MỘT SỐ VẤN ĐỀ THỂ CHẾ VÀ PHÁP LÝ CHO QUẢN LÝ DỮ LIỆU SỐ PHÁT SINH TRONG ỨNG DỤNG INTERNET KẾT NỐI VẠN VẬT Ở VIỆT NAM

Bạch Tân Sinh[1]
Học viện Khoa học, Công nghệ và Đổi mới sáng tạo

Dương Khánh Dương
Viện Chiến lược Thông tin và Truyền thông

Lòng tin là nền tảng của IoT, và sẽ không có đường tắt nào khác để có thành công.

Giulio Coraggio

Tóm tắt:

Tạo điều kiện thuận lợi để phát triển internet kết nối vạn vật (IoT) là một đòi hỏi tất yếu trong xây dựng nền kinh tế số, trong đó, lòng tin là nền tảng của IoT. Bài viết chia sẻ một số nhận định ban đầu về một số vấn đề thể chế và pháp lý liên quan đến quản lý dữ liệu phát sinh trong ứng dụng IoT ở Việt Nam từ kinh nghiệm quốc tế và hiện trạng ở Việt Nam, từ đó, đề xuất xây dựng và hoàn chỉnh khuôn khổ thể chế và pháp lý liên quan đến bảo đảm tính an toàn và bảo vệ tính cá nhân của các dữ liệu thu thập được từ IoT.

Từ khóa: *Internet kết nối vạn vật; Dữ liệu số; Quản lý dữ liệu số; Thể chế; Pháp lý.*

Mã số: *21031101*

A NUMBER OF INSTITUTIONAL AND LEGAL ISSUES CONCERNING THE MANAGEMENT OF DIGITAL DATA-BASED SOURCES DEVELOPED BY APPLYING THE INTERNET OF THINGS IN VIETNAM

Abstract:

Facilitating the development of the Internet of Things (IoT) is an indispensable requirement in building a digital economy in which trust is the foundation of the IoT. The article shares some initial thoughts about institutional and legal issues related to management of digital data-based sources developed by the applying the IoT in Vietnam from international experience and current situation in Vietnam, from which proposing the legal and institutional frameworks related to ensuring the safety and protecting the individuality of the data collected from the IoT.

Keywords: *Internet of Things (IoT); Data base; Management of data base; Institutional; Legal framework.*

---

[1] Liên hệ tác giả: sinhbt@gmail.com

1. Dẫn nhập - Định nghĩa và đặc trưng của IoT

Hiện nay, có rất nhiều định nghĩa khác nhau về IoT từ nhiều quan điểm nghiên cứu và được các tổ chức khác nhau đề xuất. Bài viết này sử dụng nghiên cứu của nhóm các nhà khoa học tiến hành trong khuôn khổ Chương trình Đào tạo tại Công ty Telecom Italia và xuất bản tại IEEE Internet of Things trong tháng 5/2015 *(Minerva R at al., 2015)*. Theo nghiên cứu này, để đưa ra một định nghĩa về IoT, cần liệt kê tính năng liên quan đến IoT nhằm giúp xây dựng nhận thức rõ ràng về IoT. Theo đó, những tính năng chính của hệ thống IoT sẽ được trình bày cụ thể dưới đây:

Sự kết nối của vạn vật: Tính năng đầu tiên của IoT bắt nguồn từ tên gọi. Nó là một hệ thống về sự liên kết của "vạn vật". Từ "vạn vật" đề cập đến bất kỳ vật thể liên quan xét từ quan điểm của người dùng hoặc người ứng dụng.

Kết nối của "vạn vật" với Internet: Từ tên gọi IoT, chúng ta có thể hiểu rằng "vạn vật" được kết nối với Internet. Theo đó, chúng ta có thể ngoại suy ra rằng, hệ thống này không phải là hệ thống kết nối nội bộ (Intranet) hoặc hệ thống kết nối bên ngoài (Extranet) của vạn vật.

Tính phổ biến: Theo định nghĩa của ITU *(ITU, SERIES Y, 2005)*, tính phổ biến là một đặc tính chính của IoT, chỉ ra một mạng lưới tồn tại ở bất cứ nơi nào và bất cứ lúc nào. Nhưng trong bối cảnh của IoT, khái niệm "bất cứ nơi nào" và "bất cứ lúc nào" không nhất thiết phải hiểu là có thể xảy ra ở cấp "toàn cầu" và "luôn luôn"; khái niệm "bất cứ nơi nào" chủ yếu đề cập đến khái niệm về địa điểm diễn ra và tương tự khái niệm "bất cứ lúc nào" đề cập đến thời điểm diễn ra.

Khả năng cảm biến: Có sự tham gia của cảm biến trong hệ thống IoT. Các cảm biến được kết nối với "vạn vật" và thực hiện sự cảm biến mà qua đó mang lại sự thông minh của "vạn vật".

Năng lực giao tiếp tương tác: Hệ thống IoT có khả năng giao tiếp dựa trên tiêu chuẩn và các quy định giao tiếp mang tính tương tác.

Khả năng tự định cấu hình: Một hành vi quan trọng khác mà hệ thống IoT có là khả năng tự định cấu hình. Do tính không đồng nhất của thiết bị bao gồm cảm biến, thiết bị lưu trữ và giám sát, điện thoại di động, mạng lưới máy tính và các thiết bị khác đang được kết nối với Internet được điều khiển từ xa hoặc qua điện toán đám mây, hệ thống IoT đang đối mặt với khả năng có thể nhân rộng. Do vậy, hướng phát triển thường thấy của thiết bị IoT là tự định cấu hình phần cứng lẫn phần mềm và tự khai thác nguồn lực của hệ thống (năng lượng, băng thông trong giao tiếp, phương tiện truy cập,...). Năng lực tự định cấu hình chủ yếu bao gồm hành động của các đối tác, tổ chức mạng và tổ chức cung cấp tài nguyên.

Khả năng lập trình: "Vạn vật" của hệ thống IoT có khả năng lập trình. Ở cấp độ đơn giản nhất, thiết bị có thể được lập trình là thiết bị có thể tự thực hiện một số hành vi khác nhau từ quyết định của người dùng mà không cần thay đổi những cấu phần của hệ thống IoT.

Phạm vi của một hệ thống IoT thay đổi từ một hệ thống nhỏ có chứa vật thể nhận dạng và cảm biến nhỏ đến một hệ thống kết nối hàng triệu vật với năng lực cung cấp dịch vụ phức tạp. Theo đó, cần có sự phân biệt về định nghĩa giữa IoT cho hệ thống nhỏ với IoT cho hệ thống lớn phức tạp.

Phương án cho IoT trong hệ thống nhỏ

Độ phức tạp thấp nhất của một hệ thống IoT là "vạn vật" có thể nhận dạng được kết nối với Internet, chẳng hạn, với các số liệu được lưu trữ tĩnh trong thẻ nhận dạng dựa trên sóng vô tuyến (thẻ RFID)[2] theo cách mà những số liệu này có thể truy cập được mọi lúc, mọi nơi với bất kỳ một thiết bị nào. Trong độ phức tạp thấp này, "vạn vật" có thể được kết nối với cảm biến để có thể cảm nhận được hiện trạng của "vạn vật", từ đó có thể đưa ra hành động dựa trên số liệu hiện có. Hệ thống này có thể tự lập trình được. Theo đó, khái niệm về IoT trong hệ thống nhỏ sẽ bao gồm "vạn vật" có thể nhận dạng, có khả năng cảm nhận và lập trình.

Với phương án này, định nghĩa về IoT trong hệ thống nhỏ được hiểu như sau:

"IoT là một mạng kết nối "vạn vật" với Internet. "Vạn vật" có khả năng cảm nhận/hành động và khả năng lập trình. Thông qua khai thác sự nhận dạng và cảm nhận, thông tin về "vạn vật" có thể được thu thập và trạng thái của "vạn vật" có thể được thay đổi mọi nơi, mọi lúc và bằng "bất cứ cách nào".

Phương án cho IoT trong hệ thống phức tạp và lớn

Hệ thống IoT có thể phát triển lên cấp độ phức tạp, trong đó, số lượng lớn của "vạn vật" có thể được kết nối để cung cấp dịch vụ mang tính phức tạp và hỗ trợ thực hiện quy trình phức tạp như được mô tả chi tiết trong Hình 1. Định nghĩa về IoT trong hệ thống lớn và phức tạp sẽ được trình bày cụ thể như sau:

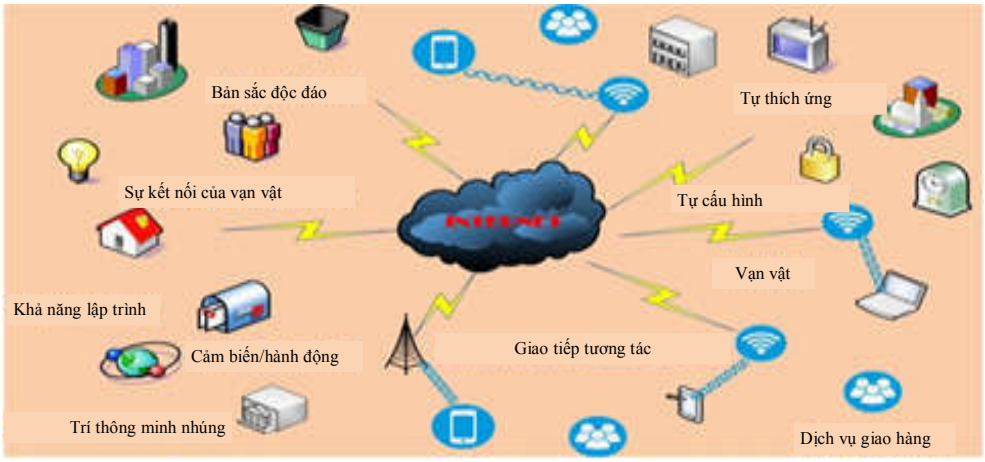
"Internet kết nối vạn vật là một mạng lưới kết nối với nhau có khả năng tự định cấu hình và thích ứng, kết nối "vạn vật" với Internet thông qua các giao thức về quy định giao tiếp theo chuẩn mực. "Vạn vật" có tính kết nối có đại diện thực hoặc ảo trong thế giới số, có khả năng cảm nhận/hành động, năng lực lập trình và là các vật thể có thể được nhận dạng. Tính đại

[2] RFID: viết tắt của Radio Frequency Identification, là công nghệ nhận dạng đối tượng bằng sóng vô tuyến.

diện hàm chứa thông tin bao gồm danh tính, trạng thái, vị trí hoặc các thông tin khác liên quan đến kinh doanh, vị trí xã hội hoặc riêng tư. Những vật cung cấp dịch vụ có hoặc không có sự can thiệp của con người, thông qua khai thác sự nhận dạng duy nhất, thu thập dữ liệu và giao tiếp, năng lực hành động. *Dịch vụ đó được khai thác thông qua việc sử dụng giao tiếp một cách thông minh, được tạo ra mọi lúc, mọi nơi và bởi mọi thứ cùng với quan tâm về bảo mật"*. Phần tử có tính phân biệt giữa khái niệm IoT với hệ thống nhỏ và IoT với hệ thống lớn là độ phức tạp của hệ thống không chỉ từ góc độ số lượng "vạn vật" mà còn từ góc độ quản lý "vạn vật" (nhấn mạnh của tác giả bài viết).

Phương án cho IoT với hệ thống phức tạp và lớn được đặc trưng bởi "vạn vật" đặt dưới sự điều hành của các cơ quan quản lý khác nhau mà giữa chúng không có mối quan hệ rõ ràng, nhờ đó mà hàng trăm, hàng nghìn thậm chí hàng triệu vật thể có thể được tiếp cận một cách dễ dàng. Trong bối cảnh đó, độ phức tạp trở thành quan trọng và các yếu tố như khả năng mở rộng, logic phân phối,... trở thành thiết yếu. Tất cả cách tiếp cận truyền thống để quản lý lòng tin, danh tính,... cần phải được thay đổi một cách căn bản nhằm đối mặt những vấn đề liên quan đến kịch bản cho IoT với hệ thống lớn và phức tạp.

Với phương án cho IoT - hệ thống phức tạp và lớn, theo đó là định nghĩa về IoT với các đặc tính như đã trình bày ở trên và tại Hình 1, nhóm tác giả sử dụng định nghĩa IoT này cho phân tích một số vấn đề thể chế và pháp lý cho áp dụng IoT ở Việt Nam trong phần còn lại của bài viết này.



Nguồn: Minerva R at al. 2015

Hình 1. Đặc tính và quy mô của hệ thống IoT.

2. IoT - sự khởi đầu cho một hình thái kinh tế-xã hội mới

Ý tưởng về vạn vật kết nối, khái niệm nền tảng của Internet kết nối vạn vật - Internet of Things (IoT) lần đầu được chuyên gia công nghệ tại Viện Đại

học MIT (Hoa Kỳ) - Kevin Ashton sử dụng vào năm 1999 trong một nghiên cứu nhằm tư vấn cho Tập đoàn P&G để nâng cao hiệu quả kinh doanh nhờ việc kết nối thông tin các thiết bị có trang bị RFID với Internet. Nghiên cứu đã chỉ ra rằng: "Nếu chúng ta có máy tính có thể biết được mọi thứ cần biết về vạn vật, sử dụng dữ liệu mà chúng thu thập được một cách tự động, thì chúng ta có thể theo dõi được mọi thứ, giảm thiểu lãng phí, mất mát và chi phí. Chúng ta có thể biết khi nào vạn vật cần phải thay thế, sửa chữa,… mặc dù trước đấy chúng có thể rất tốt. Chúng ta cần phải tăng sức mạnh cho máy tính với những thiết bị có thể thu thập thông tin, để máy tính có thể tự chúng nhìn, nghe và ngửi thế giới… Các công nghệ RFID và cảm biến có thể giúp máy tính quan sát, nhận diện và hiểu thế giới, mà không cần dữ liệu do con người nhập vào - vốn rất giới hạn"[3].

20 năm sau, những tiến bộ công nghệ, nhất là trong lĩnh vực công nghệ thông tin và truyền thông (CNTT-TT) đã biến những ý tưởng trên dần trở thành hiện thực. Từ những nền tảng cơ bản đã trở nên rất phổ biến ở Việt Nam hiện nay là những chiếc camera thông minh, tự động phát hiện và ghi lại hình ảnh các phương tiện vi phạm Luật Giao thông đường bộ để xử lý "phạt nguội", cho đến những chiếc xe tự hành đã và đang được thử nghiệm ngày càng nhiều trên xa lộ ở các nước phát triển. Đây chỉ là những ví dụ rất nhỏ của một thế giới kết nối không có giới hạn, mọi lúc - mọi nơi đang đến trong một tương lai gần. Đó là thế giới của IoT.

Thuật ngữ này có nghĩa rộng hơn các thiết bị kết nối Internet truyền thống, như máy tính xách tay và điện thoại thông minh, bởi nó bao gồm tất cả các loại vật thể và các cảm biến hiện hữu trong các không gian công cộng, nơi làm việc, các ngôi nhà, chúng thu thập và trao đổi dữ liệu với nhau và với con người. Được thiết lập để tạo khả năng về một xã hội tương tác số, siêu kết nối, IoT thực sự là một Internet của vạn vật. Ngoài việc kết nối hầu hết các thực thể vật lý, IoT còn cho phép các kết nối bằng số giữa các thành phần khác trong thế giới tự nhiên như con người, động vật, không khí và nước.

IoT là một hệ sinh thái liên kết chặt chẽ đến các nền tảng công nghệ khác, nhưng cốt yếu nhất vẫn là phân tích dữ liệu lớn. Dữ liệu chính là đầu ra, là hệ quả đem lại giá trị cho IoT. Dữ liệu của IoT có thể được sử dụng để phân tích, xử lý để hỗ trợ ra quyết định, hoặc có thể là nền tảng để kết hợp với các hệ thống tạo ra các hệ thống thông minh, hoàn toàn tự vận hành. Ngày nay, những chiếc xe ô tô tự hành đang được thử nghiệm trên đường phố đã không còn là một viễn cảnh quá xa vời.

Cũng như các công nghệ mang tính đột phá khác trong xu thế phát triển của Cách mạng Công nghiệp lần thứ 4 (CMCN 4.0), IoT sẽ có những tác động

[3] Nguồn: Lopez Research (2013).

rất lớn đến bối cảnh kinh tế-xã hội. Theo McKinsey Global Institute (2015), giá trị kinh tế của IoT đến năm 2025 ở quy mô toàn cầu sẽ vào khoảng 3,9-11,1 nghìn tỷ USD. Theo nghiên cứu của Bạch Tân Sinh và Dương Khánh Dương (2018), đầu tư cho ngành công nghiệp internet kết nối vạn vật (IIoT) sẽ tác động trực tiếp đến tăng trưởng GDP (bình quân tăng 1%/năm cho những năm tiếp theo).

Những sự kiện và thành tựu trên chỉ là khởi đầu của hàng loạt những biến đổi lớn, mà hiện nay chúng ta chỉ có thể mường tượng một phần nhỏ những tác động của nó đến kinh tế-xã hội. Đó có thể là những thay đổi tận gốc, mang tính nền tảng, làm cho cuộc sống trở nên tốt đẹp hơn. Nhưng ở một góc độ khác, IoT có thể sẽ khiến cho con người và xã hội phải đối mặt với những tác động tiêu cực, đặc biệt quyền được bảo mật của cá nhân về thông tin dữ liệu thu thập từ kết nối vạn vật,...

Chính vì thế, việc nghiên cứu những tác động và hàm ý chính sách của IoT đến khuôn khổ thể chế và pháp lý liên quan là rất cần thiết, nhằm tạo điều kiện thuận lợi cho việc tận dụng tối đa những lợi thế và hạn chế những rủi ro mà IoT có thể mang lại như tính an toàn và bảo vệ tính cá nhân của các dữ liệu thu thập được qua IoT *(Stankovic, 2014)*. Bài viết này là nỗ lực bước đầu chia sẻ kinh nghiệm của Việt Nam trong quản lý dữ liệu số phát sinh trong ứng dụng IoT.

3. Vấn đề thể chế và pháp lý về tác động của ứng dụng Internet kết nối vạn vật

3.1. Thể chế kinh tế

(i) Cạnh tranh

Ngày nay, nhân loại đang tiến tới nền kinh tế số, mà ở đó dữ liệu - vốn là đầu ra của IoT đã được mệnh danh là "dầu mỏ mới". Dữ liệu trong nền kinh tế số, cũng có vai trò như dầu hỏa trong nền kinh tế trước đây - đó vừa là nguồn năng lượng, vừa là yếu tố dẫn dắt. Các tập đoàn Alphabet (Công ty mẹ của Google), Amazon, Apple, Facebook, Microsoft và rất nhiều tập đoàn khác là những doanh nghiệp có giá trị lớn nhất thế giới, với tổng lợi nhuận vào Quý I năm 2017 đã vượt qua 25 tỷ USD. Tại Hoa Kỳ, Amazon chiếm 1/2 doanh số trực tuyến, Google và Facebook chiếm hầu hết doanh thu quảng cáo trực tuyến[4]. Đây là những tập đoàn Internet kinh doanh trên nền tảng số và dữ liệu chính là động lực đem lại cho họ lợi thế cạnh tranh. Google biết rất rõ về những gì con người tìm kiếm, Facebook biết về những thông tin được chia sẻ và Amazon là những hàng hóa được mua… Những tập đoàn này có được những "Góc nhìn của Thượng đế"[5] về những hoạt

[4] The Economist (2017); The world's most valuable resource.
[5] Nguyên bản: "God's eye view", nguồn: như trên.

động trong thị trường của họ và thậm chí hơn cả thế… Tất cả đều là do dữ liệu, hay nói đúng hơn - là khối dữ liệu lớn mà những tập đoàn này đang nắm giữ.

Bên cạnh các gã khổng lồ lớn nhất thế giới kể trên, thì các tập đoàn viễn thông cũng là những doanh nghiệp có được khối dữ liệu lớn từ khách hàng. Trung bình, một nhà cung cấp dịch vụ viễn thông điển hình tạo ra hơn một tỷ bản ghi dữ liệu cuộc gọi mỗi ngày, tương đương với việc tạo ra hơn một nửa petabyte dữ liệu mỗi tháng *(ComputerWeekly, 2018)*. Do đó, các doanh nghiệp này có rất nhiều lợi thế để trở thành tiên phong trong xu thế dữ liệu lớn. Sự xuất hiện và phát triển mạnh mẽ các công nghệ dữ liệu lớn hiện nay đang tạo cơ hội lớn cho các doanh nghiệp viễn thông nắm bắt, phân tích và tạo ra các luồng doanh thu mới từ một khối lượng thông tin khách hàng khổng lồ và dữ liệu tương tác thông qua nhiều kênh giao tiếp, phương tiện tương tác khác nhau theo thời gian thực. Với lợi thế nắm giữ những khối dữ liệu lớn về khách hàng như thế, nên các tập đoàn viễn thông sẽ chắc chắn có được những sức mạnh cạnh tranh nhất định khi họ chuyển đổi mô hình kinh doanh sang các loại hình khác.

Các tình huống điển hình về các tập đoàn Internet và dịch vụ viễn thông đã cho thấy, thể chế về cạnh tranh là một trong các khuôn khổ thể chế kinh tế chịu tác động lớn nhất bởi hệ sinh thái IoT. Bối cảnh cạnh tranh trong nền kinh tế số đã có những thay đổi căn bản so với nền kinh tế truyền thống. Đó là lợi thế cạnh tranh dựa trên dữ liệu - ai có nhiều dữ liệu hơn sẽ dành lợi thế. Đồng thời, tri thức, thông tin hay dữ liệu đều có thể được coi là một loại hàng hóa có một phần tính chất công[6], do vừa có tính không tranh giành[7], vừa là hàng khuyến dụng[8]. Vì thế, trong trường hợp này, khung thể chế về cạnh tranh cần phải có những thay đổi để đảm bảo được vai trò của nhà nước trong kiến tạo phát triển.

(ii) Hợp tác

Bên cạnh đó, đầu tư, xây dựng hệ thống IoT đòi hỏi một chi phí rất lớn do đây là hệ thống có quy mô hạ tầng rất lớn, với số lượng các thiết bị kết nối có thể lên đến hàng triệu đơn vị, bao gồm các thiết bị cảm biến, thiết bị mạng truyền dẫn, trung tâm dữ liệu, hệ thống phần mềm,… trải dài trên nhiều địa bàn khác nhau. Đơn cử là Chính phủ Ấn Độ có kế hoạch xây dựng 100 thành phố thông minh với số vốn đầu tư ước tính khoảng hơn 150 tỷ USD[9]. Mặc dù đến nay, chưa có một nghiên cứu định lượng về dự đoán nhu cầu vốn đầu tư

[6] Semi-public good.
[7] Được hiểu trên góc độ tiêu dùng, việc một cá nhân này đang sử dụng hàng hóa đó không làm ảnh hưởng những người khác cũng đồng thời muốn sử dụng nó.
[8] Được khuyến khích tiêu dùng do có lợi ích cả về góc độ cá nhân và cộng đồng.
[9] Nguồn: https://www.marketwatch.com/press-release/internet-of-things-infrastructure-market-demand-trend-review-industry-segment-and-forecast-to-2024-2018-10-11

cho hạ tầng IoT của Việt Nam, nhưng kinh nghiệm của Ấn Độ cho thấy rõ ràng xây dựng một hệ thống IoT rộng khắp, đáp ứng được nhu cầu phát triển là thách thức rất lớn về phương diện nguồn vốn đầu tư. Do đó, rất khó để một tổ chức hay doanh nghiệp có thể đơn phương thực hiện.

Cùng với đó, về bản chất, IoT là một công nghệ kết nối liên ngành. Trong tầm mức vi mô của một doanh nghiệp hay rộng hơn là một ngành hay lĩnh vực, kết nối IoT sẽ không thể đem lại giá trị gia tăng nếu không hình thành và xử lý được dữ liệu, nhằm hỗ trợ việc ra quyết định. Trên phạm vi của quốc gia, IoT sẽ chỉ mang lại những lợi ích kinh tế-xã hội rộng lớn đúng với tiềm năng, nếu dữ liệu được hình thành bởi các hệ thống IoT được kết nối, nhằm hình thành khối dữ liệu lớn của quốc gia (Big Data), và sau đó là dữ liệu mở để lan tỏa giá trị một cách rộng khắp (Open Data). Do đó, xây dựng các thể chế hợp tác trong đầu tư - xây dựng cũng như khai thác có hiệu quả hệ thống phải là chính sách quan trọng để ứng dụng và phát triển hiệu quả IoT.

3.2. Thể chế về quyền con người và quyền công dân

Thế giới của IoT là một thế giới kết nối không có giới hạn, mà ở đó, bất kỳ nơi đâu, bất kể thời gian nào, con người cũng có thể bị theo dõi, thu thập thông tin từ những hệ thống camera giám sát giao thông, hệ thống cảm biến giám sát ô nhiễm môi trường và thậm chí cả những chiếc TV thông minh trong phòng ngủ... Vào tháng 3/2017, Wikileak đã từng tiết lộ rằng, Cơ quan Tình báo Trung ương Hoa Kỳ (CIA) đã sử dụng những thiết bị kết nối để thu thập thông tin tình báo, hay vụ phần mềm gián điệp Miral đột nhập đánh cắp dữ liệu và tấn công từ chối dịch vụ (DDOS) các năm 2016, 2018 là những ví dụ mang tính điển hình cho những phiền toái mà IoT có thể gây ra cho đời sống con người. Rõ ràng, an toàn thông tin là một vấn đề cốt yếu nhất trong các vấn đề pháp lý liên quan đến IoT.

Với IoT, các chính phủ phải đối mặt với trách nhiệm điều tiết về pháp lý các luồng dữ liệu và thông tin chảy giữa một lượng lớn mạng lưới các thiết bị cảm biến, thiết bị trung gian, đảm bảo để thông tin có thể tạo ra giá trị. Một vấn đề lớn hiện nay của IoT là sự thiếu minh bạch từ phía các doanh nghiệp cung cấp dịch vụ về cách thu thập dữ liệu từ số lượng lớn người dùng, cách thức lưu trữ và sử dụng thông tin. Đây là trách nhiệm của nhà nước trong việc lựa chọn tiêu chí thích hợp cho bảo mật dữ liệu và mạng thông tin. Nhà nước phải xác minh tính bảo mật của các thiết bị IoT và cấp chứng chỉ cho các nhà sản xuất thiết bị và nhà cung cấp dịch vụ IoT. Theo Diễn đàn kinh tế thế giới, nhà nước cần phát triển và nhanh chóng làm chủ năng lực quản lý dữ liệu. Thách thức ở đây là kỹ năng và hệ thống cốt lõi cần thiết trong thời đại dữ liệu, vốn dĩ khác xa với các quy định hiện hành. Ngoài ra, cũng cần phải có các quy trình mạnh mẽ để đảm bảo chất lượng dữ liệu. Do đó, nhà nước phải xem xét một số lượng lớn hệ thống luật và

quy định hiện hành về thực thi các quy định về quyền riêng tư, bảo vệ dữ liệu, tính trung lập.

4. Kinh nghiệm của Liên minh châu Âu về bảo vệ dữ liệu

Quy định bảo vệ dữ liệu chung (GDPR) của Liên minh châu Âu (EU) 2016/679 là quy định của Luật EU về bảo vệ dữ liệu và quyền riêng tư cho tất cả các cá nhân trong Liên minh châu Âu và Khu vực Kinh tế châu Âu (EEA). Nó cũng đề cập đến việc trích xuất dữ liệu cá nhân bên ngoài EU và EEA. GDPR nhằm mục đích chủ yếu để hỗ trợ khả năng kiểm soát của công dân và cư dân trên dữ liệu cá nhân của họ và đơn giản hóa môi trường pháp lý cho kinh doanh quốc tế bằng cách thống nhất các quy định trong EU.

4.1. Sơ lược về GDPR

Định nghĩa một cách cơ bản, điều luật GDPR được ban hành là để bảo vệ thông tin riêng tư của người dùng khỏi hành vi sử dụng dữ liệu cá nhân trái phép của các công ty hoạt động trong khối Liên minh châu Âu (EU). Điều luật này đã chính thức có hiệu lực từ ngày 25/5/2018.

Về phía người dùng, điều luật GDPR không chỉ bảo vệ quyền lợi của cư dân châu Âu nói riêng mà còn áp dụng cho bất kỳ người nào có sử dụng dịch vụ do một công ty đặt tại châu Âu cung cấp. Ví dụ như ai đó đang ở Việt Nam nhưng truy cập vào trang tin BBC của Anh đọc tin tức thì BBC vẫn có nghĩa vụ phải bảo vệ dữ liệu cá nhân của người đó. Hoặc khi ai đó tra cứu tài liệu du học trên Hotcourses Vietnam ở bất kỳ đâu trên thế giới thì tổ chức đó vẫn có trách nhiệm trong việc bảo mật mọi thông tin người dùng của người đó

Về phía các doanh nghiệp, họ sẽ phải tuân theo các quy định cụ thể và rõ ràng của GDPR về cách thức thu thập thông tin cá nhân, địa điểm dữ liệu được chia sẻ và những loại thông tin nào của người dùng được sử dụng. Đối với các công ty nằm ngoài châu Âu nhưng có cung cấp dịch vụ cho cư dân châu Âu thì vẫn phải chấp hành theo điều luật GDPR.

Điều luật này sẽ được áp dụng cho toàn bộ 28 thành viên trong EU bao gồm cả Vương quốc Anh (UK) dù trên lý thuyết UK đang trong quá trình rời khỏi EU sau sự kiện Brexit vào năm 2016. Tuy nhiên, để UK chính thức tách khỏi EU theo đúng luật pháp sẽ cần một khoảng thời gian nhất định cho việc hoàn tất các thủ tục liên quan nên trước mắt UK vẫn phải tuân theo điều luật này.

Vì GDPR không phải là quy định nhất thời mà là luật bắt buộc nên mọi công ty hoạt động tại châu Âu đều phải tuân thủ nghiêm túc. Bất kỳ doanh nghiệp nào vi phạm các điều luật GDPR sẽ có nguy cơ đối mặt với án phạt lên đến 20 triệu Euro (khoảng 550 tỷ VNĐ) hoặc 4% lợi nhuận toàn cầu hàng năm của mình.

4.2. Một số nội dung chủ yếu của GDRP

Có thể nói, quyền về bảo mật thông tin cá nhân rất được EU chú trọng, trong đó, có nhiều bài học kinh nghiệm mà Việt Nam có thể tham khảo. GDPR nhằm trước hết kiểm soát việc xử lý dữ liệu riêng tư của các cá nhân và đơn giản hóa môi trường pháp lý cho hoạt động kinh doanh quốc tế thông qua việc thống nhất các quy định trong EU. Bộ phận xử lý dữ liệu cá nhân phải đưa ra các biện pháp kỹ thuật và tổ chức phù hợp để thực thi các nguyên tắc bảo vệ dữ liệu.

Các quy trình kinh doanh có tương tác với dữ liệu cá nhân phải được thiết kế và xây dựng dựa trên các nguyên tắc và các biện pháp an ninh cần thiết để bảo vệ dữ liệu (ví dụ: sử dụng bút danh hoặc ẩn danh khi thích hợp) và sử dụng các cài đặt quyền riêng tư cao nhất có thể theo mặc định, sao cho dữ liệu không sẵn sàng công bố nếu thiếu rõ ràng hoặc không đủ thông tin để xác định chủ thể dữ liệu.

GDPR quy định, dữ liệu cá nhân không được phép xử lý, trừ khi nó được thực hiện dựa trên cơ sở luật pháp và các quy định hoặc trừ khi bộ phận kiểm soát (hoặc xử lý dữ liệu) đã nhận được sự xác nhận rõ ràng và độc lập từ chủ thể dữ liệu. Chủ thể dữ liệu có quyền thu hồi sự đồng ý công bố dữ liệu bất cứ lúc nào.

Bộ phận xử lý dữ liệu cá nhân, khi có yêu cầu phải báo cáo rõ ràng việc thu thập dữ liệu, tuyên bố cơ sở pháp lý và mục đích xử lý dữ liệu và nêu rõ thời gian lưu trữ dữ liệu và quyền được phép chia sẻ với bên thứ ba hoặc tổ chức/cá nhân bên ngoài EEA. Chủ thể dữ liệu có quyền yêu cầu một bản sao giống như dữ liệu đang được thu thập xử lý theo định dạng chung và có thể xóa dữ liệu của họ trong một số trường hợp nhất định.

Cơ quan công quyền và các doanh nghiệp có hoạt động chân rết xoay quanh việc xử lý dữ liệu cá nhân thường xuyên hoặc định kỳ, phải thuê nhân công có nghiệp vụ chuyên môn về bảo vệ dữ liệu (DPO) chịu trách nhiệm bảo đảm việc tuân thủ GDPR.

Doanh nghiệp phải báo cáo về các vi phạm dữ liệu trong vòng 72 giờ nếu chúng có ảnh hưởng xấu đến quyền riêng tư của người dùng. Trong một số trường hợp, nếu là doanh nghiệp, hoặc có quy mô lớn, bên vi phạm GDPR có thể bị phạt tới 20 triệu Euro hoặc tối đa 4% doanh thu toàn cầu hàng năm của năm tài chính trước đó.

GDPR không áp dụng cho việc xử lý dữ liệu cá nhân nhằm phục vụ cho các hoạt động an ninh quốc gia hoặc thực thi pháp luật của EU. Tuy nhiên, các nhóm ngành công nghiệp có thể được viện dẫn để yêu cầu bộ phận kiểm soát dữ liệu, chiểu theo luật của nước thứ ba phải tuân thủ yêu cầu pháp lý trong quá trình thực thi pháp luật của nước đó; theo lệnh tòa án, hoặc cơ

quan an ninh nước đó cung cấp cho các cơ quan chức năng dữ liệu cá nhân của công dân EU, bất kể dữ liệu đó nằm trong hay ngoài EU.

GDPR là một bộ quy tắc duy nhất áp dụng cho tất cả các quốc gia thành viên EU. Mỗi quốc gia thành viên sẽ thành lập một cơ quan giám sát độc lập (SA) để theo dõi và điều tra các khiếu nại, xử phạt vi phạm hành chính.

Các SA ở mỗi quốc gia thành viên sẽ hợp tác, hỗ trợ lẫn nhau và tổ chức các hoạt động chung. Nếu một tổ chức có nhiều cơ sở tại EU thì tổ chức đó phải có một SA là "cơ quan chính", tại nơi diễn ra các hoạt động của trung tâm xử lý dữ liệu. Cơ quan chính sẽ đóng vai trò "một cửa" để giám sát tất cả các hoạt động xử lý của doanh nghiệp đó trên toàn EU. Ban Bảo vệ Dữ liệu châu Âu (EDPB) chịu trách nhiệm phối hợp hoạt động của các SA.

(i) Quyền của chủ thể dữ liệu

Theo Ủy ban châu Âu, dữ liệu cá nhân là bất kỳ thông tin nào liên quan đến cá nhân, nghề nghiệp hoặc hoạt động xã hội của cá nhân. Nó gồm tất cả thông tin liên quan đến tên, địa chỉ nhà, ảnh, địa chỉ email, chi tiết tài khoản ngân hàng, bài đăng trên các trang mạng xã hội, thông tin y tế hoặc địa chỉ IP trên máy tính của các cá nhân.

Các định nghĩa chính xác của những thuật ngữ như "dữ liệu cá nhân", "xử lý", "chủ thể dữ liệu", "bộ phận kiểm soát" và "bộ phận xử lý dữ liệu",... được nêu trong Điều 4 của GDPR.

Theo Điều 6, các mục đích hợp pháp [với dữ liệu] là:

(a) Nếu chủ thể dữ liệu đã đồng ý cho phép xử lý dữ liệu cá nhân của họ;

(b) Thực hiện nghĩa vụ hợp đồng với chủ thể dữ liệu hoặc cho các nhiệm vụ theo yêu cầu của chủ thể dữ liệu đang trong quá trình ký kết hợp đồng;

(c) Thực hiện hoạt động xử lý dữ liệu để tuân thủ nghĩa vụ pháp lý của bộ phận kiểm soát dữ liệu;

(d) Thực hiện hoạt động xử lý dữ liệu để bảo vệ lợi ích sống còn của chủ thể dữ liệu hoặc cá nhân khác;

(e) Thực hiện hoạt động xử lý dữ liệu để thực hiện một nhiệm vụ vì lợi ích công cộng hoặc cơ quan có thẩm quyền;

(f) Thực hiện hoạt động xử lý dữ liệu vì lợi ích hợp pháp của bên kiểm soát dữ liệu hoặc bên thứ ba, trừ khi những lợi ích này bị chi phối bởi lợi ích của chủ thể dữ liệu hoặc quyền của họ chiểu theo chương quy định về các quyền cơ bản (đặc biệt là trong trường hợp của trẻ em).

Chủ thể dữ liệu có quyền và được phép rút lại sự đồng ý này bất cứ lúc nào và quá trình thực hiện không được khó hơn so với việc chọn tham gia.

(ii) Kiểm soát và xử lý dữ liệu

Để có thể tuân thủ GDPR, bộ phận kiểm soát dữ liệu phải triển khai các biện pháp đáp ứng các nguyên tắc bảo vệ dữ liệu theo thiết kế và theo mặc định.

Bảo vệ dữ liệu theo thiết kế và theo mặc định (Điều 25) của Quy định bảo vệ Dũ liệu chung (GDPR) yêu cầu các biện pháp bảo vệ phải được thiết kế ngay trong các quy trình kinh doanh đối với sản phẩm và dịch vụ. Các biện pháp như vậy bao gồm giả danh dữ liệu cá nhân, được thực hiện bởi bộ phận kiểm soát, càng sớm càng tốt (Điều 78). Đó chính là nghĩa vụ và trách nhiệm của bộ phận kiểm soát dữ liệu triển khai các giải pháp hiệu quả và thể hiện việc tuân thủ của các hoạt động xử lý ngay cả khi việc xử lý được thực hiện bởi bộ xử lý dữ liệu thay cho bộ kiểm soát (Điều 74).

Cài đặt quyền riêng tư phải được đặt ở mức cao theo mặc định và các biện pháp kỹ thuật và thủ tục phải được thực hiện bởi bộ phận kiểm soát để đảm bảo rằng việc xử lý, trong toàn bộ vòng đời xử lý, tuân thủ quy định. Kiểm soát viên cũng phải thực hiện các cơ chế để đảm bảo rằng, dữ liệu cá nhân không được xử lý, trừ khi cần thiết cho từng mục đích cụ thể.

Báo cáo của Cơ quan An ninh mạng và thông tin Liên minh châu Âu soạn thảo kỹ lưỡng những gì cần phải làm để đạt được sự riêng tư và bảo vệ dữ liệu theo mặc định. Cụ thể, các hoạt động mã hóa và giải mã phải được tiến hành ngay tại chỗ, không được phép thực hiện bởi các nghiệp vụ xử lý từ xa, bởi vì cả khóa và dữ liệu phải nằm trong khả năng của chủ sở hữu dữ liệu để bảo đảm bí mật riêng tư.

Báo cáo chỉ định rằng, lưu trữ dữ liệu thuê ngoài trên ứng dụng điện toán đám mây từ xa là thiết thực và tương đối an toàn nếu chỉ chủ sở hữu dữ liệu, không phải dịch vụ đám mây, giữ các khóa giải mã.

GDPR đề cập đến giả danh là một quá trình được yêu cầu khi dữ liệu được lưu trữ (như là một thay thế cho tùy chọn ẩn danh dữ liệu hoàn chỉnh khác) để chuyển đổi dữ liệu cá nhân theo cách mà dữ liệu kết quả không thể được gán cho chủ thể dữ liệu cụ thể nếu không sử dụng thông tin bổ sung.

Một ví dụ là mã hóa, làm cho dữ liệu gốc không thể hiểu được và quá trình có thể được đảo ngược mà không cần truy cập vào khóa giải mã chính xác. GDPR yêu cầu thông tin bổ sung (như khóa giải mã) phải được lưu trữ tách biệt và cách ly với dữ liệu giả danh.

Một ví dụ khác về giả danh là tokenisation, đây là một cách tiếp cận phi toán học để bảo vệ dữ liệu ở phần còn lại thay thế dữ liệu nhạy cảm bằng các thay thế không nhạy cảm, được gọi là mã thông báo. Mặc dù các mã thông báo không có ý nghĩa hoặc giá trị bên ngoài hoặc có thể khai thác, chúng cho phép dữ liệu cụ thể hiển thị đầy đủ hoặc một phần để xử lý và phân tích trong khi thông tin nhạy cảm được giữ kín.

Mã thông báo không làm thay đổi loại hoặc độ dài của dữ liệu, có nghĩa là nó có thể được xử lý bởi các hệ thống cũ như cơ sở dữ liệu có thể nhạy cảm với độ dài và loại dữ liệu. Điều này cũng đòi hỏi ít tài nguyên tính toán hơn để xử lý và ít không gian lưu trữ trong cơ sở dữ liệu hơn dữ liệu được mã hóa theo truyền thống.

Bút danh được khuyến nghị để giảm rủi ro cho các chủ thể dữ liệu liên quan và cũng để giúp các bộ phận kiểm soát và bộ xử lý đáp ứng các nghĩa vụ bảo vệ dữ liệu của họ (Điều 28).

GDPR đã có hiệu lực và thu hút được sự ủng hộ của các doanh nghiệp coi đây là cơ hội để cải thiện việc quản lý dữ liệu. GDPR quy định mục tiêu rõ ràng, có thể trở thành hình mẫu cho các khu vực khác ngoài châu Âu.

Tuy nhiên, việc tuân thủ GDPR sẽ đòi hỏi các tổ chức/doanh nghiệp phải đầu tư kinh phí bổ sung, tăng cường nhân lực dành cho xử lý dữ liệu. Một số điều khoản, quyền của các pháp nhân, cá nhân liên quan đến xử lý dữ liệu vẫn còn có những tranh luận của các học giả pháp lý.

Người ta cũng còn phải chờ những phán quyết của Ban Bảo vệ Dữ liệu châu Âu, các cơ quan chức năng của EU phán xử những vụ việc cụ thể liên quan đến xử lý dữ liệu cá nhân, từ đó mới biết được GDPR cần sửa đổi những điều, khoản nào.

5. Đánh giá mức độ thích ứng của quy định pháp lý hiện hành ở Việt Nam

5.1. Luật Cạnh tranh năm 2018

Luật Cạnh tranh năm 2018 được Quốc hội khóa XIV thông qua vào ngày 12/6/2018, chính thức có hiệu lực từ ngày 01/7/2019 và thay thế cho Luật Cạnh tranh năm 2014. Với nhiều cải cách sâu rộng, Luật được kỳ vọng sẽ tạo ra cú hích lớn thúc đẩy môi trường kinh doanh, cạnh tranh tự do, bình đẳng giữa các chủ thể kinh doanh trong nền kinh tế. Với 10 Chương, 118 Điều, Luật Cạnh tranh năm 2018 mới chủ yếu tập trung vào kinh tế và chi phối thị phần.

Đối với một nền kinh tế số - nền kinh tế của IoT, mà ở đó dữ liệu là yếu tố cạnh tranh quan trọng nhất thì Luật Cạnh tranh năm 2018 chưa đề cập đến. Do đó, trong thời gian tới, việc tập trung vào dữ liệu như là một yếu tố hình thành lợi thế cạnh tranh cần được xem xét, bổ sung, sửa đổi hoàn thiện quy định pháp lý để phù hợp với bối cảnh mới.

5.2. Luật An toàn thông tin mạng

Luật An toàn thông tin mạng được Quốc hội khoá XIII thông qua vào ngày ngày 19/11/2015. Luật gồm 8 Chương, 54 Điều quy định về hoạt động an toàn thông tin mạng, quyền và trách nhiệm của cơ quan, tổ chức, cá nhân trong việc bảo đảm an toàn thông tin mạng; mật mã dân sự; tiêu chuẩn, quy

chuẩn kỹ thuật về an toàn thông tin mạng; kinh doanh trong lĩnh vực an toàn thông tin mạng; phát triển nguồn nhân lực an toàn thông tin mạng; quản lý nhà nước về an toàn thông tin mạng. Luật có hiệu lực thi hành kể từ ngày 01/7/2016.

Có thể nói, Luật An toàn thông tin mạng đã chú trọng đến bảo vệ quyền thông tin của công dân với các Điều 16, 17, 18, 19, 20 thuộc Mục 2. Bảo vệ thông tin cá nhân. Luật An toàn thông tin mạng về cơ bản đã đáp ứng được những tiêu chuẩn tối thiểu nhằm bảo vệ thông tin, dữ liệu của công dân.

Ngoài hai bộ luật nêu trên, vấn đề dữ liệu và an toàn dữ liệu cũng đã được đặt ra trong Luật Công nghệ thông tin, Luật Giao dịch điện tử, Luật Tiếp cận thông tin, và gần đây nhất là Luật An ninh mạng được Quốc hội thông qua tháng 6/2018 và có hiệu lực từ ngày 01/01/2019, Nghị định số 47/2020/NĐ-CP ngày 09/04/2020 của Chính phủ về quản lý, kết nối và chia sẻ dữ liệu số của cơ quan nhà nước. Bộ Thông tin và Truyền thông và một số địa phương (như TP. Hồ Chí Minh, Huế) cũng đã và đang tổ chức nghiên cứu, hướng dẫn các nội dung về dữ liệu, chia sẻ và bảo đảm an toàn dữ liệu trong một số ứng dụng cụ thể như xây dựng đô thị thông minh. Nghị định quy định về bảo mật dữ liệu cá nhân cũng đang được xây dựng và tổ chức lấy ý kiến trước khi ban hành. Một số tiêu chuẩn về IoT cũng đang chuẩn bị được công bố hoặc trong quá trình thẩm định để công bố.

6. Kết luận

Tạo điều kiện thuận lợi để phát triển IoT là một đòi hỏi tất yếu trong xây dựng nền kinh tế số. Tuy nhiên, đến nay vẫn chưa có nhiều bằng chứng về một chính sách IoT thành công ở tầm quốc gia, kể cả ở các quốc gia có nền công nghiệp phát triển *(Mark Purdy và Ladan Davarzani, 2015)*. Nhằm tận dụng tốt cơ hội do IoT đem lại, cũng như giảm thiểu những tác động tiêu cực về mặt xã hội, cần phải có một cách tiếp cận thận trọng với quan điểm về bảo vệ quyền công dân trong bối cảnh kết nối mọi lúc - mọi nơi. Cụ thể, cần sớm xây dựng và hoàn chỉnh khuôn khổ thể chế và pháp lý liên quan đến bảo đảm tính an toàn và bảo vệ tính cá nhân của các dữ liệu thu thập được qua ứng dụng IoT, từ đó, tạo dựng được lòng tin của các bên liên quan - nền tảng của IoT trong một nền kinh tế số đang dần được hình thành.

Qua đánh giá sơ bộ, có thể thấy, Luật An toàn thông tin mạng về cơ bản đã đáp ứng được phần nào yêu cầu. Tuy nhiên, các quyền của cá nhân về bảo mật dữ liệu của Liên minh châu Âu cũng có thể là một kinh nghiệm rất cần được nghiên cứu và có thể áp dụng một phần cho Việt Nam.

Ngoài ra, trong bối cảnh cạnh tranh chủ yếu dựa trên nguồn dữ liệu đang được tạo nên thông qua ứng dụng IoT, việc bổ sung, sửa đổi Luật Cạnh tranh năm 2018 nhằm phù hợp với tình hình mới là rất cần thiết./.

LỜI CẢM ƠN

Bài viết này sử dụng một phần kết quả của Báo cáo chuyên đề "Ứng dụng Internet kết nối vạn vật và những vấn đề pháp lý đặt ra" thực hiện trong khuôn khổ đề tài nghiên cứu cấp Bộ năm 2019 "Định hướng xây dựng và hoàn thiện hệ thống pháp luật trong bối cảnh cách mạng công nghiệp 4.0" do Viện Khoa học Pháp lý - Bộ Tư pháp chủ trì.

TÀI LIỆU THAM KHẢO

1. Bạch Tân Sinh, Dương Khánh Dương (2018). "Tác động tiềm năng của năng lực hấp thụ quốc gia trong Internet kết nối vạn vật đến kinh tế-xã hội ở một số quốc gia trên thế giới và bài học gợi suy cho Việt Nam". *Tạp chí Chính sách và Quản lý Khoa học và Công nghệ* số 4 năm 2018.
2. Angela Guimarães Pereira, Alice Benessia Paula Curvelo (2013); Agency in theInternet of Things;
3. ITU, SERIES Y: GLOBAL INFORMATION,INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS., AND NEXT-GENERATION NETWORKS, Next Generation Networks Frameworks and functional architecture models: file:///C:/Users/11598004/Downloads/T-REC-Y.2060-201206III-PDFE-E.pdf
4. Karen Rose, Scott Eldridge, Lyman Chapin (2015); THE INTERNET OF THINGS: AN OVERVIEW Understanding the Issues and Challenges of a More Connected World;
5. Mark Purdy và Ladan Davarzani (2015), The Growth Game-Changer: How the Industrial Internet of Things can drive progress and prosperity;
6. McKinsey Global Institute (2015); Unlocking the potential of the Internet of Things;
7. Minerva Roberto, Biru Abui and Rotondi Domenico (2015). Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative.
8. World Economic Forum (2018); Identity in a Digital World A new chapter in the social contract
9. Spyros G. Tzafestas (2018); Ethics and Law in the Internet of Things World
10. Stankovic, John (2014). "Research Directions for the Internet of Things". IEEE Internet of Things Journal. Vol1, No.1. Feb 2014.
11. https://www.weforum.org/agenda/2019/03/four-tips-governing-by-design-fourth-industrial-revolution-policy-making/
12. https://www.weforum.org/agenda/2015/09/5-tech-trends-transforming-government
13. https://www.weforum.org/agenda/archive/future-of-government
14. https://www.weforum.org/agenda/2017/02/role-of-government-digital-age-data/.