phạm mạng, mất niềm tin của người dùng, và bị tụt hậu so với các nước trong khu vực về năng lực bảo vệ an toàn giao dịch điện tử.

PHÁP LUẬT ĐẢM BẢO AN TOÀN THÔNG TIN TRONG GIAO DỊCH ĐIỆN TỬ Ở MỘT SỐ QUỐC GIA

1.Việt Nam

** Luật Giao dịch điện tử 2023 (20/2023/QH15)* với những nội dung sau:

- Ban hành ngày 22/6/2023, có hiệu lực từ 1/7/2024, thay thế Luật Giao dịch điện tử năm 2005.

- Mở rộng phạm vi áp dụng: Luật điều chỉnh giao dịch điện tử trong mọi lĩnh vực, kể cả những lĩnh vực trước đây không được luật cũ cho phép thực hiện bằng phương thức điện tử (ví dụ giấy chứng nhận quyền sử dụng đất, giấy chứng nhận đăng ký kết hôn, khai sinh, khai tử …) nếu các luật chuyên ngành không cấm.

- Quy định về chữ ký điện tử ("electronic signature") và chữ ký số ("digital signature"). Luật mới phân loại chữ ký điện tử theo mục đích sử dụng: chữ ký chuyên dụng, chữ ký số công khai, chữ ký chuyên môn công vụ… để đảm bảo tính xác thực.

- Công nhận chữ ký điện tử / chứng thư số nước ngoài nếu thỏa mãn điều kiện nhất định như nhà cung cấp chứng thư số nước ngoài đáp ứng tiêu chuẩn do Việt Nam quy định; có thể có đại diện tại Việt Nam...

** Các quy định đảm bảo an toàn thông tin:*

- Luật Giao dịch điện tử mới kết hợp quy định "bảo đảm an toàn thông tin, an ninh mạng, pháp luật về bảo vệ dữ liệu cá nhân" - các tổ chức, cá nhân tham gia giao dịch điện tử phải tuân thủ các luật này.

- Các hành vi bị cấm trong giao dịch điện tử (ví dụ: sử dụng giao dịch điện tử để gây hại lợi ích quốc gia, an ninh; cản trở hoặc phá hoại hệ thống thông tin; thu thập, sử dụng, công bố hoặc phát tán dữ liệu/thông điệp dữ liệu trái phép; giả mạo, làm sai lệch, xóa bỏ thông điệp dữ liệu; gian lận, giả mạo chữ ký điện tử, chứng thư số; việc sử dụng tài khoản/ chứng thư/chữ ký số trái phép).

** Những điểm mạnh, hạn chế:*

- *Ưu điểm:* Luật mới bao phủ rộng hơn, cập nhật với thực tế công nghệ; loại bỏ những "khoảng trống" mà luật cũ bỏ lại. Công nhận chữ ký điện tử/ chứng thư số nước ngoài - hỗ trợ giao dịch quốc tế. Quy định rõ các hành vi bị cấm, hình phạt, trách nhiệm pháp lý.

- *Hạn chế / thách thức:* Việc thực thi, kiểm tra, giám sát chuẩn kỹ thuật, năng lực bảo mật của các bên cung cấp dịch vụ chứng thư/chữ ký số. Yêu cầu kỹ thuật và bảo mật có thể cao, gây khó cho các tổ chức nhỏ, vùng còn hạn chế về hạ tầng. Vấn đề về bảo vệ dữ liệu cá nhân, quyền riêng tư trong giao dịch điện tử, đặc biệt khi trao đổi dữ liệu xuyên biên giới.

2. Liên minh Châu Âu (EU)

2.1. Quy định eIDAS

- Regulation (EU) No 910/2014 (eIDAS - *electronic IDentification, Authentication and trust Services*) có hiệu lực từ 1/7/2016 tại các quốc gia thành viên.

- eIDAS định nghĩa rõ các loại chữ ký điện tử: *Standard Electronic Signature* (SES), *Advanced Electronic Signature* (AES), và *Qualified Electronic Signature* (QES).

- Một chữ ký điện tử có thể bị từ chối giá trị pháp lý nếu không đáp ứng yêu cầu kỹ thuật nhiệm vụ hay nếu luật chuyên ngành yêu cầu mức cao hơn; nhưng không được từ chối chỉ vì nó ở dạng điện tử.

2.2. An toàn thông tin và dịch vụ tin cậy (trust services)

- eIDAS quy định các *trust service providers* (cung cấp dịch vụ tin cậy) phải tuân các tiêu chuẩn kỹ thuật, được chứng nhận, chịu trách nhiệm pháp lý. Bao gồm chứng thực chữ ký điện tử, dấu điện tử, xác thực điện tử,...

- Hệ thống xác thực điện tử xuyên biên giới: các chữ ký điện tử hoặc dịch vụ công nhận từ một quốc gia thành viên phải được quốc gia thành viên khác công nhận theo điều kiện.

2.3. Bảo vệ dữ liệu cá nhân

- EU có GDPR (General Data Protection Regulation) bảo vệ quyền riêng tư và dữ liệu cá nhân, áp dụng đối với mọi dữ liệu cá nhân được xử lý trong giao dịch điện tử.

- GDPR quy định rõ về sự đồng thuận (consent), quyền truy cập dữ liệu, quyền chỉnh sửa, quyền bị "quên", chế tài khi vi phạm.

3. Hoa Kỳ

3.1. ESIGN Act và UETA

- Electronic Signatures in Global and National Commerce Act (ESIGN Act) năm 2000: luật liên bang, công nhận chữ ký điện tử có giá trị pháp lý tương đương chữ ký viết tay, miễn là các bên đồng ý sử dụng phương thức điện tử; không được từ chối hợp đồng chỉ vì nó ở dạng điện tử.

- Uniform Electronic Transactions Act (UETA): luật cấp tiểu bang (hầu hết các tiểu bang áp dụng) bổ sung khung pháp lý cho giao dịch điện tử, chữ ký điện tử.

3.2. An toàn thông tin & bảo mật:

- Các luật liên bang hoặc tiểu bang về bảo vệ thông tin cá nhân, dữ liệu người dùng (ví dụ luật riêng về bảo mật dữ liệu, luật bảo vệ quyền riêng tư) hỗ trợ đảm bảo an toàn thông tin cho giao dịch điện tử.

- Yêu cầu về chứng thực, xác thực, lưu trữ hồ sơ điện tử, bằng chứng để có thể sử dụng trong tranh chấp.

4. Canada

- Có luật PIPEDA (*Personal Information Protection and Electronic Documents Act*) - luật liên bang bảo vệ thông tin cá nhân và quy định về việc sử dụng hồ sơ/tài liệu điện tử.

- Các tỉnh, bang cũng có luật riêng tương tự hoặc bổ sung khung pháp luật cho giao dịch điện tử/ chữ ký điện tử. Luật đồng bộ hóa (Uniform Electronic Commerce Act - UECA) được thông qua nhiều tỉnh bang để tạo sự thống nhất.

5. Australia

- Luật Electronic Transactions Act 1999 (ETA) ở cấp Liên bang, cùng với các quy định triển khai, cho phép giao dịch điện

tử được thực hiện và các chữ ký điện tử được công nhận.

- Các bang / lãnh thổ (States/Territories) cũng có luật riêng theo hướng tương tự. Quy định về tính xác thực, tính toàn vẹn của giao dịch, sự đồng ý của các bên, đảm bảo phương thức xác thực phù hợp tùy mức độ rủi ro.

SO SÁNH, BÀI HỌC RÚT RA

Về khung pháp lý tổng thể:

- *Các quốc gia phát triển:* Rõ ràng: luật liên quan tới giao dịch điện tử + chữ ký điện tử + bảo vệ dữ liệu cá nhân + yêu cầu an toàn thông tin + công nhận quốc tế.

- *Ở Việt Nam:* Pháp luật mới (2023) đáp ứng tốt các yếu tố tổng thể hơn so với luật cũ: mở rộng phạm vi, công nhận quốc tế, quy định rõ các hành vi bị cấm.

Công nhận chữ ký điện tử / chứng thư số / dịch vụ tin cậy:

- *Các quốc gia phát triển*: EU eIDAS đặt ra tiêu chuẩn kỹ thuật và hành chính cao với QES, AES; các quốc gia như Hoa Kỳ, Canada cho phép loại chữ ký đơn giản nếu đáp ứng điều kiện về xác thực, ý chí; Australia cũng tương tự.

- *Ở Việt Nam:* Việt Nam mới quy định phân loại chữ ký điện tử, công nhận chữ ký nước ngoài nếu đáp ứng tiêu chuẩn.

An toàn dữ liệu, bảo mật, quyền riêng tư:

- *Các quốc gia phát triển:* GDPR ở EU là chuẩn mực; luật liên bang/tiểu bang ở Mỹ; ở Canada PIPEDA; Australia có các quy định bảo mật; các nhà cung cấp tin cậy phải chịu trách nhiệm về bảo mật.

- *Ở Việt Nam:* Việt Nam có luật an toàn thông tin, luật an ninh mạng, luật bảo vệ dữ liệu cá nhân; nhưng thực thi, chuẩn kỹ thuật, năng lực vẫn là thách thức.

Xử lý hành vi vi phạm / trách nhiệm pháp lý:

- *Các quốc gia phát triển:* Có chế tài, trách nhiệm rõ: ví dụ nhà cung cấp dịch vụ tin cậy trong EU chịu trách nhiệm nếu vi phạm tiêu chuẩn; trong Mỹ, hợp đồng điện tử nếu có tranh chấp có thể đưa ra chứng cứ; GDPR có xử phạt hành chính nặng.

- *Ở Việt Nam:* Việt Nam quy định các hành vi bị cấm, trách nhiệm; cần hoàn thiện thêm quy định xử phạt, giám sát; hạ tầng kỹ thuật, tiêu chuẩn chứng thực phổ biến chưa đồng đều.

Khả năng công nhận xuyên biên giới:

- *Các quốc gia phát triển:* EU eIDAS: chữ ký điện tử và nhận dạng điện tử được công nhận giữa các quốc gia thành viên; Hoa Kỳ có thỏa thuận quốc tế; nhiều quốc gia đối tác công nhận chứng thư số quốc tế nếu đáp ứng điều kiện.

- *Ở Việt Nam:* Việt Nam mới công nhận chữ ký / chứng thư nước ngoài nếu đáp ứng các điều kiện Việt Nam quy định — là một bước tiến; song thực thi và khả năng được công nhận ở nước ngoài phụ thuộc vào tính chuẩn và sự tin cậy trong tiêu chuẩn kỹ thuật và pháp lý.

NGUYÊN TẮC VÀ BIỆN PHÁP THỰC TẾ CẦN ÁP DỤNG

Dựa trên các quy định của các quốc gia nói trên, có thể rút ra những nguyên tắc và biện pháp sau để đảm bảo an toàn thông tin trong giao dịch điện tử:

1. *Xác thực & ký số / chứng thực (Authentication & Digital Signature):* Sử dụng chữ ký điện tử được chứng thực theo tiêu chuẩn pháp luật để đảm bảo tính xác thực, tính toàn vẹn của thông điệp. (VD: Nhật Bản - Act on Electronic Signatures). Xác minh danh tính người gửi, người nhận; sử dụng chứng chỉ số, dịch vụ tin cậy.

2. *Yêu cầu kỹ thuật & tổ chức về bảo vệ dữ liệu (Technical & Organizational Measures):* Mã hóa dữ liệu khi truyền (in transit) và khi lưu trữ (at rest). Kiểm soát truy cập (access control), phân quyền rõ

ràng; theo nguyên tắc "ít quyền nhất cần thiết" (least privilege). Theo dõi, giám sát, ghi log hoạt động; phát hiện, cảnh báo vi phạm. Bảo mật vật lý cơ sở hạ tầng, môi trường lưu trữ.

3. *Quản lý rủi ro & xử lý vi phạm (Risk Management & Incident Response):*Đánh giá rủi ro thường xuyên, cập nhật các điểm yếu về công nghệ, lỗ hổng. Có kế hoạch ứng phó sự cố (incident response plan), bao gồm xác định, ngăn chặn, giảm thiểu thiệt hại, thông báo. Yêu cầu thông báo vi phạm dữ liệu theo quy định pháp luật (ví dụ 30 ngày ở Mỹ nếu đủ mức người bị ảnh hưởng).

4. *Quyền của người dùng / người tiêu dùng (User / Consumer Rights & Transparency):* Thông báo rõ ràng các điều khoản giao dịch: người bán là ai, giá, phương thức thanh toán, phương thức hủy, trả hàng … (ví dụ Nhật Bản – Act on Specified Commercial Transactions). Phải cho phép người dùng truy cập, chỉnh sửa, xóa dữ liệu cá nhân; quyền khiếu nại; biết vi phạm nếu có. Minh bạch về việc thu thập, sử dụng dữ liệu: mục đích, thời gian lưu trữ, nếu chia sẻ cho bên thứ ba.

5. *Tuân thủ các tiêu chuẩn quốc tế / công nghiệp (Standards & Certifications):* Áp dụng các tiêu chuẩn như ISO/IEC 27001 về hệ thống quản lý an toàn thông tin. Tuân thủ PCI DSS nếu xử lý thanh toán bằng thẻ tín dụng. Sử dụng các dịch vụ chứng thực tin cậy, dịch vụ định danh điện tử được pháp luật công nhận.

6. *Giáo dục, nâng cao nhận thức & trách nhiệm nội bộ:* Đào tạo nhân viên, áp dụng chính sách bảo mật nội bộ rõ ràng (password, quy trình xử lý thông tin, quyền truy cập…). Thường xuyên thực hiện kiểm tra, đánh giá bảo mật (audit, penetration test).

7. *Pháp lý & xử lý tranh chấp:* Cần quy định rõ giá trị pháp lý của thông điệp dữ liệu, chữ ký điện tử, bằng chứng điện tử trong luật. (VD: eIDAS, luật Nhật Bản về chữ ký điện tử). Có chế tài xử phạt vi phạm; trách nhiệm dân sự, hành chính – để răn đe. Cơ chế giải quyết tranh chấp, khiếu nại và giải pháp bồi thường thiệt hại cho người tiêu dùng nếu có vi phạm.

KẾT LUẬN VÀ ĐỀ XUẤT

** Kết luận:* Pháp luật về giao dịch điện tử và an toàn thông tin ở nhiều quốc gia, đặc biệt trong các nền kinh tế phát triển, đã phát triển khá hoàn chỉnh: từ khung luật, quy định về chữ ký điện tử / dịch vụ tin cậy, bảo vệ dữ liệu cá nhân, xử lý vi phạm, công nhận quốc tế, và có tiêu chuẩn kỹ thuật rõ ràng.

Việt Nam với Luật Giao dịch điện tử năm 2023 là bước tiến lớn, giúp lấp các khoảng trống trước đây, nâng cao tính pháp lý của các giao dịch điện tử, mở rộng công nhận, đảm bảo an toàn thông tin trong môi trường giao dịch số.

** Đề xuất:* Để tiếp tục hoàn thiện, Việt Nam có thể xem xét điều chỉnh các nội dung sau:

1. Hoàn thiện tiêu chuẩn kỹ thuật và quy trình cấp phép / chứng nhận: Xây dựng, ban hành các tiêu chuẩn quốc gia về bảo mật thông tin, mã hóa, xác thực, lưu trữ, sao lưu, khôi phục dữ liệu. Kiểm định năng lực của các tổ chức cung cấp dịch vụ chứng thư số / chữ ký điện tử / dịch vụ tin cậy.

2. Tăng cường thực thi, giám sát và xử lý vi phạm: Phát triển cơ quan chuyên trách giám sát an toàn thông tin trong giao dịch điện tử. Chế tài rõ ràng, nghiêm khắc đối với các vi phạm về bảo mật, giả mạo, làm sai lệch dữ liệu.

3. Bảo vệ dữ liệu cá nhân, quyền riêng tư: Đảm bảo các giao dịch điện tử thu thập dữ liệu cá nhân phải tuân thủ nguyên tắc tối thiểu, hạn chế chia sẻ không cần thiết. Xác định rõ trách nhiệm đối với thông tin bị rò rỉ, mất mát.

4. Hợp tác quốc tế, công nhận xuyên

biên giới: Thúc đẩy thỏa thuận song phương / đa phương công nhận chữ ký điện tử / chứng thư số giữa các quốc gia. Tham gia các hiệp ước quốc tế / mô hình tiêu chuẩn như UNCITRAL Model Law, eIDAS, MLETR...

5. Nâng cao nhận thức, phát triển năng lực kỹ thuật: Đào tạo cho người dân, doanh nghiệp về rủi ro an toàn thông tin, cách thức giao dịch an toàn. Xây dựng hạ tầng bảo mật, hỗ trợ các doanh nghiệp nhỏ và vùng khó khăn./.

TÀI LIỆU THAM KHẢO:

1. *Regulation (EU) No 910/2014 (eIDAS Regulation) - Electronic Identification, Authentication and Trust Services for electronic transactions in the internal market* - Khung pháp lý của Liên minh Châu Âu về nhận dạng điện tử, dịch vụ tin cậy, chữ ký số, đảm bảo tính toàn vẹn, xác thực, bảo mật thông tin.
2. *Electronic Signatures in Global and National Commerce Act (ESIGN) - Hoa Kỳ.* Luật này (năm 2000) công nhận chữ ký điện tử và hồ sơ điện tử có giá trị pháp lý tương đương chữ ký giấy trong giao dịch liên tỉa bang và quốc tế, nếu đáp ứng các điều kiện nhất định.
3. *Tài liệu nghiên cứu về chiến lược an ninh mạng quốc gia:* Bao gồm các nước châu Âu, Singapore, Australia, Hoa Kỳ, Canada… Trong đó có các nội dung về bảo đảm an toàn thông tin trong giao dịch số, thương mại điện tử.
4. *Luật Giao dịch điện tử (Luật số 20/2023/QH15) của Việt Nam.* Luật này thay thế Luật Giao dịch điện tử năm 2005, có hiệu lực từ ngày 1/7/2024. Có các quy định mở rộng về chữ ký điện tử/chứng thư số, chứng thực tin cậy, cấp tài khoản giao dịch điện tử, trách nhiệm của nhà cung cấp dịch vụ tin cậy.
5. *Các hành vi bị cấm trong giao dịch điện tử theo Luật Giao dịch điện tử 2023.*
6. *Quy định về đảm bảo tính an toàn của hệ thống thông tin phục vụ giao dịch điện tử.*