Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2023, Vol. 129, pp. 127–142

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2023.129.8

Data Contracts under Recent Developments of European Law: Novations and Paradoxes

Nataliia Filatova-Bilous

PhD in law, associate professor at the Civil Law Department
of Yaroslav Mudryi National Law University
Pushkinska 77, Kharkiv, Ukraine
Phone: +380667677373
E-mail: filatovaukraine@gmail.com

The article analyses the most recent trends of data regulation in the EU and the peculiarities of data contracts. The latest regulations adopted or proposed in the EU set an access regime for data, which means that there is no exclusive owner of data, and data may be accessed and used by everyone participating in their production. This approach has caused significant changes in Contract Law regulating data contracts. The most prominent changes are the creation of distinct types of data contracts, the dissolution of the concept of privity, the application of unfair contractual clauses to B2B data contracts, and the facilitation of contractual and pre-contractual obligations with administrative sanctions. In the article, all these novations are critically analysed, and the conclusion is made that some of them constitute paradoxes for the classical Contract Law.
Keywords: data, non-personal data, data contracts, data transfer, data flow, access regime for data.

Duomenų perdavimo sutartys pagal naujausius Europos teisės pakeitimus: naujovės ir paradoksai

Straipsnyje analizuojamos naujausios duomenų reguliavimo ES tendencijos ir duomenų sutarčių ypatumai. Naujausiuose ES priimtuose ar siūlomuose reglamentuose nustatytas prieigos prie duomenų režimas, o tai reiškia, kad nėra išskirtinio duomenų savininko, o prieiti prie duomenų ir jais naudotis gali visi dalyvaujantys jų gamyboje. Toks požiūris lėmė reikšmingus duomenų sutartis reglamentuojančios sutarčių teisės pokyčius. Ryškiausi pokyčiai yra skirtingų duomenų sutarčių tipų sukūrimas, privatumo sampratos panaikinimas, nesąžiningų sutarčių sąlygų taikymas B2B duomenų sutartims, sutartinių ir ikisutartinių įsipareigojimų palengvinimas taikant administracines sankcijas. Straipsnyje visos šios naujovės yra kritiškai analizuojamos ir daroma išvada, kad kai kurios iš jų yra klasikinės sutarčių teisės paradoksai.
Pagrindiniai žodžiai: duomenys, ne asmens duomenys, duomenų sutartys, duomenų perdavimas, duomenų srautas, prieigos prie duomenų režimas.

This research is part of the Jean Monnet Center of Excellence project European Fundamental Values in Digital Era, 101085385 – EFVDE – ERASMUS-JMO-2022-HEI-TCH-RSCH. The project was funded by the European Union. However, any views and opinions expressed below are those of the author only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.

Received: 23/06/2023. **Accepted:** 13/11/2023

Introduction

Data (both personal and non-personal) are said to be a new fuel of the modern economy. For this reason, the European Union has been making many efforts to develop the law on data which would effectively regulate transfers of data within and outside the Union, on the one hand, and guarantee fundamental human rights, on the other hand. Initially, the EU concentrated on the legislation on personal data, which gave birth to the *General Data Protection Regulation* (GDPR) (Regulation 2016/679). However, the rapid development of the *Internet of Things* (IoT) and other technologies has proven the need to provide an effective and full-fledged regulation on non-personal data as well. In response to claims voiced by IoT developers and other stakeholders, the European Commission issued several communications attempting to find the most consistent approach. Initially starting with the idea to create a kind of property regime for data described in the Communication *Building European Data Economy* (COM(2017) 9 final), in the end, the Commission changed its mind and suggested creating an access regime for data allowing various stakeholders to get access to the data co-generated by them and to use these data (COM(2020) 66 final).

The latter approach has been gradually implemented into the European secondary legislation. The first to come was Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), which allowed the re-use of data held by public sector bodies and set a general prohibition on the creation of exclusive rights for specific data. The next step was the development of the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) (COM/2022/68 final). The Proposal comprehensively deploys the access regime to data for the users of products that obtain, generate, or collect the data. It obliges manufacturers of such products and other persons who hold data (data holders) to make the data available to users and third parties (recipients) at the users' request.

In the light of these legislative developments, the role of contracts for data increases. If no one owns data, but lots of persons have access rights to data, the relationships between them remind a spiderweb of contracts since only contracts in these circumstances can effectively regulate these relationships. Therefore, the load on the contract itself increases, which leads to inevitable changes in the Contract Law regulating contracts for data. Some suggestions about these changes could already be seen in GDPR (especially with regard to contracts with data processors and contracts for the transfer of data to third countries), while others have been shown recently in the Data Governance Act and the Proposal for Data Act. However, besides the European developments in this field, one should not downplay international academic initiatives which have a significant role in determining the direction in which the Contract Law will develop in the near future. The most prominent example is a joint initiative of American and European Law Institutes which gave birth to the Principles of Data Economy (ALI-ELI Principles). The Principles outline various types of contracts for data and provide special rules for each type suggesting basic mechanisms for the way data may be supplied, used, re-used, protected from unauthorised use, etc. Although the Principles do not have regulative power *per se*, they may be used by national legislators as a pattern for creating similar mechanisms and rules in the national legislation. Thus, the provisions suggested in the Principles are worth analysing.

Therefore, this research aims to analyse the changes in Contract Law caused by the recent EU developments on data and data transfers. For this reason, the article is divided into two parts. In Part I, I shall analyse the current approach elaborated in the EU on the regime for data and data transfers within and outside the Union. I explain how this approach has been formed and where it will lead. In Part II, I shall explore the main novations of Contract Law stemming from the current approach to

data. I undertake to prove that some novations turn into true paradoxes for Contract Law owing to their extraordinary nature and dissimilarity with the classical Contract Law and the general Private Law provisions. In the conclusion, I summarise the analysis and point out whether the suggested novations are sufficiently justified.

1. Regimes for data: access regime taking over property regime

In the era of digital economy, data are indisputably a transferable asset. Although, initially, data (especially personal data) were considered an inalienable object which could be attributed only to data subjects, with the development of big tech companies, more and more voices started claiming that data should be attributed to those who have collected, processed, and stored them. In this regard, the manufacturers of the so-called 'smart products' had a significant interest since the data generated while using these products were valuable *per se* and could be bargained for with other manufacturers, software developers, etc. These voices were heard by politicians at the national and European level. Remarkably, some of them suggested even creating a 'Civil Code for Data' setting a property regime for data at the European level (Zimmer, 2017, p. 103).

This and other proposals were displayed in the Communication *Building European Data Economy* (COM(2017) 9 final) which suggested creating a new data producer's right as a right *in rem* for data and giving the persons who invested in the creation of data an opportunity to use and to transfer data to other persons (Aplin, 2017, p. 60).

This approach had apparent rationales – to provide those who have made the most significant contribution to the development of technology and economy clear and precise rights in data. From the legal perspective, it could also be justified. There has never been any general ban on processing someone else's data (even personal data) and transferring these data to other persons (selling, supplying, renting data, etc.). However, this approach has been seriously criticised by many academics and politicians. From the economic perspective, it has been claimed that there has been no persuasive justification for the creation of any property or intellectual property regime for data since such a regime could hardly solve any public good problem, create an economic incentive for the production of data or facilitate the use and trade of data (Hugenholtz, 2017, p. 80). From the legal perspective, the property (or intellectual property) regime has been disputable because of the nature of data. Unlike other assets, which are considered property, data are denoted by a non-rivalrous nature, which does not allow to set the classical Property Law regime over them (Filatova-Bilous, 2022, p. 60). Besides, data can hardly be considered an object of intellectual property since most data are created automatically and do not contain anything original, creative, or innovative, which evidences that most data lack features immanent for IP objects.

Considering the critics, the European Commission later decided to switch to another approach based on the access right to data rather than a property right. In the Communication *Towards a Common European Data Space*, the Commission admitted that stakeholders did not favour the previous approach and that "the crucial question in business-to-business sharing is not so much about ownership, but about how access is organized" (COM(2018) 232 final). Based on this position, the Commission developed the Regulation on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (recently adopted by the European Parliament) and the Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) (COM/2022/68 final).

The Data Governance Act establishes rules regulating only specific issues concerning data flows. In particular, it creates primary conditions under which certain categories of data may be given for reuse by public sector bodies holding these data. According to the Regulation, the public sector bodies

are generally prohibited from entering into contracts that grant exclusive rights to entities other than the parties of such contracts (Article 4(1)) and are obliged to make publicly available the conditions for allowing entities to re-use certain kinds of data (Article 5(1)).

In its turn, the Proposal for Data Act establishes an access regime for a far broader scope of relationships. This approach is well explained in the Preamble to the Proposal which states that "[T]his Regulation should not be interpreted as recognizing or creating any legal basis for the data holder to hold, have access to or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service" (Data Act, para 5). On the contrary, data holders (e.g., manufacturers of various products, software developers, etc.) are deprived of any proprietary rights to data (both personal and non-personal). This is specifically underlined in Article 35 of the Proposal which clarifies that the *sui generis* right does not apply to databases containing data obtained from or generated by using a product or a related service. Thus, data holders do not have any rights under Article 7 of Directive 96/9/EC on the legal protection of databases (Directive 96/9/EC) to the data obtained or generated by using physical components, such as sensors, of a connected product and a related service (Data Act, para 84). Further, in para 6 of the Preamble, the Proposal for Data Act explains the meaning of the access regime, saying that "a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use" (Data Act, para 6). These access and usage rights are attributed to the users of a product or related services, which gives them the possibility to use data (both personal and non-personal) by themselves or to share data with third parties of their choice. In particular, the Proposal obliges data holders to make available to the user the data generated by its use of a product or a related service without undue delay, free of charge, and, where applicable, continuously and in real-time (Data Act, Article 3(1)). Considering personal data, the rights to access and use personal data are also attributed to the users who are data subjects according to the provisions of GDPR (for example, Article 20 of GDPR).

Although the Proposal for Data Act makes special emphasis on the users' access and usage rights, it also grants the same rights to data holders. In particular, it can be seen in Article 4(6) which states that the data holder shall only use any non-personal data generated while using a product or a related service based on a contractual agreement with the user. Considering personal data, data holders are also granted access and usage rights to them, however not under the Proposal of Data Act, but under the provisions of GDPR, which specifically regulates these issues (Data Act, para 30). The primary ground for access to personal data for a data holder is the data subject's consent, which, together with the data holder's offer to give such consent, constitutes an agreement between the user (a data subject) and the data holder.

Therefore, in circumstances when both data holders and users have access rights to data, but none of them have exclusive rights to data, the only instrument which can facilitate fair access to and usage of data by both of them is a contract. From the Private Law perspective, this regime is very unusual. Traditionally, every asset being a plot of competing interests of different persons in Private Law is attributed to one of them under various legal regimes. Material assets are usually attributed to a person under Property Law, which makes this person an owner, while other persons are obliged not to interfere with this right. Assets of the immaterial nature (such as works protected under copyright, patents, etc.) are attributed to a person under IP rights which give this person an exclusive right to these assets and prevent other persons from unauthorised usage. In both cases, a person whose property or IP right is violated can be protected by various non-contractual remedies – by using Tort Law or special remedies (such as vindication to protect the property rights to a material asset). However, if the law does not attribute an asset to anyone but recognises access and usage rights of different categories of persons, it does not guarantee that, in reality, these persons will still have the same possibilities to access to

and to use this asset. On the contrary, as the practice shows, data holders and users are not in an equal position: since data holders are usually rather powerful economic entities, the data generated by users, in fact, are held and controlled by the data holders, while users have very few opportunities to access the data (Data Act, Explanatory Memorandum). Therefore, there needs to be a legal instrument which can balance the positions of the data holders and users and protect their rights and interests in the case of a dispute. The only option in this regard is a contract since other Private Law instruments or remedies (Property, IP, Tort Law, etc.) are not available in this case.

Thus, the load on contracts and Contract Law considering the relationships between data holders and users greatly increases. In circumstances where a contract is the only instrument to balance competing interests and protect violated rights, it must be really effective and powerful. This explains why the laws and bills on data usage (GDPR, Data Governance Act, and Proposal for Data Act) have introduced special provisions concerning contracting for data. Moreover, international academic organisations suggested adopting special legal acts concerning various Private Law issues of data usage and data flow. In particular, American and European Law institutes have been cooperating in preparing a draft of the Principles of Data Economy (ALI-ELI Principles). Remarkably, Contract Law provisions take a vital place in these suggestions. Upon analysing all these laws, bills, and drafts of principles, one can conclude that they have introduced a lot of novations in the field of Contract Law. Some of these novations merely bring some new points to the Contract Law theory, while other novations turn into paradoxes of Contract Law considering their revolutionary nature. In the next section, the main novations and paradoxes shall be analysed.

2. Novations and paradoxes of contract law with respect to bargaining for data

As mentioned in Part One, the shift from the property to the access regime for data has caused significant changes in Contract Law considering contracts for data. Together, these changes constitute new tendencies in Contract Law, the main of which, in the view of the present research, are the following: 1) creation of a separate system and types of contracts for data, which is nevertheless based on the analogy with the classical types of contracts; 2) dissolution of the concept of privity of contracts and the spread of 'virus' contractual terms and conditions; 3) extension of the scope of unfair contractual clauses beyond B2C contracts; 4) facilitation of contractual and pre-contractual obligations with administrative sanctions. In the following subsections, all these tendencies shall be analysed more thoroughly.

2.1. Creation of new types of contracts vs analogies with the traditional types of contracts

There are two basic theories on how contracts should be regulated, considering their application area and the main object. The first one is usually called 'universal' since it suggests that "contract law ought to universally embrace several key principles," and to "create certain substantive rules for all markets" (Davis et al., 2019, p. 678). The other one is called 'particularistic', and it "prescribes different rules of contract law for different markets" (Davis et al., 2019, p. 678). From the very beginning of the debate over rules regulating the bargaining for data, the particularistic approach has obviously been preferred by scholars and by policymakers (Schwartz, 1999, p. 1675; Janger, 2001, p. 1254).

This aspiration to a particularistic approach to data contracts has already been revealed in the provisions of GDPR. The Regulation names several contracts concerning data (e.g., contracts for the

processing of data in Article 28, contracts for the transfer of data to third countries in Chapter V, and others) and sets special provisions for these types of contracts. However, GDPR does not attempt to categorise these contracts in any particular way: it does not name them 'sale contracts', 'lease contracts', or 'contracts for services', but, instead, forms the rules for them, while treating them like special types of contracts. The same approach may be seen in the Data Governance Act and the Proposal for Data Act. In particular, the Data Governance Act mentions "agreements pertaining the re-use of data" (Article 4(1)) and formulates special requirements for these agreements. The Proposal for Data Act sets requirements for contractual terms concerning "the access to and use of data or the liability and remedies for the breach or the termination of data-related obligations" (Article 13(1)). However, neither of these acts attempts to categorise the contracts (agreements) for data that they mention; hence, they leave this issue aside.

This approach is also fully deployed in ALI-ELI Principles. Part II of these Principles is fully dedicated to data contracts, and it contains a number of provisions on various specific types of contracts. In particular, it distinguishes two main groups of contracts: 1) contracts for the supply or sharing of data, and 2) contracts for services with regard to data. The first group of contracts is represented by contracts for the transfer of data (for granting control over particular data to the data recipient), contracts for simple access to data (for granting the recipient access to data on a medium within the supplier's control), contracts for data pooling (under which, two or more parties undertake to share data in a data pool), as well as some other contracts. The second group involves contracts for the processing of data (under which, a processor undertakes to process data on behalf of the controller), data trust contracts (under which data holders empower the data trustee to make certain decisions about the use or onward supply of data), data escrow contracts (allowing to restrain the contracting parties from using data against legal requirements), and data marketplace contracts (under which, the marketplace provider undertakes to facilitate 'matchmaking' between the potential parties to data transactions). For all these contractual structures, the Principles set specific and detailed rules purporting to be self-sufficient and capable of regulating contractual relationships between the persons bargaining for data.

Meanwhile, the Principles do not deny the possibility of applying the classical Contract Law provisions to data contracts. On the contrary, they clarify when and to what extent these provisions can be applied to these contracts. As mentioned in the explanatory note to Principle 6 (Interpretation and Application of Contract Law), the classical rules of Contract Law "may have been drafted with traditional transactions about traditional resources (such as goods or rights) in mind," which is why "when they need to be applied to a data contract, the specificities of data must be taken into account" (Principles, p. 54). In particular, Principle 6 clarifies that, in interpreting and applying the rules and principles of Contract Law, the following factors, among others, should be considered: (a) the fact that data are a combination of (i) physical manifestations on a medium or in a state of being transmitted, and (ii) information recorded; (b) the nature of data as a resource of which there may be multiple copies and which can be used in parallel by various parties for a multitude of different purposes; (c) the fact that data are usually derived from other data, and that the original data set and a multitude of derived data sets that resemble the original data set to a greater or lesser extent may co-exist; (d) the fact that, while the physical location of data storage may change quickly and easily, data are normally utilized by way of remote access, and the physical location of data storage is typically of little importance; and (e) the issue of the high significance of cumulative effects and effects of scale (Principles, p. 53).

However, the issue of applying the Contract Law rules to data contracts does not come down merely to whether the general Contract Law rules may be applied to them. It also encompasses the question of whether provisions regulating specific contracts (such as sales, leasing, services, and other contracts)

may be applied to data contracts. Considering this issue, the Principles contain specific provisions outlining possible analogies between the data contracts and the more traditional types of contracts. In particular, Principle 7 provides criteria for applying certain Contract Law provisions by analogy to contracts for data transfer. As mentioned in the explanatory note to this Principle, "a contract for the transfer of data under which the recipient may use the data for an unlimited period of time will very often have many important characteristics of a sale;" thus, "the closest analogy may often be to the law of sale of goods" (Principles, p. 68). However, if the data contract provides that "the data may be used only for a limited period, the more appropriate analogy may sometimes be the law of lease contracts" (Principles, p. 68). Principle 8 sets rules on contracts for simple access to data and outlines criteria which may help to find an analogy to this contract among the classical contractual structures. The explanatory note to this Principle says that "the closest analogy will often be that of some kind of services contract, the service being to enable the recipient to access the data" (Principles, p. 78).

Thus, the rules proposed for data contracts combine the opposite approaches to regulation. On the one hand, they obviously tend to separate these contracts from other types of contracts and to create a self-sufficient framework for them owing to the specific features of data as the main object of these contracts. On the other hand, they still attempt to outline the criteria that may help apply the Contract Law rules initially drafted for the classical types of contracts, such as sales, lease, service, and other contracts. For this reason, the link between data contracts and the classical types of contracts is still being looked for. These opposing approaches make the current regulation of data contracts rather controversial. Moreover, it is unusual for the traditional Contract Law which has always tended to choose one approach: either to create specific rules for certain contracts, by grouping them separately from any other types of contracts, or else to regulate new types of contracts by analogy with the existing contracts.

2.2. Dissolution of the concept of privity and the spread of 'viral' contractual terms

According to a general rule, a contract is binding only upon its parties (Article 1.3. of UNIDROIT Principles of International Commercial Contracts (UNIDROIT, 2016); Article II.–1:103(1) of the Draft Common Frames of References (Bar, 2009), (French Civil Code; Article 1199). This rule constitutes one of the most fundamental principles (concepts) of Contract Law which is usually called the *principle of privity* (Cafaggi, 2008, p. 495). This principle also means that third persons who are not parties to a contract may not be bound by the contract.

However, considering data contracts, there has been a serious discussion on the need to make them enforceable against third persons. In particular, it has been suggested that "in order to facilitate enforcement [of contracts], it may be useful to make restrictions on use or transfer [of data] binding on third parties to whom data are transferred, regardless of whether they have assented to them" (Van Houweling, 2007, p. 682). Attempts to implement this argument were made for the first time at the legislative level in GDPR. The most prominent example of this implementation is Article 28, setting obligations for data processors. The article says that processing by a processor shall be governed by a contract, and that it obliges controllers to stipulate certain terms in such contracts (e.g., the subject matter and duration of processing, the obligation to process data only on documented instructions from the controller, etc.). Noticeably, it also states that where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or any other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under the Union or the Member State Law.

The same pattern is embodied in the provisions of GDPR concerning data transfers to third countries. Article 46(1, 2) says that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation if the controller or processor has provided the appropriate safeguards which may be provided, in particular, by standard data protection clauses adopted by the Commission. The *Standard Contractual Clauses* (SCC) were approved by the Commission Implementing Decision 2021/914 of 4 June 2021 (Decision 2021/914); they involve provisions concerning onward transfers of data by data importers (i.e., persons who imported data from controllers or processors from the EU Member States). In particular, Clause 8.7 says that the data importer shall not disclose the personal data to a third party located outside the European Union unless the third party is bound or agrees to be bound by these Clauses. Thus, any further transfer of data should be made in compliance with the standard contractual clauses, just like the initial data transfer from the data exporter to the data importer.

Essentially the same approach can be seen in the provisions of the Data Governance Act. In particular, Article 4(10) says that public sector bodies shall transmit non-personal confidential data or data protected by intellectual property rights to a re-user who intends to transfer those data to a third country only if the re-user contractually commits to complying with the obligations imposed under paragraphs 7 and 8 even after the data have been transferred to the third country, and also commits to accepting the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with paragraphs 7 and 8 (Data Governance Act). Obviously, this provision also attempts to make third persons bound by the agreement concluded between public sector bodies and the re-user who has entered a contract with the body.

The analysed provisions do not conflict with the principle of contract privity directly. Instead, they create a kind of a 'viral' ('infectious') contract terms. This method is already known in the contracting practice. The most prominent example of its application is the area of license agreements for open source software. These licenses require the users to make further distributions of the software provided for them under the license on the same terms as the ones deployed in the initial license agreement (Vetter, 2004). Considering data contracts, it works in much the same way. A data recipient is obliged to stipulate in the contracts with the downstream recipients (persons to whom the recipient further transfers the data) the same terms as those contained in the contract between the recipient and a data supplier. This feature helps create a network of contracts maintaining the same level of data protection while maintaining the same guarantees.

Taking the mentioned provisions as a basis, ALI-ELI Principles go even further.

First, they impose an obligation to stipulate certain contract terms in other contracts on all data suppliers and recipients regardless of the data contract type. In Chapter A of Part IV, the Principles provide a list of restrictions on data activities with regard to the rights and interests of third parties. In particular, they restrict data activities if these activities do not comply with contractual limitations enforceable by the protected party (e.g., a contractual restriction for a data processor to transfer data obtained from a data controller) (Principles, p. 186). Principle 32 states that the data recipient obliged to comply with the restrictions on data activities (in particular, with contractual restrictions) shall impose the same restrictions on the downstream recipient(s) of the data. In their turn, the downstream recipients are obliged to do the same if they supply the data to other persons and to take reasonable and appropriate steps (including technical safeguards) to assure that the new recipients and any persons to whom the recipients may supply the data will also comply with those restrictions (Principles, p. 206). Considering the wording of this provision, the obligation to stipulate contractual restrictions in contracts with data recipients relates to all types of data (both personal and non-personal) and to any person who may be considered a data supplier under certain circumstances.

Second, the Principles make contractual restrictions directly binding for third persons, regardless of whether the contracts they have concluded with a data supplier contain these restrictions. In particular, Principle 33 says that where an immediate recipient of data had a duty vis-à-vis its supplier to impose particular terms on a downstream recipient to whom the immediate recipient will supply the data, and where the immediate recipient has complied with that duty but the downstream recipient breaches the terms imposed on it, the initial supplier may proceed directly against the downstream recipient after giving notice to the immediate recipient (Principle, p. 214). In fact, this Principle provides a supplier of data with a remedy of protection of one's rights, which is very unusual from the perspective of the Contract Law: it gives the supplier a right to proceed to a person who is not a party to a contract with the supplier, but who has violated the duties imposed by the viral contractual terms. However, Principle 34 goes even further. This Principle imposes liability even on a downstream recipient who has not been bound by contractual restrictions with either the supplier or the immediate or previous data recipients. In particular, it states that a data activity by the downstream recipient who has received the data from a supplier is wrongful where (i) control by that supplier was wrongful, (ii) the supplier acted wrongfully in passing the data on, or (iii) that the supplier acted wrongfully in failing to impose a duty or restriction on the downstream recipient under Principle 32 that would have excluded the data activity, and the downstream recipient either (a) noticed the wrongfulness on the part of the supplier at the time when the data activity was being conducted, or (b) failed to make such investigation when the data was received as could reasonably be expected under the circumstances. This provision literally means that a downstream data recipient shall comply with contractual restrictions deployed in contracts with any previous data recipients even if these restrictions were not mentioned in the contract with this particular recipient. However, the recipient's interests are also protected: the recipient may be considered liable for the breach of this obligation only if one acted in bad faith (i.e., knew or could have known about the wrongful activity of the supplier).

Thus, the provisions proposed in ALI-ELI Principles demonstrate that the concept of privity is stepped over and, in fact, substituted with a new approach imposing obligations stemming from a data contract even on those data recipients who are not parties to the contract. The wording of the analysed principles resembles the wording of *in rem* remedies traditional for the protection of the classical property rights. In particular, a classical vindication suit is also based on the concept that a lawful owner may claim his property from a person who acquired it in bad faith (knew or could have known that the asset could not be alienated by the alienator). However, there are significant differences when it comes to assets like data. First, this asset is non-rivalrous, which is why it is meaningless to claim it back (the copy will always remain with the unlawful recipient). Second, according to the approach chosen in the EU legislation, data do not belong to anybody but may be used by various persons; thus, no one may be considered as an owner of data. For this reason, ALI-ELI Principles state that the analysed provisions are "essentially of tort law logic and have opted for a rather 'strong' form of third-party liability" (Principles, p. 189). Therefore, the proposed approach is based on the assumption that the breach of a data contract by a third party may lead to tort liability for this party since the breach constitutes sufficient grounds for such liability. In this scenario, a person whose interests and rights stemming from a contract or from the Law may claim for damages from the recipient providing data activities in a bad faith both in the case where one disregards the viral provisions of the contract into which one has entered, and in the case where one is not even bound by contractual obligations but could reasonably be expected to be aware of them.

The provisions and approaches analysed in this section are of such originality that they constitute a true paradox for Contract Law since they blur one of the most fundamental principles – specifically, the

principle of privity. Although they are a logical continuation of the access regime to data proposed in the EU legal acts, there is a need for a special explanation of how they may get along with the already existing concepts of Contract and Private Law.

2.3. Extension of the scope of unfair contractual clauses beyond B2C contracts

The concept of unfair contractual clauses is typical for Consumer Protection Law. For the first time, it got its full-fledged implementation in Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, which provided an indicative list of contract terms that may be considered unfair. In particular, contract terms are unfair if they have an object or an effect of inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier, or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier, requiring any consumer who fails to fulfil his obligation to pay a disproportionately high sum in compensation, etc. (Directive 93/13/ECC, Annex).

According to the general rule set by the Directive, a contract term shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract to the detriment of the consumer. Meanwhile, contract terms may be considered unfair only if they have not been negotiated individually and thus are standard contract terms (Directive 93/13/ECC).

However, the classical Contract Law regulating relationships between peers (B2B, C2C contracts) does not use this concept. There are only exceptional grounds to avoid standard contractual terms or the entire contract based on the disparity of its terms for its parties. In particular, according to the UNIDROIT Principles, standard contract terms are ineffective only if they are surprising for a party (parties), i.e., if they have such a character that the other party could not reasonably have expected them (UNIDROIT, Article 2.1.20). The Principles also allow avoiding a term or an entire contract based on a disparity which is gross: this is a situation where a contract or its term unjustifiably gives the other party an undue advantage (UNIDROIT, Article 3.2.7). Thus, the threshold in both provisions of the UNIDROIT Principles for avoiding or making contract terms ineffective is much higher than the threshold established in Directive 93/13/ ECC for consumer contracts.

Concerning data contracts, the concept of unfair contract terms becomes applicable irrespective of whether the contract is B2C or B2B. This is evidenced by the Proposal for Data Act, which creates separate and detailed provisions on unfair contract terms in B2B contracts. According to Article 13(1) of the Proposal, a contractual term concerning the access to and use of data or the liability and remedies for the breach or the termination of data-related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise shall not be binding on the latter enterprise if it is unfair. Further, the article provides that a contractual term is unfair if it is of such a nature that its use grossly deviates from the good commercial practice in data access and use, contrary to good faith and fair dealing, and lists the criteria when a contractual term is unfair and when it is presumed to be unfair (Article 13(2), (3), (4)). Recital 51 provides an explanation of these rules and the main idea behind them by stating that where one party is in a stronger bargaining position, there is a risk that this party could leverage such a position to the detriment of the other contracting party when negotiating access to data and make access to data commercially less viable and sometimes economically prohibitive. Therefore, unfair contract terms regulating the access to and the use of data or the liability and remedies for the breach or the termination of data-related obligations should not

be binding on micro, small, or medium-sized enterprises when they have been unilaterally imposed on them (Proposal, Recital 51).

Thus, the Proposal extends the scope of the concept of unfair terms, thus making it applicable to the contracts where one of the parties is a SME as defined in Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises (Recommendation 2003/361/EC). The main idea behind it is to protect the interests and rights of a contracting party that is economically weaker since it is an SME and since it does not have an influence on the content of a contract being of a 'take-it-or-leave-it' nature.

The analysed provisions are not typical for B2B regulation, but they still cannot be called extraordinary. On the contrary, they are in line with a general tendency of the recent years in the European secondary legislation to grant protection to a weaker party regardless of whether this party is a consumer or a business. The same features may be found in Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services (Regulation, 2019) regulating the relationships between the providers of online intermediation services (platforms) and their business users. Noticeably, the Regulation imposes obligations on platforms which are typical for consumer protection laws (e.g., the obligation to stipulate the contract terms in plain and intelligible language, to comply with specific formal requirements, etc.), although the scope of the Regulation involves only B2B contracts. In addition to the Regulation, there are other EU legal acts imposing B2C-like rules on parties to B2B contracts, in particular, the *Late Payments Directive* (Directive 2011/7/EU, Article 7) and the *Directive on Unfair Trading Practices in the Agricultural and Food Supply Chain* (Directive (EU) 2019/633).

However, in the Proposal for Data Act, the tendency to enlarge the scope of provisions originating in consumer protection laws to make them applicable to B2B relationships is the strongest and the most obvious. Moreover, this is not surprising considering the nature of data relationships and their peculiarities. In these relationships, usually, these are data holders (manufacturers of smart devices, software developers, etc.) who have very large opportunities and facilities to hold data and to control them and who dictate their conditions and terms to all other participants of data relationships. Initially, there is a substantial inequality between the parties of data contracts, which needs to be fixed somehow by the Law. Therefore, the provisions on unfair terms in the Proposal for Data Act are justified, although they still are very unusual for the Law regulating B2B contracts.

2.4. Facilitation of contractual and pre-contractual obligations with administrative sanctions

Traditionally, the obligations stemming from contracts rely on Private Law remedies and private liability. When a party to a contract violates its contractual obligation, the other party may claim damages and/or a fine from the party in breach. The same scheme works for pre-contractual duties: if the Law recognizes these duties (e.g., under the *culpa in contrahendo* doctrine in Germany) and a party violates them, the injured party may claim damages from the other one (Kessler et al., 1964). Private Law remedies usually also work if parties fail to include certain terms in their contracts when they are essential, and the contract cannot be enforced without them. In some jurisdictions, contracts of this kind are recognized as having never been concluded (for example, in Ukraine (Civil Code of Ukraine, Article 638)); however, unless the contract has been performed or partly performed (see Resolution of Supreme Court from 11 October 2018 in Case 922/189/18).

In the EU, the consequences of the lack of certain contract terms are addressed in sectoral legislation, which usually states that a term that has not been duly stipulated in the contract may not be

enforceable. For example, according to the Consumer Protection Law, if a contract with a consumer lacks the terms determining the price and the other costs, the consumer is not obliged to pay the price and bears no costs (see Article 6(6) of Directive 2011/83/EC).

However, regarding data contracts, the system of remedies is completely different. On top of the traditional Contract Law remedies and liability, the Law provides a system of administrative penalties and procedures. For the first time, this peculiarity was introduced in the GDPR. In parallel to the provisions of Article 82, which allows data subjects to receive compensation from data controllers or data processors, Article 83 dwells on the system of administrative sanctions. In particular, it introduces administrative fines of up to 10,000,000 EUR, or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year for controllers and processors for the breach of Articles 8, 11, 25 to 39, and 42, 43. Meanwhile, Article 28, among the listed, sets requirements for the content of the contracts between controllers and processors and obliges processors to stipulate the same terms in further contracts which they conclude with sub-processors (I have already analysed this provision in Subsection 2.2). Thus, a breach of the provisions of GDPR setting which terms shall be included in data processing contracts leads to administrative sanctions.

The Data Governance Act and the Proposal for Data Act follow in the same vein. In particular, Article 34 of the Data Governance Act obliges the Member States to lay down the rules on penalties applicable to infringements of the obligations stipulated by the Regulation. Among other obligations, the Article lists the obligation of natural and legal persons to whom/which non-personal data were granted to transfer these data to third countries in compliance with certain rules and restrictions. One of such rules (specifically, Article 5(14)) states that non-personal data may be transferred to a third country only if the re-user contractually commits to complying with the obligations imposed by the Regulation after the data have been transferred to the third country and to accepting the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body (Data Governance Act). Thus, the penalties may be applied to persons who transferred non-personal data to entities in third countries if the contract concluded by them does not stipulate the presently mentioned provisions. Therefore, in this case, failure to include some provisions in the data contract leads to the application of administrative penalties.

The Proposal for Data Act goes even further in following this line. Its Article 33(1) contains a broad rule saying that the Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. Thus, the Proposal stipulates setting penalties for violating any obligation laid down by the Proposal. Meanwhile, as mentioned in the previous subsections, the Proposal for Data Act contains a lot of obligations concerning the content of data contracts and obligations stemming from data contracts. In particular, Article 3 lists the information which the data holder shall communicate to the user before the conclusion of the contract (pre-contractual obligations), Article 8(2) obliges data holders to agree with data recipients the terms for making data available to the latter in a contract, Article 13 lays down the criteria by which the terms of data contracts may be considered unfair and thus unenforceable, Article 24 stipulates which terms shall be included into the contracts with data processors concerning switching between providers of data processing services (Proposal). Thus, again, the breach of contractual obligations may lead to administrative sanctions.

The presently discussed approach is not typical for Contract Law. However, it cannot be said to be absolutely unknown in the Modern Law. On the contrary, it seems to become a kind of a trend in the modern European legislation. When commenting on some recent European legal acts (in particular, on the *Digital Services Act* (DSA), scholars outlined that "[they pull] responsibility out of the realm

of liability and into the area of regulation" (Buiten, 2022, p. 363). This phrase describes the modern tendencies in the best way: EU secondary legislation, especially in the field of the data flow and data protection, shifts from a private liability regime to administrative regulation wherever it is possible. As violations in this field may reach a massive scale, Private Law remedies satisfying private interests cannot cope with these violations and thus need to be complemented with remedies that are more effective against violations of this kind, i.e., administrative penalties. However, this does not deny the mere fact that supplementing obligations of a contractual nature with administrative sanctions is highly unusual by its very nature.

Conclusion

The regime created by the European secondary legislation for data transfers and flow is of a rather unusual nature since it does not attribute data to any person taking part in data generation. On the contrary, this regime facilitates access to data and the possibility of using them for persons involved in their production. Under these circumstances, only contracts between these persons can protect their rights and interests.

As a result, data contracts and rules regulating their conclusion and performance become rather unusual from the perspective of the classical Contract Law. In the article, the most prominent examples of originality of these rules have been discussed. As the analysis shows, these examples constitute not only legal novations, but also paradoxes of Contract Law.

One of the most prominent paradoxes is the set of rules imposing contractual obligations on third persons who are not parties to a data contract. Since the privity of the contract is one of the fundamental concepts of Contract Law, this feature is groundbreaking. Thus, it must be carefully analysed to find a sufficient justification. In my opinion, the provisions suggested by the ALI-ELI Principles in this field are eminently revolutionary and lack sufficient grounds to overcome the concept of privity. However, since the access regime created in the EU legislation does not attribute non-personal data to anybody, the other option than to create exceptions from the privity of contracts is hard to find.

Other novations of Contract Law analysed in this article are also rather unusual; however, they cannot be called groundbreaking. They are in line with the most recent tendencies of the European Law (e.g., the application of consumer protection rules to contracts with SMEs and the facilitation of contractual and pre-contractual obligations with administrative sanctions). However, these tendencies *per se* are rather unusual from the perspectives of the classical Contract Law, which has been admitted in the legal literature. Thus, there still is a need for an in-depth analysis of these tendencies together with the newest rules on data contracts in order to find a sufficient explanation and justification for them.

Bibliography

Legal documents

ALI-ELI Principles for a Data Economy - Data Transactions and Data Rights [2021]. URL: https://principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf

Civil Code of Ukraine 2003.

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council C/2021/3972, OJ L 199.

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422) *OJ* L 124.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy" COM(2017) 9 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a common European data space" COM(2018) 232 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European strategy for data COM/2020/66 final.

Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain PE/4/2019/REV/2 *OJ* L 111.

Directive 2011/7/EU of the European Parliament and of the Council of 16 February 2011 on combating late payment in commercial transactions (recast) Text with EEA relevance OJ L 48.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, *Official Journal of the European Union,* L 304/64, 22.11.2011, 64–88.

LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (FR).

Proposal for a Regulation Of The European Parliament And Of The Council on harmonised rules on fair access to and use of data (Data Act) COM/2022/68 final.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) [2022] *OJ* L 152.

Regulation 2019/1150 on promoting fairness and transparency for business users of online intermediation services, Official Journal of the European Union, L 186, 11.07.2019, pp. 57-80.

Regulation of the European Parliament and of the Council 2016/679 of 27 April 2016 on the protection of natural persons 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) [2016] *OJ* 2 119/1.

Resolution of Supreme Court from 11 October 2018 in case 922/189/18. URL: https://reyestr.court.gov.ua/Review/77159136

UNIDROIT Principles 2016.

Special legal literature

von Bar, Ch. (ed) (2009). Principles, definitions and model rules of European private law. Draft Common Frame of Reference (DCFR**) (**Sellier European Law Publ., 2009).

Zimmer, D. (2017). Property Rights Regarding Data? *Trading Data in the Digital Economy: Legal Concepts and Tools*. Nomos Verlag. 100.

Janger, E. J., Schwartz, P. M. (2001). The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules. *MINN. L. REV*., Volume 86, 1219.

Cafaggi, F. (2008). `Contractual Networks and the Small Business Act: Towards European Principles?', *European Review of Contract Law*, Issue 4, 49.

Vetter G. R. (2004). "Infectious" Open Source Software: Spreading Incentives or Promoting Resistance? *Rutgers Law Journal,* Vol. 36. 53.

Kessler, F., Fine, E. (1964). Culpa In Contrahendo, Bargaining In Good Faith, And Freedom Of Contract: A Comparative Study. *Harv. L. Rev*. Volume 77. 401.

Davis, K. E., Marotta-Wurgler, Fl. (2019). Contracting for Personal Data. *Newyork University Law Review.* Volume 94, Number 4, 662.

Buiten, M. C. (2022). The Digital Services Act: From Intermediary Liability to Platform Regulation. *JIPITEC.* Issue 12, 361.

Van Houweling, M. Sh. (2007). The New Servitudes. *GEO. L.J.* 96, 885.

Filatova-Bilous, N. (2022). Data as a Tradeable Commodity: Propertization vs. the Concept of Exclusive Rights. *Teisė*, 124, 55–66. https://doi.org/10.15388/Teise.2022.124.4

Hugenholtz, P. B. (2017). Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? *Trading Data in the Digital Economy: Legal Concepts and Tools* Nomos Verlag 74.

Schwartz, P. M. (1999). Privacy and Democracy in Cyberspace. *VAND. L. REV.* Volume 52 1609.

Purtova, N. (2009). Property Rights in Personal Data: Learning from the American Discourse. *Computer Law & Security Review,* 25(6), 507. https://doi.org/10.1016/j.clsr.2009.09.004

Aplin, T. (2017). Trading Data in the Digital Economy: Trade Secrets Perspective. *Trading Data in the Digital Economy: Legal Concepts and Tools*. Nomos Verlag. 60.

Zech, H. (2016). Data as a Tradeable Commodity. In A. De Franceschi (Ed.), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution* (pp. 51-80). Intersentia. doi:10.1017/9781780685212.004.

Data Contracts under Recent Developments of European Law: Novations and Paradoxes

Nataliia Filatova-Bilous
(Yaroslav Mudryi National Law University (Ukraine))

S u m m a r y

Recently, there has been an extensive debate between businesses, policymakers, and scholars on the regulative regime for data transfers. Although many stakeholders claimed to create a property regime for data, the European Commission has opted for an access regime allowing every person participating in data production to access and use the data. This regime does not attribute data to anyone, but, instead, creates legal guarantees to facilitate all persons concerned with equal possibilities to access and use data. Under these circumstances, the load on Contract Law increases since only contracts between various stakeholders can provide them with the needed remedies for the legal protection of their rights and interests. In its turn, this causes significant changes in Contract Law.

This article aims to outline the most prominent novations in the Contract Law regulating data contracts and to critically analyse them.

The analysis has shown that there are many changes in the field of Contract Law in the light of the recent data regulations. Together, these changes constitute new tendencies in Contract Law, the main of which are the following: 1) the creation of distinct types of contracts for data being nevertheless based on the analogy with the classical types of contracts; 2) the dissolution of the concept of privity of contracts, and the spread of 'viral' contractual terms and conditions; 3) the extension of the scope of unfair contractual clauses beyond B2C contracts; and 4) the facilitation of contractual and pre-contractual obligations with administrative sanctions.

All of these changes are highly unusual for the classical Contract Law. Meanwhile, the dissolution of the concept of privity of contracts suggested in some provisions concerning data contracts is a true paradox of the modern Contract Law. Thus, there still is a need for an in-depth analysis of these tendencies together with the newest rules on data contracts in order to find a sufficient explanation and justification for them.

Duomenų perdavimo sutartys pagal naujausius Europos teisės pakeitimus: naujovės ir paradoksai

Nataliia Filatova-Bilous
(Nacionalinis Jaroslavo Išmintingojo teisės universitetas (Ukraina))

S a n t r a u k a

Pastaraisiais metais tarp įmonių, politikos formuotojų ir mokslininkų vyko plačios diskusijos dėl duomenų perdavimo reguliavimo režimo. Nors daugelis suinteresuotųjų šalių teigė sukuriančios nuosavybės režimą duomenims, Europos Komisija pasirinko prieigos režimą, leidžiantį kiekvienam duomenų gamyboje dalyvaujančiam asmeniui prieiti ir naudoti duomenis. Ši tvarka niekam nepriskiria duomenų, o sukuria teisines garantijas, kad visiems suinteresuotiems asmenims būtų sudarytos vienodos galimybės gauti ir naudoti duomenis. Tokiomis aplinkybėmis sutarčių teisei tenkantis krūvis didėja, nes tik įvairių suinteresuotųjų šalių sutartys gali suteikti joms reikalingų savo teisių ir interesų gynimo priemonių. Savo ruožtu tai lemia reikšmingus sutarčių teisės pokyčius.

Šiame straipsnyje apibūdinamos ir kritiškai analizuojamos svarbiausios sutarčių teisės, reglamentuojančios duomenų sutartis, naujovės.

Analizė parodė, kad sutarčių teisės srityje yra daug pokyčių, atsižvelgiant į naujausius duomenų reglamentus. Šie pokyčiai rodo naujas sutarčių teisės tendencijas, kurių pagrindinės yra šios: 1) skirtingų duomenų sutarčių rūšių

kūrimas, vis dėlto remiantis analogija su klasikinių sutarčių rūšimis; 2) sutarčių privilegumo sampratos iširimas ir „virusinių“ sutarčių sąlygų plitimas; 3) nesąžiningų sutarčių sąlygų taikymo srities išplėtimas už B2C sutarčių ribų; 4) sutartinių ir ikisutartinių prievolių vykdymo palengvinimas taikant administracines sankcijas.

Visi šie pakeitimai yra labai neįprasti klasikinei sutarčių teisei. O pagal kai kurias duomenų sutarčių nuostatas siūlomas sutarčių privilegumo sampratos panaikinimas yra tikras šiuolaikinės sutarčių teisės paradoksas. Taigi reikėtų nuodugniai išanalizuoti šias tendencijas kartu su naujausiomis duomenų sutarčių taisyklėmis, kad būtų galima rasti pakankamą jų paaiškinimą ir pagrindimą.

Nataliia Filatova-Bilous is a qualified and experienced lawyer in the area of Private Law with scientific and practical experience. For 7 years, she has been delivering lectures and training law students in Ukraine. Since 2017, she has been working as a licensed attorney in the area of Civil, Commercial and Tax Law. Nataliia Filatova-Bilous is a law researcher who has delivered a number of publications addressing, in particular, the legal aspects of e-commerce, consumer protection in the digital era, data protection, protection of the users of online transaction platforms, and the liability of platform operators.

Nataliia Filatova-Bilous – kvalifikuota ir patyrusi teisininkė privatinės teisės srityje, turinti mokslinės ir praktinės patirties. Jau 7 metus skaito paskaitas ir moko teisės studentus Ukrainoje. Nuo 2017 m. dirba licencijuota advokate civilinės, komercinės ir mokesčių teisės srityje. Teisės tyrėja, daugybės publikacijų, kuriose nagrinėjami teisiniai elektroninės prekybos aspektai, vartotojų apsauga skaitmeninėje eroje, duomenų apsauga, internetinių sandorių platformų naudotojų apsauga ir platformų operatorių atsakomybė, autorė.