



BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC KINH TẾ QUỐC DÂN



BỘ TƯ PHÁP
VỤ PHÁP LUẬT DÂN SỰ - KINH TẾ

TÀI LIỆU TỌA ĐÀM ĐỐI THOẠI CHÍNH SÁCH

**HOÀN THIỆN KHUNG PHÁP LUẬT VỀ KINH TẾ
VÀ NÂNG CAO HIỆU QUẢ TỔ CHỨC THI HÀNH PHÁP LUẬT
TRONG BỐI CẢNH CÁCH MẠNG CÔNG NGHIỆP LẦN THỨ TƯ**

Hà Nội, ngày 29 tháng 9 năm 2021



BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC KINH TẾ QUỐC DÂN



BỘ TƯ PHÁP
VỤ PHÁP LUẬT DÂN SỰ - KINH TẾ

CHƯƠNG TRÌNH TỌA ĐÀM ĐỐI THOẠI CHÍNH SÁCH

**Hoàn thiện khung pháp luật về kinh tế và nâng cao hiệu quả tổ chức
thi hành pháp luật trong bối cảnh Cách mạng công nghiệp lần thứ tư**

Thời gian : 08:00, ngày 29 tháng 9 năm 2021

Địa điểm : Trường Đại học Kinh tế Quốc dân (trực tiếp và trực tuyến)

Truy cập trực tuyến : Thông qua phần mềm Zoom:

<https://us06web.zoom.us/j/84441011437>

Meeting ID: 844 4101 1437

Passcode: 686868

Thời gian	Nội dung
08:00 - 08:15	Đăng ký và đón tiếp đại biểu
08:15 - 08:30	Tuyên bố lý do, giới thiệu đại biểu
08:30 - 8:35	Phát biểu khai mạc <i>PGS.TS. Bùi Huy Nhượng, Phó Hiệu trưởng ĐH Kinh tế quốc dân</i>
08:35 – 08:40	Phát biểu đề dẫn tọa đàm <i>Ông Nguyễn Thanh Tú, Vụ trưởng Vụ Pháp luật dân sự – kinh tế, Bộ Tư pháp</i>
08:40 – 9:00	Các mô hình kinh doanh mới trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư và một số vấn đề pháp lý đặt ra. <i>PGS.TS. Trần Văn Nam, Trưởng khoa Luật, ĐH Kinh tế quốc dân</i>
09:00 – 09:20	Hoàn thiện khung pháp luật về hợp đồng thông minh (Smart Contract) trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư. <i>Bà Lưu Hương Ly, Vụ Pháp luật dân sự - kinh tế, Bộ Tư pháp</i>
09:20 – 09:40	Quản lý các nền tảng số, kinh nghiệm của Liên minh châu Âu và một số đề xuất chính sách đối với Việt Nam. <i>Ông Ngô Đức Minh, Phó Vụ trưởng Vụ Pháp chế, Bộ Công Thương</i>
09:40 – 10:00	Bảo vệ dữ liệu cá nhân trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư – kinh nghiệm quốc tế và đề xuất, kiến nghị đối với Việt Nam <i>Ông Trần Mạnh Hùng, Công ty Luật Baker & McKenzie</i>
10:00 – 11:00	Thảo luận mở <i>Đại diện Doanh nghiệp công nghệ số Các đại biểu tham dự</i>
11:00	Tổng kết và bế mạc <i>Ông Nguyễn Thanh Tú, Vụ trưởng Vụ Pháp luật dân sự – kinh tế, Bộ Tư pháp PGS.TS. Bùi Huy Nhượng, Phó Hiệu trưởng ĐH Kinh tế quốc dân</i>

Quý đại biểu download Tài liệu Tọa đàm tại mã QR:



TỌA ĐÀM

Hoàn thiện khung pháp luật về kinh tế và nâng cao hiệu quả tổ chức thi hành pháp luật trong bối cảnh Cách mạng công nghiệp lần thứ tư

CÁC MÔ HÌNH KINH DOANH MỚI TRONG BỐI CẢNH CUỘC CÁCH MẠNG CÔNG NGHIỆP LẦN THỨ TƯ VÀ MỘT SỐ VẤN ĐỀ PHÁP LÝ ĐẶT RA

29/09/2021

PGS.TS Trần Văn Nam, Trường Đại học Kinh tế Quốc dân
TS. Phạm Quang Minh; Viện sau đại học, Đại học Claremont
Trịnh Lê Quang, Trường Đại học Princeton



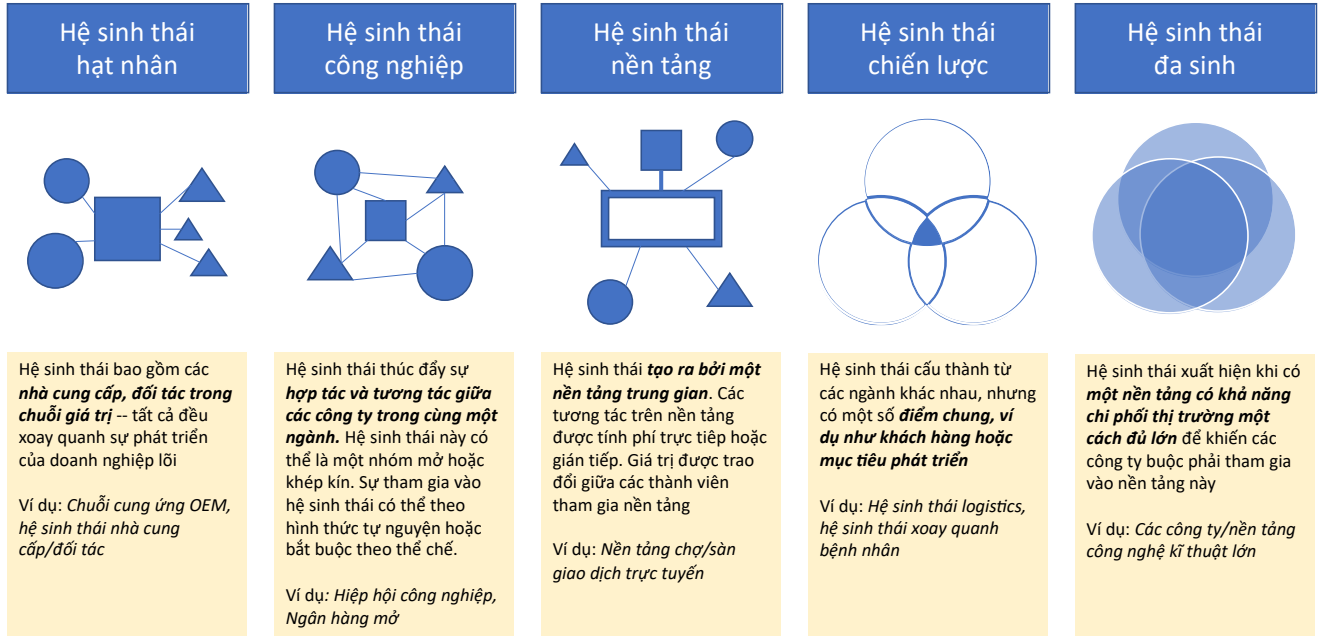
Ma trận 4 mô hình kinh tế mới ứng dụng công nghệ 4.0

Thông tin khách hàng	Toàn bộ	Mô hình nhà đa kênh <ul style="list-style-type: none"> •Tự chủ trong quan hệ khách hàng •Có thể tạo ra sản phẩm dựa trên sự thay đổi của khách hàng •Khách hàng có thể chọn kênh giao dịch •Chuỗi giá trị tích hợp <i>Ví dụ: ngân hàng, bán lẻ, công ty năng lượng</i>	Mô hình hệ sinh thái <ul style="list-style-type: none"> •Trở thành điểm đến của các công ty bán hàng khác •Có thể thêm các sản phẩm cạnh tranh hoặc tương thích •Đảm bảo trải nghiệm người dùng •Thu thập thông tin người dùng thông qua các tương tác trong hệ sinh thái •Kết nối khách hàng và nhà cung cấp •Thu phí thông qua giao dịch <i>Ví dụ: Amazon</i>
	Một phần	Mô hình nhà cung cấp <ul style="list-style-type: none"> •Bán sản phẩm/dịch vụ thông qua các công ty trung gian •Có nguy cơ mất đi quyền lực trong tương lai •Kĩ năng quan trọng: sản xuất với giá thành cạnh tranh, có sự đổi mới sản phẩm <i>Ví dụ: công ty bảo hiểm, công ty xây dựng</i>	Mô hình module <ul style="list-style-type: none"> •Sản phẩm/dịch vụ "Cắm và chạy" •Có thể thay đổi để phù hợp với nhiều hệ sinh thái •Liên tục đổi mới dịch vụ/sản phẩm <i>Ví dụ: PayPal, ví MoMo, ví ZaloPay</i>
		Chuỗi giá trị	Hệ sinh thái
Thiết kế thương mại			

Nguồn: MIT Sloan



5 Mô hình phổ biến của các hệ sinh thái trực tuyến



Nguồn: Gartner

Thực trạng kinh tế hệ sinh thái ở một số quốc gia trên thế giới

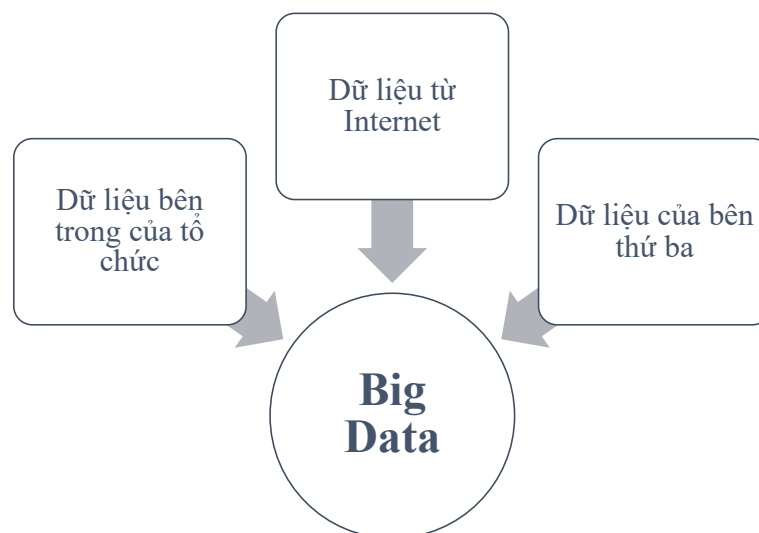
	Tỉ trọng doanh thu phân phối trực tiếp thu được thông qua các hệ sinh thái, %	Doanh thu trực tiếp thông qua các hệ sinh thái, tỷ USD	Quy mô của các hệ sinh thái, tỷ USD
Hoa Kỳ	19	3873	10688
Trung Quốc	19	2486	4900
Nhật Bản	12	536	2129
Singapore	8	24	151
Indonesia	3	32	289
Thái Lan	3	14	117
Việt Nam	2	4	50

Nguồn: McKinsey

	Vận tải		Truyền thông		Bán lẻ	Viễn thông		Tài chính	
	Grab	Sovico Group	Sea Group	VNG	Vinshop	FPT	Viettel	VP Bank	Momo
Bán lẻ offline					▲	▲	▲		
TMĐT			▲	▲		▲			
Chương trình KHTT	▲	▲			▲		▲		▲
Dịch vụ tài chính	▲	▲	▲	▲	▲	▲	▲	▲	▲
B2B Logistics		▲			▲				
B2C logistics	▲	▲	▲				▲		
Vận tải	▲	▲						▲	
Mạng xã hội hoặc công cụ tìm kiếm				▲			▲		
Giải trí hoặc nội dung số			▲	▲		▲	▲		
Thiết bị thông minh hoặc IoT						▲	▲		
Chăm sóc sức khỏe									
Môi giới nhà ở					▲				
Viễn thông						▲	▲		
Quảng cáo hiển thị số	▲			▲	▲				

Nguồn dữ liệu của Big Data

Theo: Kevin Taylor-Sakyi (2016)



Khung pháp luật Việt Nam cho kinh tế số

- *Hoàn thiện pháp luật, trước hết là pháp luật về doanh nghiệp, khởi nghiệp sáng tạo, sở hữu trí tuệ, thương mại, đầu tư, kinh doanh để tạo điều kiện thuận lợi cho quá trình chuyển đổi số quốc gia và phát triển các sản phẩm, dịch vụ, mô hình kinh tế mới dựa trên nền tảng công nghệ số, Internet và không gian mạng; đồng thời ngăn chặn kịp thời các tác động tiêu cực cả về kinh tế và xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng*

Các văn bản pháp luật liên quan

- từng bước được ban hành để điều chỉnh quan hệ của các chủ thể tham gia cuộc Cách mạng công nghiệp lần thứ tư :
 - Luật giao dịch điện tử năm 2005
 - Luật Công nghệ thông tin năm 2006
 - Luật An toàn thông tin mạng năm 2015
 - Luật An ninh mạng năm 2018

Vấn đề quản lý thông tin người dùng chưa được thể chế hoá đồng bộ.

- Việt Nam đã ban hành Luật an ninh mạng và chính thức có hiệu lực từ 1/1/2019. Tuy nhiên, chưa có Nghị định chi tiết về bảo vệ dữ liệu cá nhân, nên thực tế chưa hướng tới thực hiện triệt để quy định “thông tin người dùng Việt Nam chỉ được tồn tại trong lãnh thổ Việt Nam” bảo vệ thông tin người tiêu dùng có hiệu quả.
- Bên cạnh đó, cơ quan chức năng chưa thể kiểm soát các giao dịch xuyên biên giới tốt hơn

Chưa luật hoá các vấn đề về bảo vệ thông tin cá nhân trong môi trường số

- California đã ban hành đạo luật bảo mật người tiêu dùng CCPA
- Liên Minh châu Âu đã thông qua “Quy định bảo vệ dữ liệu chung” (GDPR)
- luật bảo vệ thông tin cá nhân Singapore (Personal Data Protection Act-PDPA)

Đề phát triển kinh tế số thời gian tới

- sớm ban hành chiến lược và quy hoạch quốc gia về chuyển đổi số, kinh tế số với mục tiêu làm chủ hạ tầng số, làm chủ các nền tảng số, làm chủ không gian mạng quốc gia, hướng tới mục tiêu hình thành các doanh nghiệp công nghệ số Việt Nam có năng lực phát triển toàn cầu.
- Tiếp tục hoàn thiện hệ thống luật pháp theo yêu cầu hội nhập quốc tế và phát triển kinh tế số, tuân thủ các chuẩn mực quốc tế, trong đó ban hành *Luật bảo vệ thông tin cá nhân* cần được xem là một ưu tiên trong thời gian tới

Trân trọng cảm ơn!

Trần Văn Nam & Team

CÁC MÔ HÌNH KINH DOANH MỚI TRONG BỐI CẢNH CUỘC CÁCH MẠNG CÔNG NGHIỆP LẦN THỨ TƯ VÀ MỘT SỐ VẤN ĐỀ PHÁP LÝ ĐẶT RA

PGS.TS Trần Văn Nam, Trường Đại học Kinh tế Quốc dân¹
TS. Phạm Quang Minh; Viện sau đại học, Đại học Claremont
Trịnh Lê Quang, Trường Đại học Princeton

Theo tạp chí MIT Sloan Management Review, có 4 mô hình kinh doanh số phổ biến hiện nay²:

Mô hình nhà cung cấp (supplier); (ii) Mô hình đa kênh (omni-channel); (iii) Mô hình mô-đun (module); (iv) Mô hình hệ sinh thái (ecosystem). Mô hình được coi là đã và đang tạo giá trị thặng dư lớn nhất là mô hình hệ sinh thái. Do vậy, bài viết này sẽ giới thiệu tổng quan về các mô hình kinh doanh phổ biến hiện nay trên thế giới; một số xu hướng kinh doanh mới đã manh nha tại Việt Nam; phân tích mô hình hệ sinh thái kinh doanh là mô hình tạo giá trị thặng dư tại Việt Nam rõ nét. Bài viết cũng đặt ra những liên hệ về pháp lý trong bối cảnh cách mạng công nghiệp lần thứ tư diễn ra tại Việt Nam.

Từ khoá: Mô hình kinh doanh; mô hình hệ sinh thái; trở ngại pháp lý; Cách mạng công nghiệp 4.0

1. Giới thiệu tổng quan về các mô hình kinh doanh phổ biến hiện nay

1.1 Đặt vấn đề

Các mô hình kinh doanh này được thực hiện dựa trên hai tiêu chí chính: kiến thức của người tiêu dùng và tỷ lệ phần trăm doanh thu từ các hoạt động của hệ sinh thái. Các doanh nghiệp của nhà cung cấp thường hoạt động trong chuỗi giá trị của một công ty lớn mạnh khác và họ không có kiến thức đầy đủ về người tiêu dùng. Ví dụ, Sony được coi là nhà cung cấp vì họ chủ yếu cung cấp hàng điện tử thông qua các nhà bán lẻ. Họ hoạt động thông qua các kênh lớn như Walmart và họ không có dữ liệu bán hàng của người tiêu dùng. Các doanh nghiệp đa kênh thường cung cấp quyền truy cập của người tiêu dùng vào sản phẩm của họ thông qua nhiều kênh, bao gồm cả kênh trực tuyến và kênh truyền thống. Họ sử dụng dữ liệu lớn để đánh giá hành vi của người tiêu dùng và có đầy đủ kiến thức về người tiêu dùng. Một ví dụ về kinh doanh đa kênh là Walmart. Các doanh nghiệp mô-đun cung cấp các sản phẩm hoặc dịch vụ có thể thích ứng với nhiều hệ sinh thái, ví dụ: PayPal. Họ chỉ có một phần kiến thức về người tiêu dùng, nhưng họ có thể tạo ra doanh thu từ các hệ sinh thái khác nhau. Tuy nhiên, để tồn tại, họ cần phải là người giỏi nhất trong danh mục của họ.

Mô hình tạo giá trị thặng dư lớn nhất là mô hình hệ sinh thái, giống như các marketplace (Amazon), chợ ứng dụng (App store, Google Play), hệ sinh thái smarthome (Xiaomi, Tuya,..). Họ có đầy đủ kiến thức về người tiêu dùng, cung cấp nền tảng có thương hiệu,

¹ Trưởng Khoa Luật, Trường Đại học Kinh tế Quốc dân; Email: namtv@neu.edu.vn

² Woerner, P.W. and S.L., n.d. *Thriving in an Increasingly Digital Ecosystem*; MIT Sloan Management Review. URL <https://sloanreview.mit.edu/article/thriving-in-an-increasingly-digital-ecosystem/> (accessed 9.23.21).

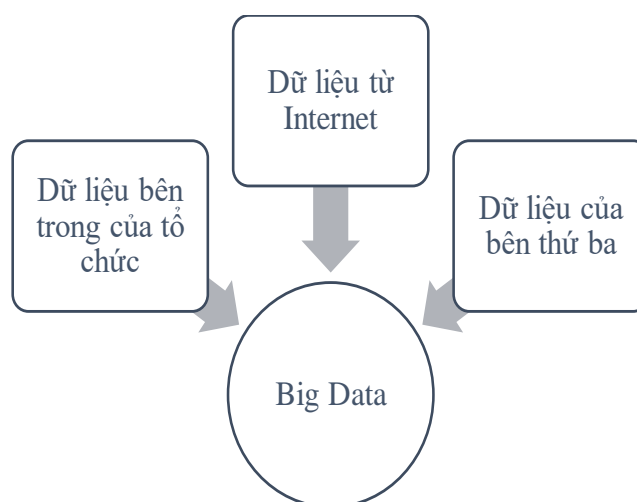
đảm bảo trải nghiệm khách hàng tuyệt vời, đáp ứng nhu cầu của khách hàng với nhà cung cấp và chiết khấu tiền thuê. Tại sao mô hình hệ sinh thái lại thành công như vậy?

1.2 Một số xu hướng kinh doanh mới trong thời kỳ kinh tế số

1.2.1 Dữ liệu lớn (Big Data)

Một trong những xu hướng thị trường quan trọng trong cấu trúc kinh doanh hiện đại là tận dụng dữ liệu lớn, trong đó nó là chức năng chính của các doanh nghiệp tham gia là thúc đẩy hệ sinh thái phát triển.

Sơ đồ 1. Nguồn dữ liệu của Big Data.



Nguồn: Kevin Taylor-Sakyi (2016).

Lợi ích của dữ liệu lớn là gì?

Tận dụng kiến thức về người tiêu dùng là điều cần thiết trong việc dự đoán hành vi của người tiêu dùng. Không giống như các mô hình kinh doanh khác, các doanh nghiệp điều khiển hệ sinh thái có thể trích xuất dữ liệu người tiêu dùng trực tiếp. Ví dụ: những điều này bao gồm tên và địa chỉ của người tiêu dùng, nhân khẩu học, địa chỉ IP, lịch sử mua hàng với công ty của bạn và với các công ty khác và quan trọng nhất là các sự kiện trong đời của họ (chẳng hạn như đám cưới hoặc sinh con sắp tới hoặc đối với doanh nghiệp, kế hoạch sáp nhập hoặc mở rộng). Những dữ liệu này giúp các doanh nghiệp hiểu được khách hàng của họ mua ở đâu, khi nào và tại sao, bảo vệ cơ sở khách hàng của công ty bằng các chương trình khách hàng thân thiết được cải thiện, nắm bắt cơ hội bán kèm và bán thêm, cung cấp thông tin khuyến mại được nhắm mục tiêu, tối ưu hóa việc lập kế hoạch và hoạt động của lực lượng lao động, cải thiện sự kém hiệu quả trong chuỗi cung ứng của công ty, dự đoán xu hướng thị trường và nhu cầu trong tương lai, giúp các công ty đổi mới và cạnh tranh hơn, đồng thời khám phá các nguồn doanh thu mới.

Tại sao big data lại quan trọng?

- Tiết kiệm thời gian: Phân tích trong bộ nhớ thời gian thực giúp các công ty thu thập dữ liệu từ nhiều nguồn khác nhau. Các công cụ như Hadoop giúp họ phân tích dữ liệu ngay lập tức, do đó giúp đưa ra quyết định nhanh chóng dựa trên những gì đã học được.
- Tiết kiệm chi phí: Các công cụ Big Data như Apache Hadoop, Spark,... mang lại lợi ích tiết kiệm chi phí cho doanh nghiệp khi phải lưu trữ lượng lớn dữ liệu. Những công cụ này giúp các tổ chức xác định các cách thức kinh doanh hiệu quả hơn.
- Giải quyết vấn đề của nhà quảng cáo và cung cấp thông tin chi tiết về tiếp thị: Phân tích dữ liệu lớn định hình mọi hoạt động kinh doanh. Nó cho phép các công ty đáp ứng kỳ vọng của khách hàng. Phân tích dữ liệu lớn giúp thay đổi dòng sản phẩm của công ty. Nó đảm bảo các chiến dịch tiếp thị mạnh mẽ.
- Hiểu các điều kiện thị trường: Phân tích dữ liệu lớn giúp các doanh nghiệp hiểu rõ hơn về các tình huống thị trường. Ví dụ, phân tích hành vi mua hàng của khách hàng giúp các công ty xác định các sản phẩm được bán nhiều nhất và từ đó sản xuất các sản phẩm đó cho phù hợp. Điều này giúp các công ty đi trước các đối thủ cạnh tranh.
- Động lực của Đổi mới và Phát triển Sản phẩm: Dữ liệu lớn làm cho các công ty có khả năng đổi mới và phát triển lại sản phẩm của họ.
- Tăng khả năng thu hút và giữ chân khách hàng: Khách hàng là tài sản quan trọng mà bất kỳ doanh nghiệp nào cũng phụ thuộc vào. Không một doanh nghiệp nào có thể đạt được thành công mà không xây dựng một cơ sở khách hàng vững chắc. Nhưng ngay cả khi có cơ sở khách hàng vững chắc, các công ty cũng không thể bỏ qua sự cạnh tranh trên thị trường. Nếu chúng ta không biết khách hàng của mình muốn gì thì điều đó sẽ làm giảm sự thành công của các công ty. Nó sẽ làm mất đi lượng khách hàng, từ đó ảnh hưởng xấu đến tăng trưởng kinh doanh. Phân tích dữ liệu lớn giúp các doanh nghiệp xác định các xu hướng và mẫu liên quan đến khách hàng. Phân tích hành vi của khách hàng dẫn đến việc kinh doanh có lãi.

Thực tiễn tốt: Sử dụng dữ liệu lớn trong lĩnh vực ngân hàng

Một trong những lợi thế của ngân hàng truyền thông là khối lượng thông tin tài chính khổng lồ mà các ngân hàng lưu trữ về hàng triệu khách hàng của mình. Mặt khác, ngân hàng có lợi thế về cấu trúc và vốn để khai thác nguồn tài nguyên mới này. Tiềm năng cho việc phân tích dữ liệu đã được nhìn nhận rộng rãi trong ngành tài chính với doanh thu từ Big Data và phân tích dữ liệu kinh doanh tăng từ 130 tỷ đô la Mỹ năm 2016 lên ước tính khoảng 203 tỷ đô la Mỹ năm 2020, trong đó lĩnh vực ngân hàng đóng góp tỷ trọng doanh thu lớn nhất khi dành 17 tỷ đô la Mỹ cho các giải pháp về Big Data và phân tích dữ liệu chỉ riêng trong năm 2016. Ngân hàng có thể sử dụng dữ liệu cho tiếp thị, phân phối và đa dạng hóa các dịch vụ cá nhân hóa, đáp ứng chính xác nhu cầu của từng khách hàng riêng lẻ. Big Data cũng cho phép các ngân hàng có thể thực hành quản trị rủi ro tốt hơn từ quản trị rủi ro tín dụng truyền thống đến những loại rủi ro thị trường phức tạp khác, từ rủi ro hoạt động nội bộ đến rủi ro từ yếu tố bên ngoài. Big Data còn trợ giúp trong việc nâng cao chất lượng dịch vụ, đưa ra các dự báo về tình hình kinh doanh và lập kế hoạch kinh doanh. Các ngân hàng ở Việt Nam nếu muốn nâng cao năng lực cạnh tranh, cải thiện lợi nhuận thì không còn lựa chọn nào khác ngoài việc gia nhập xu thế này³.

³ Trương Thị Hoài Linh; Lê Thị Như Quỳnh; *Big data và ứng dụng trong hoạt động Ngân hàng*; Tạp chí Ngân hàng số 17 tháng 9/2019

1.2.2 Xu thế nền tảng sản phẩm (Products to Platform)

Trong nhiều ngành, các công ty sử dụng nền tảng sản phẩm như một phương tiện để giảm chi phí và tiếp cận nhiều phân khúc thị trường bằng cách phát triển các biến thể sản phẩm khác nhau. Nền tảng sản phẩm là tập hợp các mô-đun hoặc bộ phận chung cho một số sản phẩm. Điểm chung này được phát triển có chủ đích nhằm đạt được những hiệu quả mong muốn nhằm tạo ra giá trị. Tài liệu về nền tảng sản phẩm hiện có cung cấp nhiều thông tin chi tiết từ góc độ cấp sản phẩm. Một nền tảng sản phẩm không chỉ là một sản phẩm mà là một tập hợp các yếu tố chung, đặc biệt là công nghệ cốt lõi cơ bản, được thực hiện trên một loạt các sản phẩm ⁴.

Chiến lược nền tảng sản phẩm nằm giữa tầm nhìn sản phẩm và chiến lược dòng sản phẩm, định hướng phát triển sản phẩm riêng lẻ ⁵. Nền tảng sản phẩm không phải là thứ được bán cho khách hàng. Việc lựa chọn các công nghệ cốt lõi được sử dụng trong các quyết định về nền tảng sản phẩm thường không thể thay đổi và có tác động lâu dài đối với sự phát triển sản phẩm.

Một trong những ví dụ điển hình của mô hình product-platform là nền tảng *Digital Hub* trong tương lai của Apple. Khi mới thành lập, Steve Jobs đã giới thiệu một số ứng dụng phần mềm cho nền tảng này, bao gồm cả iTunes, nó đã trở thành lớp đầu tiên của nền tảng sản phẩm mới này. iPod ra đời vào ngay sau đó, tạo tiền đề cho iPhone vào năm 2007, cửa hàng ứng dụng năm 2008, iPad năm 2010, cùng với iBooks và iBookstore. Apple tiếp tục mở rộng và tận dụng nền tảng của mình với Apple Pay, Apple Watch, Apple TV và Apple Music. Rõ ràng rằng sự thành công và tăng trưởng của Apple khuyết dựa trên một chiến lược nền tảng đặc biệt. Kể từ khi Steve đưa ra tầm nhìn nền tảng mới của Apple vào năm 2001, Apple đã thành công vượt bậc.

Có nhiều lợi ích khi sử dụng chiến lược nền tảng sản phẩm: giảm chi phí tổng thể, tạo ra tầm nhìn dài hạn và xây dựng dựa trên lòng trung thành của khách hàng.

- Giảm chi phí tổng thể. Việc sử dụng các thành phần và hệ thống con chung có thể giảm chi phí tổng thể, dài hạn và tận dụng các nguồn lực sẵn có để hoạt động hiệu quả hơn. Cho rằng các thành phần và hệ thống con đã được gỡ lỗi và kiểm tra, các sản phẩm thu được sẽ có chất lượng cao hơn. Vì việc phát triển nền tảng xảy ra ít thường xuyên hơn so với phát triển sản phẩm, nên các quyết định chính về nền tảng không cần phải được thực hiện thường xuyên. Điều này có tiềm năng thúc đẩy phát triển sản phẩm tinh gọn.

2. Lê Thị Thu Thủy, Nguyễn Hồng Quân; *Khía cạnh pháp lý đối với mô hình kinh tế chia sẻ: nghiên cứu thực tiễn qua mô hình chia sẻ phòng lưu trú AIRBNB*; Tạp chí Kinh tế và Phát triển, Số 278, tháng 8 năm 2020, tr. 23-31

⁴ Harland, P.E., Uddin, Z., Laudien, S., 2020. *Product platforms as a lever of competitive advantage on a company-wide level: a resource management perspective*. Rev Manag Sci 14, 137–158.

<https://doi.org/10.1007/s11846-018-0289-9>

⁵ Product Bookshelf; *Product Platform Strategy*, (2011)

<https://www.productbookshelf.com/2011/10/product-platform-strategy/> (accessed 9.23.21).

- Xây dựng dựa trên lòng trung thành của khách hàng. Khi khách hàng phát triển sở thích đối với một số nền tảng nhất định, họ có thể trở nên trung thành hơn. Điều này có thể đặc biệt đúng trong các tình huống mà khách hàng cần thay đổi hành vi để sử dụng một nền tảng khác.
- Bắt buộc phải có một tầm nhìn dài hạn. Vì nền tảng sản phẩm được thiết kế để “phù hợp” với nhiều sản phẩm trong tương lai, phương pháp tiếp cận được thiết kế để phù hợp với việc mở rộng sản phẩm trong tương lai. Điều này buộc phải có tầm nhìn dài hạn và có tiềm năng mở ra các dòng doanh thu đa dạng.

Mặt khác, có những nhược điểm tiềm ẩn: chi phí trả trước cao, nguy cơ lỗi thời của nền tảng, nguy cơ thu hồi nền tảng ảnh hưởng đến nhiều sản phẩm và tiềm năng trùng lặp nỗ lực.

- Chi phí trả trước cao. Chi phí trả trước của thiết kế và phát triển nền tảng có thể rất đáng kể. Các khoản tiết kiệm đáng kể phải được dự báo để phù hợp với khoản đầu tư.
- Nguy cơ lỗi thời của nền tảng. Sự khác biệt giữa lập kế hoạch nền tảng trước và khởi chạy các công cụ phái sinh từ một nền tảng hiện có là do thời gian. Với chiến lược nền tảng, kiến trúc nền tảng của một số sản phẩm trong tương lai được quyết định trước. Rủi ro tiềm ẩn là các giả định cơ bản bị sai sót và phương pháp tiếp cận nền tảng sẽ không hoạt động như kế hoạch. Nếu chúng trở nên lỗi thời và không được trẻ hóa định kỳ, các sản phẩm phái sinh cũng có nguy cơ lỗi thời. Do đó, nền tảng sản phẩm cần cập nhật thường xuyên.
- Nỗ lực hai chiều. Một số nền tảng cung cấp kiến trúc chung cho các dịch vụ của các nhà quản lý sản phẩm khác nhau. Trừ khi có sự liên lạc chặt chẽ giữa các giám đốc sản phẩm, nếu không có thể có sự trùng lặp về nỗ lực và giảm chi phí tiết kiệm.
- Thu hồi. Ngoài ra còn có những cân nhắc về chất lượng. Nếu có sự cố trong nền tảng cần phải thu hồi sản phẩm, thì số lượng sản phẩm sẽ cần được thu hồi nhiều hơn so với trường hợp không có chiến lược nền tảng.

1.3 Mô hình điều khiển hệ sinh thái kinh doanh (ecosystem)

Hệ sinh thái kinh doanh (Business Ecosystem) được hiểu là mạng lưới các tổ chức, bao gồm nhà cung cấp, nhà phân phối, khách hàng, đối thủ cạnh tranh, v.v., liên quan đến việc cung cấp một sản phẩm hoặc dịch vụ thông qua cả cạnh tranh và hợp tác. Khi một hệ sinh thái kinh doanh phát triển mạnh, điều đó có nghĩa là những người tham gia thị trường đã thành công trong việc sắp xếp và tổ chức hợp lý hóa luồng ý tưởng, tài năng và vốn trong toàn hệ thống. Động lực thúc đẩy hệ sinh thái là việc lưu trữ nền tảng công nghệ mà các đối tác kinh doanh và khách hàng tham gia. Trình điều khiển hệ sinh thái sở hữu dữ liệu khách hàng và cũng trích xuất một phần của mọi giao dịch giữa các đối tác nền tảng và khách hàng.

Ví dụ về các mô hình kinh doanh Hệ sinh thái phổ biến hiện nay như Uber, Alibaba, Airbnb, đáng nói nhất chính là Apple. Nếu như năm 2007 thị phần của Apple tại thị trường máy tính ít hơn 4% và không có thị phần tại thị trường điện thoại di động, bằng việc khai thác sức mạnh của Nền tảng Hệ sinh thái và tận dụng những quy luật mới trong xây dựng chiến lược, Apple gần như thống lĩnh thị trường sản xuất điện thoại di động thông minh với lợi nhuận chiếm 92% tổng lợi nhuận toàn cầu (2015), từng bước đẩy lùi các ông lớn trong thị

trường này như: Nokia, Samsung, Motorola, Sony Ericsson và LG. Sự thành công này là bài học cho các công ty trong các ngành công nghiệp khác. Những công ty không biết nắm bắt mô hình kinh doanh Hệ sinh thái và không nắm được những quy tắc chiến lược mới của mô hình này sẽ khó có thể cạnh tranh lâu dài ⁶.

Tại Việt Nam, Năm 2014, VNG trở thành doanh nghiệp phát triển theo mô hình hệ sinh thái kinh doanh đầu tiên của Việt Nam. Xuất phát điểm là một công ty nhượng quyền kinh doanh trò chơi, ngày nay VNG được biết đến nhiều nhất với ứng dụng nhắn tin Zalo, và các khoản đầu tư khác nhau vào thương mại điện tử (Tiki), trò chơi, hay thanh toán (ZaloPay). VNG không phải là doanh nghiệp chỉ tập trung vào một lĩnh vực đơn lẻ mà cung cấp một số lượng đáng kể các dịch vụ trực tuyến không thể hoạt động một cách trực quan trong cùng một ngành. Tuy nhiên, các dịch vụ này chia sẻ chi phí thu hút khách hàng (CAC) và cung cấp cho người dùng VNG nhiều nền tảng để họ có thể dành thời gian và tiền bạc. Các công ty như VNG, bao gồm Grab, SEA, và One Mount Group, bây giờ thường được gọi là doanh nghiệp hệ sinh thái ⁷.

1.4. Mô hình Kinh tế chia sẻ (Sharing Economy)

Ngày nay, nền kinh tế chia sẻ là một hệ thống kinh tế - xã hội được xây dựng xung quanh việc chia sẻ các nguồn lực. Nền kinh tế chia sẻ là một mô hình kinh tế được định nghĩa là hoạt động peer-to-peer (P2P) ⁸, thường liên quan đến cách thức mua hàng hóa và dịch vụ khác với mô hình kinh doanh truyền thống là các công ty thuê nhân viên sản xuất sản phẩm để bán cho người tiêu dùng. Nó bao gồm việc tạo ra, sản xuất, phân phối, thương mại và tiêu dùng hàng hóa và dịch vụ của những người và tổ chức khác nhau. Các hệ thống này có nhiều hình thức khác nhau, thường tận dụng công nghệ thông tin (đặc biệt là các nền tảng kỹ thuật số) để trao quyền cho các cá nhân, tập đoàn, tổ chức phi lợi nhuận và chính phủ với thông tin cho phép phân phối, chia sẻ và tái sử dụng công suất dư thừa trong hàng hóa và dịch vụ. Trong nền kinh tế chia sẻ, các tài sản nhàn rỗi như ô tô đỗ và phòng ngủ dự phòng có thể được cho thuê khi không sử dụng. Theo cách này, tài sản vật chất được chia sẻ dưới dạng dịch vụ. Ví dụ, dịch vụ chia sẻ chỗ ở Airbnb so với không gian khách sạn chỉ ra các lợi thế chi phí khi chủ nhà tận dụng các phòng ngủ trống.

Lợi ích của nền kinh tế chia sẻ:

- Kiểm tiền từ tài sản chưa được sử dụng để chia sẻ việc sử dụng một số mặt hàng với những người khác, và tăng khả năng sử dụng của chúng. Ví dụ, số tiền không sử dụng hàng ngày có thể được dùng cho người khác vay thông qua nền tảng cho vay ngang hàng. Bằng cách đó, người cho vay có được thu nhập từ lãi suất. Các ngân hàng thường không cho vay hoặc tiết kiệm hàng ngày.
- Tiết kiệm tiền và tài nguyên. Người sử dụng nền tảng kinh tế chia sẻ có thể thuê xe hơi hoặc quần áo thay vì mua chúng. Tóm lại, các nền tảng cung cấp cho mọi người

⁶ Vì sao Mô hình Hệ sinh thái trở thành Xu hướng kinh doanh hiện nay? Truy cập tại trang <https://womenleadersforum.vn/> ngày 25/9/2021

⁷ Bruce Delteil, Alex Le, and Marcin Miller; *Sáu quy tắc vàng giúp các doanh nghiệp hệ sinh thái giành thắng lợi tại Việt Nam*; McKinsey & Company, 2020

⁸ Investopedia; *Sharing Economy Definition*, <https://www.investopedia.com/terms/s/sharing-economy.asp> (accessed 9.23.21).

quyền truy cập vào các mặt hàng mà họ không thể hoặc không quan tâm đến việc mua và sử dụng về lâu dài.

- Linh hoạt hơn. Giờ đây, để kiếm thêm tiền, ai cũng có thể nhận một số công việc trên các trang trực tuyến và làm ở bất cứ đâu miễn là có kết nối internet. Để tương tác với đồng nghiệp, người làm cũng không cần phải gặp mặt trực tiếp.
- Phân bổ nguồn lực hiệu quả hơn. Cung và cầu cho các nền tảng, chẳng hạn như làm việc tự do, đến từ nhiều địa điểm khác nhau trên khắp các quốc gia. Bởi vì điều này, thị trường đã trở nên cạnh tranh hơn.
- Nhận giá cả hợp lý hơn. Sẽ có nhiều cơ hội hơn để so sánh giá cả hoặc chi phí của hàng hóa hoặc dịch vụ bạn cần. Nhiều nền tảng có xếp hạng và đánh giá được tích hợp sẵn, giúp người dùng nhận được giá cả và chất lượng tốt nhất.
- Giảm tác động đến môi trường. Nền kinh tế chia sẻ làm tăng việc sử dụng hàng hóa. Nó làm giảm số lượng hàng hóa phải sản xuất, giảm ô nhiễm công nghiệp.

Sự chỉ trích đối với nền kinh tế chia sẻ thường liên quan đến sự không chắc chắn về quy định. Các doanh nghiệp cung cấp dịch vụ cho thuê thường chịu sự điều chỉnh của chính quyền. Các cá nhân không có giấy phép cung cấp dịch vụ cho thuê có thể không tuân theo các quy định này hoặc không phải trả các chi phí liên quan. Điều này có nghĩa là mang lại cho họ một lợi thế cho phép họ tính giá thấp hơn.

Một mối lo ngại khác là thiếu sự giám sát của chính phủ sẽ dẫn đến sự lạm dụng nghiêm trọng của cả người mua và người bán trong nền kinh tế chia sẻ. Điều này đã được nhấn mạnh bởi nhiều trường hợp được công khai hóa rất nhiều về những thứ như camera ẩn trong phòng cho thuê, các vụ kiện về việc đối xử không công bằng với các nhà thầu chia sẻ chung bởi các nền tảng sử dụng họ, và thậm chí giết chết khách hàng của các nhà cung cấp dịch vụ cho thuê và chia sẻ xe thực sự hoặc gian lận.

Ngoài ra còn có nỗi quan ngại rằng lượng thông tin được chia sẻ trên nền tảng trực tuyến nhiều hơn có thể tạo ra thành kiến giữa những người dùng. Điều này có thể xảy ra khi người dùng được phép chọn người mà họ sẽ chia sẻ nhà hoặc phương tiện đi lại của họ hoặc do có sự phân biệt thống kê ngầm bởi các thuật toán chọn người dùng có các đặc điểm như lịch sử tín dụng kém hoặc hồ sơ tội phạm. Ví dụ, Airbnb đã phải đối mặt với những lời phàn nàn về phân biệt chủng tộc từ những người Mỹ gốc Phi và người Latinh sẽ là người thuê nhà do người dùng ưa thích không thuê những khách hàng này. Khi nhiều dữ liệu được trình bày hơn và nền kinh tế chia sẻ phát triển, các công ty trong nền kinh tế này đã cam kết chống lại sự thiên vị ở cả người dùng và thuật toán của họ thường bằng cách cố ý hạn chế sự sẵn có của thông tin về và về người mua và người bán.

2. Một số vấn đề pháp lý đặt ra trong bối cảnh cách mạng công nghiệp lần thứ Tư

2.1 Khung pháp lý của Việt Nam hướng tới điều chỉnh kinh tế số

Về chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ Tư đã thể hiện rõ quan điểm chỉ đạo của Đảng là :

“- Hoàn thiện pháp luật, trước hết là pháp luật về doanh nghiệp, khởi nghiệp sáng tạo, sở hữu trí tuệ, thương mại, đầu tư, kinh doanh để tạo điều kiện thuận lợi cho quá trình chuyển đổi số quốc gia và phát triển các sản phẩm, dịch vụ, mô hình kinh tế mới dựa trên nền tảng công nghệ số, Internet và không gian mạng; đồng thời ngăn chặn kịp thời các tác động

tiêu cực cả về kinh tế và xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng”⁹.

Các văn bản pháp luật từng bước được ban hành để điều chỉnh quan hệ của các chủ thể tham gia cuộc Cách mạng công nghiệp lần thứ tư có thể nhắc đến như sau:

- Luật giao dịch điện tử năm 2005
- Luật Công nghệ thông tin năm 2006
- Luật An toàn thông tin mạng năm 2015
- Luật An ninh mạng năm 2018

Đáng chú ý là theo Luật An ninh mạng, các tổ chức, cá nhân được hoạt động trên một môi trường không gian mạng quốc gia sẽ được bảo đảm an toàn, lành mạnh hơn, hạn chế tối đa các yếu tố, nguy cơ xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân như: bị đánh cắp thông tin cá nhân; bị lừa đảo, chiếm đoạt tài sản; bị vu khống, làm nhục, công kích bôi nhọ; hạn chế mã độc; loại bỏ dần các hành vi vi phạm pháp luật khác trên không gian mạng; bảo vệ dữ liệu cá nhân trên không gian mạng; bảo vệ trẻ em trên không gian mạng; bảo đảm môi trường kinh doanh bình đẳng giữa các doanh nghiệp trong nước và doanh nghiệp nước ngoài về sự quản lý, tương thích các quy định của pháp luật và trách nhiệm, nghĩa vụ phải thực hiện. Tuy nhiên, khung pháp lý này hiện cũng bộc lộ một số tồn tại sau đây:

2.1.1 Môi trường pháp lý của Việt Nam còn bất cập, thiếu đồng bộ giữa các văn bản pháp luật và còn có khoảng cách giữa quy định pháp luật với việc thực thi trong thực tế. Các quy định thường không theo kịp với tốc độ số hóa nhanh chóng của nền kinh tế. Thực tế vừa qua cho thấy, cơ quan quản lý đã lúng túng trong việc quản lý doanh thu để thu thuế cho loại hình kinh tế chia sẻ mà điển hình là sự tranh chấp giữa “taxi truyền thống và taxi công nghệ”¹⁰. Xu hướng mua hàng qua mạng đang phát triển mạnh nhưng tiềm ẩn rất nhiều rủi ro do không kiểm tra được chất lượng, nguồn gốc sản phẩm, người tiêu dùng khó xác định đầu mối để khiếu nại, đòi bồi thường.

2.1.2 Vấn đề quản lý thông tin người dùng chưa được thể chế hoá đồng bộ.

Việt Nam đã ban hành Luật an ninh mạng và chính thức có hiệu lực từ 1/1/2019. Tuy nhiên, chưa có Nghị định chi tiết về bảo vệ dữ liệu cá nhân, nên thực tế chưa hướng tới thực hiện triệt để quy định “thông tin người dùng Việt Nam chỉ được tồn tại trong lãnh thổ Việt Nam” bảo vệ thông tin người tiêu dùng có hiệu quả. Bên cạnh đó, cơ quan chức năng chưa thể kiểm soát các giao dịch xuyên biên giới tốt hơn, dễ dàng hơn trong việc truy thu thuế.

Hiện chưa có cơ chế phối hợp với các nước trong việc trao đổi, chia sẻ các thông tin liên quan đến dữ liệu tính toán thuế phải thu của các doanh nghiệp thực hiện hoạt động kinh doanh theo mô hình kinh tế chia sẻ để có thể kiểm soát được tình hình doanh thu và dòng tiền của các mô hình này có được từ việc thực hiện kinh doanh tại Việt Nam.¹¹

2.1.3 Chưa xây dựng và ban hành có hệ thống một chính sách giám sát linh hoạt để hạn chế tối đa việc thất thoát thuế.¹²

Về nguyên tắc, các ngân hàng đều nắm được thông tin các khoản thanh toán chuyển khoản, nhưng để tổng hợp xác định là không dễ vì các khoản thanh toán phát sinh từ các

⁹ Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị

¹⁰ Hồ Quế Hậu (2021) *Phát triển kinh tế số ở Việt Nam: Những bước đi ban đầu và giải pháp* Tạp chí Kinh tế và Phát triển, Số 290, tháng 08 năm 2021, tr. 2-11

¹¹ Lê Thị Thu Thủy, Nguyễn Hồng Quân; *Khía cạnh pháp lý đối với mô hình kinh tế chia sẻ: nghiên cứu thực tiễn qua mô hình chia sẻ phòng lưu trú AIRBNB*; Tạp chí Kinh tế và Phát triển, Số 278, tháng 08 năm 2020, tr. 23-31

¹² Lê Thị Thu Thủy, Nguyễn Hồng Quân; Tài liệu đã dẫn

giao dịch trên thị trường dịch vụ như AirBnB; Uber; Grab.. rất nhỏ lẻ nên thu thuế qua ngân hàng là khó thực hiện. Sự phối hợp nêu trên sẽ đạt hiệu quả trong công tác thanh tra, kiểm tra thuế để xác định doanh thu khi có dấu hiệu trốn thuế. Bổ sung quy định đơn vị cung cấp dịch vụ môi giới thương mại điện tử có tính đa quốc gia phải thành lập chi nhánh tại Việt Nam hoặc cơ quan đại diện thuế tại Việt Nam thì mới có thể vào thị trường Việt Nam khai thác. Thực hiện thu thuế theo quy định về thuế nhà thầu và tiến hành hoàn thuế khi các doanh nghiệp nước ngoài cung cấp đầy đủ giấy tờ chứng minh mình đã thực hiện các nghĩa vụ thuế đó tại nước sở tại để đảm bảo thực hiện đúng quy định về Hiệp ước chống đánh thuế hai lần mà Việt Nam tham gia ký kết.

2.1.4 Chưa luật hoá các vấn đề về bảo vệ thông tin cá nhân trong môi trường số

Một số tiểu bang của Hoa Kỳ, như California đã ban hành đạo luật bảo mật người tiêu dùng CCPA¹³ nhằm giúp cho cư dân có quyền kiểm soát với việc thu thập và sử dụng thông tin cá nhân của họ. Từ đầu năm 2020, cư dân tại California được trao quyền CCPA mới cho họ quyền kiểm soát thông tin cá nhân của họ, bao gồm nhiều dữ liệu trực tuyến họ tạo ra hàng ngày. Quyền của người tiêu dùng theo quy định của CCPA có thể được định dạng theo nhiều cách khác nhau, nhưng có thể phân loại như sau: (1) quyền được thông báo, (2) quyền truy cập, (3) quyền từ chối (hoặc quyền chọn tham gia), (4) quyền yêu cầu xóa, và (5) quyền được hưởng các dịch vụ và giá cả như nhau.

Từ tháng 5 năm 2018, Liên Minh châu Âu đã thông qua “Quy định bảo vệ dữ liệu chung” (GDPR), có hiệu lực, giới hạn các dữ liệu mà các tổ chức có thể thu thập và cần có sự đồng ý từ các cá nhân. GDPR là cách thức của Liên minh Châu Âu mang lại cho các cá nhân, khách hàng tiềm năng, khách hàng, nhà thầu và nhân viên nhiều quyền hơn đối với dữ liệu của họ nhưng quy định ít quyền lực hơn đối với các tổ chức thu thập và sử dụng dữ liệu đó để thu lợi nhuận. GDPR tập trung vào việc tạo ra một khuôn khổ pháp lý “quyền riêng tư theo mặc định” cho toàn bộ EU. GDPR yêu cầu các trang web, công ty và doanh nghiệp phải có cơ sở pháp lý để xử lý dữ liệu cá nhân ở EU, theo đó cơ sở pháp lý đầu tiên là sự đồng ý của các cá nhân.

Tại Singapore, từ năm 2012 đã ban hành đạo luật bảo vệ thông tin cá nhân (Personal Data Protection Act- PDPA), sửa đổi năm 2018. Trên cơ sở đó, cơ quan Bảo vệ Thông tin cá nhân (Personal Data Protection Agency-PDPC) được thiết lập. Cơ quan này có thẩm quyền điều tra, cảnh báo, yêu cầu cam kết khắc phục, phạt vi phạm đối với các chủ thể vi phạm về bảo vệ thông tin cá nhân.

PDPC có thể chấp nhận cam kết từ một tổ chức nếu có dấu hiệu có khả năng vi phạm Đạo luật bảo vệ dữ liệu cá nhân PDPA¹⁴.

Danh sách các doanh nghiệp là đối tượng áp dụng các biện pháp xử phạt hành chính năm 2021 (xem tại Phụ lục 1).

¹³ <https://oag.ca.gov/privacy/ccpa>

¹⁴ Quy trình này nhằm cho phép các tổ chức thực hiện một kế hoạch khắc phục không chỉ khắc phục vi phạm ngay lập tức mà còn giải quyết mọi thiếu sót mang tính hệ thống để đảm bảo tuân thủ PDPA liên tục. Khi xem xét có chấp nhận một cam kết hay không, PDPC sẽ kiểm tra tính hiệu quả của kế hoạch khắc phục do tổ chức đề xuất và sự sẵn sàng của tổ chức để thực hiện nó.

Việt Nam đã có quy định điều chỉnh thu thập thông tin cá nhân có trong Luật An toàn thông tin mạng. Điều khoản quy định này cũng là một điểm tranh cãi khi các doanh nghiệp góp ý cho dự thảo, theo đó bên xử lý thông tin có trách nhiệm thu thập thông tin sau khi chủ thông tin cá nhân đồng ý, và chỉ sử dụng thông tin đã thu thập vào mục đích khác mục đích ban đầu nếu chủ thông tin cá nhân chấp thuận. Việc chuyển tiếp thông tin cho bên thứ ba bị cấm trừ khi chủ thông tin đồng ý hoặc chính quyền yêu cầu. Trong thời gian tới, một đạo luật độc lập về bảo vệ thông tin cá nhân cần được xây dựng và ban hành tại Việt Nam.

2.2 Lời kết

Để phát triển kinh tế số thời gian tới, nhà nước cần xây dựng chiến lược chuyển đổi số phù hợp:

- Nhà nước cần sớm ban hành chiến lược và quy hoạch quốc gia về chuyển đổi số, kinh tế số với mục tiêu làm chủ hạ tầng số, làm chủ các nền tảng số, làm chủ không gian mạng quốc gia, hướng tới mục tiêu hình thành các doanh nghiệp công nghệ số Việt Nam có năng lực phát triển toàn cầu¹⁵.

- Tiếp tục hoàn thiện hệ thống luật pháp theo yêu cầu hội nhập quốc tế và phát triển kinh tế số, tuân thủ các chuẩn mực quốc tế, trong đó ban hành *Luật bảo vệ thông tin cá nhân* cần được xem là một ưu tiên trong thời gian tới. Có quy định và cơ chế phù hợp để điều chỉnh hoạt động của các tổ chức, cá nhân, doanh nghiệp tương thích với nền kinh tế số như: xây dựng luật văn bản điện tử, chữ ký số, cấp giấy phép từ cơ quan quản lý. Nhà nước cần mạnh dạn chấp nhận các mô hình kinh doanh mới và các công nghệ mới bằng cách tiếp cận mới trong quản lý mà nhiều nước áp dụng, cách tiếp cận Sandbox, cho cái mới tự phát triển, sau đó mới hình thành quy định để quản lý. Nhà nước cũng cần đẩy mạnh cải cách thủ tục hành chính để tạo thuận lợi cho các doanh nghiệp số hoạt động có hiệu quả.

- Bản thân các doanh nghiệp thuộc các ngành kinh tế cần xây dựng và thực hiện các mục tiêu chiến lược chuyển đổi số phù hợp, để tiếp cận, nhằm đáp ứng với các điều kiện thị trường liên tục thay đổi để tạo ra lợi thế cạnh tranh, nâng cao giá trị và sự hài lòng của khách hàng.

Danh mục tài liệu tham khảo

1. Hossein Hassani và cộng sự (2018), *Digitalisation and Big Data Mining in Banking*, <https://www.mdpi.com/2504-2289/2/3/18/pdf>.
2. Hồ Quế Hậu (2021); *Phát triển kinh tế số ở Việt Nam: Những bước đi ban đầu và giải pháp*, Tạp chí Kinh tế và Phát triển, Số 290, tháng 08 năm 2021, tr. 2-11
3. Kevin Taylor-Sakyi (2016), *Big Data: Understanding Big Data*, https://www.researchgate.net/publication/291229189_Big_Data_Understanding_Big_Data.
4. Mashooque A. Memon và cộng sự (2017), *Big Data Analytics and Its Applications*, https://www.researchgate.net/publication/320345031_Big_Data_Analytics_and_Its_Applications
5. Trương Thị Hoài Linh; Lê Thị Như Quỳnh (2019); *Big data và ứng dụng trong hoạt động Ngân hàng*; Tạp chí Ngân hàng số 17 tháng 9/2019

¹⁵ Hồ Quế Hậu (2021), Tài liệu đã dẫn

6. Lê Thị Thu Thủy, Nguyễn Hồng Quân (2020); *Khía cạnh pháp lý đối với mô hình kinh tế chia sẻ: nghiên cứu thực tiễn qua mô hình chia sẻ phòng lưu trú AIRBNB*; Tạp chí Kinh tế và Phát triển, Số 278, tháng 08 năm 2020, tr. 23-31
7. VinodKumar Kasipuri (2018), *Applications of Big Data as Use Cases in Different Industries*, Dzone, <https://dzone.com/articles/applications-of-big-data-as-use-cases-in-different>.
8. Tran Van Nam et al; (2021); *A New Trend of Developing the Fin-tech in Vietnam*; International Journal of Finance and Banking Research. Vol. 7, No. 3, 2021, pp. 76-81
9. Peter Weill Stephanie L. Woerner (2015); *Thriving in an Increasingly Digital Ecosystem*; MIT Sloan Management Review.
10. Bruce Delteil, Alex Le, and Marcin Miller; (2020); *Sáu quy tắc vàng giúp các doanh nghiệp hệ sinh thái giành thắng lợi tại Việt Nam*; McKinsey & Company
11. Vũ Tú Thành (2020); *Hướng đi nào cho quản lý Nhà nước trong bối cảnh xuất hiện ngày càng nhiều, càng nhanh những mô hình kinh doanh sáng tạo mới? Kỳ yếu Diễn đàn: Khoa học và Công nghệ với doanh nghiệp Việt Nam trong Cách mạng công nghiệp lần thứ 4 năm 2020*

PHỤ LỤC 01

DANH MỤC CÁC DOANH NGHIỆP CÓ DẤU HIỆU VI PHẠM QUY ĐỊNH CỦA LUẬT BẢO VỆ THÔNG TIN CÁ NHÂN SINGAPORE (NĂM 2020-2021) ĐÃ ĐƯỢC XỬ LÝ

(Nguồn: <https://www.pdpc.gov.sg/> truy cập ngày 25/9/2021)

- A financial penalty of \$35,000 was imposed on HMI Institute for failing to put in place reasonable security arrangements to protect personal data stored in its server. This resulted in the data being subjected to a ransomware attack. 10/6/2021
- A financial penalty of \$8,000 was imposed on ST Logistics for failing to put in place reasonable security arrangements to prevent the unauthorised access of 2,400 MINDEF and SAF personnel's personal data. 10/6/2021
- A warning was issued to Greatearth Corporation for failing to obtain consent to disclose personal data of 8 crane operators on the external façade of a construction site. Breach of the Consent Obligation by Greatearth Corporation, No Breach of the PDPA by Progressive Builders, 12 May 2021
- 14 Jan 2021, A financial penalty of \$9,000 was imposed on The Future of Cooking for failing to put in place reasonable security arrangements to prevent the unauthorised disclosure of its customers' personal data on its website.
- 14 Jan 2021, a financial penalty of \$5,000 was imposed on BLS International Services Singapore for failing to put in place reasonable security arrangements to prevent the unauthorised disclosure of the personal data of individuals who had submitted a booking for an appointment on its website.
- A financial penalty of \$9,000 was imposed on Iapps for failing to put in place reasonable security arrangements to prevent the unauthorised disclosure of personal data of some users of the ActiveSG mobile application. 11/3/2021

- Singapore Technologies Engineering was found not in breach of the PDPA in relation to the transfer of the personal data of its Singapore-based employees to its subsidiaries based in United States. 11/1/2021
- A financial penalty of \$8,000 was imposed on ST Logistics for failing to put in place reasonable security arrangements to prevent the unauthorised access of 2,400 MINDEF and SAF personnel's personal data. 10/1/2021

Undertakings under the Personal Data Protection Commission (PDPC)

No	Undertakings	Published Date
1	Grabcar Pte Ltd;	10 Sept 2020
2	Employment & Employability Institute Pte Ltd;	10 Sept 2020
3	HSBC Bank (Singapore) Limited;	10 Sept 2020
4	NEC Asia Pacific Pte Ltd;	14 Jan 2021
5	StarMed Specialist Centre Pte Ltd;	18 Feb 2021
6	Manulife (Singapore) Pte Ltd;	15 Apr 2021
7	DLI Asia Pacific Pte Ltd;	12 May 2021
8	Seafront Support Company Pte Ltd;	10 Jun 2021
9	Platinum Yoga Pte Ltd;	10 Jun 2021
10	Assisi Hospice;	12 Jul 2021
11	Thye Hua Kwan Moral Charities Limited;	12 Jul 2021
12	Equity Solution Pte Ltd;	12 Aug 2021
13	MindChamps Preschool Limited;	21 Sept 2021

HOÀN THIỆN KHUNG PHÁP LUẬT VỀ HỢP ĐỒNG THÔNG MINH TRONG BỐI CẢNH CUỘC CÁCH MẠNG CÔNG NGHIỆP LẦN THỨ TƯ

TS. Lưu Hương Ly
Vụ Pháp luật dân sự - kinh tế
Bộ Tư pháp

Hà Nội, ngày 29 tháng 9 năm 2021

NỘI DUNG

- 1. Khái niệm, bản chất của hợp đồng thông minh**
- 2. Thực trạng pháp luật về hợp đồng thông minh tại Việt Nam**
- 3. Kinh nghiệm quốc tế**
- 4. Nhận xét, đánh giá và đề xuất, kiến nghị**

1. KHÁI NIỆM, BẢN CHẤT CỦA HỢP ĐỒNG THÔNG MINH (SMART CONTRACT)

- **Định nghĩa**

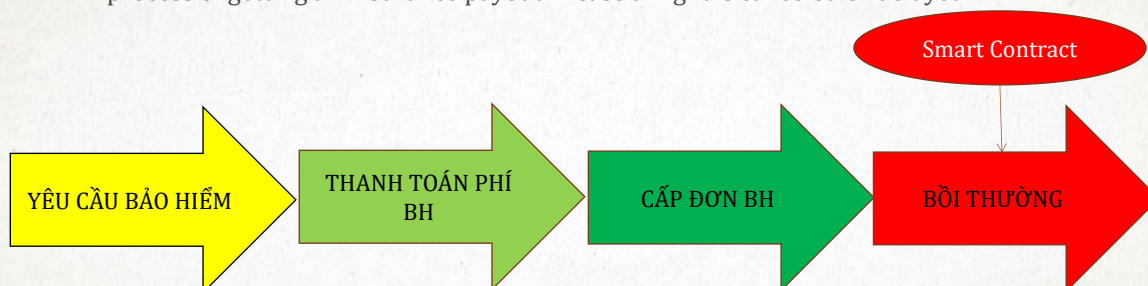
“hợp đồng thông minh là những thỏa thuận được tự động thực thi bằng các máy tính” (Max Raskin).

- **02 trường hợp:**

- (i) toàn bộ thỏa thuận giữa các bên được thể hiện tại các lệnh được mã hóa; hoặc
- (ii) hợp đồng thông minh chỉ mã hóa để tự động thực thi hợp đồng pháp lý (có thể bằng văn bản hoặc không) giữa các bên.

ETHERISC: FLIGHT DELAY INSURANCE

“Etherisc, a Zug-Switzerland-based insurance platform startup, has begun offering blockchain-based flight delay insurance, called Flight Delay, which automates the process of getting an insurance payout in case a flight is canceled or delayed.”



2. THỰC TRẠNG PHÁP LUẬT VỀ HỢP ĐỒNG THÔNG MINH TẠI VIỆT NAM

1. Bản chất và giá trị pháp lý của hợp đồng thông minh
2. Giá trị chứng cứ của hợp đồng thông minh khi giải quyết tranh chấp dân sự tại các cơ quan tài phán
3. Tính pháp lý của chữ ký mật mã và bản ghi trên Blockchain
4. Vấn đề giải thích hợp đồng
5. Vấn đề sửa đổi hợp đồng
6. Vấn đề tuân thủ pháp luật chuyên ngành
7. Vấn đề xác định pháp luật áp dụng và quyền tài phán

3. KINH NGHIỆM QUỐC TẾ

- UK
- US
- Italia
- Trung Quốc

4. KẾT LUẬN VÀ ĐỀ XUẤT, KIẾN NGHỊ

- Khung pháp luật hiện hành của Việt Nam đã khá đầy đủ để điều chỉnh các hợp đồng thông minh mà không cần có sự sửa đổi, bổ sung hay xáo trộn lớn.
- Kiến nghị sửa đổi, bổ sung một số quy định tại Luật Giao dịch điện tử năm 2005.

KIẾN NGHỊ SỬA ĐỔI, BỔ SUNG MỘT SỐ QUY ĐỊNH TẠI LUẬT GIAO DỊCH ĐIỆN TỬ NĂM 2005:

1. Hợp đồng được giao kết hoặc thực hiện từ sự tương tác giữa một hệ thống thông tin tự động với một người hoặc giữa các hệ thống thông tin tự động với nhau không bị phủ nhận giá trị pháp lý chỉ vì không có sự kiểm tra hay can thiệp của con người vào từng hành động cụ thể do các hệ thống thông tin tự động thực hiện hay hợp đồng được giao kết và bên sử dụng hệ thống thông tin tự động phải chịu trách nhiệm về các hành vi do hệ thống thông tin tự động thực hiện.

KIẾN NGHỊ SỬA ĐỔI, BỔ SUNG MỘT SỐ QUY ĐỊNH TẠI LUẬT GIAO DỊCH ĐIỆN TỬ NĂM 2005:

2. Bổ sung quy định về suy đoán về năng lực chủ thể của các bên tham gia giao dịch điện tử trong Luật Giao dịch điện tử (sửa đổi) để giảm nhẹ trách nhiệm chứng minh của các bên về hiệu lực của giao dịch khi phát sinh tranh chấp (bên nào yêu cầu tuyên bố giao dịch vô hiệu do không đáp ứng yêu cầu về năng lực chủ thể thì bên đó có trách nhiệm chứng minh).

KIẾN NGHỊ SỬA ĐỔI, BỔ SUNG MỘT SỐ QUY ĐỊNH TẠI LUẬT GIAO DỊCH ĐIỆN TỬ NĂM 2005:

3. Quy định rõ chữ ký điện tử an toàn là (i) chữ ký số (đáp ứng các điều kiện nhất định); **hoặc** (ii) chữ ký do các bên thoả thuận và đáp ứng các điều kiện nhất định. Chữ ký điện tử an toàn có giá trị chứng cứ (các bên không phải chứng minh tính xác thực và tính toàn vẹn của chữ ký điện tử an toàn), trừ trường hợp có chứng cứ chứng minh ngược lại.

TRÂN TRỌNG CẢM ƠN!!!

Hoàn thiện khung pháp luật về hợp đồng thông minh trong bối cảnh cuộc Cách mạng công nghiệp lần thứ tư

TS. Lưu Hương Ly

Vụ Pháp luật dân sự - kinh tế, Bộ Tư pháp

I. Đặt vấn đề

Tại Việt Nam, khi nói đến Blockchain người ta thường hay nghĩ đến tiền ảo (như Bitcoin) nhưng thực chất tiền ảo chỉ là ứng dụng đầu tiên của công nghệ Blockchain. Blockchain có tiềm năng ứng dụng trong vô số lĩnh vực mà một trong số đó chính là hợp đồng thông minh (Smart Contract) dựa trên công nghệ chuỗi khối¹. Với những ưu điểm như đảm bảo tính minh bạch, sự tin cậy, chắc chắn trong thực thi và giảm chi phí giao dịch, hợp đồng thông minh được coi là có tiềm năng phát triển rất lớn và đang rất được cộng đồng quốc tế quan tâm. Hợp đồng thông minh đã và đang được phát triển hoặc sử dụng trong rất nhiều lĩnh vực đa dạng như tài chính, ngân hàng, chuỗi cung ứng², y tế, giao thông... Vấn đề đặt ra là bản chất pháp lý của hợp đồng thông minh là gì, liệu các quy định pháp luật hiện hành của Việt Nam về hợp đồng có thể được áp dụng đối với các hợp đồng thông minh và trong tương lai chúng ta có cần sửa đổi, bổ sung hệ thống pháp luật về hợp đồng để điều chỉnh các hợp đồng thông minh hay không. Tham luận này sẽ tập trung phân tích, đánh giá và làm rõ những vấn đề nêu trên (lưu ý: phạm vi Tham luận này chỉ tập trung vào các hợp đồng thông minh trên nền tảng Blockchain).

II. Khái niệm, bản chất của hợp đồng thông minh

Thế giới hiện nay chưa có định nghĩa thống nhất về hợp đồng thông minh.³ Có thể định nghĩa hợp đồng thông minh là những thỏa thuận được tự động thực thi bằng các máy tính⁴. Những hợp đồng như vậy được thiết kế nhằm đảm bảo việc thực thi mà không cần đến các Tòa án cũng như loại bỏ sự

¹ Hợp đồng thông minh được coi là thế hệ thứ hai của Blockchain.

² Chẳng hạn, xem “*Cách Walmart, Alibaba cải tổ lại ngành bán lẻ với Blockchain*” tại

<https://tradingig.com/threads/cach-walmart-alibaba-cai-to-lai-nganh-ban-le-voi-blockchain.535/>

³ Xem Maren K. Woebeking, “The Impact of Smart Contracts on Traditional Concepts of Contract Law”, 10 (2019) JIPITEC 105, tr.107, xem tại https://www.jipitec.eu/issues/jipitec-10-1-2019/at_download/CompleteIssue

⁴ Max Raskin, “The Law and Legality of Smart Contract”, 1 GEO. L. TECH. REV. 305 (2017), xem tại <https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf>, tr.306.

tùy nghi của con người trong việc thực thi hợp đồng⁵. Về bản chất, hợp đồng thông minh là mã máy tính mà khi xảy ra một hoặc nhiều điều kiện nhất định có khả năng tự động thực thi những chức năng đã được lập trình sẵn⁶. Mã này được lưu trữ và xử lý trên nền tảng công nghệ sổ cái phân tán/chuỗi khối và ghi lại mọi thay đổi trên sổ cái này.⁷ Hiện nay, Ethereum là nền tảng Blockchain cho phép chạy hợp đồng thông minh phổ biến nhất hiện nay. Bản chất phi tập trung của công nghệ Blockchain tạo ra môi trường lý tưởng cho các hợp đồng thông minh.⁸ Mỗi giao dịch sẽ được ghi nhận và lưu trữ thành một khối thông tin nối tiếp nhau và có giá trị chứng minh thông qua truy xuất lịch sử giao dịch trên chuỗi. Chính đặc tính này của Blockchain làm cho hợp đồng thông minh chạy trên nền tảng này có tiềm năng ngăn ngừa hoặc nhanh chóng giải quyết tranh chấp.⁹

Có hai trường hợp có thể xảy ra với hợp đồng thông minh: (i) toàn bộ thỏa thuận giữa các bên được thể hiện tại các lệnh được mã hóa; hoặc (ii) hợp đồng thông minh chỉ mã hóa để tự động thực thi hợp đồng pháp lý (có thể bằng văn bản hoặc không) giữa các bên và hầu hết các hợp đồng thông minh hiện nay thuộc trường hợp thứ hai.¹⁰ Một số nhà nghiên cứu cũng cho rằng trong tương lai gần hợp đồng thông minh cũng sẽ chỉ được sử dụng để tự thực thi những phần của hợp đồng đủ rõ ràng đến mức có thể mã hóa được.¹¹

III. Thực trạng pháp luật về hợp đồng thông minh tại Việt Nam

3.1. Bản chất và giá trị pháp lý của hợp đồng thông minh

Theo quy định tại Điều 385 Bộ luật dân sự năm 2015 thì “*hợp đồng là sự thỏa thuận giữa các bên về việc xác lập, thay đổi hoặc chấm dứt quyền, nghĩa vụ dân sự*”. Để hợp đồng có hiệu lực thì nó phải thỏa mãn một số điều kiện nhất định¹², bao gồm:

⁵ Như trên

⁶ Chamber of Digital Commerce, “Smart Contracts: Is the Law Ready?”, September 2018, xem tại <https://digitalchamber.org/smart-contracts-paper-press/>, tr.10.

⁷ Như trên

⁸ Jack Gilcrest & Arthur Carvalho, “Smart Contracts: Legal Considerations”, available at https://www.researchgate.net/publication/330626140_Smart_Contracts_Legal_Considerations

⁹ Như trên

¹⁰ Xem Gary Tse, “Smart contracts: a boon or bane for the legal profession?” ngày 24/9/2018 tại <https://www.taylorvinters.com/article/smart-contracts-a-boon-or-bane-for-the-legal-profession>

¹¹ Primavera De Filippi and Aaron Wright, Blockchain and the Law (HUP 2018) tr.195.

¹² Xem các quy định tại Điều 116, 117, 122, 407 và 408 Bộ luật dân sự năm 2015.

- Chủ thể có năng lực pháp luật dân sự, năng lực hành vi dân sự phù hợp với giao dịch dân sự được xác lập;
- Chủ thể tham gia giao dịch dân sự hoàn toàn tự nguyện;
- Mục đích và nội dung của giao dịch dân sự không vi phạm điều cấm của luật, không trái đạo đức xã hội và
- Giao dịch dân sự đáp ứng quy định về hình thức trong trường hợp luật có quy định.

Như vậy, về nguyên tắc, hợp đồng thông minh có thể được coi là một hợp đồng và có hiệu lực ràng buộc các bên nếu đáp ứng được các yêu cầu về sự thỏa thuận và các điều kiện có hiệu lực của hợp đồng nêu trên. Ngoài ra, Luật Giao dịch điện tử năm 2005 cũng đã quy định rõ về hợp đồng điện tử và thừa nhận giá trị pháp lý của hợp đồng điện tử, theo đó, hợp đồng điện tử là hợp đồng được thiết lập dưới dạng thông điệp dữ liệu theo quy định của Luật này¹³ và giá trị pháp lý của hợp đồng điện tử không thể bị phủ nhận chỉ vì hợp đồng đó được thể hiện dưới dạng thông điệp dữ liệu¹⁴.

Tuy nhiên, Luật Giao dịch điện tử năm 2005 chưa có quy định về việc giao kết và thực hiện hợp đồng thông qua việc sử dụng hệ thống thông tin tự động. Luật Giao dịch điện tử mới chỉ quy định khái niệm giao dịch điện tử tự động, theo đó, giao dịch điện tử tự động là giao dịch điện tử được thực hiện tự động từng phần hoặc toàn bộ thông qua hệ thống thông tin đã được thiết lập sẵn (khoản 7 Điều 4). Tuy nhiên, quy định này chưa làm rõ giá trị pháp lý cũng như trách nhiệm của các bên khi tham gia vào các giao dịch điện tử tự động như vậy. Trong khi đó, Nghị định số 52 về thương mại điện tử đã có quy định về sử dụng hệ thống thông tin tự động, theo đó “*Hợp đồng được **giao kết** từ sự tương tác giữa một hệ thống thông tin tự động với một người hoặc giữa các hệ thống thông tin tự động với nhau không bị phủ nhận giá trị pháp lý chỉ vì không có sự kiểm tra hay can thiệp của con người vào từng hành động cụ thể do các hệ thống thông tin tự động thực hiện hay hợp đồng được **giao kết**.” (Điều 13). Tuy nhiên, quy định này vẫn có nhược điểm là mới chỉ quy định về việc giao kết hợp đồng mà chưa quy định về việc thực hiện hợp đồng thông qua việc sử dụng hệ thống thông tin tự động, vì vậy chưa quy định rõ giá trị pháp lý của các hợp*

¹³ Điều 33 Luật Giao dịch điện tử năm 2005

¹⁴ Điều 34 Luật Giao dịch điện tử năm 2005

đồng thông minh – là các hợp đồng được tự động thực hiện thông qua các mã máy tính.

Ngoài ra, Luật Giao dịch điện tử hiện nay của Việt Nam chưa có quy định về suy đoán năng lực chủ thể của các bên tham gia giao dịch điện tử. Hiện nay, Điều 48 Luật Thương mại điện tử năm 2018 của Trung Quốc quy định “*Các bên tham gia hoạt động thương mại điện tử được suy đoán là có năng lực hành vi dân sự đầy đủ để thực hiện hành vi pháp lý tương ứng, trừ trường hợp có bằng chứng chứng minh ngược lại*”. Quy định này có ý nghĩa quan trọng trong việc thúc đẩy sự phát triển của các giao dịch điện tử, phù hợp với đặc thù của giao dịch điện tử là khác với các giao dịch truyền thống, các bên tham gia giao dịch điện tử có thể không nhìn thấy nhau trực tiếp, thậm chí một hoặc các bên có thể ẩn danh khi tham gia giao dịch.

3.2. Giá trị chứng cứ của hợp đồng thông minh khi giải quyết tranh chấp dân sự tại các cơ quan tài phán

Hiện nay, theo quy định tại Điều 93 Bộ luật Tố tụng dân sự năm 2015 của Việt Nam thì chứng cứ trong vụ việc dân sự là những gì có thật được đương sự và cơ quan, tổ chức, cá nhân khác giao nộp, xuất trình cho Tòa án trong quá trình tố tụng hoặc do Tòa án thu thập được theo trình tự, thủ tục do Bộ luật này quy định và được Tòa án sử dụng làm căn cứ để xác định các tình tiết khách quan của vụ án cũng như xác định yêu cầu hay sự phản đối của đương sự là có căn cứ và hợp pháp. Theo quy định tại Điều 94 Bộ luật Tố tụng dân sự năm 2015 thì nguồn chứng cứ bao gồm: tài liệu đọc được, nghe được, nhìn được, dữ liệu điện tử; Vật chứng; Lời khai của đương sự; Lời khai của người làm chứng; Kết luận giám định; Biên bản ghi kết quả thẩm định tại chỗ; Kết quả định giá tài sản, thẩm định giá tài sản; Văn bản ghi nhận sự kiện, hành vi pháp lý do người có chức năng lập; Văn bản công chứng, chứng thực; Các nguồn khác mà pháp luật có quy định. Như vậy, về nguyên tắc, theo quy định của Bộ luật Tố tụng dân sự năm 2015 thì hợp đồng thông minh với tư cách là dữ liệu điện tử hoàn toàn có thể được thừa nhận là nguồn chứng cứ khi giải quyết tranh chấp dân sự tại các cơ quan tài phán.

3.3. Tính pháp lý của chữ ký mật mã và bản ghi trên Blockchain

Hiện nay, Luật Giao dịch điện tử quy định về chữ ký điện tử như sau:

“Chữ ký điện tử được tạo lập dưới dạng từ, chữ, số, ký hiệu, âm thanh hoặc các hình thức khác bằng phương tiện điện tử, gắn liền hoặc kết hợp một

cách lô gíc với thông điệp dữ liệu, có khả năng xác nhận người ký thông điệp dữ liệu và xác nhận sự chấp thuận của người đó đối với nội dung thông điệp dữ liệu được ký.”¹⁵

Đôi chiếu với quy định nêu trên thì chữ ký mật mã hoàn toàn đáp ứng các điều kiện để được coi là chữ ký điện tử. Ngoài ra, Luật Giao dịch điện tử cũng quy định chữ ký điện tử được xem là bảo đảm an toàn nếu chữ ký điện tử đó được kiểm chứng bằng một quy trình kiểm tra an toàn do các bên giao dịch thỏa thuận và đáp ứng các điều kiện: (i) Dữ liệu tạo chữ ký điện tử chỉ gắn duy nhất với người ký trong bối cảnh dữ liệu đó được sử dụng; (ii) Dữ liệu tạo chữ ký điện tử chỉ thuộc sự kiểm soát của người ký tại thời điểm ký; (iii) Mọi thay đổi đối với chữ ký điện tử sau thời điểm ký đều có thể bị phát hiện; và (iv) Mọi thay đổi đối với nội dung của thông điệp dữ liệu sau thời điểm ký đều có thể bị phát hiện.¹⁶ Luật cũng quy định chữ ký điện tử có thể được chứng thực bởi một tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử và chữ ký điện tử đã được tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử chứng thực được xem là bảo đảm các điều kiện an toàn.¹⁷ Như vậy, việc được chứng thực bởi một tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử không phải là điều kiện bắt buộc để được thừa nhận là chữ ký điện tử an toàn. Tuy nhiên, kể từ khi Luật Giao dịch điện tử được ban hành đến nay, Chính phủ mới chỉ ban hành Nghị định hướng dẫn về chữ ký số (Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số) mà chưa ban hành bất kỳ quy định nào để giải thích về chữ ký điện tử an toàn, dẫn đến nhiều vướng mắc, bất cập trong thực tiễn áp dụng pháp luật trong thời gian qua liên quan đến tính an toàn của chữ ký điện tử mà không phải là chữ ký số, dẫn đến sự thiếu tin tưởng của các bên khi tham gia giao dịch điện tử, sự nhầm lẫn giữa chữ ký điện tử và chữ ký số, thậm chí quan niệm chỉ có chữ ký số mới được coi là an toàn và có giá trị pháp lý.

3.5. Vấn đề giải thích hợp đồng

Điều 404 Bộ luật dân sự năm 2015 đã quy định các nguyên tắc chung về giải thích hợp đồng như sau:

“1. Khi hợp đồng có điều khoản không rõ ràng thì việc giải thích điều khoản đó không chỉ dựa vào ngôn từ của hợp đồng mà còn phải căn cứ

¹⁵ Khoản 1 Điều 21 Luật Giao dịch điện tử

¹⁶ Khoản 1 Điều 22 Luật Giao dịch điện tử.

¹⁷ Xem khoản 2 và 3 Điều 21 và khoản 2 Điều 22 Luật Giao dịch điện tử

vào ý chí của các bên được thể hiện trong toàn bộ quá trình trước, tại thời điểm xác lập, thực hiện hợp đồng.

2. Khi hợp đồng có điều khoản hoặc ngôn từ có thể hiểu theo nhiều nghĩa khác nhau thì phải giải thích theo nghĩa phù hợp nhất với mục đích, tính chất của hợp đồng.

3. Khi hợp đồng có điều khoản hoặc ngôn từ khó hiểu thì phải được giải thích theo tập quán tại địa điểm giao kết hợp đồng.

4. Các điều khoản trong hợp đồng phải được giải thích trong mối liên hệ với nhau, sao cho ý nghĩa của các điều khoản đó phù hợp với toàn bộ nội dung hợp đồng.

5. Trường hợp có sự mâu thuẫn giữa ý chí chung của các bên với ngôn từ sử dụng trong hợp đồng thì ý chí chung của các bên được dùng để giải thích hợp đồng.

6. Trường hợp bên soạn thảo đưa vào hợp đồng nội dung bất lợi cho bên kia thì khi giải thích hợp đồng phải theo hướng có lợi cho bên kia.”

Tuy nhiên, đây chỉ là những quy định mang tính nguyên tắc chung, trong quá trình giải quyết các tranh chấp cụ thể (chẳng hạn khi có sự mâu thuẫn giữa điều khoản trong hợp đồng thông minh và điều khoản trong hợp đồng văn bản do các bên ký kết, có thể là do mã lệnh trong hợp đồng thông minh bị nhập sai do lỗi kỹ thuật, điều khoản trong hợp đồng nào sẽ được ưu tiên áp dụng?) sẽ vẫn cần có sự giải thích pháp luật từ phía Tòa án.

3.6. Vấn đề sửa đổi hợp đồng

Điều 421 Bộ luật dân sự năm 2015 đã quy định về sửa đổi hợp đồng, theo đó, các bên có thể thỏa thuận sửa đổi hợp đồng và hợp đồng sửa đổi phải tuân theo hình thức của hợp đồng ban đầu. Tuy nhiên, như đã phân tích ở trên, với mức độ phát triển hiện tại của công nghệ Blockchain, việc sửa đổi hợp đồng thông minh ngay tại chính hợp đồng thông minh đó khá khó khăn và các bên sẽ phải đàm phán bên ngoài hệ thống Blockchain hoặc mã hóa một hợp đồng thông minh mới để thay đổi điều khoản của một hợp đồng thông minh hiện tại.

3.7. Vấn đề tuân thủ pháp luật chuyên ngành

Một điều nữa cần lưu ý là, ngoài Bộ luật dân sự, hợp đồng thông minh cũng phải tuân thủ các quy định của pháp luật chuyên ngành (tùy từng trường hợp cụ thể). Chẳng hạn, hợp đồng thông minh trong lĩnh vực kinh doanh bảo

hiểm vừa là hợp đồng bảo hiểm (chịu sự điều chỉnh của pháp luật chuyên ngành về bảo hiểm¹⁸), vừa là hợp đồng với người tiêu dùng nên cũng chịu sự điều chỉnh của pháp luật về bảo vệ quyền lợi người tiêu dùng¹⁹.

3.8. Vấn đề xác định pháp luật áp dụng và quyền tài phán

Vấn đề này có thể được giải quyết nếu các bên trong hệ thống đã lập trình sẵn (mã hóa) điều khoản về pháp luật áp dụng và quyền tài phán trong hợp đồng thông minh. Trong trường hợp, hợp đồng thông minh không lập trình sẵn về vấn đề này thì pháp luật Việt Nam hiện hành cũng đã có quy định làm cơ sở để xác định pháp luật áp dụng và thẩm quyền xét xử của Tòa án Việt Nam. Điều 683 Bộ luật dân sự năm 2015 đã quy định về luật áp dụng đối với hợp đồng, theo đó, các bên trong quan hệ hợp đồng được thỏa thuận lựa chọn pháp luật áp dụng đối với hợp đồng, trừ một số trường hợp quy định tại các khoản 4, 5 và 6 Điều 683 Bộ luật dân sự năm 2015. Trường hợp các bên không có thỏa thuận về pháp luật áp dụng thì pháp luật của nước có mối liên hệ gần bó nhất với hợp đồng đó được áp dụng. Về xác định quyền tài phán, hiện nay Điều 469 và Điều 470 Bộ luật Tố tụng dân sự năm 2015 cũng đã quy định về thẩm quyền chung của Tòa án Việt Nam trong giải quyết các vụ việc dân sự có yếu tố nước ngoài và thẩm quyền riêng biệt của Tòa án Việt Nam. Như vậy, khi có tranh chấp phát sinh từ hợp đồng thông minh các bên tranh chấp có thể dựa vào các quy định này để xác định quyền tài phán của Tòa án Việt Nam.

IV. Kết luận và đề xuất, kiến nghị

Ở thời điểm hiện tại, với mức độ phát triển hiện tại của công nghệ chuỗi khối và hợp đồng thông minh, có thể tạm thời kết luận: khung pháp luật hiện hành của Việt Nam về hợp đồng và giao dịch điện tử đã khá đầy đủ để điều chỉnh các hợp đồng thông minh mà không cần có sự sửa đổi, bổ sung hay xóa trộn lớn, trừ việc sửa đổi, bổ sung một số quy định tại Luật Giao dịch điện tử năm 2005, cụ thể như sau:

(i) Để bảo đảm giá trị pháp lý của các giao dịch điện tử tự động nói chung và hợp đồng thông minh nói riêng, trong quá trình sửa đổi Luật Giao dịch điện tử năm 2005, cần nghiên cứu bổ sung thêm quy định về sử dụng hệ thống thông tin tự động trong giao dịch điện tử theo hướng hợp đồng được giao kết hoặc thực hiện từ sự tương tác giữa một hệ thống thông tin tự động với một người

¹⁸ Luật Kinh doanh bảo hiểm năm 2000, sửa đổi, bổ sung năm 2010 và năm 2019 và các văn bản hướng dẫn thi hành

¹⁹ Luật bảo vệ quyền lợi người tiêu dùng năm 2010 và các văn bản hướng dẫn thi hành

hoặc giữa các hệ thống thông tin tự động với nhau không bị phủ nhận giá trị pháp lý chỉ vì không có sự kiểm tra hay can thiệp của con người vào từng hành động cụ thể do các hệ thống thông tin tự động thực hiện hay hợp đồng được giao kết và bên sử dụng hệ thống thông tin tự động phải chịu trách nhiệm về các hành vi do hệ thống thông tin tự động thực hiện.

(ii) Cần nhắc bổ sung quy định về suy đoán về năng lực chủ thể của các bên tham gia giao dịch điện tử trong Luật Giao dịch điện tử (sửa đổi) để giảm nhẹ trách nhiệm chứng minh của các bên về hiệu lực của giao dịch khi phát sinh tranh chấp (bên nào yêu cầu tuyên bố giao dịch vô hiệu do không đáp ứng yêu cầu về năng lực chủ thể thì bên đó có trách nhiệm chứng minh).

(iii) Luật Giao dịch điện tử (sửa đổi) cần đưa ra định nghĩa rõ ràng, phân biệt các khái niệm “chữ ký điện tử”, “chữ ký điện tử an toàn”, “chữ ký số”, trong đó cần quy định rõ chữ ký số cũng chỉ là một loại chữ ký điện tử an toàn. Đồng thời, Luật Giao dịch điện tử (sửa đổi) cần quy định rõ các điều kiện, tiêu chuẩn để chữ ký điện tử được coi là chữ ký điện tử an toàn. Cụ thể, cần quy định rõ chữ ký điện tử an toàn là (i) chữ ký số (đáp ứng các điều kiện nhất định); **hoặc** (ii) chữ ký do các bên thoả thuận và đáp ứng các điều kiện nhất định. Về điều kiện để một chữ ký điện tử được coi là an toàn và tin cậy, có thể tham khảo quy định tại Luật mẫu của UNCITRAL về Chữ ký điện tử được UNCITRAL thông qua ngày 05/7/2001, trong đó đề cao nguyên tắc trung lập về công nghệ, công nhận giá trị của chữ ký điện tử không phụ thuộc vào loại công nghệ được sử dụng trong giao dịch. Luật mẫu về Chữ ký điện tử tiếp cận trên cơ sở sử dụng công nghệ mã hóa mật mã công cộng (có tổ chức công cộng chứng nhận và thực hiện việc mã hóa), hay còn gọi là chữ ký số (digital signature). Mặc dù vậy, Luật mẫu cũng đề cập đến việc sử dụng các công nghệ mới như sinh trắc học (biometrics)- dùng các dấu hiệu của các bộ phận trong cơ thể con người như dấu vân tay, ảnh mặt, ảnh mắt... để nhận ra một cá thể; mã số xác nhận cá nhân - số PIN (Personal Identification Number) và các công nghệ tương tự.

Bên cạnh đó, Luật Giao dịch điện tử cũng cần đảm bảo giá trị pháp lý của chữ ký điện tử an toàn theo hướng: chữ ký điện tử an toàn có giá trị chứng cứ (các bên không phải chứng minh tính xác thực và tính toàn vẹn của chữ ký điện tử an toàn), trừ trường hợp có chứng cứ chứng minh ngược lại.

Ngoài ra, trong quá trình giải quyết tranh chấp vẫn có thể có cách hiểu hay giải thích pháp luật khác nhau, khi đó Tòa án nhân dân tối cao cần ban hành Nghị quyết hay án lệ để giải thích và hướng dẫn áp dụng pháp luật một cách thống nhất, chẳng hạn như hướng dẫn về việc giải thích hợp đồng khi có sự mâu thuẫn giữa điều khoản trong hợp đồng thông minh và điều khoản trong hợp đồng văn bản do các bên ký kết; hướng dẫn cách hiểu về pháp luật của nước có mối liên hệ gắn bó nhất với hợp đồng thông minh... Tuy nhiên, cần ghi nhớ rằng công nghệ hiện nay đang thay đổi với tốc độ rất nhanh, Blockchain và hợp đồng thông minh cũng không phải là ngoại lệ, vì vậy, vấn đề này vẫn cần tiếp tục được theo dõi, nghiên cứu để điều chỉnh pháp luật nếu cần thiết./.

Chính sách, pháp luật EU trong thị trường số

Ngô Đức Minh – Vụ Pháp chế - Bộ Công Thương

Mục lục

1. Luật Thị trường số (Digital Market Acts - DMA)
2. Luật Các Dịch vụ số (Digital Services Acts – DSA)
3. Cập nhật hiện trạng pháp lý Việt Nam trong lĩnh vực thị trường số
4. Một vài gợi ý chính sách cho Việt Nam

1. Luật Thị trường số Châu Âu (1)

Mục tiêu

- Mục tiêu:
- Mục tiêu tối thượng: Duy trì cạnh tranh lành mạnh trong thị trường nội khối trong lĩnh vực số
- Mục tiêu cụ thể: Điều tiết các dịch vụ nền tảng lõi (core platform services) được định danh là các nền tảng gác cổng “Gatekeepers” – Điều 3.2

1. Luật Thị trường số Châu Âu (2)

Phạm vi điều chỉnh

- Điều chỉnh **các dịch vụ** hướng đến người sử dụng là thương nhân - “*business users*” được thành lập ở trong lãnh thổ EU hay các người dùng cuối cùng - “*end users*” được thành lập/cư trú trong lãnh thổ EU **không phụ thuộc vào** vị trí địa lý, quốc gia nơi thành lập pháp nhân của các pháp nhân “*người gác cửa*” .
- DMA không ảnh hưởng đến việc thực hiện Điều 101, 102 của Hiến pháp Châu Âu (TFEU) – các điều khoản liên quan đến hoạt động cạnh tranh nội khối.
- DMA không ảnh hưởng đến quyền lực các cơ quan cạnh tranh của quốc gia thành viên

1. Luật Thị trường số Châu Âu (3)

Đối tượng áp dụng: Các gatekeepers

- Điều 3.2 quy định các dịch vụ nền tảng lõi gồm:
- Dịch vụ trung gian trực tuyến (định nghĩa tại Quy định của EU về Nền tảng trực tuyến vs Doanh nghiệp – [P2B regulation](#))
- Dịch vụ tìm kiếm trực tuyến (định nghĩa tại P2B)
- Dịch vụ mạng xã hội trực tuyến (Chỉ thị về dịch vụ nghe nhìn, truyền thông – [Audiovisual Media Services Directive](#))
- Dịch vụ nền tảng chia sẻ video trực tuyến
- Dịch vụ OTT ([number – independent interpersonal communication services](#))
- Hệ điều hành
- Dịch vụ điện toán đám mây
- Các dịch vụ quảng cáo đi liền với các nền tảng trên

1. Luật thị trường số Châu Âu (4)

Các nội dung quan trọng (1)

Nhà cung cấp dịch vụ nền tảng lõi bị coi là gatekeepers khi đáp ứng <u>đồng thời 3</u> tiêu chí sau:	Tiêu chí định lượng theo Điều 3.2.
1. Có ảnh hưởng đáng kể đến thị trường nội khối	<ul style="list-style-type: none"> - Thuộc pháp nhân có doanh thu trên thị trường khu vực kinh tế Châu Âu (EEA*) lớn hơn hoặc bằng 65 tỉ Euros trong 3 năm tài chính gần nhất; - Giá trị vốn hóa trung bình hoặc giá trị thị trường tương đương của pháp nhân sở hữu lớn hơn hoặc bằng 65 tỉ Euros trong năm tài chính gần nhất; - Cung cấp dịch vụ tới tối thiểu là 3 nước thành viên <p><small>* EEA = EU + EFTA (Iceland, Norway, Liechtenstein, trừ Thụy Sĩ)</small></p>
2. Dịch vụ là cổng kết nối quan trọng giữa thương nhân và người dùng cuối	<ul style="list-style-type: none"> - Có hơn 45 triệu end users/ tháng tại EU (active users) - Có hơn 10.000 thương nhân/năm (active, thương nhân thành lập tại EU trong năm tài chính gần nhất)
3. Giữ vị trí trên thị trường trong một thời gian đáng kể (bao gồm hiện tại và tương lai gần)	<ul style="list-style-type: none"> - Có các tiêu chí tại 2) duy trì trong 3 năm tài chính gần nhất

Ghi chú: Điều 3.6 quy định ngay cả khi các tiêu chí này không hoàn toàn phụ thuộc vào tiêu chí định lượng mà có thể được đánh giá bổ sung.

1. Luật Thị trường số Châu Âu (2) Trình tự, thủ tục (2)

- Khi một nền tảng lõi thỏa mãn các ngưỡng tại Điều 3.2 thì phải có nghĩa vụ thông báo cho Ủy ban Châu Âu (EC) trong vòng 3 tháng.
- EC sẽ ấn định nền tảng này là Gatekeeper trừ trường hợp nền tảng cung cấp các chứng cứ phản biện. Với trường hợp có chứng cứ phản biện, EC sẽ tiến hành đánh giá.
- EC đánh giá trường hợp các ngưỡng không thỏa mãn nhưng các tiêu chí định tính vẫn thỏa mãn (Điều 3.6) thì các nền tảng vẫn bị coi là Gatekeeper.
- Điều 4 quy định việc rà soát định kỳ (2 năm /lần) hoặc đột xuất hoặc theo yêu cầu.

1. Luật Thị trường số Châu Âu (2) Quy định trách nhiệm, điều cấm (3)

Trách nhiệm của các Gatekeepers	Điều cấm thực hiện của Gatekeeper
<ul style="list-style-type: none"> - Cho phép cài đặt các phần mềm, kho ứng dụng của bên thứ ba trên hệ điều hành của mình. - Cung cấp cho nhà xuất bản nội dung, quảng cáo công cụ truy cập vào các ứng dụng đánh giá hiệu quả của Gatekeeper. - Cho phép công cụ hữu hiệu để lấy dữ liệu (Quy định chung về bảo vệ dữ liệu - GDPR). - Cung cấp cho người dung thương nhân công cụ truy cập dữ liệu thời gian thực tạo ra từ hoạt động thương mại của họ trên nền tảng. - Áp dụng công bằng, không phân biệt đối xử các điều kiện truy cập các kho ứng dụng, phần mềm đối với người dung là thương nhân 	<ul style="list-style-type: none"> - Cấm đối xử ưu ái thông qua xếp hạng sản phẩm, dịch vụ của chính nền tảng so với các sản phẩm, dịch vụ bên thứ ba (self referencing in ranking). - Cấm kết hợp dữ liệu người dung cuối cùng thu thập được từ các dịch vụ của mình hoặc từ các dịch vụ của bên thứ ba mà không có sự chấp thuận của người dùng hoặc không cho người dung từ chối. - Phải có điều khoản MFN đối với các người dùng là thương nhân* - Cấm việc ngăn cản thương nhân tiếp cận khách hàng chỉ vì thương nhân đó có giao kết hợp đồng không thông qua nền tảng. - Cấm yêu cầu thương nhân mua dịch vụ, sản phẩm cung cấp kèm theo dịch vụ nền tảng lõi. - Cấm việc ngăn cản người dung gỡ bỏ các phần mềm, ứng dụng cài đặt sẵn <p>* MFN= thương nhân không được bán, cung cấp sản phẩm, dịch vụ với giá, điều kiện bán hàng khác với bình thường khi cung cấp trên nền tảng</p>

1. Luật Thị trường số Châu Âu (2) Thẩm quyền, miễn trừ, thông báo TTKT(4)

- Điều 7 (2) quy định: EC có quyền quy định chi tiết các biện pháp mà nền tảng phải thực hiện.
- Điều 8: Ngưng áp dụng một số nghĩa vụ cụ thể
- Điều 9: Miễn trừ có thể được cho phép vì lý do đạo đức xã hội, sức khỏe cộng đồng hay an ninh, an toàn xã hội.
- Điều 10: Các nghĩa vụ có thể được bổ sung bởi EC
- Điều 12: Quy định nghĩa vụ thông báo khi tiến hành tập trung kinh tế: Không áp dụng ngưỡng kiểm soát tập trung kinh tế nếu bên bị sáp nhập, mua lại, hợp nhất cũng hoạt động trên thị trường số.
- Điều 13: Kiểm tra, kiểm toán cơ chế định danh người dùng (consumer profiling).

1. Luật Thị trường số Châu Âu (2) Thẩm quyền, biện pháp xử lý vi phạm (5)

- **Mức phạt**
 - Phạt tiền nếu không tuân thủ (đến 10% doanh thu)
 - Quyền yêu cầu cung cấp thông tin, thực hiện khảo sát, phỏng vấn và nhất là áp dụng các biện pháp ngăn chặn (dawn raids).
 - Quyền áp dụng các biện pháp tạm thời hoặc yêu cầu cam kết
 - Quyền được khiếu nại và tiếp cận hồ sơ, tài liệu và kiện ra Tòa
- **Quyền tiến hành điều tra thị trường**
 - Để xác định nền tảng là gatekeepers (theo tiêu chí, ngưỡng)
 - Kiểm tra việc không tuân thủ có hệ thống và ấn định các biện pháp khắc phục hậu quả
 - Để xác định các hành vi mới, dịch vụ, thị trường mới

2. Luật các dịch vụ số (1)

Mục tiêu (1)

- Xây dựng trên cơ sở các nguyên tắc chính đã được quy định tại [Chỉ thị](#) về thương mại điện tử.
- Đảm bảo các điều kiện tốt nhất cho sáng tạo dịch vụ số trong thị trường khu vực
- Đảm bảo an toàn, an ninh mạng
- Bảo vệ quyền cơ bản
- Xây dựng cấu trúc quản trị mạnh mẽ, lâu dài để điều tiết các dịch vụ trung gian trực tuyến.

2. Luật các dịch vụ số (1)

Phạm vi điều chỉnh

- Áp dụng cho tất cả các nội dung vi phạm pháp luật
- Bao gồm các vấn đề về IP
- Phân quyền cho các nước thành viên giám sát, thực thi đối với các nền tảng thành lập tại các nước đó.
- Nghĩa vụ công bố việc sử dụng thuật toán.
- Các quy định của Chỉ thị về TMĐT không bị bãi bỏ.

2. Luật các dịch vụ số (2)

Đối tượng áp dụng

- Các dịch vụ trung gian trực tuyến (bao gồm nền tảng trực tuyến, mạng xã hội, sàn TMĐT).
- Các nền tảng lớn (≥ 45 triệu người sử dụng hàng tháng).
- Điều chỉnh đối với các nhà cung cấp dịch vụ của EU và xuyên biên giới nhưng có hoạt động trong lãnh thổ.

2. Luật các dịch vụ số (2)

Nội dung (1)

- Chương 1: Phạm vi, đối tượng và định nghĩa
Các dịch vụ trung gian, nền tảng trực tuyến; các nội dung trái pháp luật bị cấm
- Chương 2: Các trường hợp miễn trách
 - Chỉ cung cấp hạ tầng truyền dẫn (mere conduit)
 - Caching, hosting
 - Thực hiện lệnh của cơ quan có thẩm quyền
- Chương 3
 - Mục 1: Trách nhiệm chung của các nhà cung cấp dịch vụ trung gian (trừ báo chí trực tuyến, e-mail, nhắn tin, website bán hàng)
 - Mục 2: Trách nhiệm của dịch vụ hosting
 - Mục 3: Trách nhiệm của nền tảng trực tuyến (trừ SMEs)
 - Mục 4: Trách nhiệm của nền tảng trực tuyến lớn
 ≥ 45 triệu người dung/tháng = 10% dân số

2. Luật các dịch vụ số (2)

Chương 3: Trách nhiệm của các nhà cung cấp dịch vụ (2)

Mục 1: Tất cả các nhà cung cấp	Mục 2: Trách nhiệm hosting	Mục 3: Trách nhiệm của nền tảng trực tuyến	Mục 4: Nền tảng trực tuyến lớn
<ul style="list-style-type: none"> - Phải có đầu mối liên lạc hoặc đại diện pháp lý - Phải có và thực thi có trách nhiệm các điều khoản dịch vụ (Term and Conditions) - Báo cáo hàng năm về các hoạt động liên quan đến nội dung 	<ul style="list-style-type: none"> - Mô tả cơ chế cho phép hiển thị thông báo về các nội dung trái pháp luật - Không thoái thác trách nhiệm khi có thông báo - Cung cấp lý do chi tiết về việc gỡ bỏ nội dung cho người dùng 	<ul style="list-style-type: none"> - Có cơ chế cho người dùng khiếu nại, giải quyết khiếu nại trên nền tảng; - Có cơ chế giải quyết tranh chấp nội bộ (ngoài Tòa án); - Cho phép ưu tiên các thông báo đánh giá của người dung uy tín (trusted flagger) trong đó bao gồm cả các đối tượng chủ thể quyền. - Có cơ chế tạm ngưng sử dụng dịch vụ của các người dung tái phạm. - Có cơ chế báo cáo các vi phạm hình sự - Có cơ chế thông tin, kiểm chứng về thương nhân trong các giao dịch từ xa (thông tin cơ bản như địa chỉ, đăng ký kd...) - Công bố báo cáo về việc áp dụng cơ chế giải quyết tranh chấp nội bộ, tạm ngưng dịch vụ, sửa đổi nội dung tự động... - Minh bạch hóa hoạt động quảng cáo trực tuyến (<i>Lý do người dung bị nhắm đến như tính chất, tiêu chí, nhóm người dung liên quan</i>) 	<ul style="list-style-type: none"> - Đánh giá rủi ro hàng năm - Xây dựng cơ chế để xử lý các rủi ro - Phải được kiểm tra, kiểm toán hàng năm về nghĩa vụ tuân thủ - Công khai các thông số chính được sử dụng trong hệ thống gợi ý dịch vụ và quảng cáo (thương hiệu quảng cáo) - Cung cấp dữ liệu cho cơ quan có thẩm quyền để giám sát - Phải có chuyên viên kiểm soát tuân thủ - Báo cáo 2 lần/năm - Đánh giá rủi ro và biện pháp xử lý phải được công khai hàng năm

2. Luật các dịch vụ số (2)

Chương 4: Thực thi (3)

- Các quốc gia thành viên phải chỉ định cơ quan thực thi tại quốc gia mình và điều phối viên tham gia Cơ quan dịch vụ số EU
- Nhà cung cấp có trụ sở tại quốc gia thành viên nào thì quốc gia đó có thẩm quyền quản lý
- Nếu nhà cung cấp dịch vụ xuyên biên giới không có trụ sở, đại diện pháp lý tại EU, tất cả các quốc gia thành viên đều có thẩm quyền quản lý
- Có quyền khiếu nại với Cơ quan dịch vụ số EU về vị trí địa lý người sử dụng hoặc nơi thành lập nhà cung cấp dịch vụ.
- Cơ quan dịch vụ số có quyền phạt tới 6% tổng doanh thu.

3. Hiện trạng pháp lý của Việt Nam trong thị trường số (1) Hệ thống pháp luật hiện hành

- Luật Thương mại 2005
- Luật Giao dịch điện tử 2005
- Luật Điện ảnh 2006
- Luật Công nghệ thông tin 2006
- Luật Viễn thông 2009
- Luật Tần số vô tuyến điện 2009
- Luật Bảo vệ quyền lợi người tiêu dùng 2010
- Luật An toàn thông tin mạng 2015
- Luật Hỗ trợ doanh nghiệp vừa và nhỏ 2017
- Luật An ninh mạng 2018
- Luật Cạnh tranh 2018

3. Hiện trạng pháp lý của Việt Nam trong thị trường số (2) Hệ thống pháp luật đang được hoàn thiện

- Luật Điện ảnh (sửa đổi): Trình tháng 10/2021 và thông qua 6/2022
- Luật Giao dịch điện tử (Sửa đổi): Đang ở giai đoạn lập Đề nghị
- Luật Chính phủ số (dự kiến): Nhiệm vụ giai đoạn 2022 – 2024 theo NQ 50/NQ-CP 2021
- Luật Công nghiệp công nghệ số: Nhiệm vụ giai đoạn 2022 - 2024 theo NQ 50/NQ-CP 2021
- Luật Tần số vô tuyến điện (sửa đổi), Luật Viễn Thông (sửa đổi);
- Nghị định sửa đổi, bổ sung về thương mại điện tử
- Nghị định sửa, bổ sung về viễn thông, tần số vô tuyến điện
- Nghị định sửa, bổ sung về thanh toán không dùng tiền mặt
- Nghị định sửa, bổ sung về phát thanh, truyền hình, internet, quảng cáo xuyên biên giới
- Nghị định thủ tục hải quan đối với hàng hóa xk, nk qua giao dịch thương mại điện tử
- Nghị định về định danh, xác thực điện tử
- Nghị định về bảo vệ dữ liệu cá nhân
- Các Nghị định quy định chi tiết Luật An ninh mạng

3. Hiện trạng pháp lý của Việt Nam trong thị trường số (3) Hệ thống chính sách, quan điểm chỉ đạo

- [Chiến lược Kinh tế - Xã hội](#) 10 năm 2021 – 2030: “chuyển đổi số”, “kinh tế số”
- [Nghị quyết số 52-NQ/TW](#) ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư
- [Nghị quyết 50/NQ-CP 20/5/2021](#) Chương trình hành động của Chính phủ thực hiện Nghị quyết Đại hội XIII
- Quyết định số 942/QĐ-TTg ngày 15/6/2021 của Thủ tướng Chính phủ Phê duyệt Chiến lược phát triển Chính phủ điện tử hướng tới Chính phủ số giai đoạn 2021 - 2025, định hướng đến năm 2030
- Quyết định số 1017/QĐ-TTg ngày 14/8/2020 Phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025
- Quyết định số 749/QĐ-TTg ngày 03/06/2020 của Thủ tướng Chính phủ Phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”
- Quyết định số 645/QĐ-TTg ngày 15/05/2020 của Thủ tướng Chính phủ phê duyệt Kế hoạch tổng thể phát triển thương mại điện tử quốc gia giai đoạn 2021 – 2025
- Quyết định số 458/QĐ-TTg ngày 3/4/2020 của Thủ tướng Chính phủ : Phê duyệt Đề án “Lưu trữ tài liệu điện tử của các cơ quan nhà nước giai đoạn 2020 – 2025
- Quyết định số 431/QĐ-TTg ngày 27/3/2020 của Thủ tướng Chính phủ Phê duyệt Đề án quản lý hoạt động thương mại điện tử đối với hàng hóa xuất khẩu, nhập khẩu
- Chỉ thị số 01/CT-TTg ngày 14/01/2020 của Thủ tướng Chính phủ : Về thúc đẩy phát triển doanh nghiệp công nghệ số Việt Nam
- Quyết định số 999/QĐ-TTg ngày 12/08/2019 của Thủ tướng Chính phủ Phê duyệt Đề án thúc đẩy mô hình kinh tế chia sẻ
- Quyết định số 1072/QĐ-TTg 28/8/2018 của Thủ tướng Chính phủ: Thành lập Ủy ban Quốc gia về Chính phủ điện tử

4. Một vài gợi ý chính sách

- **1. Quan điểm, định hướng: Quản lý thông thoáng**
- Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị: “*Cuộc Cách mạng công nghiệp lần thứ tư yêu cầu phải đổi mới tư duy về quản lý kinh tế, quản lý xã hội, xây dựng, hoàn thiện thể chế cho phù hợp. Cần có cách tiếp cận mở, sáng tạo, cho thí điểm đối với những vấn đề thực tiễn mới đặt ra, tạo mọi thuận lợi cho đổi mới sáng tạo.*”
- Nghị quyết số 50/NQ-CP của Chính phủ: “*Xây dựng cơ chế quản lý linh hoạt, phù hợp với môi trường kinh doanh số, tạo không gian thuận lợi cho đổi mới sáng tạo.*”
- **2. Chiến lược: Xây dựng đồng bộ**
- **3. Xây dựng pháp luật: Bao trùm – Linh hoạt**
- Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị:
 - “- Hoàn thiện pháp luật, trước hết là pháp luật về doanh nghiệp, khởi nghiệp sáng tạo, sở hữu trí tuệ, thương mại, đầu tư, kinh doanh...”
 - - Chủ động tham gia vào các khuôn khổ pháp lý khu vực và toàn cầu để phát triển kinh tế số. Hoàn thiện pháp luật, chính sách về dữ liệu, quản trị dữ liệu, tạo thuận lợi cho việc tạo dựng, kết nối, chia sẻ và khai thác dữ liệu bảo đảm an toàn, an ninh mạng trong nước, tiến tới kết nối với khu vực ASEAN và quốc tế. Xây dựng hành lang pháp lý cho định danh số và xác thực điện tử quốc gia; thiết lập khung danh tính số quốc gia.”

Chiến lược quốc gia về phát triển kinh tế số và xã hội số	Bộ TTTT	Bộ KHCN	Tháng 8/2021	TTgCP
Luật Giao dịch điện tử và Kinh tế số (sửa đổi, bổ sung Luật Giao dịch điện tử 2005)	Bộ TTTT	Các cơ quan liên quan	2022	Quốc hội
Luật Chính phủ số	Bộ TTTT	Các cơ quan liên quan	2022-2024	Quốc hội
Luật Công nghiệp công nghệ số	Bộ TTTT	Các cơ quan liên quan	2022-2025	Quốc hội
Chiến lược phát triển khoa học, công nghệ và đổi mới sáng tạo giai đoạn 2021-2030	Bộ KHCN	Các cơ quan liên quan	2021	TTgCP
Chương trình đổi mới công nghệ quốc gia	Bộ CT	Các cơ quan liên quan	2021	TTgCP
Chương trình hành động quốc gia về phát triển và chuyển đổi sang sử dụng nền tảng điện toán đám mây	Bộ TTTT	Các cơ quan liên quan	2021-2022	TTgCP
Đề án Nâng cao nhận thức, đào tạo kỹ năng và phát triển nguồn nhân lực chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030	Bộ TTTT	Các cơ quan liên quan	2021	TTgCP
Đề án hỗ trợ chuyển đổi số cho các doanh nghiệp năm 2025, định hướng đến năm 2030	Bộ KHĐT	Bộ TTTT, các cơ quan liên quan	2021	TTgCP
Chiến lược tổng thể phát triển các ngành dịch vụ của Việt Nam đến năm 2030, tầm nhìn 2050	Bộ KHĐT	Các cơ quan liên quan	2021	TTgCP
Đề án phát triển thanh toán không dùng tiền mặt tại Việt Nam giai đoạn 2021-2025	NHNNVN	Các cơ quan liên quan	2021	TTgCP
Đề án tái cơ cấu các ngành công nghiệp và thương mại giai đoạn 2021-2030	Bộ CT	Các cơ quan liên quan	2021	TTgCP
Chương trình phát triển công nghiệp công nghệ thông tin, điện tử - viễn thông đến năm 2025, tầm nhìn đến năm 2030, chủ động tham gia Cuộc cách mạng công nghiệp lần thứ tư	Bộ TTTT	Bộ CT, Bộ KHĐT	2021	TTgCP
Chiến lược dữ liệu quốc gia giai đoạn 2021-2025, định hướng đến năm 2030	Bộ TTTT	Các cơ quan liên quan	2021	TTgCP
Quy hoạch hạ tầng thông tin và truyền thông quốc gia thời kỳ 2021- 2030, tầm nhìn đến năm 2050	Bộ TTTT	Các cơ quan liên quan	2021	TTgCP
Chiến lược Hạ tầng số đến năm 2025 và định hướng đến năm 2030	Bộ TTTT	Các cơ quan liên quan	2021	TTgCP
Chiến lược an toàn, an ninh mạng quốc gia giai đoạn 2021-2025, tầm nhìn đến năm 2030	Bộ CA	Các cơ quan liên quan	2021	TTgCP

QUẢN LÝ CÁC NỀN TẢNG SỐ

KINH NGHIỆM CỦA LIÊN MINH CHÂU ÂU VÀ MỘT SỐ ĐỀ XUẤT CHÍNH SÁCH ĐỐI VỚI VIỆT NAM

Ngô Đức Minh
Vụ Pháp chế - Bộ Công Thương

I. LUẬT THỊ TRƯỜNG SỐ (DMA)

1. Phạm vi điều chỉnh và đối tượng áp dụng

Các dịch vụ liên quan là những dịch vụ mà Ủy ban đã xác định là “các dịch vụ nền tảng cốt lõi” (CPS) (Điều 2 (2)) được định nghĩa:

- a) Dịch vụ trung gian trực tuyến;
- b) Công cụ tìm kiếm trực tuyến;
- c) Các dịch vụ mạng xã hội trực tuyến;
- d) Các dịch vụ nền tảng chia sẻ video;
- e) Các dịch vụ liên lạc giữa các cá nhân không phụ thuộc vào số điện thoại;
- f) Hệ điều hành;
- g) Dịch vụ điện toán đám mây;

h) Các dịch vụ quảng cáo được cung cấp bởi một nhà điều hành cung cấp bất kỳ dịch vụ nào trong mục (a) - (g).

Một số thuật ngữ nêu trên được định nghĩa trong các văn bản khác (ví dụ: “*dịch vụ xã hội thông tin*”, “*công cụ tìm kiếm trực tuyến*” và “*dịch vụ nền tảng chia sẻ video*”) trong khi một số định nghĩa mới được đưa ra như “*dịch vụ mạng xã hội trực tuyến*” và “*các kho ứng dụng*” để đảm bảo tính nhất quán trong hệ thống quy định kỹ thuật số.

Các nhà khai thác dịch vụ sẽ bị nhắm đến bởi các quy định này là những doanh nghiệp được chỉ định là “*người gác cổng*” theo Điều 3. Điều 3 (1) bao gồm phép thử ba giai đoạn:

- Sự tồn tại của một tác động đáng kể đến thị trường nội khối;
- Hoạt động của CPS “*đóng vai trò như một cửa ngõ quan trọng để người dùng doanh nghiệp tiếp cận người dùng cuối*”;
- Một vị trí cố định và lâu dài trong các hoạt động của các nền tảng này trên thị trường.

Các phép thử được đánh giá bằng các tiêu chí định lượng (dựa trên doanh thu hoặc giá trị thị trường và phạm vi tiếp cận của người dùng), đưa ra giả định có thể bác bỏ về tình trạng của nhà vận hành và được tinh chỉnh bằng cách tham khảo các tiêu chí định tính. Ban đầu, các nền tảng tự đưa ra đánh giá này và thông báo cho Ủy ban.

Điều 5 liệt kê các nghĩa vụ đối với *người gác cổng*.

Điều 6 có danh sách các hành vi khác có thể được quy định đối với *người gác cổng*. Các nghĩa vụ bao gồm các nghĩa vụ tích cực và các điều cấm, về cơ bản là các hành vi được xác định từ các vụ việc điều tra cạnh tranh trước đây và hoàn thiện lại các quy định cạnh tranh không hiệu quả với các nền tảng này.

Các quy định này đã được chi tiết hóa và dự kiến Ủy ban có thể cập nhật danh sách các hành vi bị cấm theo kinh nghiệm thực thi. Quy định cũng đưa ra khả năng có các trường hợp ngoại lệ, bao gồm miễn trừ vì các lý do đặc biệt quan trọng đối với lợi ích công cộng (đạo đức công cộng, sức khỏe cộng đồng và an ninh công cộng).

2. Hành vi bị cấm

- Không kết hợp dữ liệu cá nhân có nguồn từ các dịch vụ nền tảng cốt lõi này với dữ liệu cá nhân từ bất kỳ dịch vụ nào khác được cung cấp bởi người quản lý cổng hoặc với dữ liệu cá nhân từ các dịch vụ của bên thứ ba và từ việc đăng nhập người dùng cuối vào các dịch vụ khác của người quản lý cổng để kết hợp cá nhân dữ liệu (Điều 5(a));

- Không ngăn cản hoặc hạn chế người dùng doanh nghiệp nêu vấn đề với bất kỳ cơ quan quản lý nhà nước nào về đến bất kỳ hoạt động nào của *người gác cổng* (Điều 5d);

- Không yêu cầu người dùng doanh nghiệp sử dụng, cung cấp hoặc tương tác với dịch vụ nhận dạng của *người gác cổng* (Điều 5e);

- Không yêu cầu người dùng doanh nghiệp hoặc người dùng cuối phải đăng ký hoặc không được đăng ký với bất kỳ dịch vụ nền tảng cốt lõi nào khác (Điều 5f);

- Hạn chế sử dụng bất kỳ dữ liệu không công khai nào về hoạt động của người dùng doanh nghiệp hoặc người dùng cuối của họ để cạnh tranh với những người dùng doanh nghiệp đó (Điều 6(1)(a));

- Ngăn người dùng cuối hủy cài đặt bất kỳ ứng dụng phần mềm được cài đặt sẵn nào (Điều 6(1)(b));

- Xếp hạng các sản phẩm của chính người gác cổng có lợi hơn so với các sản phẩm tương tự của bên thứ ba (Điều 6 (1) (d));

- Về mặt kỹ thuật, hạn chế khả năng của người dùng cuối chuyển đổi và đăng ký với các ứng dụng và dịch vụ phần mềm khác nhau được truy cập bằng hệ điều hành của *người gác cổng* (Điều 6 (1) (e)).

3. Các nghĩa vụ tích cực

- Cho phép người dùng doanh nghiệp cung cấp các sản phẩm hoặc dịch vụ giống nhau cho người dùng cuối thông qua các dịch vụ trung gian trực tuyến của bên thứ ba với mức giá hoặc điều kiện khác với giá hoặc điều kiện được cung cấp thông

qua các dịch vụ trung gian trực tuyến của *người gác cổng* (điều khoản MFN). (Điều 5b));

- Cho phép người dùng doanh nghiệp quảng cáo ưu đãi cho người dùng cuối có được thông qua dịch vụ nền tảng cốt lõi và ký kết hợp đồng với những người dùng cuối này bất kể vì mục đích đó họ có sử dụng dịch vụ nền tảng cốt lõi của *người gác cổng* hay không (Điều 5c));

- Cho phép người dùng cuối truy cập và sử dụng ứng dụng phần mềm của người dùng doanh nghiệp nơi phần mềm được mua lại mà không cần sử dụng các dịch vụ nền tảng cốt lõi của *người gác cổng* (Điều 5c));

- Cung cấp cho các nhà quảng cáo và nhà xuất bản mà họ cung cấp thông tin về giá dịch vụ quảng cáo liên quan đến dịch vụ quảng cáo (Điều 5g);

- Cho phép cài đặt và sử dụng có hiệu quả các ứng dụng phần mềm của bên thứ ba hoặc kho ứng dụng phần mềm đang sử dụng hoặc tương tác với hệ điều hành của *người gác cổng* đó và cho phép các ứng dụng phần mềm hoặc kho ứng dụng phần mềm này được truy cập bằng các phương tiện khác với các dịch vụ nền tảng cốt lõi của người giữ cổng đó (Điều 6(1)(c));

- Áp dụng các điều kiện FRAND cho xếp hạng (Điều 6(1)(d));

- Cung cấp cho người dùng doanh nghiệp và nhà cung cấp các dịch vụ phụ trợ quyền truy cập và khả năng tương tác với cùng một hệ điều hành, các tính năng phần cứng hoặc phần mềm có sẵn hoặc được sử dụng bởi chính *người gác cổng* (Điều 6(1)(f));

- Cung cấp dữ liệu để cho phép xác minh độc lập không gian quảng cáo (Điều 6(1)(g));

- Đảm bảo tính khả chuyển dữ liệu hiệu quả và truy cập thời gian thực (Điều 6(1)(h));

- Cung cấp miễn phí cho người dùng doanh nghiệp quyền truy cập hiệu quả, chất lượng cao, liên tục và theo thời gian thực để sử dụng dữ liệu tổng hợp và không tổng hợp (tuân theo GDPR) (Điều 6(1)(i));

- Cung cấp quyền truy cập cho các nhà cung cấp bên thứ ba của công cụ tìm kiếm theo các điều khoản công bằng, hợp lý và không phân biệt đối xử (FRAND) để xếp hạng, truy vấn, nhấp và xem dữ liệu do người dùng cuối tạo ra (Điều 6(1)(j));

- Điều kiện FRAND để người dùng doanh nghiệp truy cập vào cửa hàng ứng dụng của *người gác cổng* (Điều 6(1)(k)).

Ngược lại với quan điểm của luật cạnh tranh, Ủy ban sẽ không phải chứng minh tác động của các hành vi của các nền tảng đối với cạnh tranh trên thị trường và khả năng can thiệp của Ủy ban theo quyền hạn cạnh tranh của mình vẫn không bị ảnh

hưởng. Quy định cũng đưa ra các điều khoản trao quyền cho Ủy ban thực hiện các cuộc điều tra thị trường cho bất kỳ mục đích nào trong ba mục đích: xác định những *người gác cổng* không bị các ngưỡng định lượng của DMA; xác định các dịch vụ khác cần được thêm vào danh sách các dịch vụ nền tảng cốt lõi hoặc các hoạt động mới có thể không công bằng; xác định các biện pháp xử lý hành vi hoặc cấu trúc tương xứng trong trường hợp *người gác cổng* vi phạm có hệ thống các quy tắc.

Điều 10 trao cho Ủy ban quyền thông qua các hành vi được ủy quyền để cập nhật danh sách trong Điều 5 và 6 khi Ủy ban phát hiện ra các hành vi không công bằng trong một cuộc điều tra thị trường.

DMA yêu cầu những người giữ cổng thông báo cho Ủy ban về bất kỳ sự hợp nhất hoặc mua lại nào liên quan đến một nhà cung cấp dịch vụ nền tảng cốt lõi khác hoặc bất kỳ dịch vụ nào khác được cung cấp trong lĩnh vực kỹ thuật số. Với quy định này, việc mua lại như vậy không liên quan đến quy tắc kiểm soát sáp nhập của EU (hoặc quốc gia). Đây không phải là một chế độ sáp nhập chuyên ngành mà để cho phép Ủy ban xem xét các chỉ định và nghĩa vụ của *người gác cổng*.

DMA quy định tiền phạt tới 10% doanh thu hàng năm trên toàn cầu của *người gác cổng* do vi phạm các quy định của Luật tương tự như các hình phạt áp dụng trong các trường hợp cạnh tranh. Các biện pháp xử lý dưới dạng tái cấu trúc vẫn có thể thực hiện trong trường hợp các vấn đề đang diễn ra hoặc các hành vi không mang tính chất hình sự, cục đoạn (Điều 16) và chỉ áp dụng khi không có biện pháp khắc phục hành vi có hiệu quả tương đương.

II. LUẬT CÁC DỊCH VỤ SỐ (DSA)

1. Các đối tượng áp dụng

DSA phân biệt giữa bốn cấp đối tượng dựa trên định nghĩa về "dịch vụ xã hội thông tin" (information society services):

- Các nhà cung cấp dịch vụ trung gian (định nghĩa tại Điều 2 (f));
- Các nhà cung cấp máy chủ và nền tảng trực tuyến (định nghĩa tại Điều 2 (h));
- Nền tảng trực tuyến;
- Các nhà cung cấp nền tảng trực tuyến rất lớn (Điều 25 được định nghĩa).

Các nền tảng trực tuyến bao gồm các mạng xã hội và sàn giao dịch thương mại trực tuyến.

Mỗi đối tượng phải tuân theo các quy định khác nhau theo “*nguyên tắc tương xứng*”. “*Các nền tảng rất lớn*” được xác định theo dân số ở cấp độ EU – có nghĩa là nền tảng rất lớn nằm dưới sự kiểm soát của cấp độ EU.

2. Chương II: Duy trì quyền miễn trừ cho nội dung của các bên thứ ba

Các quan điểm quản lý cơ bản được duy trì theo Chỉ thị thương mại điện tử. Theo đó, miễn trừ trách nhiệm bên thứ ba với các dịch vụ trung gian đối với nội dung truyền tải hoặc lưu trữ với điều kiện là nhà cung cấp dịch vụ chỉ “*hành động khẩn cấp để xóa hoặc vô hiệu hóa quyền truy cập thông tin*” mà không có nghĩa vụ cụ thể phải giám sát các nội dung đó (Điều 7).

3. Chương III: Quy tắc chung

Có một số nghĩa vụ cụ thể liên quan đến tất cả các nhà cung cấp dịch vụ trung gian:

- Thiết lập đầu mối liên lạc (SPoC);
- Thành lập đại diện pháp lý trong EU cho các nhà cung cấp không được thành lập ở EU;

- Các nhà cung cấp phải thực hiện các điều khoản và điều khoản của họ một cách 'siêng năng, khách quan và tương xứng';

- Trừ trường hợp là SMEs, nhà cung cấp phải công bố ít nhất một lần/năm các báo cáo “*rõ ràng, dễ hiểu và chi tiết*” về bất kỳ sự kiểm duyệt nội dung nào mà họ đã thực hiện trong thời gian liên quan (nội dung của các quy định cụ thể được viện dẫn trong Chỉ thị).

Các nhà cung cấp dịch vụ lưu trữ, bao gồm cả các nền tảng trực tuyến, phải tuân theo các quy định bổ sung:

- Các cơ chế báo cáo cho nội dung bất hợp pháp (chứa các yếu tố cụ thể) - được gọi là “*cơ chế thông báo và hành động*”

- Cung cấp lý do liên quan đến quyết định xóa / vô hiệu hóa quyền truy cập vào các mục nội dung cụ thể và nội dung của lý do được quy định tại Điều 15 (2)

- Các quyết định phải được đưa ra trong cơ sở dữ liệu do Ủy ban quản lý.

Có thể thấy các nghĩa vụ này được tập trung nhiều việc xử lý các vấn đề phát sinh từ nội dung (độc hại, phi pháp). Thay vì xác định cụ thể các nội dung đó thì quy định hướng về các cơ chế mà các nền tảng trực tuyến cần có để giải quyết các vấn đề. Quan điểm này có thể được thấy trong các nghĩa vụ chung hơn được áp dụng đối với các nền tảng trực tuyến, đặc biệt là các nền tảng trực tuyến rất lớn.

3.1. Mục 3: Các quy định liên quan đến nền tảng trực tuyến

Các nền tảng trực tuyến phải đáp ứng những nghĩa vụ sau:

- Cho phép người dung truy cập vào hệ thống xử lý khiếu nại nội bộ miễn phí, hiệu quả liên quan đến các quyết định đình chỉ tài khoản hoặc xóa / vô hiệu hóa nội dung;

- Cung cấp cơ chế giải quyết tranh chấp khác ngoài công cụ tòa án liên quan đến các tranh chấp với các nền tảng;

- Có một hệ thống người đánh giá đáng tin cậy (trust flagger) cho phép xử lý những thông báo vi phạm không bị xử lý chậm trễ;

- Những người đánh giá đáng tin cậy phải đáp ứng các tiêu chí nhất định (Europol hoặc các tổ chức INHOPE sẽ đáp ứng các tiêu chí này (đoạn 46 lời mở đầu).

Họ phải chịu các nghĩa vụ bổ sung sau:

- Các nền tảng trực tuyến có nghĩa vụ tạm ngừng, trong một khoảng thời gian hợp lý và sau khi đã đưa ra cảnh báo trước:

+ Việc cung cấp dịch vụ cho những người nhận dịch vụ thường xuyên cung cấp nội dung bất hợp pháp rõ ràng;

+ Việc xử lý các thông báo và khiếu nại của các cá nhân hoặc tổ chức hoặc bởi những người khiếu nại thường xuyên gửi các thông báo hoặc khiếu nại mà rõ ràng là không có cơ sở;

- Các nền tảng có nghĩa vụ thông báo nghi ngờ hoạt động tội phạm

- Nền tảng được yêu cầu để đảm bảo rằng các nhà giao dịch sử dụng nền tảng của họ có thể truy vết được (cung cấp thông tin cụ thể).

Có các yêu cầu báo cáo về tính minh bạch được nâng cao, bao gồm tính minh bạch của quảng cáo trực tuyến (rằng thông tin là một quảng cáo; ai đã đặt nó và lý do tại sao người dùng nhìn thấy quảng cáo đó, bao gồm thông tin liên quan đến bất kỳ hồ sơ nào (đoạn 52 lời mở đầu).

3.2. Mục IV: Nền tảng trực tuyến rất lớn

Mục 4 đề cập đến “các nền tảng trực tuyến rất lớn” là các nền tảng có 45 triệu người tham gia ở Liên minh Châu Âu trở lên. Do đó, họ phải chịu các nghĩa vụ khác ngoài những nghĩa vụ đã được quy định:

- Đánh giá 6 tháng/lần về “bất kỳ rủi ro hệ thống đáng kể nào” gồm:

+ Đánh giá hoạt động của kiểm duyệt nội dung, hệ thống thuật toán đề xuất và quảng cáo mục tiêu đồng thời quy định xử lý tài khoản giả, việc sử dụng bot và các hành vi tự động hoặc tự động một phần khác;

+ Đánh giá việc thực hiện “các biện pháp giảm thiểu hợp lý, tương xứng và hiệu quả” và các biện pháp này phải được đánh giá độc lập - những người thực hiện cuộc đánh giá phải đáp ứng các tiêu chí nhất định;

- Báo cáo liên quan đến quá trình đánh giá rủi ro, giảm thiểu rủi ro và kiểm toán:

- Giải trình về các tham số được sử dụng trong hệ thống khuyến nghị và cung cấp cho phép người sử dụng sửa đổi các hệ thống đó;

- Trách nhiệm minh bạch đối với quảng cáo trực tuyến bằng cách thiết lập một kho lưu trữ các quảng cáo;

- Cung cấp dữ liệu cần thiết để giám sát việc tuân thủ quy định này;
- Các điều khoản về quyền tiếp cận các nhà nghiên cứu đã được kiểm tra;
- Yêu cầu phải có một nhân viên tuân thủ (người phải có kinh nghiệm / trình độ chuyên môn nhất định).

4. Thể chế và Thực thi

Chương IV đề cập đến các thể chế thực hiện và thực thi.

+ Một Quốc gia Thành viên phải chỉ định một cơ quan có trách nhiệm làm Điều phối viên Dịch vụ Kỹ thuật số (DSC) của mình.

+ Ban Châu Âu về Dịch vụ Kỹ thuật số (EBDS) được thành lập để tư vấn cho các DSC và Ủy ban tương ứng.

DSC điều phối phản ứng quốc gia và có các nhiệm vụ cụ thể theo quy định (Điều 41).

+ EBDS được tạo thành từ các DSC, được đại diện bởi các quan chức cấp cao.

III. BÀI HỌC KINH NGHIỆM CHO VIỆT NAM

1. Quan điểm, định hướng: Quản lý thông thoáng

1.1. Quan điểm chỉ đạo của Đảng

Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư đã thể hiện rõ quan điểm chỉ đạo¹:

“- Chủ động, tích cực tham gia cuộc Cách mạng công nghiệp lần thứ tư là yêu cầu tất yếu khách quan...”

- Cuộc Cách mạng công nghiệp lần thứ tư mang lại cả cơ hội và thách thức. Phải nắm bắt kịp thời, tận dụng hiệu quả các cơ hội để nâng cao năng suất lao động, hiệu quả, sức cạnh tranh của nền kinh tế, hiệu lực, hiệu quả quản lý xã hội thông qua nghiên cứu, chuyển giao và ứng dụng mạnh mẽ các thành tựu tiên tiến của cuộc Cách mạng công nghiệp lần thứ tư cho các lĩnh vực của đời sống kinh tế - xã hội, nhất là một số ngành, lĩnh vực trọng điểm, có tiềm năng, lợi thế để làm động lực cho tăng trưởng theo tinh thần bắt kịp, tiến cùng và vượt lên ở một số lĩnh vực so với khu vực và thế giới...

- Cuộc Cách mạng công nghiệp lần thứ tư yêu cầu phải đổi mới tư duy về quản lý kinh tế, quản lý xã hội, xây dựng, hoàn thiện thể chế cho phù hợp. Cần có cách tiếp cận mở, sáng tạo, cho thí điểm đối với những vấn đề thực tiễn mới đặt ra, tạo mọi thuận lợi cho đổi mới sáng tạo.”

¹ Mục II.1 về Quan điểm chỉ đạo

1.2. Định hướng của Chính phủ, Thủ tướng Chính phủ

Nghị quyết số 50/NQ-CP của Chính phủ ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết số 52-NQ/TW ngày 27 tháng 9 năm 2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư đã thể hiện định hướng của Chính phủ, Thủ tướng Chính phủ như sau:² “*Xây dựng cơ chế quản lý linh hoạt, phù hợp với môi trường kinh doanh số, tạo không gian thuận lợi cho đổi mới sáng tạo. Sớm ban hành khung thể chế thử nghiệm có kiểm soát để triển khai thí điểm sau đó nhân rộng đối với các công nghệ, sản phẩm, dịch vụ, mô hình kinh doanh mới hình thành từ cách mạng công nghiệp lần thứ tư có tiềm năng gây rủi ro cao. Việc triển khai thí điểm, thử nghiệm phải xác định rõ phạm vi không gian và thời gian.*”

Như vậy, quan điểm chỉ đạo của Đảng, định hướng hành động của Chính phủ là đã thể hiện tầm nhìn chính xác, thông thoáng, rộng mở làm tiền đề căn bản cho hoạt động hoạch định chiến lược, chính sách, pháp luật của các cơ quan, tổ chức.

2. Chiến lược: Xây dựng đồng bộ

Từ năm 2018 trở lại đây, Thủ tướng Chính phủ ban hành nhiều Quyết định có nội dung chính sách về lĩnh vực kinh tế số, chuyển đổi số, giao dịch điện tử trong nhiều lĩnh vực như Chính phủ số, an toàn thông tin mạng, chuyển đổi số... Các chính sách dưới dạng Đề án về cơ bản đã được thể chế hóa, xây dựng thành quy định của pháp luật. Hiện còn các chính sách về nền kinh tế chia sẻ, phát triển doanh nghiệp công nghệ số vẫn còn nhiều nội dung cần được tiếp tục nghiên cứu, xây dựng thành quy định của pháp luật.

Tiếp theo đó, theo Nghị quyết 50/NQ-CP 20/5/2021 của Chính phủ ban hành Chương trình hành động của Chính phủ thực hiện Nghị quyết Đại hội XIII đã quy định danh mục các đề án, chính sách mà Chính phủ, Thủ tướng Chính phủ sẽ ban hành trong giai đoạn 2021 – 2025 và hướng đến 2030. Trong đó, Thủ tướng Chính phủ sẽ tiếp tục ban hành nhiều Chiến lược, Đề án, Chương trình.

Nhìn vào danh sách này, có thể thấy các Chiến lược đã bao quát hầu hết các lĩnh vực của nền kinh tế số. Tuy nhiên, để các Chiến lược mang tầm nhìn dài hạn, việc xây dựng các Chiến lược này phải được theo dõi, giám sát về tính thống nhất, đan xen và bổ trợ cho nhau.

3. Xây dựng pháp luật: Bao trùm – Linh hoạt

- Nghị quyết số 48-NQ/TW ngày 24 tháng 5 năm 2005 của Bộ Chính trị về Chiến lược xây dựng và hoàn thiện hệ thống pháp luật Việt Nam đến năm 2010, định

² Mục 2. a) Chương trình hành động.

hướng đến năm 2020 về xây dựng và hoàn thiện pháp luật về dân sự, kinh tế, trọng tâm là hoàn thiện thể chế kinh tế thị trường định hướng xã hội chủ nghĩa có chỉ đạo: *“Xây dựng và hoàn thiện pháp luật về sở hữu, quyền tự do kinh doanh. Xác định rõ trách nhiệm pháp lý của chủ sở hữu nhà nước và các chủ sở hữu khác, cơ chế bảo đảm quyền sở hữu và hạn chế quyền sở hữu...”*

- Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư đã thể hiện rõ quan điểm chỉ đạo:

“- Hoàn thiện pháp luật, trước hết là pháp luật về doanh nghiệp, khởi nghiệp sáng tạo, sở hữu trí tuệ, thương mại, đầu tư, kinh doanh để tạo điều kiện thuận lợi cho quá trình chuyển đổi số quốc gia và phát triển các sản phẩm, dịch vụ, mô hình kinh tế mới dựa trên nền tảng công nghệ số, Internet và không gian mạng; đồng thời ngăn chặn kịp thời các tác động tiêu cực cả về kinh tế và xã hội, bảo đảm quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

- Chủ động tham gia vào các khuôn khổ pháp lý khu vực và toàn cầu để phát triển kinh tế số. Hoàn thiện pháp luật, chính sách về dữ liệu, quản trị dữ liệu, tạo thuận lợi cho việc tạo dựng, kết nối, chia sẻ và khai thác dữ liệu bảo đảm an toàn, an ninh mạng trong nước, tiến tới kết nối với khu vực ASEAN và quốc tế. Xây dựng hành lang pháp lý cho định danh số và xác thực điện tử quốc gia; thiết lập khung danh tính số quốc gia.”

**Baker
McKenzie.**

Bảo vệ dữ liệu cá nhân trong bối cảnh Cách mạng công nghiệp lần thứ tư – kinh nghiệm quốc tế và đề xuất, kiến nghị đối với Việt Nam

Trần Mạnh Hùng
Nguyễn Tuấn Linh

| Tháng 9 năm 2021

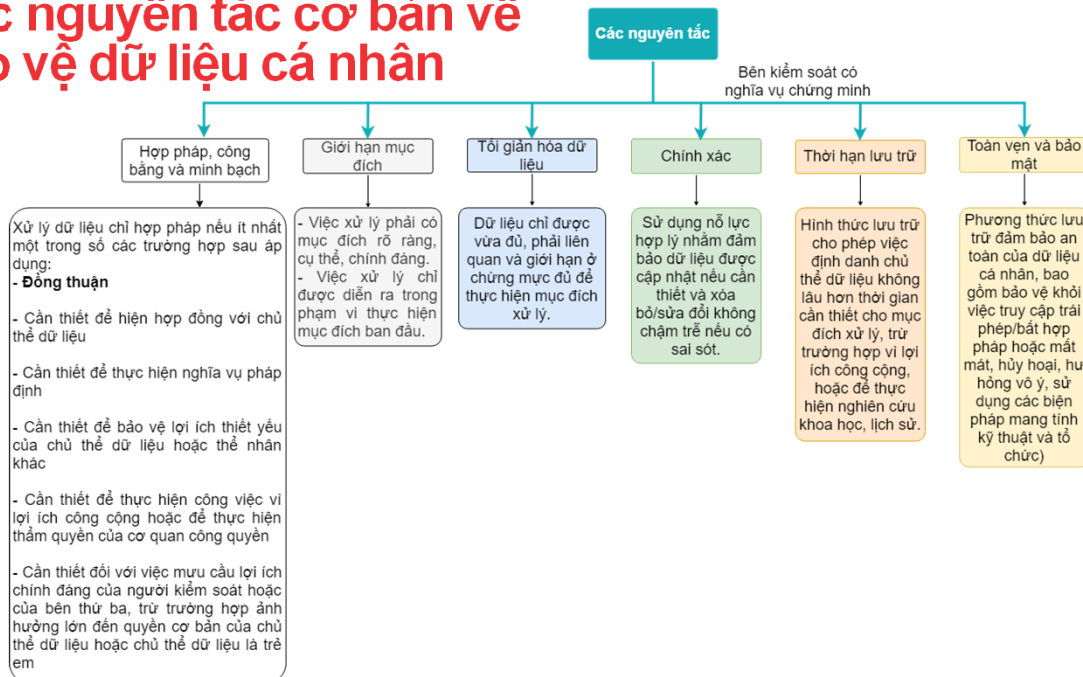
Mục lục

- 1** MỘT SỐ KHÁI NIỆM CƠ BẢN
- 2** CHUYỂN DỮ LIỆU CÁ NHÂN QUA BIÊN GIỚI
- 3** MỘT SỐ VÍ DỤ THỰC TIỄN
- 4** KHUYẾN NGHỊ CHO VIỆT NAM

1

Một số khái niệm và các chủ thể liên quan đến bảo vệ dữ liệu cá nhân

Các nguyên tắc cơ bản về bảo vệ dữ liệu cá nhân



Các khái niệm chính

Dữ liệu cá nhân

Chủ thể dữ liệu

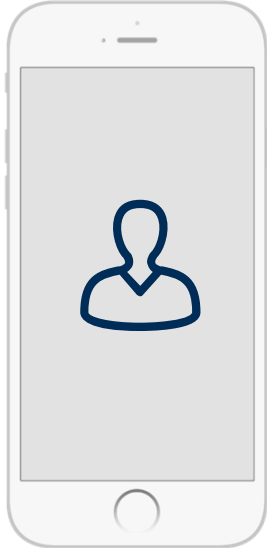
Bên kiểm soát dữ liệu

Bên xử lý dữ liệu

Dữ liệu cá nhân



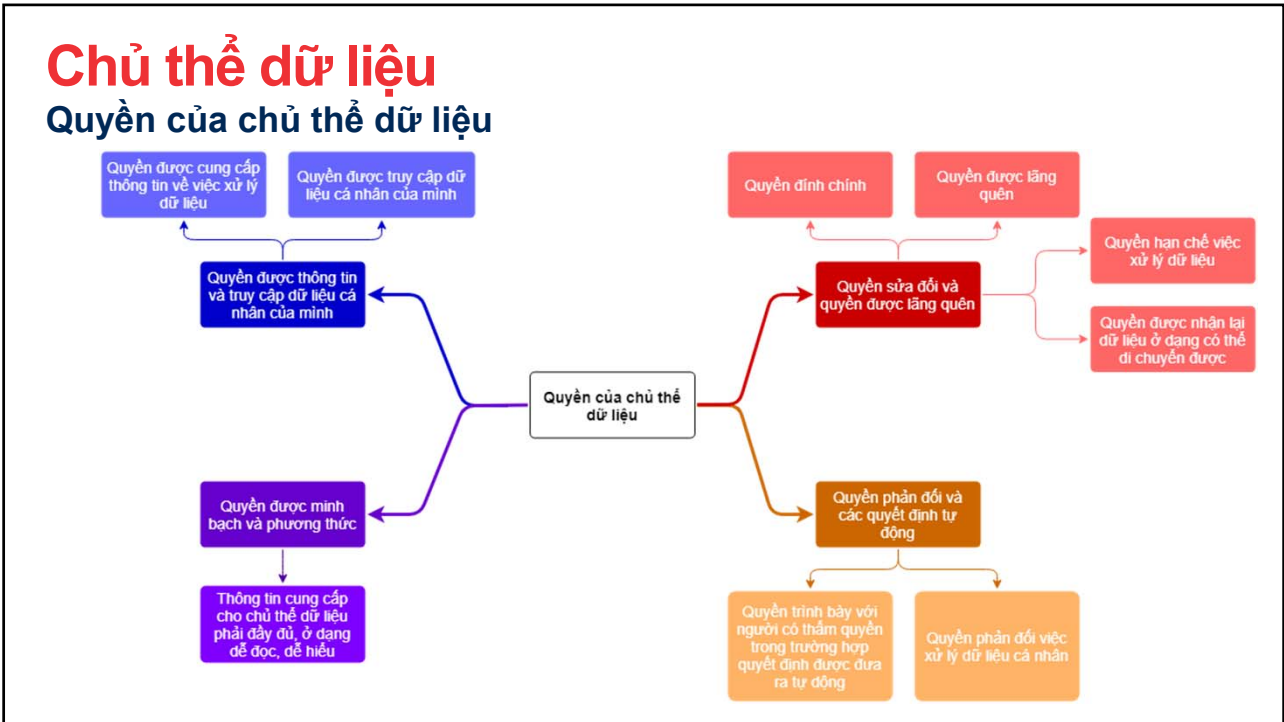
- “Dữ liệu cá nhân” là bất kỳ thông tin nào liên quan đến một người xác định hoặc có thể được xác định



Chủ thể dữ liệu (data subject)

Gắn liền với định nghĩa của “dữ liệu cá nhân”:

- “Dữ liệu cá nhân” là bất kỳ thông tin nào liên quan đến một người xác định hoặc có thể được xác định (“**Chủ thể dữ liệu**”)
- Một thể nhân có thể được xác định một cách trực tiếp hay gián tiếp, cụ thể thông qua một số đặc điểm nhận dạng như *tên, mã số định danh, dữ liệu vị trí, một định danh trực tuyến* hoặc một hay nhiều yếu tố liên quan đến *đặc điểm thể chất, sinh lý, gen di truyền, tâm thần, kinh tế, văn hóa hoặc xã hội* của thể nhân đó



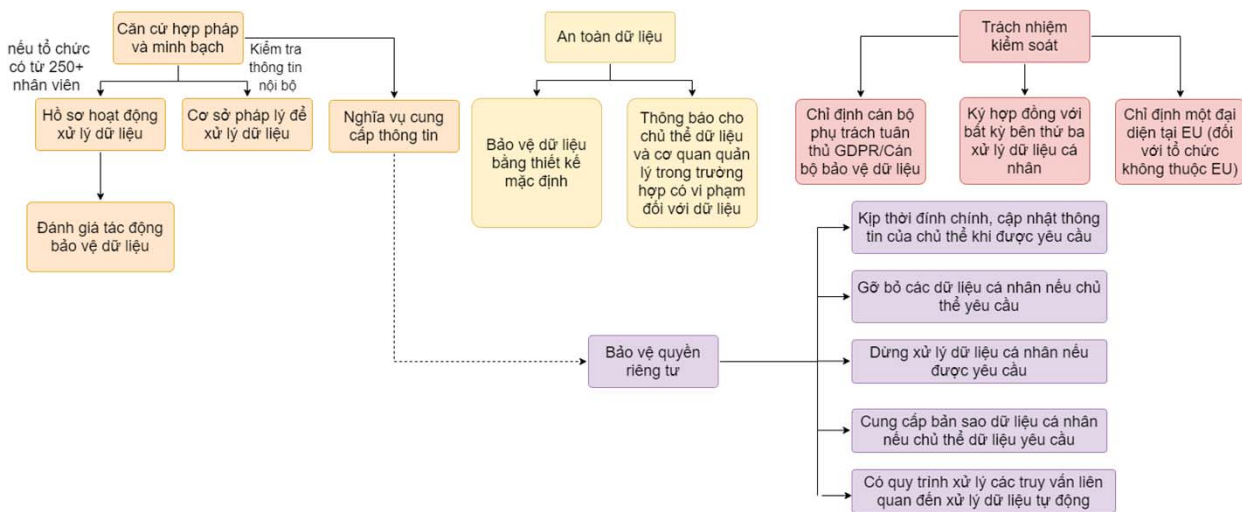
Bên kiểm soát (Data controller)



“Bên kiểm soát” là một pháp nhân hoặc thể nhân, một cơ quan công quyền, một mình hoặc cùng với các bên khác, quyết định mục đích và phương thức xử lý dữ liệu cá nhân

Bên kiểm soát

Nghĩa vụ của bên kiểm soát



Bên xử lý (Data processor)

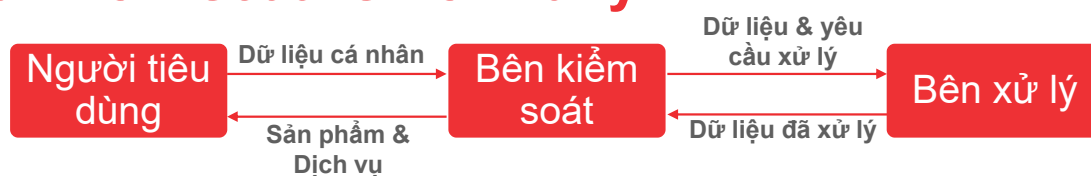


Một pháp nhân, thể nhân, hoặc cơ quan công quyền xử lý dữ liệu cá nhân thay mặt bên kiểm soát

“Xử lý” là bất kỳ hoạt động hoặc chuỗi hoạt động nào được thực hiện đối với dữ liệu cá nhân hoặc tập hợp dữ liệu cá nhân, bất kể bằng phương thức tự động hay không, ví dụ như:

- thu thập, ghi, sắp xếp, tổ chức, lưu trữ, hiệu chỉnh hoặc thay đổi, truy xuất, tham vấn, sử dụng,
- tiết lộ bằng đường truyền, phát tán, hoặc làm cho sẵn có bằng phương thức khác,
- xếp, kết hợp, hạn chế, hoặc hủy bỏ.

Bên kiểm soát vs Bên xử lý



Việc phân biệt giữa “Bên kiểm soát” và “Bên xử lý” là cần thiết vì:

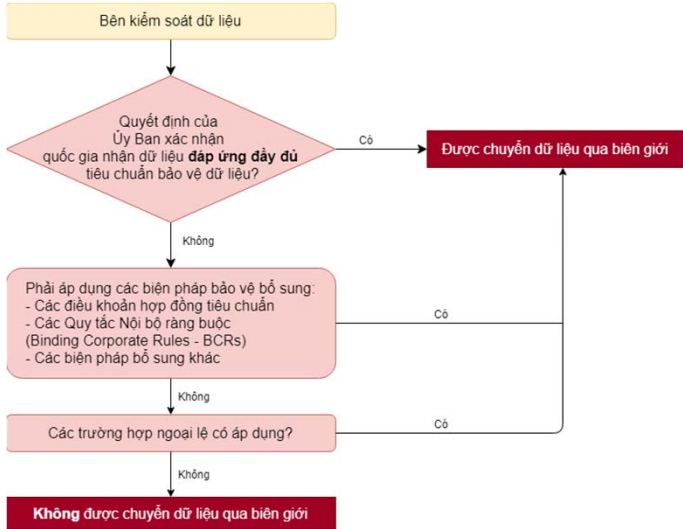
- Giúp nhà làm luật **xác định trách nhiệm phù hợp** của các bên liên quan tham gia vào hoạt động xử lý dữ liệu.
- Giúp **tạo điều kiện và khuyến khích sự phát triển** của các dịch vụ xử lý dữ liệu thuê ngoài.
- Thiếu đi sự phân biệt giữa hai chủ thể, **Bên xử lý không có khả năng thực hiện một số nghĩa vụ và trách nhiệm của Bên kiểm soát.**
- Các nghĩa vụ/trách nhiệm giống nhau tại có thể phải thực hiện hai lần.

2

Chuyển dữ liệu qua biên giới

Chuyển dữ liệu qua biên giới

Khi nào thì được phép chuyển dữ liệu qua biên giới



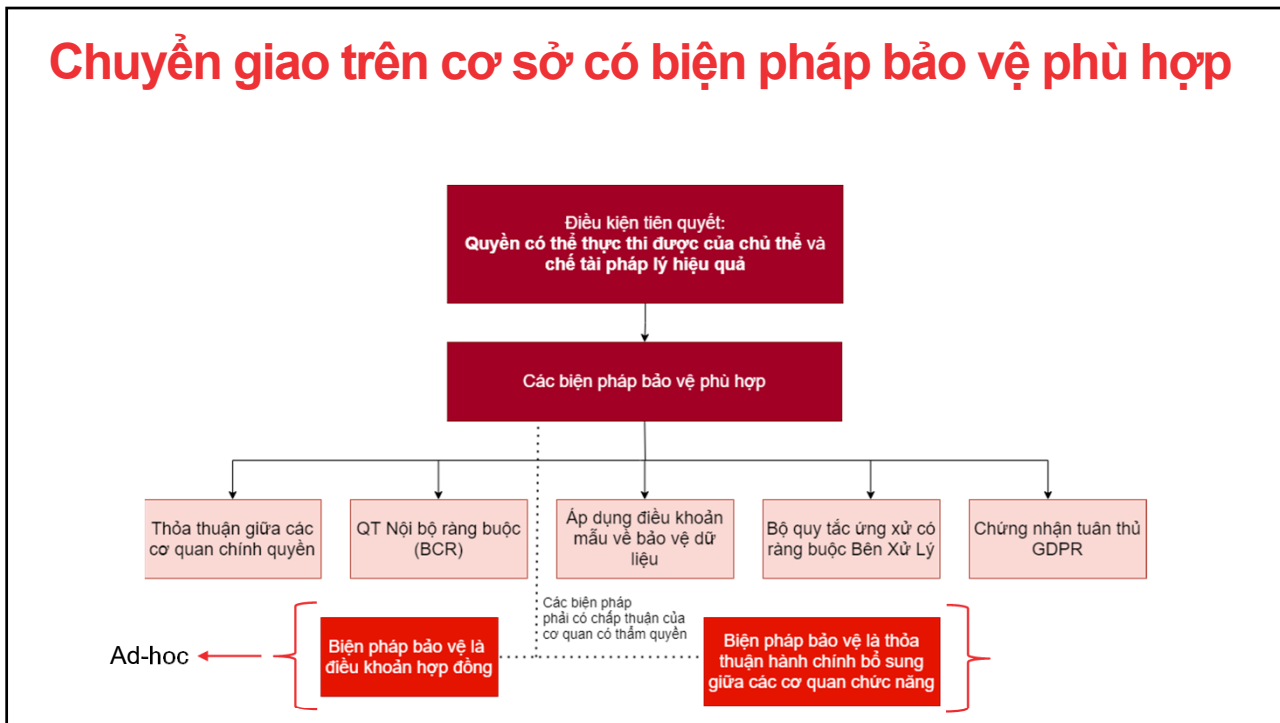
Chuyển giao trên cơ sở Quyết định về tính đầy đủ (Adequacy decision)

- Ủy ban Châu Âu (European Commission – **EC**) có quyền đưa ra Quyết định xác định một quốc gia hoặc tổ chức quốc tế thứ ba có đáp ứng đủ các yêu cầu về bảo vệ dữ liệu cá nhân hay không.
- Nếu sẵn có một quyết định như trên của EC đối với một quốc gia, việc chuyển dữ liệu tới quốc gia đó không cần phải xin phép.
- Quyết định này sẽ dựa trên ba tiêu chí chính:
 - **Quy định pháp luật:** quyền con người, pháp luật về an ninh quốc gia, luật hình sự, v.v.;
 - Sự tồn tại và tính hiệu quả của một **cơ quan độc lập** giám sát việc tuân thủ quy định về bảo vệ dữ liệu; và
 - Các **cam kết quốc tế** của quốc gia/tổ chức quốc tế đó.

Quyết định về tính đầy đủ (Adequacy decision)

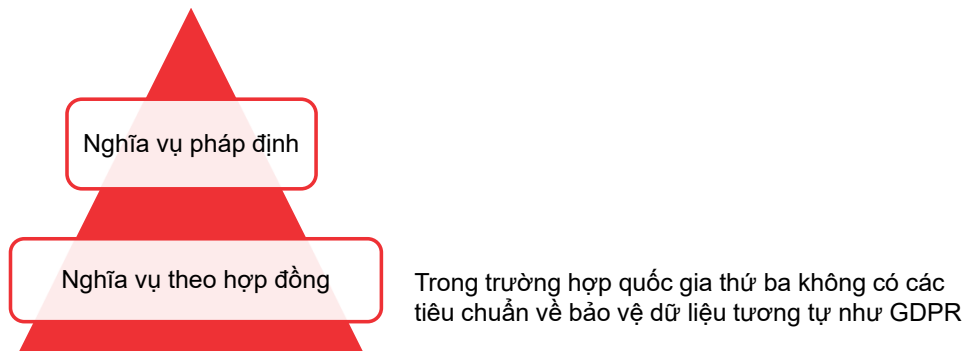
- EC hiện đã công nhận **13 quốc gia/vùng lãnh thổ** có mức độ bảo vệ dữ liệu tương đương GDPR, bao gồm:
 - Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Nhật Bản, Jersey, New Zealand, Thụy Sĩ, Uruguay và Vương quốc Anh (sau khi nước này rời khỏi EU).
 - **Nước Mỹ không được công nhận về tính đầy đủ.**
- EC đang trong quá trình xét duyệt công nhận Hàn Quốc (từ tháng 6 năm 2021)

Chuyển giao trên cơ sở có biện pháp bảo vệ phù hợp



Điều khoản mẫu

- EC cũng đã công bố điều khoản hợp đồng mẫu giữa Bên Kiểm Soát ở EU (là bên gửi dữ liệu) và bên thứ ba nằm ngoài EU (bên nhận dữ liệu) – Quyết định thi hành số 2021/914 ngày 04 tháng 6 năm 2021
- Các điều khoản hợp đồng mẫu này đảm bảo nếu quốc gia thứ ba không áp đặt (hoặc áp đặt không đủ chặt chẽ) các nghĩa vụ bảo vệ dữ liệu lên bên nhận dữ liệu, thì các nghĩa vụ này sẽ được quy định trong hợp đồng mẫu



Quy Tắc Nội Bộ Ràng Buộc (BCRs)

Phải được **chấp thuận của cơ quan giám sát**, với điều kiện:

- có **ràng buộc pháp lý** với mọi doanh nghiệp thành viên và nhân viên của tập đoàn
- thể hiện rõ ràng **quyền của chủ thể dữ liệu** đối với việc xử lý dữ liệu cá nhân
- thỏa mãn các yêu cầu về nội dung

Chủ thể dữ liệu có thể khởi kiện Bên Kiểm Soát/Bên Xử Lý nếu Bên Kiểm Soát/Bên Xử Lý vi phạm BCR.

→ BCR không chỉ có tính chất của một quy tắc nội bộ, mà còn **có tính chất của một hợp đồng**.

Nội dung chủ yếu của BCR:

- các chuyển giao dữ liệu, [...] tên của (các) quốc gia thứ ba nơi dữ liệu được chuyển đến.
- các quyền của chủ thể dữ liệu và phương thức thực thi quyền (quyền khiếu nại với cơ quan quản lý, quyền phản đối các quy trình tự động, quyền đòi bồi thường, ...)
- hiện diện thương mại của bên kiểm soát chịu trách nhiệm đối với vi phạm BCR của một thành viên khác nằm ở nước ngoài
- cách thức thông tin cho chủ thể dữ liệu
- quy trình khiếu nại
- cơ chế báo cáo với cơ quan giám sát liên quan đến các bảo đảm trong BCR

BCR

Ví dụ

Hiện tại một số công ty/tập đoàn quốc tế đã xây dựng BCR cho công ty/tập đoàn mình và được cơ quan quản lý có thẩm quyền chấp thuận, ví dụ như:

- Công ty sinh dược học UCB của Bỉ https://www.ucb.com/up/ucb_com_home/documents/UCB_BCRs_2021_v4.pdf
- Hãng tư vấn Accenture của Ireland <https://www.accenture.com/us-en/about/binding-corporate-rules>
- eBay <https://static.ebayinc.com/assets/Uploads/PrivacyCenter/ebay-corporate-rules-english.pdf>, theo đó eBay Luxembourg sẽ chịu trách nhiệm chính về đảm bảo tuân thủ GDPR của toàn tập đoàn
- Ngân hàng đầu tư JPMorgan Chase https://www.jpmorgan.com/content/dam/jpm/global/documents/us-privacy-policies/Global_Privacy_Code_Binding_Corporate_Rules.pdf, theo đó JP Morgan Chase Bank, N.A. London Branch sẽ chịu trách nhiệm chính về tuân thủ GDPR

Bộ quy tắc ứng xử

GDPR, Điều 40

Các bộ quy tắc ứng xử do các hiệp hội/tổ chức ban hành cần có các nội dung:

- Xử lý minh bạch
- Lợi ích chính đáng mà Bên Kiểm Soát mưu cầu trong các hoàn cảnh cụ thể
- Thu thập dữ liệu
- Khử nhận dạng dữ liệu cá nhân (Pseudonymisation)
- Thông tin công bố công khai hoặc được cung cấp cho các chủ thể dữ liệu
- Việc thực thi quyền của các chủ thể dữ liệu
- Thông tin cung cấp cho (cũng như để) bảo vệ trẻ em
- Quy định về trách nhiệm của bên kiểm soát/bên xử lý liên quan đến áp dụng các biện pháp bảo vệ
- Quy định về thông báo cho cơ quan giám sát có thẩm quyền trong trường hợp xảy ra xâm phạm dữ liệu
- Quy định về chuyển dữ liệu tới các quốc gia hoặc tổ chức quốc tế là bên thứ ba
- Các quy trình ngoài tòa án và thủ tục giải quyết tranh chấp giữa bên kiểm soát và chủ thể dữ liệu liên quan đến việc xử lý dữ liệu. Các quy trình này không được làm phương hại đến quyền khiếu nại/khiếu kiện của chủ thể dữ liệu.

Các trường hợp ngoại lệ và ví dụ

Trường hợp và ví dụ

CHỦ THỂ DỮ LIỆU ĐỒNG Ý RÕ RÀNG

Bên kiểm soát thông báo rõ ràng cho chủ thể rằng quốc gia nơi dữ liệu được chuyển đến không có tiêu chuẩn cao như GDPR nhưng chủ thể vẫn đồng ý và chấp nhận.

HỢP ĐỒNG GIỮA BÊN KIỂM SOÁT VÀ CHỦ THỂ

Công ty đại lý đặt vé máy bay (Bên Kiểm Soát, có trụ sở tại EU) đặt vé hộ cho khách hàng (Chủ thể) trên chuyến bay của một hãng hàng không Singapore. Việc công ty đại lý về chuyển dữ liệu của khách hàng cho hãng hàng không thuộc trường hợp này.

HỢP ĐỒNG VÌ LỢI ÍCH CỦA CHỦ THỂ DỮ LIỆU

Một công ty Pháp tài trợ học bổng du học cho 01 nhân viên để du học tại Việt Nam, chuyển dữ liệu của nhân viên đó cho ngân hàng ở Việt Nam để ủy thác chi trả tiền học bổng cho nhân viên đó.

LỢI ÍCH CÔNG CỘNG

Chuyển dữ liệu giữa các cơ quan thuế, cơ quan cạnh tranh, cơ quan giám sát tài chính; giữa các dịch vụ an sinh xã hội, y tế công cộng. Ví dụ: hoạt động truy vết các bệnh truyền nhiễm; hoạt động nhằm loại bỏ doping trong thể thao...

Trường hợp và ví dụ

BẢO VỆ QUYỀN HỢP PHÁP

Công ty X là một công ty đa quốc gia, bị kiện ở Mỹ vì phân biệt đối xử phụ nữ. Công ty X sử dụng dữ liệu về các nữ quản lý của mình trên toàn cầu (bao gồm dữ liệu gửi từ châu Âu) để chứng minh mình không phân biệt đối xử.

LỢI ÍCH QUAN TRỌNG CỦA CHỦ THỂ DỮ LIỆU

Tổ chức bảo vệ quyền phụ nữ trụ sở tại Bỉ thu thập được một danh sách các đối tượng chịu ảnh hưởng bởi cuộc chiến ở Afghanistan. Tổ chức này gửi các thông tin nói trên tới nhà tài trợ có trụ sở tại Úc để chuẩn bị công tác cứu trợ nhân đạo. (Việc có được đồng thuận trong trường hợp này là không thực tế).

CHUYỂN GIAO DỮ LIỆU CÓ TẠI HỒ SƠ/DANH SÁCH ĐƯỢC QUY ĐỊNH THEO LUẬT

Danh sách các luật sư thuộc đoàn luật sư Paris.

NGOẠI LỆ ĐẶC BIỆT

Các trường hợp chuyển giao dữ liệu thỏa mãn 8 điều kiện luật định

5

Một số ví dụ thực tiễn

CASE STUDY

Quyết định về tính đầy đủ (Adequacy Decision)

Án lệ Schrems I (2015) của CJEU – Tình tiết

- Tại thời điểm 2015, EC công nhận Mỹ là nước đáp ứng đầy đủ yêu cầu về bảo vệ dữ liệu cá nhân tương đương với EU. (**Safe Harbour**)
- Trong scandal liên quan đến NSA, cựu nhân viên tình báo Edward Snowden tiết lộ rằng NSA thực hiện giám sát và theo dõi người dân ở quy mô lớn
- Điều này làm dấy lên sự phản đối của công chúng và thu hút nhiều tranh luận liên quan đến cân bằng **lợi ích công cộng** (theo dõi và ngăn ngừa khủng bố) với **lợi ích cá nhân** (quyền riêng tư)

Quyết định về tính đầy đủ (Adequacy Decision)

Án lệ Schrems I (2015) của CJEU – Tình tiết

- Max Schrems, công dân Áo, lúc đó là một sinh viên, căn cứ vào các công bố của Snowden, cáo buộc rằng tiêu chuẩn về bảo vệ dữ liệu ở Mỹ là không đầy đủ. Dữ liệu của công dân EU, sau khi được chuyển sang Mỹ, sẽ có thể bị truy cập bởi NSA mà không phải chịu kiểm soát đáng kể nào (thấp hơn GDPR).
- Schrems yêu cầu Ủy viên Bảo vệ Dữ liệu Ireland (DPC, Ireland là nơi Facebook đặt trụ sở ở Châu Âu) điều tra tính hợp lệ của Safe Harbour.
- DPC căn cứ vào một adequacy decision của EC, cho rằng mình không có thẩm quyền và cũng không cần phải xét lại quyết định của EC.
- Tòa án Ireland yêu cầu CJEU trả lời 2 câu hỏi pháp lý:
 - Liệu DPC có hoàn toàn bị ràng buộc và phải tuân theo (absolutely bound by) adequacy decision của EC, trong trường hợp quốc gia thứ ba (nước Mỹ) không đáp ứng đầy đủ tiêu chuẩn về bảo vệ dữ liệu? (hoặc)
 - DPA (i.e. **DPC**) có nghĩa vụ phải điều tra độc lập về vấn đề được khiếu nại hay không?

Quyết định về tính đầy đủ (Adequacy Decision)

Án lệ Schrems I (2015) của CJEU – Phán quyết

- CJEU cho rằng: cơ quan chức năng của các nước thành viên, trường hợp này là DPC, có đủ thẩm quyền để điều tra độc lập về tính “adequacy” trong bảo vệ dữ liệu của quốc gia thứ ba.
- Tuy nhiên, thẩm quyền tuyên bố một adequacy decision là vô hiệu chỉ thuộc về duy nhất CJEU.
- Đối với người khiếu nại (Schrems), DPC có nghĩa vụ đảm bảo quyền khiếu nại của người này.
- Trong trường hợp này, tòa tuyên Safe Harbour là vô hiệu do vượt quá thẩm quyền (điều 3 của Safe Harbour rút ngắn trái luật quy trình xét duyệt tính đầy đủ)

→ Hệ quả: EC và chính quyền Obama phải thương thảo một thỏa thuận thay thế, với tên gọi mới là **Privacy Shield**.



Adequacy decision/Thỏa thuận giữa các nước

Schrems II (2018) CJEU – Tình tiết

- Schrems I được đưa ra trước khi GDPR được áp dụng.
- Schrems II đề cập trực tiếp đến GDPR.
- Phán quyết của Tòa đề cập đến một số vấn đề chính:
 - Privacy Shield cũng bị tuyên vô hiệu, do luật pháp Mỹ không bảo vệ đầy đủ dữ liệu cá nhân.
 - Việc áp dụng các SCCs là điều kiện cần, song không phải là điều kiện đủ để thực hiện chuyển dữ liệu ra ngoài EU.

Một số nhận xét về quy định của EU

Sau phán quyết Schrems I

- Do Tòa án tuyên Safe Harbour vô hiệu, các công ty thực hiện chuyển dữ liệu từ EU sang Mỹ căn cứ vào Safe Harbour bỗng nhiên bị coi là chuyển dữ liệu trái pháp luật
- EC vì vậy phải thỏa thuận với các công ty nói trên, cho phép 03 tháng **thời gian ân hạn** (grace period), theo đó EC sẽ không truy cứu hay xử phạt, và các công ty phải sử dụng khoảng thời gian này để thực hiện các chính sách tuân thủ bổ sung
- EC cũng phải thực hiện đàm phán một thỏa thuận mới với chính quyền Mỹ, trở thành **Privacy Shield** sau này

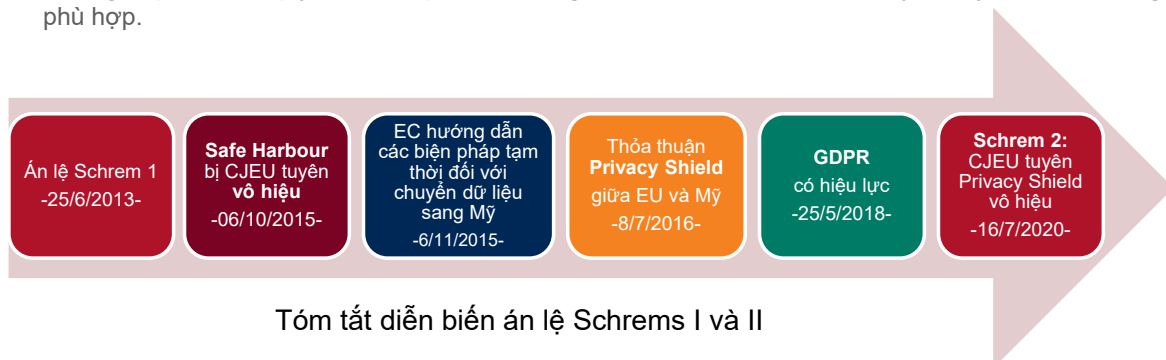
Một số nhận xét

Phán quyết Schrems II

- CJEU không nói rõ nếu áp dụng SCCs như điều kiện cần để chuyển dữ liệu qua biên giới, (các) điều kiện đủ (nếu có) là gì.
 - Berlin, Đức: Chuyển dữ liệu từ Berlin tới Mỹ bị **cấm**
 - Pháp, Đan Mạch: Nhà chức trách diễn giải phán quyết của CJEU theo hướng **công nhận** SCC, tuy vậy vẫn đang soạn thảo các hướng dẫn liên quan đến các biện pháp bổ sung **đi kèm** với SCC
- Như vậy mỗi quốc gia lại có một cách hiểu khác nhau về cách diễn giải phán quyết Schrems II
- Điểm bất hợp lý: Bên Kiểm Soát đặt tại Berlin có thể lách quy định nói trên bằng cách chuyển dữ liệu sang Đan Mạch (không bị hạn chế), sau đó chuyển sang Mỹ (phải áp dụng SCCs và một số biện pháp bảo vệ)

Một số nhận xét về quy định của EU

- GDPR trao quyền cho cơ quan quản lý (EC và cơ quan chuyên trách của EC là EDPB). Cơ chế kiểm soát này tuy có điểm mạnh là bảo vệ chặt chẽ quyền lợi của chủ thể dữ liệu, song lại có thể tạo ra các vùng xám, khiến cho việc tuân thủ khó khăn hơn.
- GDPR hay các quy định dưới luật được ban hành căn cứ GDPR luôn phải phù hợp với thực tế. Trong trường hợp EU, các quy định luôn phải chịu sự giám sát của CJEU và sẽ bị tuyên hủy nếu như không phù hợp.



4

Một số khuyến nghị cho Việt Nam

Một số khuyến nghị cho Việt Nam

*Về cơ chế chuyển dữ liệu xuyên biên giới

- ❖ Nếu Nhà nước đã ban hành quyết định xác định một quốc gia có đầy đủ cơ chế để bảo vệ dữ liệu cá nhân, bên xử lý có thể chuyển dữ liệu tới quốc gia đó mà không cần sự chấp thuận cụ thể của cơ quan nhà nước.
- ❖ Nếu bên xử lý đã có các biện pháp bảo vệ theo thỏa thuận/hợp đồng **hoặc/và** đã cam kết, có đánh giá rủi ro đầy đủ thì họ cũng không cần xin chấp thuận cụ thể của cơ quan có thẩm quyền. (sự đồng ý của chủ thể dữ liệu; bên gửi và nhận dữ liệu cá nhân chịu ràng buộc về nghĩa vụ pháp lý đối với sự an toàn của dữ liệu cá nhân...)

Một số khuyến nghị cho Việt Nam

*Về cơ chế chuyển dữ liệu xuyên biên giới

*Ngoại lệ: ?

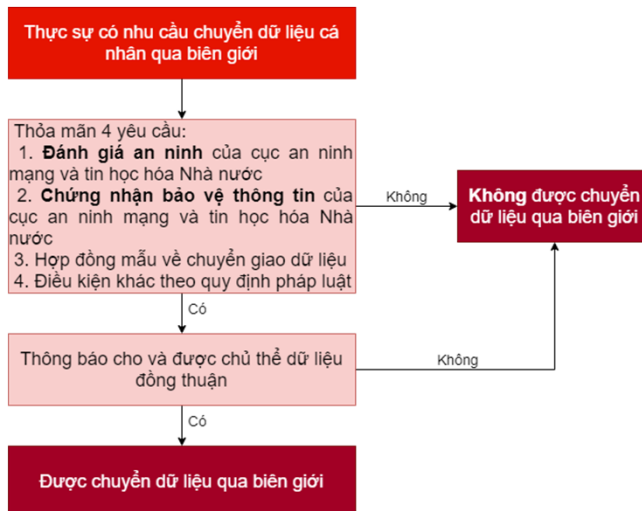
Việc chuyển giao được chứng minh là:

- Cần thiết cho việc thực hiện hợp đồng;
- Cần thiết cho việc ký kết hợp đồng;
- Thực hiện hợp đồng được ký kết vì lợi ích của chủ thể dữ liệu;
- Cần thiết cho mục đích theo đuổi các lợi ích hợp pháp bắt buộc của bên xử lý dữ liệu cá nhân

Một số khuyến nghị cho Việt Nam

Kinh nghiệm từ Trung Quốc

- Ngày 20 tháng 8 năm 2021, Đại hội Đại biểu Nhân dân (Quốc hội) Trung Quốc ban hành Luật Bảo vệ thông tin cá nhân
- Chuyển dữ liệu qua biên giới được đề cập trong Chương III
- Các yêu cầu theo luật này tương đối nặng nề và khó khăn để các công ty tuân thủ
- Việt Nam có thể tham khảo nhưng phải trên cơ sở có chọn lọc các quy định hợp lý.



Quy định về chuyển dữ liệu qua biên giới theo Điều 38, Luật Bảo vệ thông tin cá nhân 2021 của Trung Quốc



Baker McKenzie.

This presentation has been prepared for clients and professional associates of Baker & McKenzie. Whilst every effort has been made to ensure accuracy, this presentation is not an exhaustive treatment of the area of law discussed and no responsibility for any loss occasioned to any person acting or refraining from action as a result of material in this presentation is accepted by Baker & McKenzie.

Baker & McKenzie (Vietnam) Ltd., a limited liability company, is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2021 Baker & McKenzie (Vietnam) Ltd.
bakermckenzie.com

BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG BỐI CẢNH CÁCH MẠNG CÔNG NGHIỆP LẦN THỨ TƯ – KINH NGHIỆM QUỐC TẾ VÀ ĐỀ XUẤT, KIẾN NGHỊ ĐỐI VỚI VIỆT NAM

(Trần Mạnh Hùng/Nguyễn Tuấn Linh, Công ty luật quốc tế Baker McKenzie Việt Nam/ BMVN)

I – MỘT SỐ KHÁI NIỆM VÀ CÁC CHỦ THỂ LIÊN QUAN ĐẾN BẢO VỆ DỮ LIỆU CÁ NHÂN

1. Các nguyên tắc cơ bản về bảo vệ dữ liệu cá nhân

Quy định chung về bảo vệ dữ liệu được ban hành bởi Nghị viện Châu Âu vào ngày 27 tháng 4 năm 2016 (“**GDPR**”) đã đặt ra cơ sở pháp lý khá toàn diện cho vấn đề bảo vệ dữ liệu của mọi công dân thuộc Liên minh Châu Âu (“**EU**”). Theo đó, Điều 5 GDPR đã đặt ra sáu nguyên tắc cơ bản liên quan tới việc xử lý thông tin cá nhân:

Thứ nhất, việc xử lý phải hợp pháp, công bằng, và minh bạch. Theo Điều 6, việc xử lý dữ liệu chỉ được coi là hợp pháp nếu thuộc ít nhất một trong các trường hợp sau đây:

- Chủ thể dữ liệu đã đồng thuận với việc xử lý dữ liệu cá nhân của mình;
- Việc xử lý là cần thiết cho việc thực hiện hợp đồng trong đó chủ thể dữ liệu là một bên giao kết, hoặc việc xử lý là để tiến hành các bước tiền hợp đồng dựa trên yêu cầu của chủ thể dữ liệu;
- Việc xử lý là cần thiết để bảo vệ lợi ích thiết yếu của chủ thể dữ liệu hoặc thể nhân khác;
- Việc xử lý là cần thiết để thực hiện công việc vì lợi ích công cộng hoặc để thực hiện thẩm quyền của cơ quan công quyền;

- Việc xử lý là cần thiết đối với những mưu cầu lợi ích chính đáng của bên kiểm soát hoặc bên thứ ba, trừ trường hợp ảnh hưởng lớn đến quyền cơ bản của chủ thể dữ liệu hoặc chủ thể dữ liệu là trẻ em.

Thứ hai, việc xử lý phải có mục đích rõ ràng, cụ thể, chính đáng, và chỉ được diễn ra trong phạm vi thực hiện mục đích ban đầu. Việc tiếp tục tiến hành xử lý thông tin nhằm mục đích lưu trữ, dựa trên cơ sở lợi ích công cộng, mục tiêu nghiên cứu khoa học, lịch sử, hay dữ liệu sẽ không được coi là trái với mục đích xử lý thông tin ban đầu.

Thứ ba, dữ liệu cá nhân được xử lý chỉ được vừa đủ, liên quan, và giới hạn ở chừng mực đủ để thực hiện mục đích xử lý ban đầu.

Thứ tư, dữ liệu cá nhân được xử lý phải chính xác và cập nhật (nếu cần thiết). Mọi nỗ lực hợp lý cần phải được tiến hành nhằm đảm bảo dữ liệu sai sót được xóa bỏ hoặc sửa đổi kịp thời.

Thứ năm, hình thức lưu trữ cho phép việc định danh chủ thể dữ liệu không lâu hơn thời gian cần thiết cho mục đích xử lý, trừ trường hợp vì lợi ích công cộng hoặc để thực hiện mục đích nghiên cứu khoa học hay lịch sử.

Thứ sáu, phương thức lưu trữ cần đảm bảo an ninh dữ liệu cá nhân, bao gồm việc bảo vệ khỏi sự truy cập trái phép/bất hợp pháp hoặc mất mát, hủy hoại, hư hỏng do vô ý, sử dụng các biện pháp mang tính kỹ thuật và có tổ chức.

2. Một số khái niệm chính

2.1. Dữ liệu cá nhân

Dữ liệu cá nhân được định nghĩa là bất kỳ thông tin nào liên quan đến một người xác định hoặc có thể được xác định.

2.2. Chủ thể dữ liệu

Chủ thể dữ liệu là một thể nhân có thể được xác định một cách trực tiếp hay gián tiếp thông qua một số đặc điểm nhận dạng như tên, mã số định danh, dữ liệu vị trí, một định danh trực tiếp hoặc một hay nhiều yếu tố liên quan đến đặc điểm

thể chất, sinh lý, gen di truyền, tâm thần, kinh tế, văn hóa, hoặc xã hội của thể nhân đó.

Chương III GDPR quy định bốn nhóm quyền năng của chủ thể dữ liệu. Theo đó, chủ thể dữ liệu sẽ có:

- Quyền được minh bạch và phương thức: Thông tin cung cấp cho chủ thể dữ liệu phải đầy đủ, minh bạch, dễ đọc, và dễ hiểu;
- Quyền được thông tin và truy cập dữ liệu cá nhân của mình: Bên kiểm soát phải cung cấp cho chủ thể dữ liệu các thông tin về bên kiểm soát và thông tin liên lạc, mục đích xử lý dữ liệu và cơ sở pháp lý, bên nhận dữ liệu (nếu có), ý định của bên kiểm soát muốn chuyển dữ liệu sang một nước hay tổ chức thứ ba...
- Quyền sửa đổi và quyền được lãng quên: Chủ thể dữ liệu có quyền được bên kiểm soát đính chính dữ liệu các nhân liên quan đến mình và không được trì hoãn vô lý. Bên cạnh đó, chủ thể dữ liệu cũng có quyền được yêu cầu bên kiểm soát xóa dữ liệu cá nhân của mình và không được trì hoãn vô lý trong các trường hợp như khi dữ liệu cá nhân không còn cần thiết (xét trên mục đích xử lý ban đầu), hay khi chủ thể dữ liệu rút lại sự đồng thuận ban đầu (nếu căn cứ xử lý ban đầu dựa trên sự đồng thuận) mà bên kiểm soát không còn căn cứ nào khác...
- Quyền phản đối và các quyết định tự động: Tại mọi thời điểm, chủ thể dữ liệu, căn cứ vào trường hợp cá nhân của mình, có quyền phản đối việc xử lý dữ liệu cá nhân của mình nếu căn cứ xử lý là lợi ích công cộng hoặc dựa trên mưu cầu lợi ích chính đáng của bên xử lý. Ngoài ra, chủ thể dữ liệu cũng không bị ràng buộc bởi quyết định có hiệu lực pháp lý đối với họ mà được dựa trên quá trình xử lý hoàn toàn tự động.

2.3. Bên kiểm soát dữ liệu

Bên kiểm soát dữ liệu được hiểu là một pháp nhân, thể nhân, hoặc cơ quan công quyền, một mình hoặc cùng với các bên khác quyết định mục đích và phương thức

xử lý dữ liệu cá nhân. Dựa trên bản chất, phạm vi, bối cảnh, và mục đích của việc xử lý cũng như mọi rủi ro có thể xảy đến tới các quyền của một thể nhân, bên kiểm soát dữ liệu có nghĩa vụ đưa ra các biện pháp phù hợp để đảm bảo dữ liệu được xử lý đúng với quy định của GDPR.

2.4. Bên xử lý dữ liệu

Bên xử lý dữ liệu được định nghĩa là một pháp nhân, thể nhân, hoặc cơ quan công quyền xử lý dữ liệu cá nhân thay mặt bên kiểm soát. Theo đó, “xử lý” được hiểu là bất kỳ hoạt động hoặc chuỗi hoạt động nào được thực hiện đối với dữ liệu cá nhân hoặc tập hợp dữ liệu cá nhân, bất kể bằng phương thức tự động hay không, ví dụ như: thu thập, ghi, sắp xếp, tổ chức, lưu trữ, hiệu chỉnh hoặc thay đổi, truy xuất, tham vấn, sử dụng; tiết lộ bằng đường truyền, phát tán, hoặc làm cho sẵn có bằng phương thức khác; xếp, kết hợp, hạn chế, hoặc hủy bỏ.

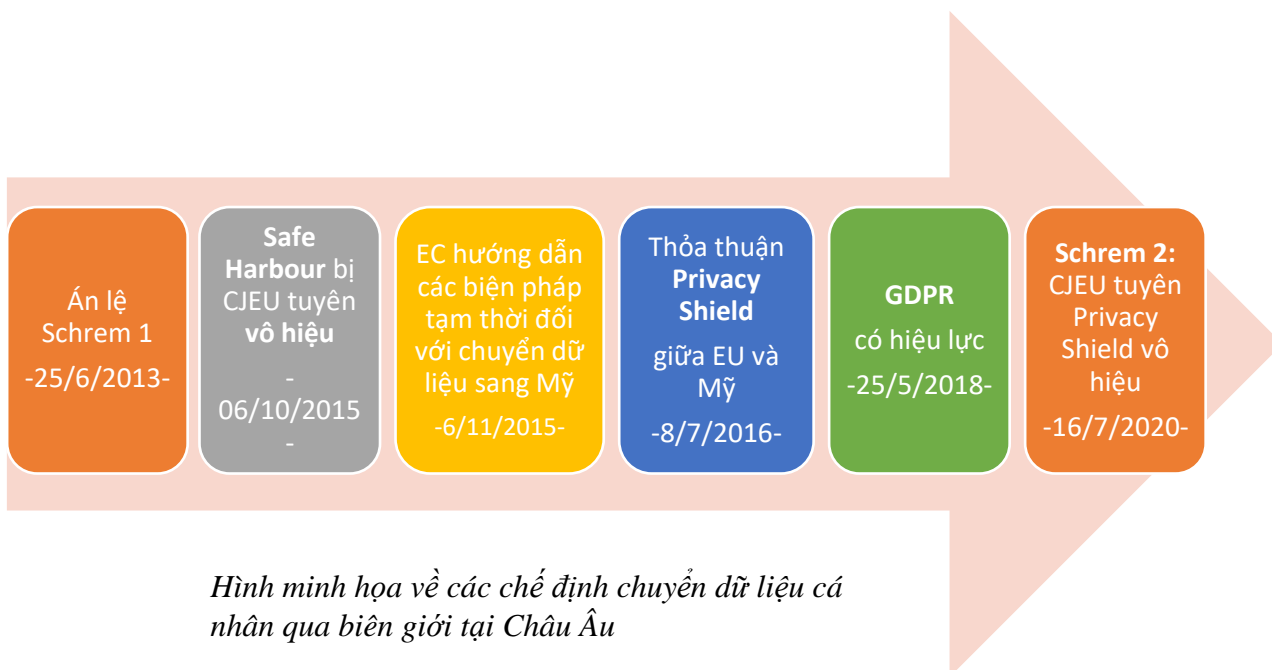
Việc phân biệt giữa “Bên kiểm soát” và “Bên xử lý” về bản chất cũng như khả năng thực hiện một số quyền và nghĩa vụ của mỗi bên là cần thiết nhằm giúp nhà làm luật xác định trách nhiệm phù hợp của các bên liên quan tham gia vào hoạt động xử lý dữ liệu, đồng thời tạo điều kiện và khuyến khích sự phát triển của các dịch vụ xử lý dữ liệu thuê ngoài.

II – CHUYỂN DỮ LIỆU QUA BIÊN GIỚI

Dựa vào tầm quan trọng của khách thể chịu tác động bởi việc chuyển dữ liệu qua biên giới, GDPR quy định một bài kiểm tra ba lớp cần được vượt qua trước khi bên kiểm soát dữ liệu được phép tiến hành việc chuyển dữ liệu này. Theo đó, lớp kiểm tra thứ nhất yêu cầu một quyết định của Ủy ban Châu Âu (“EC”) trong việc xác nhận xem quốc gia nhận dữ liệu có đáp ứng đầy đủ các tiêu chuẩn về bảo vệ dữ liệu hay không. Đáp ứng được điều kiện này, việc chuyển dữ liệu qua biên giới có thể được tiến hành. Trong trường hợp không có xác nhận của EC, lớp kiểm tra thứ hai sẽ được áp dụng. Theo đó, nếu bên kiểm soát dữ liệu có áp dụng các biện pháp bảo vệ bổ sung như sử dụng các điều khoản hợp đồng tiêu chuẩn (“SCCs”), các quy tắc nội bộ ràng buộc (“BCRs”), hay các biện pháp khác, thì sẽ được chuyển dữ liệu qua biên

giới. Nếu điều kiện này vẫn không được thỏa mãn, thì việc chuyển dữ liệu này có được tiến hành hay không sẽ phải phụ thuộc vào việc đây có thuộc vào một trong các trường hợp ngoại lệ cho phép việc chuyển dữ liệu qua biên giới hay không - lớp kiểm tra cuối cùng. Một số ví dụ về trường hợp ngoại lệ có thể kể đến như khi chủ thể dữ liệu đã đồng ý rõ ràng; tồn tại hợp đồng giữa bên kiểm soát và chủ thể dữ liệu hoặc hợp đồng vì lợi ích của chủ thể dữ liệu; chuyển dữ liệu vì lợi ích công cộng, lợi ích quan trọng của chủ thể dữ liệu, hay lợi ích hợp pháp của cá nhân...

III – MỘT SỐ VÍ DỤ THỰC TIỄN VỀ VIỆC CHUYỂN DỮ LIỆU QUA BIÊN GIỚI (CASE STUDY)



Như đã nêu ở phần II, quyết định về tính đầy đủ của EC là điều kiện xuất hiện ở lớp kiểm tra thứ nhất cho việc chuyển dữ liệu qua biên giới. EC hiện đã công nhận 13 quốc gia và vùng lãnh thổ có mức độ bảo vệ dữ liệu tương đương GDPR, bao gồm: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Nhật Bản, Jersey, New Zealand, Thụy Sĩ, Uruguay, và Vương quốc Anh (sau khi nước này rời khỏi EU). Hoa Kỳ là một trường hợp đặc biệt. Tại thời điểm năm 2015, EC từng công nhận Hoa Kỳ là một quốc gia đáp ứng đầy đủ yêu cầu

về bảo vệ dữ liệu cá nhân tương đương với EU (“**Safe Harbour**”). Trong vụ bê bối liên quan đến Cơ quan An ninh Quốc gia Hoa Kỳ (“**NSA**”), cựu nhân viên tình báo Edward Snowden tiết lộ rằng NSA đã và đang thực hiện việc giám sát và theo dõi người dân ở quy mô lớn. Điều này làm dấy lên sự phản đối của công chúng và thu hút nhiều tranh luận liên quan đến việc cân bằng lợi ích công cộng (theo dõi và ngăn ngừa khủng bố) với lợi ích cá nhân (quyền riêng tư). Max Schrems, công dân Áo, lúc đó là một sinh viên, dựa trên các công bố của Snowden, đã cáo buộc rằng tiêu chuẩn về bảo vệ dữ liệu ở Hoa Kỳ là không đầy đủ. Cụ thể, dữ liệu của công dân EU, sau khi được chuyển sang quốc gia này, sẽ có thể bị truy cập bởi NSA mà không phải chịu kiểm soát đáng kể nào. Schrems sau đó đã yêu cầu Ủy viên Bảo vệ Dữ liệu Ireland (“**DPC**”) điều tra tính hợp lệ của Safe Harbour. Tuy nhiên, căn cứ vào một quyết định về tính đầy đủ của EC, DPC đã cho rằng mình không có thẩm quyền cũng như không cần phải xét lại quyết định được đưa ra bởi EC. Tòa án Công lý Châu Âu (“**CJEU**”), dựa trên yêu cầu của Tòa án Ireland, phán quyết rằng DPC có đủ thẩm quyền để điều tra độc lập về tính đầy đủ trong bảo vệ dữ liệu của quốc gia thứ ba cũng như có nghĩa vụ đảm bảo quyền khiếu nại của Schrems. Tuy nhiên, cũng theo CJEU, thẩm quyền tuyên bố một quyết định về tính đầy đủ là vô hiệu chỉ thuộc về duy nhất CJEU và trong trường hợp này, tòa đã tuyên Safe Harbour là vô hiệu do vượt quá thẩm quyền (điều 3 của Safe Harbour rút ngắn trái luật quy trình xét duyệt tính đầy đủ). Điều này đã khiến cho EC và chính quyền Tổng thống Obama lúc bấy giờ phải thương thảo một thỏa thuận thay thế với tên gọi mới là Privacy Shield. Tuy vậy, trong phán quyết của CJEU vào tháng 7 năm 2020 (“**phán quyết Schrems II**”), Privacy Shield bị tuyên vô hiệu do luật pháp Hoa Kỳ không bảo vệ dữ liệu cá nhân một cách đầy đủ và việc áp dụng SCCs là điều kiện cần, song không phải là điều kiện đủ để thực hiện chuyển dữ liệu ra ngoài EU. Do không quy định rõ điều kiện đủ trong trường hợp áp dụng SCCs, phán quyết Schrems II dường như đang được các quốc gia thành viên EU tiếp cận với các cách hiểu khác nhau, từ đó tạo ra một vùng xám của pháp luật.

IV – MỘT SỐ KHUYẾN NGHỊ CHO VIỆT NAM

Việt Nam nên tham khảo cách tiếp cận của GDPR, cụ thể là tạo ra nhiều cơ chế cho doanh nghiệp tuân thủ. Theo đó, nếu Nhà nước đã ban hành quyết định xác định một quốc gia có đầy đủ cơ chế để bảo vệ dữ liệu cá nhân, bên xử lý có thể chuyển dữ liệu tới quốc gia đó mà không cần sự chấp thuận cụ thể của cơ quan nhà nước.

Mặt khác, nếu bên xử lý đã có các biện pháp bảo vệ theo thỏa thuận/hợp đồng, họ cũng không cần xin chấp thuận cụ thể của cơ quan có thẩm quyền. Cụ thể, việc chuyển dữ liệu xuyên biên giới nên được cho phép nếu:

- Có sự đồng ý của chủ thể dữ liệu về việc chuyển dữ liệu này; hoặc
- Tổ chức chuyển dữ liệu đã áp dụng các bước cần thiết để đảm bảo rằng bên nhận dữ liệu cá nhân chịu ràng buộc về nghĩa vụ pháp lý khả thi trong việc cung cấp một sự bảo vệ đối với dữ liệu cá nhân ở mức độ bằng hoặc hơn so với sự bảo vệ được quy định trong Dự Thảo.

Trong trường hợp cả hai điều kiện trên đều không được thỏa mãn, Dự Thảo nên cho phép bên xử lý dữ liệu cá nhân chuyển dữ liệu qua biên giới khi thuộc một trong các trường hợp sau:

- Việc chuyển dữ liệu này là cần thiết cho việc thực hiện hợp đồng giữa chủ thể dữ liệu và bên xử lý dữ liệu hoặc cho việc thực hiện các biện pháp tiền hợp đồng trước sự yêu cầu của chủ thể dữ liệu;
- Việc chuyển dữ liệu này là cần thiết cho việc ký kết hợp đồng hoặc thực hiện hợp đồng được ký kết vì lợi ích của chủ thể dữ liệu giữa bên xử lý dữ liệu cá nhân và một thể nhân hoặc pháp nhân khác; hoặc
- Việc chuyển dữ liệu là cần thiết cho mục đích theo đuổi các lợi ích hợp pháp bắt buộc của bên xử lý dữ liệu cá nhân mà chủ thể dữ liệu cho là hợp lý.

***Kinh nghiệm từ Trung Quốc**

Gần đây nhất, ngày 20 tháng 8 năm 2021, Đại hội Đại biểu Nhân dân (Quốc hội) Trung Quốc ban hành Luật Bảo vệ thông tin cá nhân (“PIPL”), trong đó vấn đề về chuyển dữ liệu qua biên giới được đề cập tới tại Chương III. Khác với GDPR, các yêu cầu theo luật này tương đối nặng nề và khó khăn để các công ty có thể tuân thủ. Theo đó, dựa trên nhu cầu thực sự trong việc chuyển dữ liệu cá nhân qua biên giới, bên chuyển dữ liệu phải đảm bảo đủ bốn điều kiện: (i) có đánh giá an ninh của Cục An ninh mạng và Tin học hóa Nhà nước (“SCID”), (ii) có chứng nhận bảo vệ thông tin của SCID, (iii) có hợp đồng mẫu về chuyển giao dữ liệu, và (iv) tuân thủ các điều kiện khác theo quy định của pháp luật. Thỏa mãn được cả bốn yếu tố này, bên có nhu cầu chuyển dữ liệu còn cần phải thông báo cho chủ thể dữ liệu và có được sự đồng thuận của họ thì mới có thể tiến hành chuyển dữ liệu qua biên giới. Trong quá trình soạn thảo dự thảo PDPD, Việt Nam cần thực hiện việc tham khảo PIPL trên cơ sở có chọn lọc các quy định hợp lý để đảm bảo tính khả thi của các quy phạm pháp luật khi được áp dụng trên thực tiễn đời sống.