UDC 341.1/.8
DOI https://doi.org/10.17721/2227-796X.2023.2.02

THE SHARING OF BUSINESS-TO-GOVERNMENT DATA

Problem. *The value of the Internet of Things (IoT) is the mechanized welding that processes sensitive data in the real-time interface when the sharing of Business-to-Government Data (B2G) provides business capacity for the generated data in the factory of the IoT system to be open for the public partakers. At the same time, the designed approach is suited to govern spatially circulated human characteristics affecting the replication of sensitive outcomes and supporting their fragmentation. The study identifies this problem in the Data Act of the European Union because it permits its operation.*

Purpose. *The authors advocate the actual safety designation. Thus, the research article aims to solve the question of how (sensitive) data – a subject to the conflicting rights of others – can be business-to-government shared on the way to the achievement of safe settings and safe data, and avoidance loss factors of its integrity.*

Methods. *The research applied measures aligned for the secondary use of sensitive data spawned by businesses and illustrated the experience of the Nordic Smart Government (NSG&B). Under this cure, the authors stand for the like-to Nordic cross-border data exchange shapes, and, at the same time, advance incident prevention relevant to the preparation process before as to convey data publicly. To support the argument for such a stand, the authors present the experience of the Taiwanese Tsai et al. v. National Health Insurance Administration case of 2014 and 2017 regarding the sharing of personal health data when the main plaintiff, Tsai, sued the National Health Insurance Administration for permitting third parties to access the National Health Insurance database for research drives on the name of sharing interests.*

Results. *The case study provided would potentially contribute to the practical realization of the sharing of the Business-to-Government data approach in the framework of alike projects such as NSG&B.*

Conclusions. *This research underlines the extent of addressing the sensitive nature of data sharing within IoT designs, mainly in the context of B2G relations. It stresses the condition for bars that prioritize data safety, integrity, and incident deterrence. The discoveries also propose potential implications for policy and regulation, significantly in the European Union.*

Key words: B2G, sensitive data, a subject to the conflicting rights of others’ data, Internet of Things, cybersecurity.

Bulgakova Daria,
Ph.D. in International Law,
Researcher, Visiting
Scholar at the Law
Department
Uppsala University
orcid.org/0000-0002-8640-3622
dariabulgakova@yahoo.com

Stupnik Victoriia,
Pedagogue-Methodist
of the Highest Category,
Supervisor of Scientific
Manuscripts on History
and Law,
Lecturer
Kryvyi Rih Gymnasium
№ 91
orcid.org/0009-0006-8953-2477
vikysjakrul@gmail.com

1. Introduction to the sharing approach

Economic growth and higher competition and innovation are key benefits for the European data economy and data mobility. In February 2020, the Commission published a European strategy on data (Communication, 2017) enclosing the promotion of sharing means between companies and public administration ((B2G) for the public interest (Commission, 2020). And, E.U. categorized a wave of sharing data initiatives depicted as 'accessible public data that people, companies, and organizations can use to launch new ventures, analyze patterns and trends, make data-driven decisions, and solve complex problems' (Gurin, 2014). Hence, the demand for shared data grows. The B2G conflicted IoT-I-data has released raw data settings by adopting open initiatives about collection, and storage of data concerning sharing interests, and integrating standards for data interaction and inference relevantly to mundane devices, allowing for the measurement, sharing, and dispatch of data via data networks[1].

Furthermore, European Union has worked on reusing sensitive data in the past few years to achieve the smart E.U. city's goal, as well as, the proposed Regulation on harmonised rules on fair access to and use of data (Data Act) (European Commission, 2022) adopted by the Commission on 23 February 2022 provides business capacity for the generated data on the Internet of Things factory to be open for the public partakers exploring the opportunities for an innovative smart city. Thus, the significance of the research has been formulated by the variety of such projects, likewise, the Nordic Smart Government and Business (NSG&B) (European Commission, 2017). Therefore, there is a need for a regulatory mechanism for data flow across the E.U. for economic benefits by enhancing the government's reuse of commercial sector data for shared benefits and flowing data among various databases. Thus, governments and businesses have posed tremendous policy challenges for reusing sensitive data, the use of which is subject to conflicting rights of others (Communication from the Commission to the European Parliament, the Council,

[1] *See, e.g.*, Markus Perkmann & Henri Schildt (2015) *Open Data Partnerships Between Firms and Universities: The Role of Boundary Organizations*, 44 Rsch. Pol'y 1133, 1134–35.

the European Economic and Social Committee, and the Committee of the Regions, 2020). For instance, the E.U. Open Data Directive No. 2019/1024 is the initial manifestation of this trend, backed by estimates that the opening E.U. public data could drive economic benefits of EUR 250 billion (Deloitte, Open Evidence, Wik Consult, timeless, Spark, The Lisbon Council, 2018). Hence, small and medium-sized enterprises (S.M.E.s) perceive data sharing as essential to acquire data from other companies like it is happening with biometric data for unique identification practice (European Commission, 2019) through the comprise of the unique identifiers to detect individuals, device holders, etc.

Due to the relocation of the E.U. visions for smart city governance, the approach to widespread B2G conflicted IoT-I-data is applicable for digital set up meaning that dispatch is without territorial constraints. Given the study, has significantly increased the risk of disseminating studied data without appropriate precautions with business-government partnerships priorities (Atzori et al., 2010). For example, when IoT-I records biometric data, a user's data shape is shared between the user and IoT-I tech or S.M.E.s facilities where the last party shall secure biometrics through 'unsolicited contact' (Gaba and Estremadura, 2020). Such an advanced course remains in action because businesses often use a sharing approach 'to offer fast and efficient services to consumers' (Streinz, 2021). Simply set, it is an interconnection of the capability to share data with demanding state-of-the-art interaction. Therefore, it is indispensable to gradually devote safety capabilities for data conformity, providing stable guarantees for B2G conflicted IoT-I-data set in Articles 51 (b) and 52 of the Cybersecurity Act known as the Regulation (E.U.) № 2019/881 with further safety-focused techniques. It is actual since the IoT-I products depend laboriously on data from a massive network that reacts to the environment or changes. Therefore, the integrity element is considered a legal direction for a safe data setting of B2G conflicting data standards to mitigate hazardous shortcomings in the hardware and promote the conservation of stored data against accidental destruction breaking the hardware chain, and the secure traceability of data value. In this outlook, it is sufficient to employ conditions without entitling unintended credentials, system changes, or data confines. Regardless, the disbandment of low-cost products and the rapid penetration of intelligent and complex devices in the market pose challenges to certifying the calibration of the data substitutions.[2] On the other hand, it is mainly for technical facets, not legal.

The lack of studies about the safety of business-to-government sensitive data processing (generated by the Internet of Things for the industrial shared interests (B2G conflicted IoT-I-data)) is especially questionable for solving, likewise, for such projects as NSG&B.[3] Moreover, as long as new IoT-I products become available in an internal market, it is desirable to retain the existing storage system and gradually apply safety capabilities. The compliance measures require the controller to be

[2] ISO/IEC JTC 1/SC 27, 2018.

[3] *See* more at https://nordicsmartgovernment.org/.

in action for safety results delivering stability guarantee during hazardous faults and accidental destruction. That necessity is set in the updated cybersecurity law of Regulation (EU) 2019/881 of Articles 51 (b) and 52.

Taking the above into consideration, the authors aim to find out how to govern spatially circulated human characteristics that face negative sharing outcomes in means of replication effect and avoid its broking. Thus, the research question is *how (sensitive) data – subject to the conflicting rights of others – can be business-to-government shared on the way to the achievement of safe settings and safe data, and avoidance loss factors of its integrity*.

2. The sharing of sensitive data (a subject to the conflicting rights of others)

The sensitivity core of data – a subject of the conflicting interests of others – is especially on the table when identifiable and identified B2G IoT-I-data is subject to different likelihoods of hazards[4] when, among other things, extra safety and privacy rules shall apply referring to the regulatory requirements (European Data Protection Board, 2020). Since the more effortlessly B2G conflicted IoT-I-data can be accessed and circulated, the more noteworthy safety and privacy criteria are for those drives. Eventually, the B2G conflicted IoT-I-data is currently not disclosed and not covered by the Public Sector Information (P.S.I.)/Open data directive. Under the E.U. novel sharing approach, this sensitive data flow is no longer limited between users and S.M.E.s, instead, it is viewed as a 'medium of governance,' unlike the flow of data from government to business (G2B).

The analysis of the issue of sharing B2G remains largely unaddressed. Under the Data Act core: 'European data law is bound to become a form of meta-regulation of legal governance by and with data.' Considering B2G conflicted IoT-I-data features, the research has been dedicated to developing more advanced and evolved technology to improve the efficiency of sharing assigned data. NSG&B phenomena have made B2G conflicted IoT-I-data more vulnerable to unwanted fragmentation and duplication. Moreover, Nordic citizens' – participants of NSG&B – confidentiality became less reliable to the privacy of unique data. As a result, open B2G conflicted IoT-I-data have rendered business records accessible to the government, encouraged IoT-I innovation for the NSG&B mission, and motivated B2G concentration[5]. Again, whether a newmade Data Act could cost Nordic citizens' interests for data safety and whether this data sharing is privacy appropriate are suspicious and should be under lodestar when making B2G conflicted IoT-I-data NSG&B policies[6].

[4] *See* A. Alemanno, "Data for Good. Unlocking Privately-Held Data to the Benefit of the Many", Eur J Risk Regul 9(2) (2018) 183–191.

[5] *See* Smart Cities Cybersecurity and Privacy (Danda B. Rawat & Kayhan Zrar Ghafoor eds., 2018); How Smart is Your City? Technological Innovation, Ethics, and Inclusiveness (Maria Isabel Aldinhas Ferreira ed., 2020).

[6] *See,* e.g., Ben Green et al., Open Data Privacy 3 (2017); Ben Green et al., *Open Data Privacy: A Risk-benefit, Process-oriented Approach to Sharing and Protecting Municipal Data*, Berkman Klein Center for Internet & Society (2017), Available at https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf

From this perspective, the policies could acquire pertinent social benefits by facilitating data sharing (Verhulst and Young, 2018). The research has thus concentrated on sensitive data of shared interest (Pailhès, 2018). Private companies often collect data of shared interest. The pass to such data would allow for the repurposing of 'private intent data' vs. 'public intent data' (World Bank (2021)[7]. For a model, a shared approach for sensitive data can scrutinize public health and mitigate the spreading of diseases. In this concern, sharing may instruct combining datasets from different data holders. Thus, poor data interoperability hampers datasets from various sources, which could result in the structure of datasets differently. This trouble would lead to B2G conflicted IoT-I-data fragmentation and the combination of data to insufficient quality. It means there is a need for additional integrity safety within combining different B2G datasets. A comprehensive B2G conflicted IoT-I-data safety program is the key to fulfilling the promises of the E.U.'s open data envision. The rapid and broad available sensitive data flow approach reasoned B2G conflicted IoT-I-data in favor of the appropriate mixture of private and public sector benefits for urban planning and future intelligent cities' safety data tasks. For instance, incorrect data service due to conflicted sensitivity between data and algorithmic designs can generate reproduction, stabilization, or amplify social and economic inequality[8]. One example of how one could realise the values of such an ecosystem is by aligning the digital business systems on the S.M.E.s' accounting systems with other B2G processing data designs. The Danish Government's response to the public consultation on the Data Act as well as the Ministry of Industry, Business, and Financial Affairs shows a mount of these ambitions and welcomes efforts to enhance the public sector's capacity to share and utilize B2G data of shared interest under a fair, predictable, and transparent process of obtaining these data. The ecosystem for data sharing approach builds upon 1) the purpose of B2G data and 2) a functional shared data infrastructure. Thus, any rights for the public sector to access B2G conflicted IoT-I-data private data for shared interest should be carefully assembled. The ecosystem of the sharing approach should portray the public interest and the purpose of sharing data. How, when, and why the government may accumulate such data should be precise and only for legalised purposes, giving businesses predictable framework conditions and constructing businesses' environment to provide B2G data through an operational data-sharing infrastructure. Therefore, this must be in place before considering the business burdens of sharing data with the government. Further, assessing whether seating such infrastructure would form advantages that outrank the costs and whether it would fulfill the market is paramount. Data sharing infrastructure should

[7] *Note* Public intent data is data collected with the intent of serving the shared well by informing the design execution, monitoring, and evaluation of public policy, or through other activities.

[8] *See* J. Drexl (2018) Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC.

be effortless and give businesses credentials for B2G data to review it from the government. Hence, it is required to confine true-to-life safeguards and to find an adequate balance between the interests at stake (The World Bank, 2020).

Given the research view, the safety condition is essential because B2G conflicted IoT-I-data is at risk of harm due to its integrity loss within the sharing process affects the replication of sensitive outcomes and results in data (subject to conflicting rights of others) fragmentation. The study seeks to propose design-oriented and control compliance configurations defending the factory that shares data faced the cost of security risk associated with the intended use of the IoT-I product.

Hereinafter, the research flags input related to an open IoT-I-data dispute facilitates sharing states for B2G conflicted IoT-I-data; and, establishes safe settings-data technique and privacy stress, including the ambiguity of shared interest. Under that outline, by placing vital share prerequisites, the research stands for the cross-border exchange shapes of data, the use of which is subject to the conflicting rights of others within specific regions, and advances cybersecurity incident prevention before conveying it publicly.

3. Safe settings – safe data

Working with B2G conflicted IoT-I-data, NSG&B requires services to provide the necessary safe settings; and independent conflicted data privacy governance by a technical design framework for eco-environment (Safe Havens) and work alongside a comprehensive regime. Yet, the Data Act acknowledges that some sensitive data is shielded by national ruling for national security, statistical, and/or commercial confidentiality when supplementary steps are mandated before it is conceivable to share it publicly for data the value of which is subject to the conflicting rights of others. In line with the high estimate of the value of public sector data, by opening up some of this data under Directive (E.U.) 2019/1024, likewise, health data as it is subject to the rights of patients (Deloitte, Open Evidence, Wik Consult, timeless, Spark, The Lisbon Council, 2018) that 'develop personalised medicine or advance research to find cures for specific diseases' (European Commission, 2020). At the European level, there is an ongoing discourse within the research community on how B2G conflicted IoT-I data can be shared and made available for research purposes. European projects, including EUDAT CDI[9] and EOSC-hub[10] have engaged on this issue, producing the secure sharing of this data. The types of safety measures considered go well to link the data back to the individual concerned (European Commission, 2018), and point out (a) promoting free sharing of B2G conflicted IoT-I-data; (b) providing a 'safe haven' – a secure environment for research work with B2G conflicted IoT-I-data; (c) the merits of central vs. distributed storage. Furthermore, safety methods for technical element compliance are under

[9] *See* more about EUDAT Collaborative Data Infrastructure at https://eudat.eu/eudat-cdi

[10] *Note* European Open Science Cloud hub – providing support services for developing a European Open Science Cloud and a single point of contact for researchers for resources for advanced data-driven research.See https://www.eosc-hub.eu/about-us

Regulation (E.U.) 2019/881 of Articles 51 (b) and 52, for example, the out-of-the-box configuration, a signed code, secure update, and heap memory have in common with the security functionalities and legal conditions. That is allocated to optimize conformity schemes for the manufacturers that target to place IoT-I products on the European market and deployed depending on the information model available and network criteria. The central research assumption is that the control rules for B2G conflicted IoT-I-data must be initiated and implemented. It is proposed to be done relevantly to data-driven and first-principles modeling. The control first step approach is to identify a sensitive data set of a particular hardware model especially when the device does not designate dynamics within data processing. Involving its technique, it is possible to assess the plant model without identifying risk from the subject and without decommissioning the plant to carry out assessment experiments. To that end, observer-based cybersecurity conformity is an essential criterion for sensitive data hardware, which can be carried out independently for the distributed design. Specifically, a study addresses legislators to out-of-the-box configuration, a signed code, secure update, and heap memory measurements to improve the hardware's overall performance.

The second safe settings-data scenario relies on parametrizing all stabilizing controllers for a given data processing work. This methodology has the advantage of affine data motion in the design parameter.[11] It indicates the design nuisance has an open-loop-like quality, which can thus gauge cybersecurity enactment during the data transition wiggles in the hardware within defaulting of relevant to IoT-I products set of conducts. A study does not intend to provide a rigorous comparison of the methods but contrariwise that the hardware control problem is feasible in practice, and preservation of IoT-I products hardware could solve hazardous faults and accidental destruction. For example, in IoT-I functioning household scenario delivering measure is a data observation programming submitted through the IoT-I products infrastructure to its hardware controller and elaboration system. This workflow scenario, where hardware monitoring assessments with network production exchange messages appliance to a reference model for establishing a vast network of IoT-I devices and optimized data sharing. Dissecting this chain, the conformity is applicable by individuating the Information Communication Technology (I.C.T.) to the IoT-I infrastructure, hardware, and its risk controller.[12] Thus, conditions contain the measurements to be exchanged and the protocols used where IoT-I products are placed.

The safe safe setting-data asset is subject to cybersecurity traceability. IoT-I products system must be under a security scheme since the hardware chain

[11] *See* Aranha, Helder, Massimiliano Masi, Tanja Pavleska, et al. (2021) 'Securing the Metrological Chain in IoT Environments: An Architectural Framework', 2021 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT), 704–709.

[12] *See* Shackelford, S. J. (2019 – 2020) Smart Factories, Dumb Policy: Managing Cybersecurity and Data Privacy Risks in the Industrial Internet of Things. Minnesota Journal of Law, Science and Technology, 21, pp. 1–36.

spans the entire sharing and data storage, where hazardous faults and accidental destruction can inhibit the measure's value. Therefore, it is suggested to comply with straightforward security functionalities under Article 52 of the Regulation (E.U.) 2019/881, such as authentication, permit control, and data availability assessment to secure the chain.

The risk analysis and cost-effectiveness would be realistic by categorizing the Plan-Do-Check-Act cycle conception (Bulgakova, 2023) and developing a target IoT-I product together with its smart grids' legislative governance. These residual risks are suggested to be identified in the IoT-I product functionality together with other smart connections. Also, the end-user shall control the residual risks to dangers assuring complementary protective measures for the data storage and stabile system operation. Necessary warnings directed to the end-user must escort the residual risks where end-users shall carry out cyber-hygiene to underestimate vulnerability. In the view of the authors, the Plan-Do-Check-Act shall consist of a safety strategy depending on the complexity of the IoT-I hardware system and end-user familiarity. The eco infrastructure discussed in the previous paragraph shall provide the end user information on how to carry out start-up, operation, servicing, maintaining, and repairing the IoT-I product, including which of these operations can or cannot be carried out by the end user. Likewise, under contract law, all manufacturers and service providers must deliver their customers the required and appropriate security information. In principle, the information should cover safety aspects for the whole life cycle of the product: device, pack, start-up, functions, maintenance, disassembling, and discarding[13].

The scenario further develops the IoT-I model's information assurance and security aspects, focusing on a sensitivity-sharing toolchain by automation system control. However, an additional legislative framework is needed to implement a set of rules that would address a complete set of security default goals at a hardware level, counting the protection by design. Thus, the authors address the lack of security assessment leaving technical aspects to cybersecurity specialists when all elements that may compromise cybersecurity conditions regarding the intended sharing and any reasonably foreseeable misuse must be covered.

As a next step, the authors explore the integration of the security objectives defined by regulatory conditions within the Regulation (E.U.) 2019/881 Article 51 for better certification and to benefit the cost and efficiency of end-sharing. The specific conditions for a particular model may be deemed a legal concretization of the B2G conflicted IoT-I-data Plan-Do-Check-Act Proposal. Offered incorporated practical tool is generally not so difficult to follow concerning well-known designs and their associated primary risks based on a set of standards devoted. Yet, innovative technology and dependency on check-based procedures raise unique safety aspects that merit legal consideration. Hazards and accidental scenarios may be more

[13] *Note* It shall only be to the extent that is useful or reasonably appropriate for the end-user.

difficult to place, dissect, and evaluate for cycle units or plants. This is especially the case where new materials are in the market, manufacturing operation feedings, or changing outpours. Therefore, it is justified to seek legislative clearance in state-of-the-art measurement.

The research proposes for the mitigation of hazardous and sensitive data fragmentation preferable compliance[14] through consistent reasoning and relative negation of argumentations in the applicable frameworks tailored to offset risks based on the different behavior manufactured needs in terms of the default structure, the designed service of priorities, and the nature of adverse incidents.[15] Authors state that a compliant argumentation would bear time and effort comparatively for the manufacturer but would help encode applicable legislation for end-users to handle the inconsistency, as well as a range of values that may be given based on the intended applications. It is especially relevant in cases when studied legislation is upcoming, and manufacturers are running to adapt new safety control systems encoded in legislation (Annex III to the Proposal for a Regulation on Machinery Products, 2021, at 4.3.1). In this statement, identifying and documenting such dependencies enables to enhancement of stake-sharing risk by control shifting, for example, within command exposure and remediation procedures.[16] The undertakings sector should configure machinery hardware products designed by them to ensure a higher level of security, enabling the end-user to acquire a default configuration with the most safety settings possible, thereby reducing the burden on end-users of having to configure an IoT-I product.

Machinery systems are equipped with native control systems such as a secure out-of-the-box configuration, a signed code, secure update, and heap memory. Those practical control systems tend to be designed at the hardware to implement classically invented (and often conservatively tuned) security loops. It helps handle various automated processes, such as production facilities, that come directly from the manufacturer and work immediately when the product is in service. The problem is that a vast majority of design methodologies load from a full-scale model of an uncontrolled (open-loop) default system, outlasting a complete, multi-variable control system, which does not exploit any knowledge or functionality from

[14] *See* Batsakis, S. et al. ‘Legal Representation and Reasoning in Practice: A Critical Comparison’ in 'Legal Knowledge and Information Systems: JURIX 2018: The Thirty-First Annual Conference', Anonymous Translator, Volume 313, pp. 31-40 (Palmirani, Monica ed., Amsterdam, IOS Press, 2018). doi:10.3233/978-1-61499- 935-5-31.

[15] For example, in a case about Zoomlion Internet of Things exploitation concerning Li Sen, He Limin, Zhang Fengbo, and others about the Destruction of a Computer Information System based on the Circular of the Supreme People's Court that Issued the 20th Batch of Guiding Cases. Promulgator: Supreme People's Court; Effectiveness: Effective; Effective region: National (China); Document no: Fa [2018] No. 347; Effective date: 25 December 2018 issued through discussion by the Judicial Committee of the Supreme People's Court; Judges of the Effective Judgment: Li Fan, Liu Gang, He Lin.

[16] *See* Jespen, Torben. 'Risk Assessments and Safe Machinery: Ensuring compliance with the EU Directives, Anonymous Translator, (Switzerland, Springer, 2016).

novel designs.[17] Thus, it has become sensual to adopt new legislative requirements for performance reasons of hardware. If components or subsystems are newly added to existing systems, the IoT-I, in principle, has to be redone due to the risk of hazardous faults as well as accidental destruction of storage performance and, therefore, requires conformity for the hardware sustainability and its compliance with cybersecurity requirements set in Article 51 (b) of the Regulation (E.U.) 2019/881 about the protection of stored, transmitted, or otherwise processed data against accidental destruction, loss, alteration or lack of availability during the entire life cycle of the I.C.T. product to the IoT-I products relevantly, for the assurance in technical controls decreasing the risk of, and preventing cybersecurity hazard under Article 52 of the mentioned regulation.

Thus, when the new IoT-I products applicable to in the Proposal for a Regulation (E.U.) 2021/0105 on Machinery Products become questionable for placing in the market for its use, it is necessary to enclose the Cybersecurity Act and apply the new control capabilities rather than decommissioning the former control systems and replacing it with the novel constructed (such change may lead to hazardous situations); in that sense, a manufacturer shall prevent modifications to the settings or rules generated by the IoT-I product, where such shifts may lead to hazardous situations of data sharing operation (Annex III to the Proposal for a Regulation on machinery products, 2021, at 1.2.1). Furthermore, from an industrial application-oriented point of view, the ability to switch back to an existing, proven control design in case of unsatisfactory a new one – provides a complex mobility setup compliant preference in practical oscillations to protect against mechanical risks that harm hardware due to exerting excessive strain on its structure (Annex III to the Proposal for a Regulation on machinery products, 2021, at 3.4.1), otherwise, it causes the degradation of sharing performance.

Preferable compliance is also proposed to be viewed from the preferable use of IoT-I yield functionality. A conformity examination about whether specified requirements relating to IoT-I products are fulfilled from an industrial application-oriented point of view would be potential if, on a case-by-case basis, a hazard and usability breakdown leads to the deduction that a set by default is not viable. Thus, by default, cybersecurity should not mandate comprehensive technical understanding on the user's part to work efficiently when executed. Under any circumstances, end-users should be prompted to opt for a secure setting by design. It is, likewise, the ability to switch back to an existing, proven control or more complex design against the unsatisfactory practical operation or application of a safety-critical interlocking circuit control system. Cybersecurity by design should be ensured throughout the hardware lifetime by regularly maturing setup by default and evolution methods to decrease the discussed risks. Therefore, this approach is a significant advantage for a safety-critical interlocking for B2G conflicted IoT-I-data

[17] *See* Chinen, Mark A. (2016) The Co-Evolution of Autonomous Machines and Legal Responsibility, Virginia Journal of Law and Technology, vol. 20/no. 2, 339.

circuit. The research defines the concept of mobility incorporating practical hardware tools to ensure cybersecurity scheme also pursuing a stake-tech capacity for the I.C.T. automatic service system by necessity on specification industry-related area for the preferable backward of remote-controlled IoT-I machinery (Annex III to the Proposal for a Regulation on machinery products, 2021, at 3.6.1, 3.6.3).

Under the European Data Strategy, B2G conflicted IoT-I-data fully or partially evolved to control systems, varying autonomous hardware's capability to use and reuse it. Despite the theoretically large quantity of available data, its sharing requires appropriate protection by default when a fault in the hardware or the logic of the control system does not lead to hazardous situations (Annex III to the Proposal for a Regulation on Machinery Products, 2021, at 1.2.1). Cybersecurity standards, in the view of the study, could prevent hazardous hardware faults and protect it's sharing data storage against integrity loss by an algorithmically conceptual design of IoT-I products that can generate safety boxes of invented B2G data models based on the delivered information. The machinery product shall identify the software installed on it that is necessary for it to share data safely and shall be able to always provide that information in an easily accessible form. In this respect, distinctive software is preferable to be installed (Annex III to the Proposal for a Regulation on Machinery Products, 2021, at 1.1.9). Hardware features with the relevant health and safety requirements shall be designed so, together with software and data that are critical for the sharing due to their sensitivity shall be identified as such. Thus, the IoT-I product shall collect evidence of a legitimate or illegitimate intervention in the hardware component. At the same time, it is proposed that the following B2G conflicted IoT-I-data deficiencies should be indicated in the following areas: data legality, data structuration, data integrity, and data referencing and determination of its source. The planned solutions are expected to provide coordination that will allow vendors to increase the level of data assurance under that cybersecurity scheme.

There is no stable cybersecurity model since even a high level of cybersecurity certification cannot guarantee that the sharing process is entirely secure. Indeed, IoT-I products rely on B2G data sharing on one or more third-party technologies and components such as software modules, libraries, or application programming interfaces. This reliance is a dependency and could pose additional cybersecurity risks as vulnerabilities are found in third-party components. In this regard, the technical setup is slightly error-prone. Applying defeasible deontic logic that is based on presumptions, permissions, and obligations, the cybersecurity scheme for B2G conflicted IoT-I-data is expected to work with specified requirements for the mobility of machinery, focusing on the protection of the hardware integrity for the related data storage safety throughout its sustainable life cycle and responding to the posed risks by default to the criteria of defeasible deontic logic accordingly. The research defends that this tool allows the preferable verities to be used in inferences, ensuring that no form of adverse outcome of eruption is achievable. Indeed, it is impossible to set the cybersecurity scheme compliantly with all sharing processes requirements. For example, due to the lack of some form of attestation of the data inconsistency, hazardous substances are rudimentary for the circumstances where the inconsistency results from mistaken data input. For that reason, addressing inconsistent intake can be helpful, depending on whether the effectiveness is to detect inconsistencies or derive results despite them.

Furthermore, the research weighs in with capabilities integrating the data governance and assurance of performance, risk, and compliance activities across hardware, including technical infrastructure protection and data safeguard that may be subject to B2G data destruction, fragmentation, or integrity loss. In this situation, cybersecurity due diligence is preferable for reviewing the governance, procedures, and safety controls. This helps identify and drive cybersecurity best practices across actors with industrial respect and IoT-I infrastructure protection.

4. The lesson from Taiwan

Government instruments and private companies must reorient their mindset to rectify the oversights made while executing open data agendas. The Taiwanese lesson portrays the shortage of a thoroughgoing privacy-saving plan, the defective privacy shield law, and the governmental and judicial delinquency determining the volume of respective privacy. These facets donate to the elucidative gamble of endless B2G conflicted IoT-I data and surveys as applicable illustrations to sidestep those privacy marks in the Nordic region. Therefore, it is fair to press that state mechanisms and establishments are committed to fending conflicting data they have been assigned and lead exact upkeep toward containing B2G conflicted IoT-I-data. By creating vigorous privacy watchdog means, the administration and private thespians should not merely defend data subjects' solitariness but also cover conceivable litigation menaces stemming from legal fates, as exemplified below in Tsai case (Taipei Administrative High Court, 2014; Supreme Administrative Court, 2017).

A cluster of urbane data regulations is the bedrock of rugged privacy defense, and the legend to a triumphant unclogged data agenda where open data is paramount to boosting data access to Nordic inhabitants, facilities, and companies and can prompt smart city monetary play-by-play sensation, scientific, and corporate accountability (European Data Portal, 2020) for such projects as the NSG&B: *(a)* the safeness of sensitive data, with the numeral shared interests involved, it is far-fetched that Data Act could cover all occurrences. Nonetheless, the enforcement reigns could equip grounds for schoolings in patrolling B2G conflicted IoT-I-data.; (b) de-identification prerequisites that also can be seen in the General Data Protection Regulation known as the GDPR or a Regulation (E.U.) 2016/679 where deidentified data solicit nonnative stations of de-identification for special categories. Which categorises dissimilar data as identified. Nevertheless, the Data Act has a deficiency de-identification instrument for IoT-I-conflicted data to comply with[18]. After yielding with lessened privacy wagers, the reuse of the sensitive data strength is in the table of legalisation. For instance, the GDPR in Article 89 (1) allows data controllers and processors to use personal data for connotations beyond their original collection without obtaining consent from the data subjects if the intention is for public interests

[18] *See* Mike Hintze (2018) *Viewing the GDPR Through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency*, 8 Int'l Data Priv. L. 86, 87.

such as statistical purposes or scientific research. The GDPR questions member states to portray the shared attraction and levies more intricate safeguards. This is extraordinarily required to construct an additional layer of precaution for data subjects in models when public interests are found to trump individual solitude; (c) the privilege of opt-out, likewise, in the United States, the Health Insurance Portability and Accountability Act.[19] And (d) the obscurity of shared inquisitiveness. Hence, the symmetry between shared stakes and individual privacy is a subject admirable of contemplation by lawmakers. Also, concoct grounds, interconnected normal, and different tracks for those who deal with studied data to heed. Even though unrestricted data timetables deliver benefits for IoT-I, these concessions stay shaky if the agendas are executed without specific techniques for privacy safeguard to help offset individual and shared interests that might be a plausible mechanism for the NSG&B regime that rescues data sensitivity. The above thoughts are based on the Taiwanese experience as follows.

The Taiwanese governance has commanded residents, including foreign nationals living there, to be wrapped under the National Health Insurance (TNHI) agenda. As of June 2019, 23,894,289 individuals participated, correlating to 99.9% of the inhabitants (TW, Ministry of Health & Welfare, 2020). For this mission, the oversight power instrument Taiwanese National Health Insurance Administration (TNHIA) together with its branch Ministry of Health and Welfare (TMHW) branch to successfully dispense nationwide health experiences, the TNHIA collect, process, and retain insured patients' and state agents' details.[20] It has taken over the database and evolved into the sole data aid for TNHI that does not demand consent from its data subjects before, during, or after sensitive processing. For data de-identification, the TMHW encrypts it in its locale before pivoting on the Center operation to reduce the crapshoots of data fragmentation (Ho Ming-Syuan et al., 2016). Regardless, eight individuals, including from the Taiwan Association of Human Rights, filed a lawsuit (2012) against the TNHIA due to data sharing from the Center database[21] to third parties, because data was not correctly de-identified, not align with shared interests (Tsai, 2014, at 3, 6). This implies that inhabitants have no opt-out mechanism because individuals have no option to bid about stopping data sharing.[22]

Meanwhile, earlier, the Taiwanese regime has trolled B2G data.[23] Although privacy is not itemized in its Constitution, the Constitutional Court has placed privacy as an implied right safeguarded under Constitution Article 22 to preserve

[19] *See* U.S. Dep't Health & Hum. Serv. (2015) *Guidance Regarding Methods for Deidentification of Protected Health Information following the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*.

[20] *See* JianKang yu YiLiao ZihLiao de JiaJhih YingYong (2012) Cyuanmin Jiankang Baosian Zihliaoku Jianjie, Health and Medical Data Value-Added Application 2: Introduction to the National Health Insurance Database. Available at https://pansci.asia/archives/18437.

[21] *See* more National Health Insurance Research Database, available at: http://nhird.nhri.org.tw/news

[22] *See* Chang Chen-Hung (2018) *Controversy over Information Privacy Arising from Taiwan's National Health Insurance Database*, 40 Chung Yuan Christian Univ. L. Rev. 185, 187.

[23] *See* Mei-Chun Lee & Po-yu Tseng, Open Culture Foundation, Taiwan 2014-2016 Open Government Report 2 (2017). Available at https://opengovreport.ocf.tw/assets/pdf/report-en.pdf

human dignity.[24] Plaintiffs debated that 1) an ordinance should confine the scope of the agent's commitments, 2) if the service discussed data for the shared interest beyond the extent, – these data should be de-identified, 3) no shared interest was affected in the agency's intention, 4) the revelation of the data to third detachments disregarded the data subjects' solitariness (Tsai, 2014, at 3, 6). The TNHIA reacted to shared interest because data had been profitable to break and scholarly periodicals. The suers responded to the absence of ascertaining a forthright tie of the shared interest as well as visibility of poor technical benchmarks of sharing improperly encrypted the subject of conflicting interests of others' data. This safety is vital since a person concerned could be re-identified without reasonable encryption by integrating data reserved in the databases with data stored elsewhere. The TNHIA stands for data safeguarding completion via multiple coatings of encryption to ensure the data's safety and prevent data subjects' re-identification (Tsai, 2017, at 6).

Suers raised the matter due to an opt-out from succeeding data sharing to let data subjects decide to share or not, as well as 'to what extent, at what time, in what manner and to whom, and correct any erroneous entries'. They are also reasoned about the condition for sensitive data to have a command sharing by an opt-out means to request data not be exploited. The argument used on defense is freedom from disfavored intrusion into one's private life and personal autonomy over one's data that are constitutional, not absolute rights; therefore, the state could saddle an individual with unavoidable limitations, when like in a case study, databases contributed to medical studies that benefited all citizens, which was more important than protecting individual privacy[25]. Thus, the case study implies opt-out when data subjects are privileged to ask about data cease (Tsai, 2014, at 4)[26]. However, individuals' privilege to control data might stand rear when their privacy varies with the shared interest. Analysing foreign example, in response to the incapability of unaffected shared interest, the High and the Supreme Courts justified shared interests by establishing that databases count weight to the complainants' data by nursing with shared health matter and need for the research and education to reach the welfare of locals[27].

[24] *See* Taiwan, Judicial Yuan Interpretation № 603 of 28 September 2005.

[25] *See* Interpretation № 689, 2011 53 Judicial Yuan Gazette 11, 11 (Sifayuan Dafaguan Huiyi 29 July 2011), translation available at http://cons.judicial.gov.tw/jcc/enus/jep03/show?expno=689.

[26] *Note* According to Tsai et al. v. National Health Insurance Administration of 2017 the plaintiffs lost their case in the Taipei High Administrative Court because it had been appealed to the Supreme Administrative Court. Furthermore, in 2016, the Supreme Court also oversaw against the plaintiffs, prejudicing the TNHIA.

[27] *See* Tsai, 2014, at 14: "The goal of establishing HWDC is adding value to individual health raw data and thus generating collective data worth putting into an application. This data can also enhance the quality of decisions on public health, academic research, and innovations in health as well as the medical industry, and bring about benefits to all the Taiwanese people ... It is obvious that the data is used for academic purposes and is characterized by public interest."; *see* also Tsai, 2017, at 38: "The macro data on all the citizens' body, health, and medical treatment plays a significant role in the progress of national health and welfare, which also holds great public interests" (Translated).

The High Court determined that factual data de-identification and its necessary sharing by technique slightly tainted to person’s privacy (Tsai, 2014, at 17). Thus, B2G conflicted data seeing valid through compensation between sharing interests based on the model that depends upon pressing B2G sectors. Looking at the experience in Taiwan, the Supreme Court poised the masses’s sharing interests against an individual’s privacy, recognizing B2G data to be a priceless jovial aid, and a comprehensive database to be an essential and worthwhile public good. Respectively, an intermediate prospect that accepts models through compensation or reputational benefits is the practice of volitional data-sharing without necessarily causing it imperative-based to achieve public welfare (ibid.)[28]. Also, the government’s data cluster corresponds to sampling in executing a study emphasizing that ‘in the process of sampling, one needs to be sure the samples could precisely be representative of the original population ... if we allow there are any options for the samples, would severely impact the quality of the samples’ (ibid.).

The Supreme Court expressed reference to when it would be slim to permit the users to opt out of the databases for privacy safe (Tsai, 2014, at 42)[29]. An important concern was raised about the extent of de-identification when the TNHIA lacked about safeguards for cultivated de-identification and only being answerable for handling Taiwanese residents’ health data. By relying on questionable shared interests, the TNHIA ignored viable prospects for protecting privacy subjects. Some scholars acknowledged that anonymisation and de-identification would not be the ultimate assurance of privacy protection. Hereinafter, anonimisation, is the process when data cannot be associated with a specific individual, therefore, an individual cannot be identified or identifiable. Thus, data is not considered personal and does not fall within the scope of GDPR. But could be applicable to achieve irreversible de-identification. Else measures such as encryption for the data process would be relevant by using secret keys to transform it reducing the risk of misuse and keeping confidentially for a given time. Due to needs when the original data must be accessible, the transformation applied by encryption algorithms to make data reversible – decryption. Decryption provokes data to be readable, and consequently, the identification of the person is possible. Another measure is pseudomisation – the processing when sensitive data can no longer be attributed to a specific data subject without the use of additional information. Such extra details are kept apiece and are subject to technical and organizational bars operating to ensure

[28] Tsai, 2014, at 17: “As for thoroughly excluding specific subjects’ data for the reason of respecting individuals’ information privacy, it would exceed reasonableness and even become an obstacle to the realization of public interests ... If allowing the selection of the samples that are gathered, the quality of sampling result would be gravely impacted” (Translated).

[29] Tsai, 2014, at 42: "[I]f a few people were allowed to opt-out of the [sampling], then a majority of individuals could also ask for the same treatment based on the requirement of enforcement equality, which would further bring about the "broken window effect," and result in the unnecessary waste of the cost of data gathering" (Translated).

that sensitive data is not attributed to a pinpointed or identifiable natural person and auxiliary information is used for the identification of the individual. Although data subjects must not be competent of standing identified after the sensitive data is shared, the regulation itself stays imprecise about deidentification criteria and to what proportions deidentification is paramount. As a result, the strength of privacy is uncertain since the law has a gap in technical estimations and relies on the inner approaches of government agendas. Although, the Supreme Court in Taiwan accused data defenders of probable privacy transgressions (Tsai, 2017, at 36). Governments worldwide have opted for boosted privacy safeness that can encourage data-sharing action, likewise, the TW Organization for Economic Cooperation and Development stands for governments' commitment to enrich database safeguards. The Supreme Court roamed in the opposite direction and neglected to urge the B2G regime toward privacy guard priority for sensitive medical data safety sharing. Also, the sharing interest has poorly messed up with public purpose without urbane reasoning of doable bars.[30] Courts erroneously correlated public intent with shared interest likewise in Tsai, 2017, at 36, 37; however, as mentioned in Tsai, 2014, at 16 'If the defendant claimed the measures were adopted for a public purpose, whether for medical research or innovation, the courts assumed that there was a potential public interest'.

Regardless of the above lesson, for privacy safety, such projects as NSG&B shall *(a)* define the deidentification burden; *(b)* offer deidentification for sensitive types of data sets; *(c)* establish an opt-out mechanism; *(d)* introduce evaluation and criteria of shared interest and public purpose when business and government agents must estimate shared interest against individuals' privacy. Thus, a successful B2G conflicted data program should be based on three pillars: (1) a moral pillar when the data publisher should consider the privacy of data subjects; (2) a legal pillar that must respect data protection law; and (3) pragmatically pillar where public confidence must be maintained.

5. Conclusions

The B2G conflicted IoT-I-data is not only a matter related to technology but one where a legal condition is equally important. A stewardship E.U. legal model leads to commitments to build official statements about how the Data Act is highly consistent. The developed IoT-I technology significantly transformed how sensitive B2G data is shared. The distributed reliability depends not only on the calibration of hardware but also on the legal conditions for unintended sharing and system change for a prolonged B2G conflicted IoT-I-data life cycle use respectively. That poses intense challenges in fulfilling high-security standards. A factory of IoT-I products shall

[30] *See* Tsai, 2014, at 18 states that conveying data to third parties was "[f]or scholarly study. Data transfer for academic purposes, and it is for the shared interest."); At the same time, according to Tsai, 2017, at 36 the Supreme Court did not determine what "shared interest" is, and underscores that "the facility of an extensive database is significant for quantitative study."

supersede evaluation workouts with matching outcomes when such an examination is inappropriate. For this reason, a sharing governance model is needed to guarantee sustainability and long-term maintenance of safe data-setting characteristics. These governance norms confine standards and solutions into modules at design time to build complex interconnected hardware outsets and adopt the architectural approach to secure the entire hardware chain by safe data safe settings vision and support its governance along the whole IoT-I system life cycle. Still, it is essential that for B2G conflicted IoT-I-data cybersecurity traceability is considered as the primary artifact to keep track of the overall industrial goals and to link them with the corresponding conceptual indications for both innovators and the end-users. Therefore, authors go along with the legal-technical B2G system welfare eliminating and adequately reducing inherently compliant IoT-I design and confirming cybersecurity assurance about its sustainable hardware functionality and proper system sharing B2G conflicted IoT-I-data control.

The B2G conflicted IoT-I-data model lacks a practical demonstration of legal representation about how businesses can use data sharing approach and safety tools and assure privacy compliance. The research shows compliance can vary, especially when conflicting rules without preferences or conflicting facts are included; particular attention is needed to employ the most appropriate settings and provide the legal encoding that corresponds to the intended end-user depending on machinery's expressive outset and its efficiency. Therefore, a further legislative step is to adopt a B2G conflicted IoT-I-data assessment scheme for IoT-I hardware systems which is expected to protect categorized device functioning through:

1) Site of the market where IoT-I product is placed for operation asset;
2) Material and physical interchange of machinery working operations and end-users;
3) Statuses of data sensitivity on storage shapes.

This research's main contribution is the mitigation of the cybersecurity control problem and its assessment that increases assurance in sustainable life-cycle operation for sharing B2G conflicted IoT-I-data. The study proposes two leading solutions to control problems depending on the available dispatch IoT-I model. The central assumption is that the control laws for B2G data concerning sharing through hardware are suggested to be implemented relevantly to data-driven sensitiveness modeling. The control first step approach is to identify a B2G data set of hardware. The risk is identified straightforwardly when the IoT-I product does not designate dynamics within data sharing. Involving its technique, it is possible to assess the plant model without identifying risk from the subject and without decommissioning the plant to carry out assessment experiments. To that end, observer-based safety is an essential criterion, which can be carried out independently for the distributed IoT-I design. Specifically, a study addresses out-of-the-box configuration, a signed code, secure update, and heap memory measurements to modify inputs to an existing B2G sharing process to improve the hardware's overall performance. The second course relies on parametrizing all stabilizing controllers for a given B2G data-sharing work. This methodology has the advantage that the machinery running functions by affine data motion in the design parameter. It means the design problem has an open-loop-like nature, which can thus measure safety performance during the data sharing switches in the hardware within default functioning relevant to IoT-I products set of conducts. A study does not provide a rigorous comparison of the modes but contrariwise that the sharing control problem in the hardware is feasible in practice, and its preservation could solve data hazards, destruction, and fragmentation, and prevent loss of its integrity.

The second contribution is privacy protection, given the sensitive nature of B2G data and certain impediments to facilitating data sharing and upholding the public interest via medical analysis. Given the sharing approach, this research has proposed that health data is subject to a review process when B2G data is used in a study as long as there is proof that it is for medical research to seek public interest. Thus, for sensitive data research, it is worth assuming whether the wide medical data may be exempted from the classic privacy rules and used for medical examination. Tsai's case reveals how the health data had been safeguarded by an encryption technique and stored in the National Health Insurance Research Database Center in this technique format which does not directly identify a specific person. And, because the risk and possible privacy harm for the key-coded data is moderately low if the data are not re-identified, it is worth reexamining whether it is necessary to apply other requirements to B2G data. This course might not increase the risk of privacy disadvantages and deliver enhanced privacy safety because the re-identification itself augments the risk of privacy disservice. The Tsai lesson benefits as a starting point and basis for NSG&B realisation for emendations to privacy.

Bibliography:

1. Annex III (2021) to the Proposal for a Regulation on Machinery products, C.O.M. (2021) 202 final.
2. Atzori, L., and others (2010) 'The Internet of Things: A Survey, 54 Computer Networks 2787, 2788–90.
3. Bulgakova, D. (2023) The Conformity of Cybersecure Hardware for Machinery Products. Europarättslig Tidskrift, 1/2023, 63–78. URL: https://doi.org/10.53292/c3e75aab.f231956b.
4. Commission (2020) 'A European strategy for data' (n 9) 15 Towards a European strategy on business-to-government data sharing for public interest: Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing (E.U.).
5. Communication (2017) 9 final and Commission, 'Towards a common European data space', Communication (2018) 232 final. The strategy has started to be implemented with the package proposals, including the Data Act.
6. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions (2020) A European strategy for data.
7. Deloitte, Open Evidence, Wik Consult, timeless, Spark, The Lisbon Council (2018) Study to support the review of Directive 2003/98/E.C. on reusing public sector information. URL: https://ec.europa.eu/digital- single-market/en/news/impact-assessment-support-study-revision-public-sector-information-directive.

8. Directive (E.U.) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information, Parliament and Council Directive 2019/1024/E.U. of 20 June 2019 on open data and the reuse of public sector information [2019] OJ L172/56.

9. European Commission (2019) S.M.E. panel consultation on B2B data-sharing principles and guidance – Report on the results. URL: https://ec.europa.eu/digital-single-market/en/news/sme-panel-consultation-b2b-data-sharing.

10. European Commission (2022) Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act).

11. European Commission (2020) Shaping Europe's digital future – Questions and Answers. URL: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_264.

12. European Commission (2017) Synopsis report: Consultation on the 'building a European data economy' initiative.

13. European Commission (2018) Synopsis Report – Consultation: Transformation Health and Care in the Digital Single Market.

14. European Data Portal (2020) *Analytical Report 3: Open Data and Privacy*, at 3.

15. European Data Protection Board (2020) Guidelines 3/2019 on Processing Personal Data through Video Devices, para 74, p. 18.

16. Gaba J. & Estremadura J. (2020) *Data Protection of Biometric Data and Genetic Data,* 64 (3) ATENEO LAW JOURNAL 960.

17. Gurin Joel (2014) Open Data Now: The Secret to Hot Startups, Smart Investing, Savvy Marketing, and Fast Innovation 9.

18. Ho Ming-Syuan, ShuWei ShiDai de YinSi BianJie: Yi JianBao ZiLiaoKu yu E.T.C. JiaoTong ZiLiaoKu WeiLi (2016) The Rights to Privacy in the Digital Age: The Case of the Health Insurance Research Database and the E.T.C. Traffic Database], 3 Taiwan Hum. Rts. J. 1 39, 143.

19. Pailhès, B. (2018) 'How to define and regulate 'data of general interest'?' Enjeux numériques; Richter (n 12) passim.

20. Regulation (E.U.) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and information and communications technology cybersecurity certification and repealing Regulation (E.U.) № 526/2013 (Cybersecurity Act), O.J. L 151/15.

21. The World Bank (2020) 'Unraveling Data's Gordian Knot: Enablers & Safeguards for Trusted Data Sharing in the New Economy.' 25.

22. TW, Ministry of Health & Welfare (2020) National Health Insurance Administration, National Health Insurance 2019-2020 Annual Report, 9.

23. Verhulst, S. G. and Young, A. (2018) 'How the Data That Internet Companies Collect Can Be Used for the Public Good.' Harvard Business Review.

24. World Bank (2021) 'World Development Report 2021: Data for Better Lives', 54 (Washington, DC: World Bank). doi:10.1596/978-1-4648-1600-0

Case study:

25. Taiwan, Tsai et al. v. National Health Insurance Administration (2014) 102 NianDu Su Zi № 36, Taipei GaoDeng XingZheng FaYuan which is a Taipei Administrative High Court.

26. Taiwan, Tsai et al. v. National Health Insurance Administration (2017) 106 NianDu Pan Zi № 54, ZuiGao XingZheng FaYuan which is a Supreme Administrative Court.

СХЕМА ОБМІНУ ДАНИМИ: БІЗНЕС – УРЯД

Дар’я Булгакова,
доктор філософії з міжнародного права,
дослідник, запрошений науковець кафедри права
Уппсальського Університету
orcid.org/0000-0002-8640-3622
dariabulgakova@yahoo.com

Вікторія Ступнік,
педагог-методист вищої категорії,
науковий керівник дослідницьких робіт з історії та права,
викладач
Криворізької гімназії № 91
orcid.org/0009-0006-8953-2477
vikysjakrul@gmail.com

Проблематика. *Цінність Інтернету Речей полягає в механізованому зварюванні, яке обробляє конфіденційні дані в інтерфейсі реального часу. Запропонований Регламент про узгоджені правила справедливого доступу до даних і використання даних, прийнятий Комісією 23 лютого 2022 року, забезпечує бізнес-спроможність для відкритих даних, згенерованих у фабриці системи Інтернету Речей, для учасників процесу по обміну даних для публічних інтересів. Розроблений Інтернет Речей спроектований для керування просторово переміщеними людськими характеристиками, що впливають на відтворення чутливих результатів, і підтримує його фрагментацію. Дослідження визначає цю проблему в законі Європейського Союзу знаного як Акт про Дані, який дозволяє його роботу, захищаючи фактичне позначення безпеки.*

Мета. *Дослідницька стаття має на меті вирішити питання про те, як (чутливі) дані – предмет суперечливих прав інших – можуть бути передані між бізнесом і урядом, уникаючи факторів втрати їх цілісності та досягаючи безпечних налаштувань.*

Методи. *Вирішення проблематики досягається за допомогою заходів, спрямованих на вторинне використання чутливих даних, ілюструючи проєкт Nordic Smart Government (NSG&B). Таким чином, автори відстоюють подібні до скандинавських транскордонні форми обміну даними, використання яких залежить від суперечливих прав інших, і, в той же час, просувають методи по запобігання інцидентам, пов’язаними з передуючим процесом підготовки щодо передачі даних публічно. Тим самим автори роблять вклад шляхом виокремлення надійних умов обміну даними між бізнесом і урядом. Для підтвердження авторської позиції, стаття представляє дослідницький матеріал Тайванської справи Tsai та інші проти Національної Адміністрації Медичного Страхування 2014 та 2017 років щодо обміну персональними даними про здоров’я, коли головний позивач, Tsai, подав до суду з розгляду адміністративних справ позов на Національну Адміністрацію Медичного Страхування з приводу апелювання дозволу третім сторонам отримувати доступ до бази даних Національного Медичного Страхування з метою дослідження та досягнення спільних інтересів.*

Результати. *Відповідно, на думку авторів, представлена судова практика сприятиме практичній реалізації підходу обміну даними між бізнесом і урядом у рамках подібних проектів, таких як NSG&B.*

Висновки. *Представлене дослідження встановлює ступінь вирішення чутливого характеру обміну даними в рамках IoT продуктів, головним чином в контексті відносин B2G. Автори пропонують регуляторні умови, які надають пріоритет безпеці даних, цілісності та стримуванню інцидентів, а також виокремлюють потенційні наслідки для політики та регулювання, значною мірою в Європейському Союзі.*

Ключові слова: B2G, конфіденційні дані, предмет конфлікту прав на дані інших, Інтернет речей, кібербезпека.