Wisniewski, Radosław; Oleksiuk, Inga; Iwanowska, Bożena

Article

Privacy of European citizens in the face of the development of new data-driven business models

Contemporary Economics

Provided in Cooperation with:
University of Finance and Management, Warsaw

Suggested Citation: Wisniewski, Radosław; Oleksiuk, Inga; Iwanowska, Bożena (2021) : Privacy of European citizens in the face of the development of new data-driven business models, Contemporary Economics, ISSN 2300-8814, University of Finance and Management in Warsaw, Faculty of Management and Finance, Warsaw, Vol. 15, Iss. 4, pp. 442-456, https://doi.org/10.5709/ce.1897-9254.459

This Version is available at:
https://hdl.handle.net/10419/297582

Primary submission: 26.06.2021 | Final acceptance: 22.12.2021

Privacy of European Citizens in the Face of the Development of New Data-Driven Business Models

Radosław Wiśniewski, Inga Oleksiuk, and Bożena Iwanowska

ABSTRACT The main objective of the paper is to identify the imbalance between the right to privacy and the business objectives of entities creating new Data-Driven Business Models (DDBMs) of consumers (EU citizens). Information about the consumer and their characteristics has nowadays become a service or market commodity thanks to which new economic processes, based on the use of advanced data processing technologies, are created. In digital space, new types of DDBM are established, which provide entrepreneurs with added value, based on the mass use of the consumer's data collected often without their knowledge, on the margins of legality. This paper analyzes the impact of the development of DDBMs on selected privacy areas: personal data, the right to be forgotten, confidentiality of communications, one's image and identity. In each of these areas, situations are identified that indicate a progressive re-evaluation of citizens' privacy rights. The authors suggest that disruption of the balance between the right to privacy and business objectives may lead to unambiguous consequences, not only for the consumer (EU citizen), but also for the business entities.

KEY WORDS: Data-Driven Business Models, right to privacy, personal information, right to be forgotten, confidentiality of communications, image, identity.

JEL Classification: D18, M2, M13.

University of Economics and Human Sciences in Warsaw, Poland

1. Introduction

Intensive development of new business models of the DDBM type, in the EU and globally, based on the use of data and information about consumers, has become a fact (in this paper the word "data" will be used instead of "information"). Data has become a valuable market commodity. It is obtained not only as part of business processes but also is created in digital space with modern technological tools. For this reason, it is acquired on a large scale from all possible sources and using technology that has not previously been used by humans. In this context, the issue of privacy of EU citizens (in the following part of the work, the term "EU citizen" will be understood as an EU consumer) takes on a completely different dimension in the economic, social, political and, perhaps above all, legal field. The first space defines the need for new business instruments affecting the functioning of consumers in the second and third space, and the latter should provide mechanisms protecting citizens from misuse of their data.

Based on the above observations, the research problem has been defined in this paper. This problem is the diagnosis of the re-evaluation of the right to privacy of EU citizens from the perspective of its use for business purposes. The re-evaluation of the right to privacy of the citizens is aimed, on

Correspondence concerning this article should be addressed to: **Radosław Wiśniewski**, University of Economics and Human Sciences in Warsaw, Okopowa 59 , Warszawa 01-043 Poland.
E-mail: r.wisniewski@vizja.pl

the one hand, at creating space and conditions for the creation of modern tools of the EU digital economy, and on the other hand, at ensuring adequate protection of EU citizens' data. It is worth emphasizing that the process of re-evaluation of the right to privacy should be carried out with the active participation of the legislator (EU, EU Member State), the citizen and the business entity in the area of new technologies.

The research presented concerns economic and legal aspects resulting from the development of business models, based on the data processing of EU citizens in the area of the right to privacy. Economic aspects are analyzed from the perspective of DDBM, and legal aspects in the context of the defined aim of this study which is to reveal and demonstrate the imbalance between the right to privacy and the business objectives of economic operators.

Considering the purpose of the study, the defined object of research and the research problem, the authors have adopted the following research hypothesis: *The right to privacy of EU citizens is appropriated by business processes using new technologies of the 21st century.* This hypothesis will be analyzed using the heuristic method, analysis and logical construction, and individual cases (case studies).

The current study has a synthesizing character and focuses on several problematic issues. In the research of the normative system both formal-dogmatic and functional methods were used. The implementation of both methods is supported by the complex, multidimensional nature of issues related to the protection of privacy of users of digital space, including new media. In addition, the evaluation of law in action makes it possible to show the dynamics of social and economic processes. With the above in mind, key primary materials (regulations and rulings) have been identified and critically analyzed, taking into account the potential of new technologies and the possibilities of applying innovative solutions by European entrepreneurs in this area. Accordingly, Chapter 2 will discuss DDBMs, Chapter 3 will analyse concepts from the area of privacy rights in the context of DDBMs. In Chapter 4, a case-study analysis will be conducted, which will identify areas of privacy rights violations of EU citizens in the context of the operation of DDBMs. The paper concludes in Chapter 5 with a summary of the research and a presentation of the results obtained.

2. Data-Driven Business Models (DDBM)

The business model (BM) is a category of business science and practice claimed by scholars conducting research in both the discipline of economics and management science (Niemczyk & Trzaska, 2020). In both disciplines, the EU citizen, in this case the EU consumer, and the data they hold play a primary causal role. Most business model definitions from research papers published between 2000-2019 capture the BM from the perspective of the resource approach. Even the most popular business model of Osterwalder and Pigneur (2013) refers to key resources, key activities and key partners organized by the criterion of expected value generated for the customer, namely, the elements distinguished in the resource approach (Gorevaya & Khayrullina, 2015; Niemczyk & Trzaska, 2020). Other definitions of a BM point to the creation of value from generated data (Kagermann et al., 2013; Porter & Heppelmann, 2014), and still others to the specific use of a particular, selected type of technology in building value. As classified by Zott et al. (2011), research on BMs generally falls into three major categories:

– e-business and the use of IT in organizations,
– strategic issues – such as value creation, competitive advantage and the performance of a company,
– innovation and technology management.

According to Niemczyk and Trzaska (2020), classifications of business models in the literature can be grouped into four basic groups of models, distinguished by the dominant logic adopted in a given classification. The study by Niemczyk and Trzaska (2020) adopted classifications of business models based on:

– data (DDBM),
– product-service systems,
– apparently unscaled actions,
– strategies of modern market competition.

Schroeder (2016) distinguishes five classifications of data-driven business models:

– model for informing business decisions - in this model, data collected internally within the organiza-

 DOI: 10.5709/ce.1897-9254.459

tion helps make decisions,

– data broker model – which is based on monetizing proprietary data by treating it like a product and selling it to others,

– data analytics model as a service – this is a common business model in companies providing analytical services in the sphere of large collections,

– consultancy services model – based on taking full advantage of the benefits of big data,

– tool provider model – focuses on infrastructure and software delivery.

Another classification of data-driven business models (DDBM) is proposed by Levallois (2021). He distinguishes six DDBM models:

– creating data, selling data – Thomson Reuters, Nielsen, Twitter, Meteo France, Orange, ImDB,

– gathering data, selling ads – Facebook, Yahoo, Microsoft, Google, LinkedIn, Twitter,

– gathering data, selling predictive analytics – Tilkee, Visa, PerdPol, InfraTest,

– adding data value to products – Babola, Withings, Nest, Vessyl, Google,

– adding data value to existing services – ABN Amro, KLM Meet & Sit,

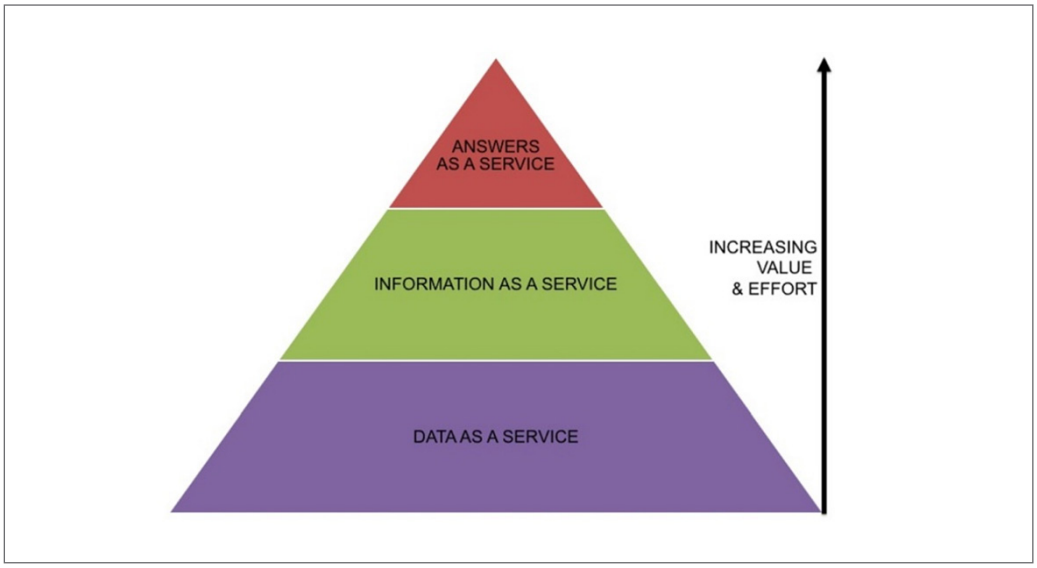
– creating new services enabled by data mining – Uber, Crowd-sourced, Waze, Coyote, MOOCs.

In the sources it is difficult to find classifications of business models based on data resulting from research work. Hence, Niemczyk and Trzaska (2020) used information gleaned from subject blocks that are present on the internet in the form of accessible but non-peer-reviewed knowledge. One proposal for classifying data-driven business models, Niemczyk and Trzaska (2020) constructed as a pyramid of the increase in value delivered and effort required to obtain results (Figure 1). The base of the pyramid is the data as a service (DaaS) model. DaaS focuses on providing ways to extract insights from data. The next level is information as a service (IaaS). IaaS focuses on providing more comprehensive information based on analysis of the processed data. The upper level is answers as a service (AssS). AssS focuses on providing answers to specific questions, rather than just selling information that can be used to get the answer.

All of the classifications presented are based on the substance of these models, namely data. What is missing from the literature are classifications that take into account the aspect of conscious or uncon-

Figure 1

Three Core Data-driven Business Models and the Value they Bring. Source: Lokitz (2021)



Source: Lokitz (2021).

scious interference with privacy rights. In the classifications presented, data is a commodity regardless of who it describes. It is worth noting that these classifications will incorporate aspects of privacy rights in the future.

Today the fastest growing companies have no physical assets. Instead, they create innovative digital products and new data-driven business models (Kotorov, 2020). They capture a huge market share fast and their capitalizations skyrocket. The success of these digital giants is pushing all companies to rethink their business models and to start digitizing their products and services (Kotorov, 2020).

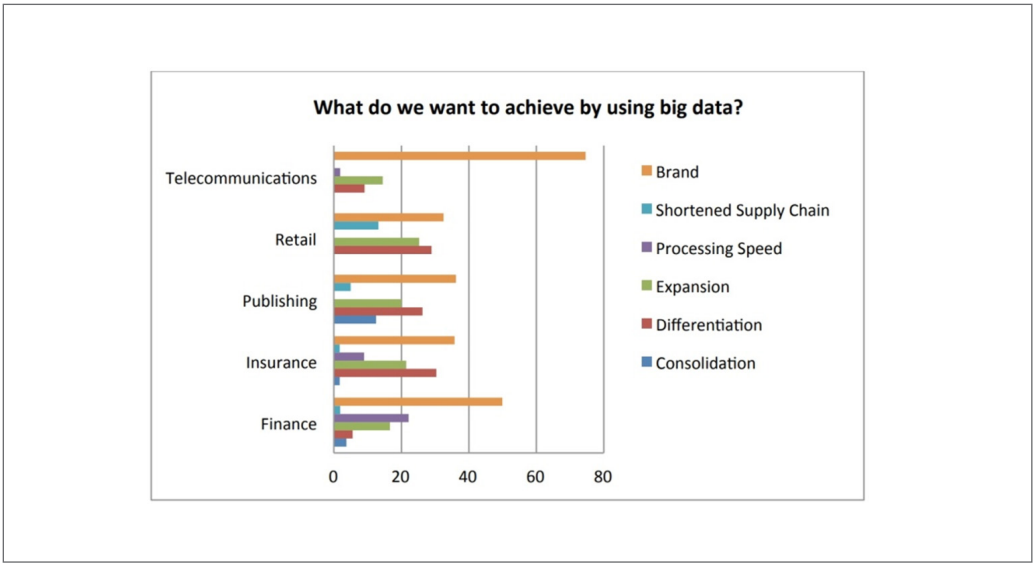
Companies with data-driven business models base their core business on data. This focus, or dependence, on data can affect all dimensions of a business model (Fraunhofer Center for Applied Research, 2021). Added value is generated from data by making data the company's key resource. This means its core activities include data acquisition, data evaluation or data use (Fraunhofer Center for Applied Research, 2021).

Now and in the future, successful business models will be built around data. While data is at the core of all digital business models, the monetization strategies vary across products, services, and business models (Kotorov, 2020). Data-driven business models scale not through asset accumulation and product standardization, but through disaggregation of supply and demand. The winners in the new economy master the demand for one and the supply to millions (Kotorov, 2020).

Data-driven businesses have been demonstrated to have an output and productivity that is 5–6 per cent higher than similar organizations which are not utilizing data-driven processes (Brynjolfsson et al., 2011). Data is obviously fundamental to a DDBM. Deciding which data is most applicable, and the nature of that data's acquisition, is pivotally important to the success of a DDBM construction (Brownlow et al., 2015). Established businesses with a substantial number of customers, and therefore potential customer interaction points, are well positioned to effectively utilize customer-provided data within their DDBM.

Figure 2

Demonstrating What Each Analyzed Sector Wanted to Achieve by Utilizing Big Data



Source: Brownlow et al. (2015).

Customer-provided and acquired data was utilized by 80 per cent of the business organizations analyzed (Brownlow et al., 2015; Hartmann et al., 2016; Pang et al., 2019). As shown in Figure 2, customer-provided data is utilized and regarded as important across all of the analyzed sectors, which is suggestive of established business organizations viewing data as a source of leverage.

The concept of a DDBM is built around data as a product – it lays out benefits for users of data-based services and introduces methods for managing (i.e., promoting, pricing, sale, and delivery) of such products (Bange & Derwisch, 2016).

For years, data has been handled by tech giants – Google, Apple, and Microsoft – and small start-ups that began their business adventure by creating a DDBM. Perhaps the best example of a company's focus on leveraging data are its Mergers and Acquisitions deals (M&A deals), including Google's purchase of Boston Dynamic. In 2013, Google invested in an MIT start-up called Boston Dynamic (BD), looking to build the first humanoid robots together. Over time, it became clear that data would be a more important resource (Niemczyk & Trzaska, 2020).

3. Right to Privacy

The contemporary trends indicated in the previous chapter show that DDBMs are modern and advanced business tools that allow the creation of business processes related to modern economics. It is not without significance that the development of these models depends on technological progress in the area of data acquisition, analysis, processing, and visualization. Another important element conditioning the directions of development of the models in question is the law regulating the rules of collecting, processing, and using data (Regulation (EU) 2016/679).

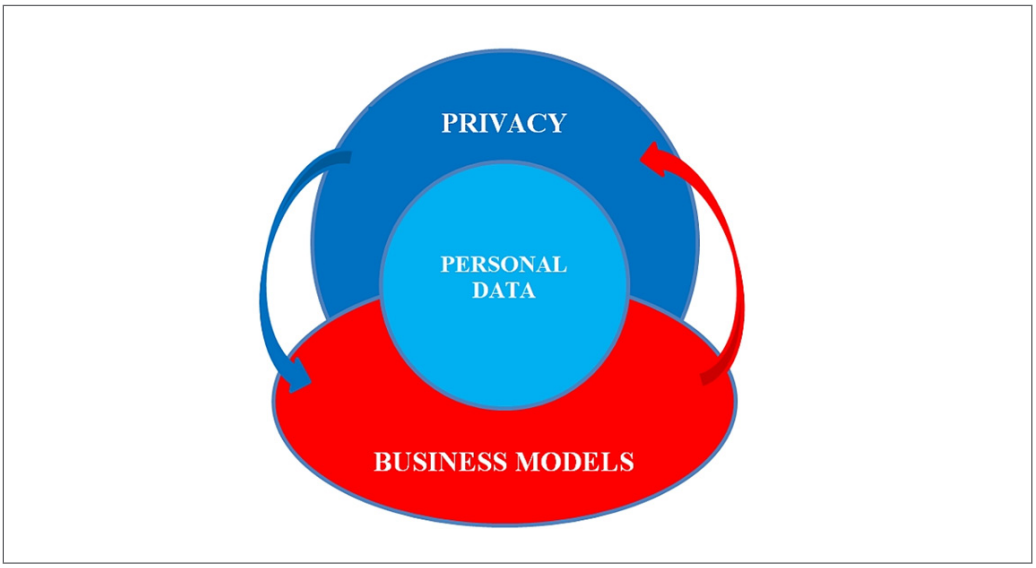
Originally created DDBMs, at the level of the data itself, were non-subject, that is, it was not important who the data concerned. Today, the source of added value beyond the subject level is primarily personal data, namely, the subject level of data in DDBMs. Predatory technological solutions based on innovative algorithms like artificial intelligence have started a far-reaching exploration of the subject level, often without the knowledge and thoughtful consent of the subject whose data is being extracted and processed. Thus, there has been an imbalance between the right to privacy and the business objectives of the operators creating new DDBMs. This balance should be seen in terms of a dynamic equilibrium (Figure 3), and simultaneously from the perspective of the impact of business models on the right to privacy (red arrow in Figure 3) and the impact of the right to privacy on business models (blue arrow in Figure 3). On the one hand, it depends on the analyzed business entity (its power of influence) and the extent and intensity of the interference with the right to privacy. On the other hand, it depends on how the right to privacy is perceived (conservative, pragmatic, developmental, etc.), its position in the system of fundamental rights, the strength of its market impact, and its position and importance in the economic system. Disruption of the balance between the right to privacy and business objectives may lead to negative consequences, not only for the loser, but also for the winner. The latter may lead to a situation in which they themselves will have to repair the damages caused by the unlawful intrusion into one's private life.

Thus, on the one hand, the prevalence of the right to privacy may limit the development of businesses. On the other hand, the predominance of new business models may lead to fundamental changes in the existing state of protection for EU citizens' privacy rights.

According to the classic definition given by S.D. Warren and L.D. Brandeis (19th century), the essence of the normative concept of privacy is the right to be left alone (Warren & Brandeis, 1890). In the sources of the 20th century, an original conception of privacy was presented by A. Kopff, whose view was that it is the right of the individual to live his own life, arranged according to his own will with all outside interference kept to a minimum (Kopff, 1972; Szpunar, 1979; Oleksiuk, 2000).

It should be emphasized that, currently, guaranteeing EU citizens the right to be "left alone" is considered by EU authorities as one of the most difficult regulatory challenges (European Parliament, 2016). As a result of qualitative technological advances, businesses have tools that allow them to identify consumers' views, needs and behaviors as never before. The benefits associated with the use of DDBMs have been described above, and here the authors critically review the issues that are of interest to legal doctrine and have

Figure 3
Privacy and Personal Data Versus Business Model



been or may become the subject of evaluation by the Court of Justice of the European Union (CJEU) and the courts of the EU member countries. In the opinion of the authors, recognizing the legal considerations of the investment in DDBMs is essential for the safety of business entities and consumer confidence.

The first crucial concept rooted in the right to privacy is the concept of personal data. In this context, its legal definition in Article 4 of the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016) should be recalled, according to which personal data means "any information relating to an identified or identifiable natural person ("data subject")". It is noteworthy that the definition of personal data is evolving accordingly. For instance, in Poland, Article 6 of the Personal Data Protection Act of 29 August 1997 (Journal of Laws 2016, item 922) did not initially mention location data and other online identifiers of a citizen. In response to technological advances, these elements were later added (European Data Protection Board [EDPB], 2020; DIGITALEUROPE, 2020)

Currently, personal data includes typical information that identifies legal entities: address, first names, surname, place of birth, parents' names, personal identification number, taxpayer identification number, as well as fingerprints, retina pattern and the above mentioned: location data and internet identifiers. Over the next decade, more sophisticated systems for identifying individuals, such as those using images of the blood system, are expected to become commonplace. These are "biometric data" which constitute a special category of personal data within the meaning of Article 4(14) of the GDPR 2016/679. They result from special technical processing, concern physical, physiological or behavioral characteristics of an individual and enable or confirm the unambiguous identification of that person; these include facial image or dactyloscopic data. "Special technical processing" means the use of such methods and means, the purpose of which is to analyse biometric features which leads to the identification of the natural person on the basis of the analysis carried out. This type of data can only be processed in exceptional cases (Article 9(2), GDPR).

 DOI: 10.5709/ce.1897-9254.459

Considering the above and the pandemic-related changes in the way work is delivered, it is worth noting that measuring working time by means of biometrics has been declared unlawful. Considering the above and the pandemic-related changes in the way work is delivered, it is worth noting that measuring working time by means of biometrics has been declared unlawful (Article 5 Regulation (EU) 2016/679; EDPB, 2020).

This is because an employer, by using an employee's biometric data to record working time, would be in breach of the principles set out in the GDPR (Article 5(1)). In particular, the employer would be processing data contrary to the principles of lawfulness (point a), purpose limitation (point b) and data minimization (point c), as they would not be able to demonstrate why and on what legal basis they were processing employees' biometric data for the purposes of verifying their attendance at work (EDPB, 2020).

Additionally, there can be no voluntary consent in a situation where there is a clear imbalance between the data subject and the controller. Consent given in such a situation will not provide a legal basis for the processing of personal data (Recital 43 of the GDPR).

Keeping in mind, the main topic of analysis, namely, personal data, it would also be necessary to clarify the scope of meaning of the term: "online identifiers." In the light of the GDPR, this includes information such as IP addresses, cookie identifiers and other information generated by internet user devices, applications, tools, and protocols, for example: identifiers generated by RFID tags. Moreover, the internet service providers develop qualitatively new instruments that cause their users to leave electronic footprints. These are data that, in combination with unique identifiers and other information obtained by servers, can be used to create profiles and to identify every individual. Therefore, it is worth mentioning that under current law (GDPR), profiling means any form of automated processing of personal data that involves the use of data to evaluate certain characteristics of an individual, in particular to analyze or forecast their economic situation, health, personal preferences, interests, reliability and behavior, including work performance.

The primary source of these data is online communication. Thus, in the opinion of the authors, it is not necessary for information to be in a structured database or file in order for it to be considered personal data. A review of the judgments of the CJEU leads to the conclusion that a broad interpretation of this concept is applied in the EU. In this context, it is worth recalling the position of the Court on information published on websites. In Lindqvist (2003, p. 25), the Court stated that an operation consisting of posting personal data on a website is to be regarded as "(...) the processing of [personal data]". At the same time, the European Court of Justice took the view that the publisher of source websites containing personal data is the controller "of the processing of personal data within the meaning of the directive. In that status, the publisher is bound by all the obligations which the directive imposes on data controllers".

However, the considerations presented above should be supplemented by the observation that neither the review of the case law nor the doctrine allows for a clear and unambiguous conclusion that each internet address, email address, login or profile name registered by a user of social networking sites constitutes personal data. It is postulated that the subjectivity of (internet) markings under the GDPR should be considered in concreto. For this purpose, it should be determined whether, for example, the internet address enables third parties to identify the given internet user. The above-mentioned indications may be considered on their own or together with other processed information concerning the natural person. To conclude the issues analysed here, it is worth recalling the case Patrick Breyer v Bundesrepublik Deutschland (2016 ref. C-582/14). In the cited case, the Court was asked whether the Internet Protocol address (IP address) that a service provider records in connection with access to its website already constitutes personal data for it when the third party (here: the access provider) has the additional knowledge required to identify the person concerned. In response, it was argued that in specific circumstances, even a variable IP address allows indirect identification of a website user, and therefore IP can be considered personal data. In light of the case law of the CJEU and the Directive implemented in the national legal order, registration of an IP address by a service provider may be considered as the processing of personal data if the service provider is able to identify the user (Regulation (EU) 2016/679).

Studies devoted to the right to privacy, including

the processing of personal data, signal the problem of the right to be forgotten. This issue is related to the analysis of the activities of business entities offering information retrieval services. In fact, one of the most important CJEU judgments in this area concerns the inclusion of personal data in the list of results of an internet search engine. On 13 May 2014, in the case between Google SpainSL and Google Inc. v AgenciaEspañola de Protección de Datos (AEPD) and MariCosteszeGonzález (ref. C-131/12), the CJEU addressed the scope of the right of erasure and/or the right to object, in relation to "the right to be forgotten" ("derecho al olvido") (the case was heard under Directive 95/46/EC of the European Parliament and of the Council). In considering the above issue, the CJEU identified and justified its position on a number of important issues that raised privacy concerns. Taking into consideration the activities of a search engine operator, the CJEU found that if the business entity's activity consists in finding information published or uploaded on the internet by third parties, indexing it automatically, storing such information temporarily, and, finally, making it available to internet users according to a particular order of preference, then it must be considered as "processing of personal data" (Article 2(b)) in cases where that information contains personal data (GonzalezC-131/12, p. 100).

The question of whether "the right to erasure and blocking of data" and "the right to object" should be interpreted as covering the right of the data subject to address search engine operators in order to prevent the indexing of the information concerning them personally that was lawfully published on third parties' websites, was central to the final outcome of this case. The CJEU in the Gonzalez case (C-131/12) confirmed that an individual has the possibility to object to the processing of personal data and to request the erasure of such data. In doing so, it should be emphasized that the CJEU held that a data subject's requests do not require proof of harm to the data subject. It is sufficient that the requests are based on the data subject's will, including that the data subject just wishes to "be forgotten."

The "right to be forgotten" regulation was one of the most controversial legislative issues of the GDPR. It is worth mentioning that the Gonzalez ruling came at a time when the provisions of the GDPR were subject to public consultation. The opponents of the new regulation pointed out that privacy protection resulting from the recognition of the right to object and delete data goes beyond the necessary, justified, and proportionate interference with the freedom of internet users. The following were mentioned as competing goods: freedom of expression, right to information, and the economic freedom of providers of content or online services. Representatives of these actors showed that guaranteeing internet users the right to be forgotten poses a threat to DDBM-type business models based on the use of personal data for advertising and analytical purposes. Representatives of data operators and controllers point out that guaranteeing internet users the right to be forgotten may pose a threat to DDBM-type business models based on the use of personal data for advertising and analytical purposes (DIGITALEUROPE, 2020; CJEU 2019; Google v. CNIL, C-507/17, p. 59; Walker, 2017).

Although "the right to be forgotten" is currently subject to supranational and national regulation, the level of protection varies (EDPB, 2019; Google v. CNIL, 2019 C-507/17).The aforementioned right corresponds to the obligation of data controllers to apply an internal procedure to exercise the rights of data subjects (The de-referencing right). However, in a recent judgment the CJEU (C-507/17) has recognized that there is no obligation under EU law, for a search engine operator who grants a request for de-referencing to apply it for countries outside the EU (Google, 2021; EDPB, 2021).

Another important aspect of privacy protection on the internet is the confidentiality of communications. Bearing in mind the obligation of the legislator to protect the autonomy of the individual against undue interference by business, the EU member states ensure, through national legislation, the confidentiality of communications and related traffic data through publicly available communications networks and publicly available electronic communications services (European Union, 2012 [Art. 7, 8 of the Charter of Fundamental Rights of the European Union]). In particular, the EU member states shall prohibit listening, recording, storing, or otherwise intercepting or surveillance of communications and related traffic data without the consent of concerned users. Confidentiality of communications is subject to exceptions specified by law.

 DOI: 10.5709/ce.1897-9254.459

The challenge in the application of the regulation specifying the exceptions concerns the premises excluding the unlawfulness of violation of privacy. This issue was analyzed by the CJEU in the case of Ministerio Fiscal (C 207/16). In this ruling, the Court decided that criminal offences that are not of a particularly serious nature may justify access to personal data retained by providers of electronic communications services, as long as such access does not cause a serious invasion of privacy (CJEU, PR No. 141/18, Luxembourg, 2 October 2018, Judgment in Case C-207/16, Ministerio Fiscal). The cited case concerned the legitimacy of interference by public authorities with the right to privacy. According to the judgment presented, Article 15(1) of the Directive on privacy, in conjunction with Art. 7, 8 of the above-mentioned Charter, must be interpreted narrowly. The access by public authorities to data for the purpose of identifying holders of specific communication devices (such as name, surname and, where applicable, address) results in interference with the fundamental rights of communication devices holders. However, the Court underlined that interference with the fundamental rights guaranteed by the Charter (including the right to privacy) is not such as to make it necessary to limit the access of public authorities to data which identify individuals in so far as this is necessary for the prevention, investigation, detection and prosecution of criminal offences. The case discussed involved SIM cards running in a stolen cell phone.

One's image is another recognized legally protected good, the use of which is important for the development of new business models. The conceptual category discussed (Balcarczyk, 2009, p. 10 et seq.), in accordance with the position presented in the sources, should be understood as the likeness of a specific person (or persons) presented by means of plastic, photographic and other techniques of visual creativity. In the Hannover v. Germany judgment, the CJEU explained that "[A] person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development. It mainly presupposes the individual's right to control the use of that image, including the right to refuse publication thereof…" (Grand Chamber, 7 February 2012, par. 96). According to the authors, the image concerns all physical aspects of a person, which have the ability to identify a particular person, including the voice and distorted image of a person or caricature. The notion of dissemination should be understood as making an image available to the public. Therefore, it is an action which consists in allowing an unspecified (i.e., open) number of people to get acquainted with the image.

The subject of the right discussed is the natural person depicted in the image. As a rule, he/she is entitled to agree for the dissemination of his/her likeness. It means that, according to the general rule, every subject may - without giving a reason - oppose to making his/her image available to an unlimited circle of people.

The consent for dissemination of the image cannot be implied. The opinions presented in the judicial and academic literature (Balcarczyk 2012), according to which the person giving such consent must be fully aware of the circumstances of the publicity of the image, including the form of presenting the image, in connection with an inappropriate form of presenting it or comparing it with other images, should be considered reasonable.

It is rightly admitted in the doctrine that the current regulation does not exhaust all the issues related to the protection of privacy in the scope discussed, for example: facial recognition and biometrics, the problem of creating the image without the consent of the portrayed person, and the use of the image in photomontage.

Bearing in mind the aim of this paper, which is a consideration of the imbalance between the right to privacy and business purposes of economic entities, it is worth paying attention to the consequences of the development and use of facial recognition techniques. With the spread of these methods, the question arises whether the use of photos in which the image of a natural person is recorded can constitute the processing of biometric data. As already indicated above, this is a new and special category of personal data, the collection of which is subject to significant restrictions. In the light of the current law, the vast majority of pictures currently available online do not constitute biometric data. Nevertheless, the possibility cannot be excluded that a specific picture in which the

image of a colleague, employee or student is captured may be considered biometric data; more specifically, the fixation of an image, in digital form, using technical tools that allow the unambiguous identification of a specific natural person. The use of techniques to confirm identity concerns a narrow category of cases. However, technological progress, in particular the development of identification methods using artificial intelligence systems, raises new challenges for lawmakers and law enforcement agencies. The entities using advanced facial recognition techniques collect both data on physical aspects and a number of sensitive data that are integrally related to one's image. Biometrics reveals much more information than one might initially think: there are data on personality, health and emotional states, among others. Biometric data are not only unique in nature (EDPB 2020). Additionally, they can also be immutable over time (for example, fingerprints, or blood systems). This means that the business entity using DDBMs is obliged to provide adequate data security measures, or their activity may cause irreversible consequences for the subjects whose data they are processing. The consequences of losing biometric data can be permanent and the damage impossible to remove. Therefore, their processing is not only beneficial but also involves a high risk of violating the rights and freedoms of individuals (GDPRhub, 2020)

Another important issue related to online privacy and DDBMs is online identity of EU citizens. To clarify the concept of identity in the context of its protection, one can refer to administrative and criminal law. Thus, from the GDPR discussed above, it can be deduced that an identifiable person is a person whose identity can be established, directly or indirectly, on the basis of the personal identification number or one or more factors determining his or her physical, physiological, mental, economic, cultural, or social characteristics. The elements indicated above may constitute a determinant of identity.

In relation to the criminal aspect (identity theft), two important elements should be mentioned: one's image and personal data. The elements indicated serve to individualize and differentiate one person from another, allowing him to be described and confirming his identity (Budyn-Kulik, 2011).

As presented above, the development of marketing, sales and promotional models has led to the creation of technologies that have begun to capture data in ways that are different from those of the past. The demand for data is growing, not only in terms of quantity, but also in terms of the type of data being required. In order to meet this demand (quantitative-qualitative) and due to the development of new technologies (big data, data mining, artificial intelligence, etc.), a kind of game has started between the EU citizen, and the business, which needs data to meet consumer needs. This game takes different forms, from the simplest voluntary data transfer by the consumer, to qualitatively new forms of interference with the right to privacy and acquisition of data without the participation of the citizen. The latter process continues, and modern technologies only strengthen this process. Mass access to innovative applications and social networks enables qualitatively new forms of violations and the development of criminal activity, which threatens the rights of citizens, but also the economic interests of innovative companies. A prominent expression of this is the growing phenomenon of creating false identities, including the use of the image and personal data of real people. Impersonation of someone's identity can cause moral harm, which justifies the recognition of such action as unlawful interference in personal rights, regardless of whether the person interfering in this sphere of rights did so with the intention of causing damage.

Proposals formulated in the sources to supplement or replace the rigor of civil liability with the rigor of criminal liability is a manifestation of changes relating to the principles of the legal system (Budyn-Kulik, 2011). Comprehensive protection of personal rights, including privacy, has been provided for in civil law. However, in case of identity misuse, visual recognition of humans and processing biometric data, it may be necessary to strengthen privacy protection with criminal law instruments. Such a solution would secure further progress and the economic development of the EU.

4. Data-Driven Business Models (DDBMs) vs Right to Privacy

The previous chapters described DDBMs and selected components of EU citizens' privacy rights. In the con-

 DOI: 10.5709/ce.1897-9254.459

texts described, it is appropriate to look at technology companies within the 3 processes of interference with the right to privacy:

1. violations of the balance between the right to privacy and the business objectives of operators using DDBM models,

2. reevaluating the right to privacy from the perspective of business uses and purposes,

3. the appropriation of areas of privacy rights by companies using DDBM models.

These processes were analyzed in the context of the classification of business models proposed by Levallois (2021). Table 1 summarizes six DDBMs and 5 areas of privacy rights: protection of personal data, protection of the right of being forgotten, protection of image, confidentiality of communication, and protection of identity. The evaluation was based on an ordinal scale, where 1 indicates low protection of a given privacy right area, 2 indicates medium protection of a given privacy right area, and 3 indicates high protection of a given privacy right area.

In the above comparison, the lowest protection in all the analyzed areas of the right to privacy was estimated to be for DDBMs of the type "Creating data, selling data" and the type "Gathering data, selling ads". For these models, there was a re-evaluation of the right to privacy from the perspective of its use for business purposes. An asymmetry in favor of DDBM models has emerged. The evaluation of such models also indicates that the balance between the right to privacy and the business objectives of the operators using DDBM models is likely to be disturbed. All of this indicates

Table 1

DDBMs and Five Areas of Privacy Rights

Specification	DDBM type					
	Creating data, selling data	**Gathering data, selling ads**	**Gathering data, selling predictive analytics**	**Adding data value to products**	**Adding data value to existing services**	**Creating new services enabled by data mining**
Protection of personal data	1	1	1	1	2	2
Protection of the right to be forgotten	1	1	2	2	3	3
Protection of image	1	1	1	1	3	3
Communications Confidentiality	2	2	2	2	2	2
Protection of identity	1	1	1	2	2	2
Company using the DDBM	Thomson Reuters, Nielsen, Twitter, Meteo France, Orange, ImDB	Facebook, Yahoo, Microsoft, Google, LinkedIn, Twitter	Tilkee, Visa, PerdPol, InfraTest	Babola, Withings, Nest, Vessyl, Google	ABN Amro, KLM, Meet & Sit	Uber Crowd-source, Waze, Coyote, MOOCs

that entities using data, creating data, selling data and gathering data have appropriated selected portions from particular areas of the right to privacy.

In the case of models such as "Gathering data, selling predictive analytics" and "Adding data value to products", the processes of reevaluating the right to privacy from the perspective of using it for business purposes exists at an average level. The asymmetry observed has a dimension slightly in favor of DDBMs. Companies using such models violate the balance between the right to privacy and business goals at a medium-to-low level. The process of appropriation from particular areas of the right to privacy does occur, but it is not significant.

Models of the type "Adding data value to existing services" and "Creating new services enabled by data mining" belong to the group of models in which the process of re-evaluation of the right to privacy from the perspective of its use for business purposes is justified. There is no asymmetry in favor of DDBMs. Companies using such models do not upset the balance between the right to privacy and business objectives. In this case, the process of appropriation from particular areas of the right to privacy does not occur. It means that these models are a good example of the coexistence of the right to privacy and the goals of business entities using DDBMs.

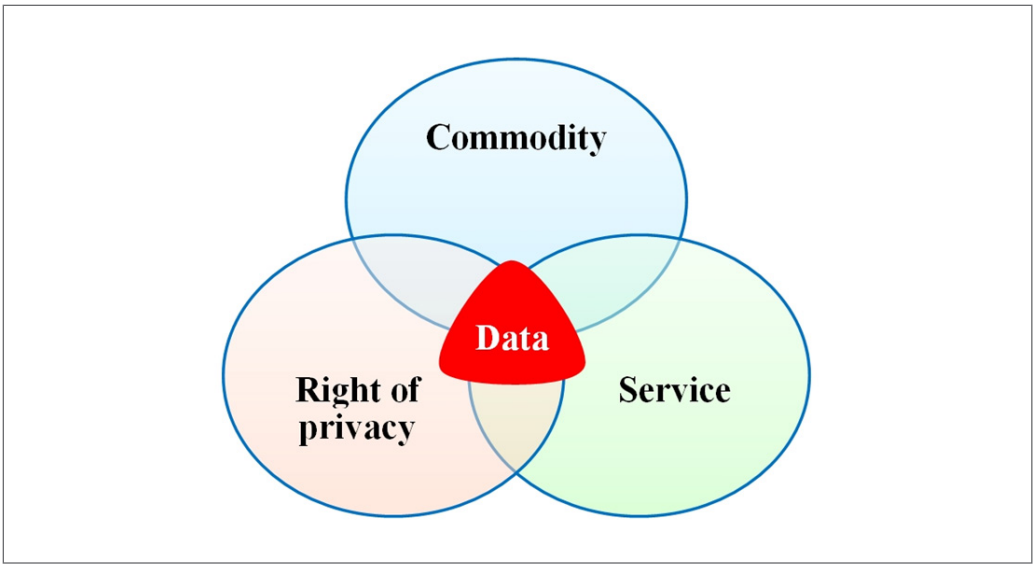
5.Summary and Conclusions

In the light of the studies and analyses presented in this paper, contemporary regulatory challenges to the right to privacy primarily arise from the difficulty of adapting the level and means of legal protection to the opportunities created by new information technology tools (which are part of DDBM-type models). These tools become instruments of violations of the rights of EU citizens. This concerns, in particular, broadly understood notions of privacy, including personal data, confidentiality, one's image and identity.

Entrepreneurs, seeing the enormous opportunities associated with capturing, processing, using, and sharing data, have focused their work on developing tools and technologies that will process data and then create value-added chains from it. Innovative technologies originally relied on data extracted from traditional sources (analog data), often by digitizing datasets. At this stage, the privacy rights of EU citizens (then EEC member states) were guaranteed through legal protection of the content found in analog sources. The next stage of development saw the emergence of digitized sources and digital sources. This moment marked the beginning of a new era, which can be called the DataEra (the

Figure 4

Data as a Commodity, Service, and Right to Privacy



 DOI: 10.5709/ce.1897-9254.459

Data Age). In DataEra, data became a commodity, a service, but also a core component of the right to privacy (Figure 4).

A new beginning in the world of data is also the beginning of a new era in the development of data industry technologies and business models. The data industry is a significant growth industry in many economies around the world. DDBMs have been the right models for emerging and growing data industry companies over the last 2-3 decades. Today, the world's largest corporations are technology giants for whom DDBMs are the primary business models.

However, the development of new IT tools and their business applications cause conflicts of legally protected interests, which require the development of new legal solutions. The key challenge in this regard is to strike a balance between various fundamental rights, such as privacy on the one hand and the freedom to conduct business, including personal data, on the other.

The imbalance between the right to privacy and the business objectives of economic operators (the main focus of the paper) has contributed to changes in the relationship between the EU citizen and the operator acquiring the data. The prevalence of models of the DDBM-type (everyone uses these models) has spurred the beginning of a process of re-evaluation of the right to privacy of EU citizens from the perspective of their use for business purposes. The process of re-evaluation analyzed in this paper results in the conclusion that both positive and negative sides should be noted. The authors of this paper draw attention to the formation of innovative DDBMs, the spread of which is having an increasingly positive impact on the functioning of not only economic entities but also EU citizens. Thanks to these models, the citizens are guaranteed access to a number of services that make their functioning easier, more efficient, and also cheaper.

Thus, it should be emphasized that re-evaluation of the right of privacy is not an categorical phenomenon. It cannot be treated unambiguously only in win-lose terms. Having in mind the developmental goals of the EU, the use of citizens' data cannot be strictly prohibited to economic operators, because without the possibility to create new business models, these operators will not be able to develop. The absolute protection of EU citizens' data is also not beneficial for the citizens themselves, as through such rigorous protection they will not get access to new products that could be created in the development of new business models based on citizens' data. In this case, the imbalance between the right to privacy and the business objectives of the operators is ambiguous in nature (Wisniewski & Brzezicka, 2020). The EU citizen, while sharing data and diminishing the level of his or her privacy rights, can at the same time benefit from innovative business solutions.

Business models based on citizens' data (of the DDBM type) are an indispensable part of the economic development of the European Union. Data is the fuel of one of the future development pillars of the EU - the digital economy. This economy is expected to give the European Union a competitive advantage, provide tools to stimulate economic growth and new taxes, eliminate digital exclusion, create space for technological growth, and much more.

Having in mind the above-mentioned advantages of DDBMs, it should be noted that all activities and aspects of an individual's life can be monitored, documented, captured, extracted, and processed in DDBM-type models and, of course, sold. This situation raises privacy issues, from the perspective of theoretical academic discussions, but also as one of the main problems of civilizational development. It is worth stating that the dynamic discussion of the meaning of this notion has caused the definition of privacy to undergo a fundamental evolution, such that nowadays it covers the following areas:

1. protection of physiological-physical aspects of human beings, including biometrics (related to their active activities): fingerprints, palm and footprints, DNA, health studies, health-related studies, etc.,
2. protection of psycho-physical aspects of a person, including biometrics (not related to their active actions): image in visual form, voice, retinal pattern, body temperature, image of the blood system, etc.,
3. all elements of the inner life: the right to protect thoughts, feelings, emotional states, and even character traits,
4. personal data protection (GDPR),
5. aspects of the protection of personally identifiable digital data relating to assets, commitments, business activities, judgments, decisions, etc.,

6. right to seclusion, solitude, anonymity, confidentiality, etc.,

7. the right to confidentiality of electronic communications,

8. aspects of protecting human geographic location data and the digital location of human-used devices (location used to identify an electronic address for communication between information systems),

9. aspects of protecting one's image and visual recognition,

10. aspects of protecting online identities and digital identities (digital signatures, log-ins, usernames, passwords), aspects of protection of avatars (representation of a person in virtual reality).

Studies and analyses conducted in this area lead to the conclusion that the main area of interest for EU authorities should be the interdisciplinary evaluation and codification of the above-mentioned 10 areas of EU citizens' privacy protection. These actions should aim at balancing the economic freedom of entrepreneurs developing innovative products and services against the EU citizens' right to privacy.

References

Balcarczyk J. (2009). *Prawo do wizerunku i jego komercjalizacja [The right to image and its commercialization]*. Wolters Kluwer Polska.

Balcarczyk J. (2012) *Rights of personality in the XXI century. New values, rules, technologies*. Wolters Kluwer Business.

Bange, C. & Derwisch, S. (2016). *Building data products to realize data-driven business models*. http://blog-sap.com/analytics/2016/11/21/building-data-products-to-realize-data driven-business-models

Braucher, J. (2000). Delayed disclosure in consumer e-commerce as an unfair and deceptive practice. *Wayne L. Rev., 46,* 1805-200. https://heinonline.org/HOL/LandingPage?handle=hein.journals/waynlr46&div=58&id=&page.

Brownlow, J., Zaki, M., Neely, A. & Urmetzer, F. (2015). *Data and analytics – data-driven business models: A blueprint for innovation*. University of Cambridge.

Brynjolfsson, E., Mitt, L., & Kim, H. (2011). *Strength in numbers: How does data-driven decision making affect firm performance?* Social science research network paper.

Budyn-Kulik, M. (2011). *Komentarz do przepisu art. 190a k.k. [Commentary to the provision of Article 190a of the Criminal Code]*. LEX/el, vol. 15-16.

DIGITALEUROPE. (2020). Response to draft EDPB Guidelines on the right to be forgotten in search engine cases [Policy paper 5 February 2020]. https://www.digitaleurope.org/wp/wp-content/uploads/2020/02/Response-to-draft-EP-DB-guidelines-on-RTBF-in-search-engine-cases.pdf

European Data Protection Board. (2019). The European Data Protection Board Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1). https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en .

European Data Protection Board. (2020). *The state of biometrics update from the European Data Protection Supervisor*. https:// edps.europa.eu/sites/default/files/publication/20-10- 07_edps_biometrics_speech_en.pdf

European Union. (2012*). Charter of fundamental rights of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=PL

Fraunhofer Center for Applied Research on Supply Chain Services SCS. (2021). *Data-driven business model*. https://www.scs.fraunhofer.de/en/research/data-driven-business-models.html

Google. (n.d.) Right to be forgotten overview. https://support.google.com/legal/answer/10769224?hl=en

Gorevaya, E., & Khayrullina, M. (2015). Evolution of business models: past and present trends. *Procedia Economics and Finance, 27*, 344–350.

GDPRhub. (2020). Decision of the Office for Personal Data Protection ZSZZS.440.768.2018. https://gdprhub.eu/index.php?title=UODO_-_ZSZZS.440.768.2018

Hartmann, P., Zaki, M., Feildman, N. & Neely, A. (2016). Big data for big business? A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations and Production Management, 36*(10), 382-1406, https://doi.org/10.1108/IJOPM-02-2014-0098.

Judgment of the ECJ of 6 November 2003 in Case C 101/01, Bodil Lindqvist.

Judgment of the ECJ of 16 December 2008 in Case C-524/06 Huber.

Judgment of the ECJ of 7 May 2009 in Case C-553/07 Rijkeboer.

Judgment of the ECJ of 19 April 2012 in Case C 461/10

Bonnier Audio and Others.
Judgment of the ECJ (Grand Chamber) of 13 May 2014, C-131/12 - Gonzalez, Google Spain and Google.
Judgment of the ECJ of 19 October 2016 in Case C-582/14, Bundesrepublik Deutschland.
Judgment of the ECJ (Grand Chamber) of 2 October 2018 in Case C-207/16, Ministerio Fiscal.
Judgment of the CJEU of 24 September 2019 in Case C-507/17, Google LLC, successor in law to Google Inc. v CNIL OJ C 347.
Judgment of the The European Court of Human Rights (Grand Chamber) of 7 February 2012 - Applications nos. 40660/08 and 60641/08, Case of Von Hannover v. Germany (no. 2).
Kagermann, H., Helbig, J., Hellinger, A. & Wahlster W. (2013) *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry*. Final report of the Industrie 4.0 Working Group. Forschungsunion. https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf
Kopff, A. (1972). *Koncepcja prawa do intymności i do prywatności życia osobistego [The concept of the right to intimacy and to privacy of personal life]. Studia Cywilistyczne, 20*.
Kotorov, R. (2020). *Data-Driven Business Models for the Digital Economy*. Cab Intl.
Lokitz, J. (2021). *Exploring big data business models & the winning value propositions behind them*. www.businessmodelsinc.com/big-data-business-models/
Levallois, C. (2021). *Six business models based on data*. www.slideshare.net/seinecle/six-business-models-based-on-data
Niemczyk J., & Trzaska R. (2020). *Klasyfikacja modeli biznesowych w Industry 4.0* [Business models classification in Industry 4.0]. In S. Gregorczyk, G. Urbanek (Eds.), *Zarządzanie strategiczne w dobie cyfrowej gospodarki sieciowej* [Strategic management in the digital age of the networked economy]. WUŁ. http://dx.doi.org/10.18778/8220-335-6.17
Oleksiuk I. (2002) Prawo do prywatności w Internecie [Internet privacy]. *Przegląd Ustawodawstwa Gospodarczego, 3,* 11-19
Osterwalder, A. & Pine, I. (2013). *Building of business models*. Alpina Publisher Series.
Pantielieieva, N., Khutorna, M., Lytvynenko, O., & Potapenko, L. (2020). FinTech, RegTech and traditional financial intermediation: Trends and threats for financial stability. In D. Ageyev, T. Radivilova, & N. Kryvinska (Eds.), *Data-centric business and applications. Lecture Notes on Data Engineering and Communications Technologies*. Springer. https://doi.org/10.1007/978-3-030-35649-1_1.
Pang, C., Wang, Q., Li, Y., & Duan, G. (2019). Integrative capability, business model innovation and performance: Contingent effect of business strategy. *European Journal of Innovation Management, 22*(3), 541-561. https://doi.org/10.1108/EJIM-09-2018-0208.
Porter, M. E., & HeppelmannJ. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 64–88.
Rambarran, I.A. (2002). I accept, but do they? ... The need for electronic signature legislation on mainland China. *Pacific McGeorge Global Business & Development Law Journal,(15)*2, 406-436.
Reed, C. (2000). What is a Signature? *The Journal of Information, Law and Technology, 3.* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.
Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (EIDAS regulation) (2014), Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) Corrigendum to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
Schroeder, R. (2016). Big data business models: Challenges and opportunities. *Cogent Social Sciences, 2*(1), 1–15. https://doi.org/10.1080/23311886.2016.1166924
Szpunar, A. (1979). *Ochrona dóbr osobistych [Protection of personal rights]*. PWN.
Walker, K. (2017). Defending access to lawful information at Europe's highest court. https://blog.google/around-the-globe/google-europe/defending-access-lawful-information-europes-highest-court/
Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, *4*(5).
Wisniewski, R. & Brzezicka, J. (2020). Translocality on the real estate market: A new extended approach. *Land Use Policy, 97*, 104731. https://doi.org/10.1016/j.landusepol.2020.104731
Zott, C., Amit, R. & Massa, L. (2011). The business model: recent developments and future research. *Journal of Management, 37*(4), 1019-1042. https://doi.org/10.1177/0149206311406265.