УДК 342.1
DOI https://doi.org/10.24144/2788-6018.2022.01.39

THE PROTECTION OF COMMODIFIED DATA IN E-PLATFORMS

Булгакова Д.А.,
доктор філософії з міжнародного права,
науковий дослідник, юрист
ORCID https://orcid.org/0000-0002-8640-3622

Булгакова Д.А. Захист комодифікованих даних на цифрових платформах.

Через великий потік даних, користувач класифікує такі, тим самим обмежуючи себе у кількості переглядів того чи іншого розділу на цифрових платформах. Так як користувач має схильність до неоптимальних рішень, то шляхом перегляду інформації, він нерозбірливо виключає з зору читання тих чи інших цифрових елементів. Під їх категорію підпадають комодифіковані персональні дані, і тому потребують правового захисту. У дослідженні використовується метод пом'якшення правового ризику щодо недостатнього захисту комодифікованих даних на цифрових платформах. Мета статті — знайти спосіб захисту таких даних при використанні електронних платформ. Це важливо, оскільки атрибути користувача, які дозволяють іншим впізнавати один одного, тісно узгоджені з істотою людини, коли ідентифікація можлива за допомогою цих атрибутів. Таким чином, вони є важливими для користувача, а тому необхідний правовий гарантор для захисту. Ключем до цього є правового закріплення положення про те, що особистість користувача цифрових платформ має бути гідною - невідчужуваною. Тому задача данної статті полягає у знаходженні способів захисту даних шляхом реалізації технічних та організаційних гарантій закріплених у статті 25 та recital 78 General Data Protection Regulation.

Концепція Європейського Союзу просуває новий правовий підхід, коли користувачі є утримувачами своїх даних. Це дозволяє їм керувати даними у захищеному, локальному та впорядкованому режимі зберігання, розподіляючи дані за прямим вибором особи. Такими є параметри виконання даних та узгодження їх обробки. Цей метод пом'якшення захищає від незаконних методів профілювання, та є важливими заходами для зниження ризику комодифікації передачі даних. Таке рішення побудовано на основі досвіду таких цифрових платформ як Mydex, NextCloud, MyData Global. Дослідження приходить до висновку про необхідність правового регулювання точності оброблюючих автоматизованим шляхом даних, резервування часу такої обробки та інформативністю користувачів через розвинений дизайн е-кабінету.

Ключові слова: цифрові платформи, користувач, обробка персональних даних, підтвердження особистості, технології підвищення конфіденційності

Bulgakova D. The protection of commodified data in e-platforms.

Using limited information, notably excluding paramount items in e-platforms, the user leads to sub-optimal decisions regarding his/her data to digital commodes. Thus, the study statement: personal data has been commodified. The study uses a method the mitigation of data commodification risk**.** It aims to find a way for data protection when a person uses e-platforms. It is important because user's attributes that allow others to recognize each other are closely aligned with a person's being, and individuals identify themselves through these attributes. As such, they are essential to personhood and warrant protection. The personality of user in e-platforms must be dignity - inalienable.

Based on the GDPR Article 25 and Recital 78, the measure for the data protection is assumed to comply when data systems go along with technical and organizational safeguards. The EU's concept advances a new legal approach where users are holders of their data. It allows them to manage data in secure, local, and online storage orderliness, dispensing it by person's choice. Selves are capable to select settings for data execution and data accord. This mitigation technique acknowledges a human-centric distinction and increased e-platforms for empowered designs. It can also guard against unlawful profiling techniques that strive to circumvent critical measures for the risk mitigation of data commodification. The solution is found aground in the experience of e-platforms such as Mydex, NextCloud, and MyData Global. In this regard, the article defends the digital integrity in e-platforms through data protection by design, informed consent, and the prohibition in e-platforms to consider data - a source of financial gain. The conclusion would remain to go along with data accuracy, time reservation, and user informativeness.

Key words: e-platforms, user, personal data processing, identity proof, privacy-enhancing technologies

Introduction

Emerging technologies are a crucial tool for personal data processing in the era of big data. A user is a person that sourced personal data through the capabilities of a digital cabinet thereof. While a person has obtained an authorization through the digital confirmation of the user's identity, stakeholders of digital service are confident that a particular user is a legitimate one for a network platform. At the same time, users are convinced about legitimate personal capacity. In this context, the article is considered parties involved on behalf of stakeholders of the digital platforms that modulate secure and protected capabilities for the platform data system and users on the one hand.

The regulation of legal relationships between mentioned parties has considered the 'Your Europe' approach [21, Recital 14]. It stimulates the interaction of extensive data between citizens and businesses [21, Recital 5]. It ensures uniform implementation based on the gateway conditions [21, Recital 58]. The respect for fundamental rights is in line with the Charter of Fundamental Rights of the European Union [21, Recital 75]. In contrast, user-centric and user-friendly practices compensate for digital platforms' commodification risk [21, Recital 13]. In 2020 EU presented 'A European strategy for data' with an intention to excellence and trust and foundation of a sole European Data Space, promoting peaceful technological expansion and footprint reproduction in the digital economy [22, Article 58 (3) (c)].

Statement of the Problem

Personal digital identity becomes challenging for a network platform usage. For example, social security numbers have become trendy, and they were not understood initially as the means of identifier. As soon as the government and private sectors recognized them [11, p. 69], the network footage required a person's e-recognition. It is crucial because an authorization operation processes personal data. It creates a risk of obtaining by stakeholders of the e-platform selected data to be commodified for goods exchange.

Given that the private sector spurred the commodification of social security numbers, the extensive commercial e-industry, similarly to the example provided, managed personal data by employing automotive processing. In that way, stakeholders exchange data for goods and services without the knowledge of the individuals [18, p. 842]. Therefore, the processed data is the source of commercial gain and commodification of users' identities in e-platforms. Likewise, the builders of the Titanic were so confident of its stability that they did not have enough lifeboats when the ship sank [15, p. 201]. Compared with the Titanic Phenomenon, the human-centric strategy's breach happens when proponents view the technology as infallible. Data systems will fail, and there will not be adequate safeguards [15, p. 201]. Thus, how individuals can control personal data flow is uptime. In March 2019, a Eurobarometer survey showed that 51% of the respondents observed solely unfair control over, while 30% supposed that they were out of control at all. Just 14% deemed they were in complete control.

Main body

Commodified personal data is a public benefit [6, p. 743]. Commodification inefficient exclude others from data access. It is costly to use and transfer. Nevertheless, personal data is a personhood component because the processing attributes are detachable to personal e-identity. Personal data is a part of human beings of black box society.

On the other hand, providing personal data to e-platforms, the processing does not preclude a user from sharing this data. It makes personal data freely available to the public, and the fundamental right established in the CFREU Article 3 (c) for the security allocation is prior. Cryptographic capabilities created guarantees for the authenticity of a user and relied on the authorized and sanctioned remembrance periods carrying confidentiality and uprightness of repositories. Applying cryptography measures, the moderation of the interference is running the anonymization process.

To explain the data commodification problem and lack of safeguards, the economic theory of non-market behavior is another relation. The source of digital data commodification gain is concerned with efficiency. This statement is proposed based on the efficiency definition of a voluntary market transaction where the legitimate interest of both parties is beneficial from the transaction [4, 152]. Moreover, by creating a metaphorical market of denial and deprivation of fundamental rights, the autonomous person is constituted as an individual of an established state of inequality among human beings [13, p. 13], where everything becomes a market transaction [17, p. 678]. This approach treats human attributes, relationships, and social interactions as commodities. Due to the digital challenges, processing data becomes a tradable good. In that way, an article plurally defines data. It is a non-material bit, a material part of a person, and a value with a price. For user has oriented the system of voluntary data transfers as presumptively efficient to characterize personal data sufficiently to salable or tradable value [18, p. 845]. In the view of the article, it creates a data market where a person is

a source of e-attributes and e-identities. Because personal data processing is a will of the parties involved, the economic theory supports this sourcing as long as its leads to efficient outcomes [8, p. 59]. Therefore, when big data fails, as any market is, intervention with the law is necessary to remedy misaligned incentives. It is creating a legal reconsideration of a personal digital identity costly to preceding individual capacity in the black box society. Hence, personal data processing suffers from market failure persisting the Titanic Phenomenon.

In the view of the article, it is possible to mitigate regardless of the subsequent findings. The EU's Personal Information Management System (hereinafter referred to as 'PIMS') is a step forward. Together with a Personal Data Cloud Identification [23], users of PIMS able to have self-control over personal data processing based on the data protection by design. By doing so, PIMS promotes a novel legal call for an autonomous online identity. This innovation advanced self-operation and personal data management capability. It allows users to control personal data processing contained in the cloud server orderliness. Also, individuals have the capacity to the settings changes and execution and dispense of data system process. Essential, extra elements of PIMS focused on data storage and data transfer. It ensures data safeguard based on organizational measures for a secure run of e-platforms through applications of interoperable and portable cores. Data is shielded because the processing varies on freewheeling service software (SaaS) treated as Application Programming Interfaces (API). That interplay grants the capacity to admit and deny access to an ad-hoc postulate accordingly.

Solution

Legislators protecting data commodified in e-platforms need to prevent the Titanic Phenomenon by implementing an ecosystem for data processing. Progressively is the experience of the Mydex smart entitlement that offers a portable and, at the same time, interoperable online identifier. Verified activities and records are protected when, for example, users and co-providers would need to authenticate a data storage center. It ascertains the facilitation of individuals to hunt back false data processing. Also, individuals can customize the types of data they want to assign and with whom. Users are able to delete comprehensive information. NextCloud's content collaboration platform contributed to the data protection commodified in e-platform because it empowers cloud sets of assigning files beyond various NextCloud servers. In that way, the processing of users' commodified data is protected. A user can access processed data through a personal online data storage secured by compatible apps. In the view of the study, it creates decentralized personal data flow. It means that data is secure. MyData Global's e-platforming vision demands big data to consolidate the automotive data processing ecosystem by defending the grant for individuals to self-determination. However, in the view of the article, mentioned appliances are not correctly conceived, especially when a user is not enabled to run personal digital identity or when a user is ignorantly determined. In this context, the study recommends legally specifying the data processing period in e-platforms.

The next step forward is traceability mitigation of dashboards. In the view of the article, traceability could be an extra measure designed to ensure data protection from unauthorized processing, accidental processing, or errored modification. The implementation shall rely on privacy-enhancing technologies (PET). It is needed because human nature only pays attention to a limited number of things but ignores inconspicuous items. Even if the hidden items' shrouded attributes are vital, humans may ignore and detriment them [10, p. 1846]. A person may not see or not consider factors whether data was stored or disclosed. Even if not ignoring shrouded costs/benefits, humans may undervalue them or fail to recognize them. Those errors are needed to be subjected to PET because individuals have difficulty manually processing all the relevant information, and therefore, they rely on simplified models. Thus, the PET environment is a trusted domain for personal data processing, homomorphic encryption, and multiparty computation of differential privacy.

Moreover, e-platforms reserve the right to change their policy or terms. The task shall focus on its accurate explanation to its users. Hence, when an e-platform decides to utilize a data system due to its breach, the interest of enrolling users can be unjustified and harmed. Therefore, due to the need for security measures to reduce fraud, e-platforms have a right to run down users' data. In this circumstance, the company fails to consider the cost imposed on its users when the company's force relies on vulnerable and irreplaceable measures [12, p. 838]. Thus, the user bears the cost, which is external to the company. This cost has become dominant when unique identification has become actual for automatic online identity proof. Biometric attributes allow recognizing a user as a particular person aligns with a person's capacity in e-partnerships. Indeed, substantive human characteristics shall be dignity inalienable. An article thinks a person may decide on his own will the disposal. Therefore, for users, identity proof is questionable because '[S]ome people

might not feel comfortable that you are taking their body features and that you are making their body algorithmic […], It can humiliate people' [24, p. 43]. Unique identity proof is practiced by e-platforms legitimate only when there is genuine respect for human dignity. It is important to be justified because the use of biometrics by the commercial sector for various purposes creates human monetization [18, p. 864]. Otherwise, it makes a disproportionate correlation with the biological nature of human origin. The article supports data minimization because it promotes the implementation of a processing scope for e-platforms. The frame includes only those bits of personal data that could avoid the absolute identity proof of the person concerned in the process of unique recognition and, at the same time, could be enough to verify a user concerned personhood.

Conclusion

In the law theory, people are related to each other as natural members of a whole, whereas individuals are entirely independent of one another. Human-centric distinction increased the design of e-platforms guarded to face commodified techniques and circumvent legal guardians.

Black box society is intelligent. Therefore, the legal implementation of the ecosystem for e-platforms focuses on data breach prevention through the postulation of norms about the realization of technical and organizational measures established in GDPR Article 25, secure access to commodified data, and specify the procedure of how to administer it.

As more e-platforms implement unique identity proof, individuals will be left with fewer choices regarding the 'must' enrolling biometric characteristics as a security method. However, bearing in mind the Titanic Phenomenon, biometric recognition will fail, and therefore, the neglection of human dignity cannot be allowed in principle; otherwise, it leads to reconstructing an individual's personhood to the commodified credentials of affection.

REFERENCES:

Academical Framework

1. Cherry, A. (2013). Cyber commodification. *Maryland Law Review,* 72 (2), 381-451. [in English].
2. Diega, L. & Noto, G. (2018). Against the Dehumanisation of Decision–Making. *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law,* 9 (3 (1)), 3-34. [in English].
3. Feldman, R. (2003). Considerations on the emerging implementation of biometric technology. *Hastings Communications and Entertainment Journal,* 25(3), 653-682. [in English].
4. Gayer, G., et al. (2014). Pareto Efficiency with Different Beliefs. *Journal of Legal Studies,* 43, S151-S172. [in English].
5. Hirschl, R. & Shachar, A. (2019). Spatial Statism. *International Journal of Constitutional Law,* 17 (2019), 387-438. [in English].
6. Juutilainen, T. (2016). Law-based commodification of private debt. *European Law Journal,* 22 (6), 743-757. [in English].
7. Le Metayer, D. (2016). *Whom to Trust? Using Technology to Enforce Privacy.* In LGTS, Volume 25, Enforcing Privacy. Springer, 395-437 pp. [in English].
8. Lemieux, P. (2020). More Data is Good, but... *Regulation,* 43, 59-61. [in English].
9. Monajemi, M. (2018). Privacy regulation in the age of biometrics deal with a new world order of information. *University of Miami International & Comparative Law Review*, 25 (2), 371-408. [in English].
10. Peerani, A. (2016). The Reasonable Person*, Law Now,* 41 (6), 1837. [in English].
11. Pucket, C. (2009). The Story of the Social Security Number*. Social Security Bulletin,* 69, 55-74. [in English].
12. Rosenbaum, S. (2018). The Irreplaceable Program in an Era of Uncertainty. *Journal of Law, Medicine, and Ethics,* 46 (4), 883-886. [in English].
13. Sangroula, Y. (2014). Bringing People at the Threshold of Development: The State's Unconditional Accountability to Protect Human Rights*. Kathmandu School of Law Review,* 4, 13. [in English].
14. Slokenberga, S. (2021). *Setting the Foundations: Individual Rights, Public Interest, Scientific Research, and Biobanking.* In LGTS, Volume 43, GDPR and Biobanking. Springer, 11-30p. [in English].
15. Solove, D*.* (2011). *Nothing to Hide: The False Tradeoff between Privacy and Security (Thesis)*. George Washington University Law Faculty Publications. [in English].
16. Tamo-Larrieux, A. (2018). *Designing for privacy and Its legal framework. Data Protection by Design and Default for the Internet of Things.* Springer, 254 p. [in English].
17. Todorova, T. (2016). Transaction Costs, Market Failures, and Economic Development. *Journal of Advanced Research in Law and Economics,* 7 (3), 672-684. [in English].
18. Walker, M. (2015). Biometric boom: How the private sector commodifies human characteristics. *Fordham Intellectual Property Media & Entertainment Law Journal*, 25 (3), 831-867. [in English].

Legal Framework

19. Charter of Fundamental Rights of the European Union, OFFICIAL JOURNAL OF THE EUROPEAN UNION C 202/389 (2016/C 202/2).

20. Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and the Free Movement of such Data and Repealing Directive 95/46/EC (GENERAL DATA PROTECTION REGULATION), OFFICIAL JOURNAL OF THE EUROPEAN UNION L 119/1 (2016).
21. Regulation (EU) 2018/1724 of the European Parliament and the Council of 2 October 2018 on the Establishing a Single Digital Gateway to Provide Access Information, to Procedures and Assistance and Problem-Solving Services and Amending Regulation (EU) 1024/2012, OFFICIAL JOURNAL OF THE EUROPEAN UNION L 295/1 (2018).
22. Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices, and Agencies and on the Free Movement of such Data and Repealing Regulation (EC) NO 45/2001 and Decision NO 1247/2002/EC, OFFICIAL JOURNAL OF THE EUROPEAN UNION L 295/39 (2018).
23. European Union Agency for Network and Information Security. Final Report on Privacy and Security in Personal Data Clouds (2016).
24. European Union Agency for Fundamental Rights. Report Freedoms under Watchful Eyes: Biometrics, EU IT Systems, and Fundamental Rights (2018).
25. European Data Protection Supervisor. Opinion 9/2016 on Personal Information Management Systems Towards More User Empowerment in Managing and Processing Personal Data (2016).