UNIVERSITY OF BIALYSTOK
FACULTY OF LAW

BIALYSTOK LEGAL STUDIES

BIAŁOSTOCKIE STUDIA PRAWNICZE

BIAŁYSTOK 2025 VOLUME 30 no. 3

BIALYSTOK LEGAL STUDIES
BIAŁOSTOCKIE STUDIA PRAWNICZE

VOLUME 30 no. 3

Editor-in-Chief of the Publisher Wydawnictwo Temida 2: Dariusz Kijowski

Chair of the Advisory Board of the Publisher Wydawnictwo Temida 2: Rafał Dowgier

Advisory Board:

Representatives of the University of Białystok: Leonard Etel, Ewa M. Guzik-Makaruk, Dariusz Kijowski, Cezary Kulesza, Agnieszka Malarewicz-Jakubów, Maciej Perkowski, Joanna Sieńczyło-Chlabicz, Mieczysława Zdanowicz

Representatives of other Polish Universities: Marek Bojarski (University of Law in Wrocław), Dorota Malec (Jagiellonian University in Kraków), Tomasz Nieborak (Adam Mickiewicz University in Poznań), Maciej Szpunar (University of Silesia in Katowice; Advocate General at the Court of Justice of the European Union), Stanisław Waltoś (University of Information, Technology and Management in Rzeszów), Zbigniew Witkowski (Nicolaus Copernicus University in Toruń)

Representatives of Foreign Universities and Institutions: Lilia Abramczyk (Janek Kupała State University in Grodno, Belarus),Vladimir Babčak (University of Kosice, Slovakia), Renata Almeida da Costa (University of La Salle, Brazil), Jose Luis Iriarte Angél (University of Navarra, Spain), Andrew S. Horsfall (Syracuse University, USA), Jolanta Kren Kostkiewicz (University of Bern, Switzerland), Martin Krygier (University of New South Wales, Australia), Anthony Minnaar (University of South Africa, South Africa), Antonello Miranda (University of Palermo, Italy), Petr Mrkyvka (University of Masaryk, Czech Republic), Marcel Alexander Niggli (University of Fribourg, Switzerland), Lehte Roots (Tallinn University of Technology, Estonia), Jerzy Sarnecki (University of Stockholm, Sweden), Rick Sarre (University of South Australia, Australia), Kevin Saunders (Michigan State University, USA), Bernd Schünemann (University of Munich, Germany), Liqun Cao (Ontario Tech University, Canada)

Editors:

Editor-in-Chief: Elżbieta Kużelewska

Editorial Secretary: Ewa Lotko, Paweł Czaplicki, Diana Dajnowicz-Piesiecka

Other Editors: Tanel Kerikmäe, Christopher Kulander, Andrzej Sakowicz, Urszula K. Zawadzka-Pąk, Bruna Žuber

© Copyright by Author(s) under the Creative Commons CC BY NC ND 4.0 license

No part of this work may be reproduced and distributed in any form or by any means (electronic, mechanical), including photocopying – without the written permission of the Publisher.

The original version of the journal is a print one.

ISSN 1689–7404

e-ISSN 2719–9452

Volume Theme Editor: Paweł Czaplicki

Language Editors: Jakub Redo, Claire Taylor-Jay

Statistical Editor: Ewa Glińska

Graphic and Typographic Development: Eliza Wasilewska, Jerzy Banasiuk

Cover Design: Bogusława Guenther

Publisher: Faculty of Law, University of Białystok; Temida 2

All volumes can be purchased from Wydawnictwo Temida 2. Address: ul. A. Mickiewicza 1, 15-213 Białystok, Poland. E-mail: temida2@uwb.edu.pl, Tel. +48 85 745 71 68

Spis treści

Dominik Mateusz Mizerski, Piotr Pinior, Dušan Rostáš

The Admissibility of Blockchain-Based Solutions for Share Trading and Maintaining Shareholders' Register in the Context of the Dematerialisation of Shares 9

Bartłomiej Gliniecki

Charakter prawny umowy o prowadzenie rejestru akcjonariuszy oraz obowiązek zapewnienia bezpieczeństwa i integralności danych zawartych w rejestrze 23

Katarzyna Szczepańska, Karol Ryszkowski

Problem adekwatności rozwiązań prawnych przyjętych przez polskiego ustawodawcę dla zgromadzeń online wspólników spółek kapitałowych – ze szczególnym uwzględnieniem regulacji dotyczących prostej spółki akcyjnej 37

Marcin Tomasz Mazgaj

Cyfrowe pole bitwy: strona internetowa spółki jako miejsce publikacji ogłoszeń a spory domenowe i korporacyjne 57

Przemysław Katner

Prawo do jednostki kryptowaluty – uwagi de lege lata, prawnoporównawcze i de lege ferenda 73

Konrad Zacharzewski

Model i środki bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy kryptoaktywów w prawie polskim 93

Paweł Czaplicki

Stosowanie Rozporządzenia DLT Pilot Regime w polskim i francuskim porządku prawnym – analiza prawnoporównawcza 111

Tomasz Tomczak

Nadzór AML nad kryptoaktywami od 30.12.2024 – zmiany w Dyrektywie 2015/849 wprowadzone rozporządzeniem 2023/1113 125

Michal Kozieł, Martin Cahlík, Michael Kohajda, Simona Kurtinová

Digital Currency in the Context of the Czech Financial System: Legal and Regulatory Challenges for a Two-Tier Banking System 139

Luljeta Plakolli-Kasumi

AI in the Banking Sector: Lessons from the Schufa Case..... 155

Karol Karski, Paweł Mielniczek

Generative AI in International Trade Law: Navigating Opportunities and Challenges 167

Dariusz Szostek, Agnieszka Malarewicz-Jakubów, Maddalene Castellani

Koncepcja i podstawy prawne dla nowego ujęcia rejestru – „Rejestr 3.0”..... 181

Mariusz Maciejewski

Administracja publiczna rynku finansowego wobec innowacji. Centrum innowacji (innovation hub), piaskownica regulacyjna (regulatory sanbox) i inne specjalne instytucje regulacyjne innowacji..... 197

Krystian Bartnik

Can a National Financial Supervisor Support the Development of the Fintech Sector? Innovation Hubs as a Tool for Supporting Innovation: The Examples of Poland, Estonia, and Italy 215

Piotr Konik

Umowy o dostarczanie treści cyfrowej lub usługi cyfrowej – uwagi dotyczące charakteru prawnego 231

Contents

Dominik Mateusz Mizerski, Piotr Pinior, Dušan Rostáš

The Admissibility of Blockchain-Based Solutions for Share Trading and Maintaining Shareholders' Register in the Context of the Dematerialisation of Shares 9

Bartłomiej Gliniecki

The Legal Nature of the Agreement on Maintaining the Register of Shareholders and the Obligation to Ensure the Security and Integrity of the Data Contained in the Register 23

Katarzyna Szczepańska, Karol Ryszkowski

The Problem of the Adequacy of Legal Solutions Adopted by the Polish Legislator for Online Shareholder Meetings in Companies, with Particular Emphasis on the Regulation of Simple Joint-Stock Companies 37

Marcin Tomasz Mazgaj

The Digital Battlefield: Company Websites as a Place to Publish Advertisements and Domain and Corporate Disputes 57

Przemysław Katner

The Right to a Cryptocurrency Unit: de lege lata, Comparative Law and de lege ferenda Considerations 73

Konrad Zacharzewski

The Model and Means of Direct Protection of the Individual Rights of Buyers and Holders of Cryptoassets in Polish Law 93

Paweł Czaplicki

The Application of the DLT Pilot Regime in the Polish and French Legal Systems: A Comparative Analysis 111

Tomasz Tomczak

AML Supervision of Cryptoassets since 30 December 2024: Changes to Directive 2015/849 Introduced by Regulation 2023/1113 125

Michal Kozieł, Martin Cahlík, Michael Kohajda, Simona Kurtinová

Digital Currency in the Context of the Czech Financial System: Legal and Regulatory Challenges for a Two-Tier Banking System 139

Luljeta Plakolli-Kasumi

AI in the Banking Sector: Lessons from the Schufa Case 155

Karol Karski, Paweł Mielniczek

Generative AI in International Trade Law: Navigating Opportunities and Challenges 167

Dariusz Szostek, Agnieszka Malarewicz-Jakubów, Maddalene Castellani

The Concept and Legal Basis for a New Approach to Registers: 'Register 3.0' 181

Mariusz Maciejewski

The Public Administration of the Financial Market towards Innovation: Innovation Hubs, Regulatory Sandboxes and Other Special Regulatory Institutions of Innovation 197

Krystian Bartnik

Can a National Financial Supervisor Support the Development of the Fintech Sector? Innovation Hubs as a Tool for Supporting Innovation: The Examples of Poland, Estonia, and Italy 215

Piotr Konik

Contracts for the Supply of Digital Content or Digital Services: Considerations of Their Legal Nature 231

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

sciendo

DOI: 10.15290/bsp.2025.30.03.01

Received: 16.11.2024
Accepted: 4.07.2025

Dominik Mateusz Mizerski
University of Silesia, Poland
dominik.mizerski@us.edu.pl
ORCID ID: https://orcid.org/0000-0002-8253-5038

Piotr Pinior
University of Silesia, Poland
piotr.pinior@us.edu.pl
ORCID ID: https://orcid.org/0000-0003-2084-0325

Dušan Rostáš
Pavol Jozef Šafárik University in Košice, Slovakia
dusan.rostas@upjs.sk
ORCID ID: https://orcid.org/0000-0003-1973-9203

The Admissibility of Blockchain-Based Solutions for Share Trading and Maintaining Shareholders' Register in the Context of the Dematerialisation of Shares[1]

Abstract: The mandatory dematerialisation of shares, which involves converting physical share certificates to electronic records, has unified the trading framework for registered and bearer shares. This paper examines the impact of mandatory dematerialisation on the regulations governing the trading and registration of shares in non-listed joint-stock companies, where shares are registered in the shareholders' register. The analysis is conducted in the context of modern technologies, such as smart contracts, distributed ledger technology and tokenisation, and their role in these processes. The authors refer to the possibility of concluding a share transfer agreement using smart contract technology and argue that, although maintaining a shareholders' register in the form of a distributed and decentralised database

1 This work was supported by the Slovak Research and Development Agency under the Contract no. APVV–23–0331 and by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences (VEGA) under the Contract no. 1/0598/25.

© 2025 Dominik Mateusz Mizerski, Piotr Pinior, Dušan Rostáš published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

is permitted, the provisions currently in force do not allow or fully enable the exploitation of the benefits available through blockchain technology, particularly the tokenisation of shares.

Keywords: shares, dematerialisation, shareholders' register, blockchain, smart contracts, tokenisation

Introduction

The mandatory dematerialisation of shares in joint-stock companies entered into force in Polish law on 1 March 2021 as a result of the Act Amending the Commercial Companies Code and Certain Other Acts of 30 August 2019 (Dematerialised Shares Act). As a result, neither registered nor bearer shares are in physical form, and the regulations on transferring all classes of shares have been unified.[2] All shares, which were securities incorporated in physical documents, have been replaced by dematerialised shares subject to registration either in the shareholders' register (Article 328(1) Commercial Companies Code (CCC)) or in the National Securities Depository (Article 328(11) CCC); it is not possible to register shares in both (Article 328(12) CCC).

The mandatory dematerialisation of shares led to significant changes in the regulations governing the trading and registering of shares in non-listed limited joint-stock companies. The legislature's declared aims included enhancing market transparency, investor security and trading efficiency (Sejm of Poland, 2019). However, a closer analysis suggests that the amendment, though technically a modernisation, only partially addresses the practical and normative conditions necessary for integrating innovative technologies into the legal framework governing the trading and registration of shares of non-listed joint-stock companies. In particular, the reform appears to have been driven more by the need to identify the owners of bearer shares than by a genuine intention to embrace transformative technological developments, such as blockchain-based systems. As a result, the dematerialisation process, while symbolically aligned with digitisation efforts, falls short of creating a legal environment conducive to the adoption of more advanced technological solutions, including the tokenisation of shares.

The purpose of this paper is to present the impact of the mandatory dematerialisation on the rules for the trading and registration of shares in non-listed joint-stock companies whose shares are registered in the company's shareholders' register, in light of the use of modern technology in these processes. First, the article demonstrates that the dematerialisation of shares has introduced a new manner of transferring shares, resulting in a significant alteration in the share-trading regime. Second, it argues that, despite its formal openness, the provisions of Polish law cur-

2 The provisions on shares in joint-stock companies also applies to limited joint-stock partnerships (Article 126 § 1 point 2 CCC). The provisions on shares apply accordingly to subscription warrants, utility certificates, promoters' certificates and other titles to participate in the income or distribution of a company's assets (Article 328 § 2 CCC).

rently in force actually impose significant limitations on the effective use of modern, blockchain-based technologies in the trading and registration of shares in non-listed joint-stock companies. These limitations arise not only from the rigidity of regulatory requirements, but also from the functional design of the shareholders' register. In this respect, we focus strictly on the admissibility of using smart contracts as the basis of transferring shares, maintaining shareholders' registers as a diffused and decentralised database, along with the tokenisation of shares. Despite the introduction of profound changes in the form of shares and trading of shares in light of the mandatory dematerialisation, the Polish legislature has failed to take full advantage of the opportunities offered by blockchain-based technologies to apply their functionality when transferring and registering shares in shareholders' registers.

The analysis is based primarily on a legal-dogmatic approach. In addition, selective references to foreign literature and European legislation highlight both the shortcomings and the potential of the Polish system with regard to the possibility of using blockchain-based solutions in share trading and share registration.

1. The transfer of shares or the establishment of limited rights in rem in light of mandatory dematerialisation

The dematerialisation of shares under the Dematerialised Shares Act unified the legal rules governing the transfer of both registered and bearer shares in non-listed joint-stock companies, leading to it being regulated autonomously by the provisions of the Commercial Companies Code. New provisions replaced the previous regime for the transfer of shares, which were essentially based on the Civil Code (CC). The dematerialisation of shares has resulted in the moment of the transferral of shares being linked with an entry in the shareholders' register. A share transfer becomes effective upon entry in the register, which is, in principle, constitutive (Article 328(9) § 1 CCC).[3] Consequently, the dispositive effect is excluded when concluding a contract obliging the parties to transfer shares, and the intention of the parties to create a dispositive effect is reflected in the request for entry into the register (Popiołek, 2024, p. 875). Only the entity entered into the register is legally recognised as a shareholder, and this also applies to the establishment of limited rights *in rem*. The entity operating the register makes entries at the request of the company or of an interested party, based on documents justifying the entry or a shareholder's statement on the

3 The constitutive nature of an entry in the shareholders' register does not apply to the subscription of shares (except as provided for in Article 452 § 1 CCC) or the transfer of shares by way of inheritance, legacy, contribution in kind to the company, merger, division or transformation of the company, or any other legal event whereby a share or a limited right *in rem* relating to it is transferred by operation of law to another entity.

obligation to transfer shares or to encumber shares with limited rights *in rem* (Article 328(4) § 4 CCC).

The provisions of the Dematerialised Shares Act do not define the form of the agreement on the transfer of shares, leaving this choice to the parties. While the format of this agreement is not defined by law, it is indicated in the literature that it must at least be in documentary form (Pabis, 2022, p. 1702; Popiołek, 2024, p. 876), though an entry in the register may also be made on the basis of the shareholder's declaration of an obligation to transfer the shares. Hence the form of the agreement or the shareholder's obligation is discretionary and minor regarding constitutive entry in the shareholders' register.

In some cases, such as the creation of a pledge on shares, specific forms, such as a written form with a certified date or entry in a separate register, are required due to *lex specialis* rules (Article 329 § 1 CC). In particular, registered pledges must be in a specific form under the provisions of the Act on Registered Pledges and the Pledge Register, which requires a pledge contract to be concluded in writing and then entered in the pledge register. We support the view that an entry in the pledge register is constitutive, because the act of the Act on Registered Pledges and the Pledge Register is a *lex specialis* towards the provisions of the Commercial Companies Code (Mizerski, 2022, p. 50; Sobociński, 2022, p. 36; for a contrary view, see Popiołek, 2020, p. 7).

Importantly, the entity maintaining the shareholders' register is only required to assess the formal correctness of the submitted documents but is not obliged to verify their legality or authenticity, unless there are justified doubts (Article 328(4) § 5 CCC). The assessment of whether the doubts are justified is the responsibility of the entity maintaining the register, which must exercise due diligence when considering applications to make entries. In the event of any doubts, it should take appropriate action, in particular to obtain the statements of interested parties (Popiołek, 2024, p. 868; Sójka, 2021, p. 31). Consequently, it should be emphasised that if the entity maintaining the shareholders' register fails to perform its duties properly, it may become liable for damage inflicted to the company or to anyone with a legal interest.

In this respect, the situation where a purchaser, acting in good faith, buys shares from an unauthorised entity has become rather controversial. Some representatives of the doctrine grant protection to the purchaser in good faith under Article 169 § 1 CC, due to the entry in the shareholders' register (Opalski, 2019, p. 6; Sójka, 2020, p. 9), even though protection under this article refers to a purchaser of property rights incorporated in bearer documents. This is the reason why opponents of this view argue that attempts to extend the protection under Article 169 §1 CC to dematerialised shares are unjustified (Dybiński & Weber, 2022, p. 229; Popiołek, 2024, p. 876). In our opinion, protection under Article 169 § 1 CC does not apply to dematerialised shares because the transfer of rights attached to bearer shares in documentary form cannot be equated with an entry in a shareholders' register. Consequently, in the case of purchasing dematerialised shares from an unauthorised seller, the purchaser does not

become a shareholder due to the lack of legal legitimacy. Regardless of the interpretative doubts, the provisions of the Commercial Companies Code do not resolve the issue of unlawful entries in a shareholders' register, so only legislative initiatives to provide for a proper protection system can be a remedy for such entries.

2. Smart contracts on the transfer of shares

The lack of specified forms of contract for the disposal of shares opens up the possibility of using modern technologies, particularly the institution of 'smart contracts'. These are defined as contractual provisions written in the form of a self-executing algorithm, a cryptographically secured computer code (Szabo, 1997); another definition describes them as agreements whose execution is automated (Raskin, 2017, p. 309). A common feature of all these definitions is the possibility of using blockchain technology to conclude these contracts (Maxwell et al., 2017, pp. 79-97). Since the terms and conditions are recorded in the blockchain and cannot be amended, any uncertainty surrounding the possibility that one party might wish to renegotiate the contract is removed (Van der Elst & Lafarre, 2018, p. 5).

Under civil law, smart contracts should not be qualified as a separate type of contract; they are simply a means of concluding and (self-)executing a contract, provided this aligns with the intended purpose and the specific content of the computer program (code) (Pecyna & Behan, 2020, p. 207; Verstappen, 2023, p. 85; Załucki, 2024, p. 25). Furthermore, smart contract technology can also be used as an enrolment tool to reflect a previous contract concluded in the traditional manner (Mmereole, 2023, p. 31; Szostek, 2018, p. 121). From this perspective, the smart contract functions as a letter of confirmation.

To support the view that a smart contract is a means of concluding and executing an agreement, it is useful to consider whether contracts employing such technology may be used for the transfer of shares. The blockchain is divided into blocks that store transaction data, and these blocks are linked to each other by the cryptographic hash of the preceding block being placed in each block (except for the block that starts the blockchain, which is called the genesis). Like a file system, the blockchain has an internal structure in which the data is stored. The smallest identifiable element of this structure is a single transaction, which at the same time is the most appropriate element for consideration as a document (Szczerbowski, 2018, p. 5).

In view of this, it should be stated that an agreement concluded using smart contract technology meets the requirement of a declaration of intent being recorded as a document within the meaning of Article 77(3) CC. The requirement to identify the entity making the declaration is also met, as when an agreement is concluded via intelligent software, an individual transaction is always identified by the user's account name and digitally signed by the user. Furthermore, agreements concluded

as smart contracts always arise as a result of human intention, and it is irrelevant whether the program expressed that intention (Mmereole, 2023, p. 31). In addition, within the smart contract framework the condition on which the performance of the contract depends should be qualified as a condition under civil law (Gołaczyński, 2024). As indicated in the literature, the construction of the smart contract is consistent with the general rules of civil law, with agreements concluded as smart contracts able to meet the requirements for documentary form as set out in the Civil Code (Hadrowicz, 2020, p. 38).

With this in mind, we argue that, in the absence of specific form requirements for share transfer agreements under the Commercial Companies Code, the conclusion of such an agreement using smart contract technology can be considered as a document justifying the entry of the share transfer into the shareholders' register in the meaning of Article 328(4) § 4 CCC. The same applies to a usufruct contract. By contrast, a pledge or registered pledge agreement cannot be concluded using smart contracts under the requirements on the contract form (as explained above).

The conclusion of an agreement using smart contract technology does not exempt an entity maintaining a shareholders' register from the obligation to examine the legality and veracity of the documents justifying the entry, if any justified doubts arise in this regard (Article 328(4) CCC). The literature rightly emphasises that this examination concerns in particular the analysis of circumstances outside the computer program governing the process of concluding contracts, such as defects in the declaration of the will of the parties to the agreement or limitations on the legal capacity of those parties (Sójka, 2021, p. 30). Furthermore, it seems that the entity maintaining the shareholders' register cannot refuse to consider an application for registration solely on the grounds that it is based on an agreement concluded using smart contract technology. In particular, a refusal to recognise such an agreement as a ground for registration cannot be justified by the fact that the entity maintaining the register does not have the technical ability to verify the agreement. An exception to this principle concerns a situation where an agreement with an entity maintaining a shareholders' register, or the bylaws of such an entity, provides for restrictions on the form of the agreement that may be the basis for making an entry into the register.

The issue of smart contracts can be studied from a perspective broader than the system of self-executing contracts. Once the assumption that smart contracts constitute computer programs is accepted (Szabo, 1997), their potential application becomes inherently tied to the regulation of the underlying technology, which enables not only their formation but also their execution. From both a technical and a legal standpoint, it is not merely the conclusion of an agreement that is of importance, but also the performance of the obligations it entails, which is essential to ensuring fulfilment. Therefore the development of legal regulations on smart contracts can, in essence, be a regulation of a wider ecosystem that enables their use and execution, which means the regulation of technology.

3. Shareholders' registers in the form of diffused and decentralised databases

The primary function of a shareholders' register is to identify entities entitled to shares, as it contains information on shares issued by a company as well as its shareholders (Article 328(3) CCC). The shareholders' register can only be maintained by entities authorised to keep securities accounts under the provisions of the Act on Trading in Financial Instruments. The entity operating the register performs three functions simultaneously: first, it is the custodian that registers a series of shares in the name of the issuer and monitors the conformity of the number of shares in circulation with the size of the issue; second, it keeps an account of dematerialised shares in the name of each entitled shareholder; and third, it is the settlement entity recording changes in the shareholdings of each entitled shareholder (Sójka, 2021, p. 28).

In principle, the Polish legislature has maintained technological neutrality regarding the rules governing the maintenance of a shareholders' register. The organisation of the register depends mainly on the technical possibilities of the entity maintaining it. The legislature merely requires that the shareholders' register be kept in electronic form, which may be a diffused and decentralised database (Article 328(1) § 3 CCC). Regardless of the form of the register, the entity operating the register must keep it in a manner that ensures the security and integrity of the data contained therein (Article 328(1) § 4 CCC), in particular shareholders' personal data.

Under the current legislation, shareholders' registers can be kept using distributed ledger technology (DLT), in particular a database based on blockchain technology (Bronowska & Matraszek, 2020, p. 23; Dybiński & Weber, 2022, p. 214; Sejm of Poland, 2019; conversely, Michalski, 2021, pp. 241–242, who highlights limitations on the use of blockchain technology in keeping shareholders' registers). The data of the transactions in a block are stored using 'Merkle trees', which are constructed bottom-up. Here, one can find individual transactions (i.e. the underlying data) and their hashes. New hashes are constructed from pairs of such hashes, and the action is repeated until there is only one hash left. The single hash situated at the top of the Merkle tree is also called the Merkle root. Since changing any transaction (including the order) will change the Merkle root, the transaction data can be verified and validated (making it immutable) (Van der Elst & Lafarre, 2019, p. 126). The use of blockchain technology brings several benefits, including reduced costs, simple access and the security of the stored data. However, there are risks associated with these benefits, including the threat of data being tampered with before it is stored, operational risks (including improper or incorrect coding) and risks from increased levels of transparency (Andhov, 2019, pp. 14–16; Panisi et al., 2019, p. 216).

Blockchains can be public (permissionless) or private (permissioned) (Armstrong et al., 2019, p. 12; Szostek, 2018, pp. 49–50; Van der Elst & Lafarre, 2019, p. 126). Anyone on the internet can access a public blockchain without permission;

therefore anyone can become a user, receive a copy of the ledger and can propose and validate new blocks. In the absence of an intermediary, the validation of a transaction relies on a consensus being reached between all the parties or nodes. Conversely, private blockchains require permission from administrators for any of the above (Stocker, 2023, p. 452). Both blockchain systems are decentralised, with each participant in the blockchain keeping a replica of the ledger. These replicas are synchronised via a consensus mechanism, like the proof-of-work concept (Governatori et al., 2018, p. 386).

Using DLT is prima facie appropriable for a shareholders' register, since blockchain can be described as an open, distributed ledger that can record transactions between (unknown) parties in a verifiable and immutable way (Iansiti & Lakhani, 2017). However, with regard to the use of such technology for the operation of a shareholders' register, the Justification to the Dematerialised Shares Act (Sejm of Poland, 2019) directly indicates the possibility of using blockchain technology in operating the register but is devoid of further reflection. It must be emphasised that the use of blockchain technology would have to involve an entity that approves individual transactions or the blockchain of such transactions, making entries of them in the register (Dąbrowska, 2022, pp. 24–25; Sójka, 2021, pp. 29–30). Thus, in our view, it opens up the possibility of the register being based solely on a private blockchain, with the assigned tasks of the entity being maintaining the register (as a trusted third party), approving individual transactions and entering them into the register. Third parties would be excluded from the private blockchain, because shareholders and the company would have exclusive access to the register (Article 328(5) CCC). For this reason, the use of blockchain technology and the benefits associated with its use are currently significantly limited, due to the fact that the current legal framework does not fully embrace the potential of blockchain, meaning that it remains a theoretical option rather than a practical solution.

4. The tokenisation of shares at the dawn of the European Union legislation and in light of mandatory dematerialisation under Polish law

The question of the possible tokenisation of shares is essentially one of transforming traditional securities into a digital representation (Jiménez-Gómez, 2023, p. 671). Tokenisation has emerged as a corollary of blockchain development; it is the phenomenon of using DLT to reflect the economic value itself in the form of a token, or to reflect a given existing good in the form of a token indicating the rights and obligations associated with that good (secondary tokenisation), or to create tokens that are inextricably linked to a newly created good (primary tokenisation) (Langer & Pinior, 2023, p. 11). Tokens represent a particular asset or utility that usually re-

sides on top of another blockchain, and can represent any fungible and tradeable asset, from commodities to loyalty points and even cryptocurrencies (Obrist & Pfister, 2019, p. 305).

One of the most important legal acts defining the principles of using DLT, including the consequences of the possibility of tokenising shares, is Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology, and Amending Regulations (EU) no. 600/2014 and (EU) no. 909/2014 and Directive 2014/65/EU (the DLT Regulation). This legal act has been effective since 23 March 2023 and is called a 'pilot regime'; it creates a regulatory landscape where existing market infrastructure operators can deploy and test new DLTs. This 'sandbox' is not primarily intended for new market entrants but rather for existing operators on the market (Priam, 2022, p. 379), with the aim of assessing the potential of new technologies. It is emphasised in the literature that the pilot regime of the DLT Regulation should be seen only as a temporary legal regulation of technology to make it possible to test DLT (Hrabčák & Štrkolec, 2024, p. 33).

The idea of the DLT pilot regime is to temporarily relieve the sandbox participants from obligations that might otherwise prevent them from developing DLT solutions for trading and settling transactions in cryptoassets that qualify as financial instruments (Recital 6 of the DLT Regulation). Exemptions are not generally permitted for the participants. The sandbox regulation only entitles already-licensed market infrastructure operators to request an individual exemption from certain obligations from the competition authority under their default regulation regime (i.e. Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU (MIFID II), or Regulation (EU) no. 909/2014 of the European Parliament and of the Council of 23 July 2014 on Improving Securities Settlement in the European Union and on Central Securities Depositories and Amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) no. 236/2012). The pilot regime is also accompanied by several restrictions regarding the nature of financial instruments and the market capitalisation of the issuer (Article 3 of the DLT Regulation). Exemptions can be granted only on an individual basis.

The DLT sandbox distinguishes between several types of market infrastructure, namely DLT multilateral trading facilities (MTF) and the DLT trade and settlement system (TSS), which can be operated by investment firms or a market operator under MIFID II, and the DLT transaction settlement system (SS), operated by a central securities depository under Regulation (EU) no. 909/2014. A significant advantage of DLT is that it is capable of combining a multilateral trading system and a settlement system into one, in a new TSS system (Priam, 2022, p. 377).

The possibilities of taking advantage of the tokenisation of shares are very limited in the case of non-listed companies. The DLT Regulation does not govern this

issue explicitly either: it offers a list of various exemptions, one of which is an exemption from the obligation to comply with the 'book-entry form' of shares (Article 5(2)(a)). This exemption could also be applied to the DLT SS, which can be operated by a central securities depository. Considering the scope of Regulation (EU) no. 909/2014 (which affects shares in non-listed companies) and Article 7(9) of the DLT Regulation (which applies to a central securities depository that only operates the settlement systems infrastructure), it seems that exemptions under the DLT pilot regime could also be awarded for settling transactions of shares in non-listed companies. The question arises whether it would be possible, under the DLT pilot regime (in the case of a granted exemption), to permit shareholders to self-execute transfers of tokenised shares in non-listed companies via DLT.

Under the rules for the DLT MTF infrastructure, it is clearly stated that this infrastructure can also be open for natural and legal persons (Article 4(2) of the DLT Regulation). For the DLT SS, at the request of a depository, the relevant authority can also admit as participants entities that would not be considered participants in the meaning of Directive 98/26/EC on Settlement Finality in Payment and Securities Settlement Systems (Article 5(5) of the DLT Regulation). This means that the DLT SS system can potentially also be open to third parties. Unlike the exemption for the DLT MTF, the wording of the DLT SS exemption does not distinguish between natural and legal persons. Given that an operator requesting exemptions must demonstrate that an exemption is justified and proportionate (Recital 37 of the DLT Regulation), and given the duty of the relevant authority to consider investor protection, market integrity and financial stability (Recital 17), it is not clear whether such an exemption should also be awarded for natural and legal persons acting as shareholders. The final answer depends on the relevant authority, an individual assessment of the particular market infrastructure and the limits of technology. Theoretically, the transfer of tokenised shares in a non-listed company can be exempted under the DLT Regulation.

The EU legislature is expected to take a legislative initiative on the use of DLT to maintain shareholders' registers. This seems all the more likely given that it has already acted to establish a legal framework for the use of blockchain technology under the DLT Regulation (Hrabčák & Štrkolec, 2024, p. 31). The current DLT sandbox is likely to be in force until at least 24 March 2026. After that date, the Commission is set to submit a report on the pilot regime, setting out cost–benefit analyses to the European Parliament and Council for further action.

From the perspective of the Polish legislation resulting from the mandatory dematerialisation of shares, the tokenisation of shares in joint-stock companies only partially meets the conditions for share tokenisation in the form of maintaining a distributed shareholders' register when such a register is in the form of a private blockchain. However, due to the closed nature of the access to such a register, which prevents access to third parties (i.e. anyone other than the company, the shareholders and the entity maintaining the register), there is no justification and few practical im-

plications for the tokenisation of shares in non-listed joint-stock companies (see also Dąbrowska, 2022, p. 23; Pinior & Langer, 2024, p. 5). Consequently, the admissibility of the tokenisation of shares requires further legislative initiative by the Polish legislature, for which the provision of the DLT pilot regime might be a significant complementary contribution.

Conclusions

The Dematerialised Shares Act unified the rules governing the transfer of shares in non-listed joint-stock companies. The amendment introduced significant alterations, notably removing the requirement of a specified form for a share transfer agreement, excluding the dispositive effect in agreements obliging the transfer of shares, and linking the transfer of shares with a constitutive entry in the shareholders' register. The dematerialisation of shares also prompted a reassessment of previous views in the doctrine concerning the traditional meaning of securities in the form of physical certificates. As explained above, the issue of unlawful entries in shareholders' registers requires further legislative steps.

At the same time, blockchain-based technology will almost certainly play a pivotal role in share trading. At present, however, this role seems to be quite limited in the Polish legal system. Under the provisions of the Commercial Companies Code, there are no requirements for the form of a share transfer agreement, so the conclusion of such an agreement using smart contract technology can be considered as a document justifying the entry of the share transfer into the shareholders' register. Consequently, as presented in the paper, the legislature's application of technological neutrality enables the use of modern technologies. In particular, it is admissible to use blockchain technology to maintain a shareholders' register; however, as outlined above, it would be based solely on a private blockchain, which limits the potential use of this technology.

Furthermore, the provisions introduced by the Dematerialised Shares Act do not provide sufficient basis under national law to permit the tokenisation of shares in non-listed joint-stock companies. Allowing this possibility would require a profound overhaul of the chief elements of a joint-stock company, particularly the possibility of maintaining a shareholders' register as a public (permissionless) blockchain. Given the importance of the issue and the significant harmonisation of securities trading in EU Member States, it would be advisable to regulate this issue at the European level. Overall, it seems that the application of DLT, particularly blockchain technology, in keeping a shareholders' register may require legislative intervention to regulate the technologies that may be used.

REFERENCES

Andhov, A. (2019). Corporations on blockchain: Opportunities and challenges. *Cornell International Law Journal*, *53*, 1–40.

Armstrong, K. C. D., Hyde, D., & Thomas, S. (2019). *Blockchain and cryptocurrency: International legal and regulatory challenges*. Bloomsbury.

Bronowska, M., & Matraszek. J. (2020). Blockchain a rejestr akcjonariuszy. *Przegląd Prawa Handlowego*, *4*, 23–29.

Dąbrowska, J. (2022). Cyfrowa rewolucja. Rozważania o ucyfrowieniu spółki akcyjnej w świetle koncepcji organizacji biurokratycznej Maxa Webera i założeń ekonomii instytucjonalnej. In A. Kidyba & A. Olejniczak (Eds.), *Nowoczesne technologie. Szansa czy zagrożenie dla funkcjonowania przedsiębiorców w obrocie prawnym i postępowaniach sądowych* (pp. 13–36). Wolters Kluwer Polska.

Dybiński, J., & Weber A.-M. (2022). Mandatory dematerialization of shares in Polish private companies: A missed opportunity to do things right. *European Company and Financial Law Review*, *19*(2), 203–238.

European Parliament. (1988, 19 May). Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems (O. J. L 166, 11.06.1998).

European Parliament. (2014, 15 May). Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on Markets in Financial Instruments and Amending Directive 2002/92/EC and Directive 2011/61/EU (O. J. L 173, 12.06.2014).

European Parliament. (2014, 23 July). Regulation (EU) no. 909/2014 of the European Parliament and of the Council of 23 July 2014 on Improving Securities Settlement in the European Union and on Central Securities Depositories and Amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) no. 236/2012 (O. J. L 257, 28.08.2014).

European Parliament. (2018, 30 May). Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology, and Amending Regulations (EU) no. 600/2014 and (EU) no. 909/2014 and Directive 2014/65/EU (O. J. L 151, 02.06.2022).

Gołaczyński, J. (2024). Pojęcie i rodzaje umów elektronicznych. In J. Gołaczyński (Ed.), *Prawo umów elektronicznych. Zarys systemu* (pp. 1–70). Wolters Kluwer.

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law*, *26*(4), 377–409.

Hadrowicz, S. (2020). Smart kontrakt jako umowa. *Międzynarodowe Prawo Handlowe*, *4*, 32–42.

Hrabčák, L., & Štrkolec, M. (2024). EU regulation of the crypto-assets market. *Białostockie Studia Prawnicze*, *29*(1), 27–42.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review*, *95*(1), 118–127.

Jiménez-Gómez, B. S. (2023). Distributed ledger technology in financial markets: The European Union experiment. *Cuadernos de Derecho Transnacional*, *15*(2), 665–678.

Langer, M., & Pinior, P. (2023). Tokenizacja praw udziałowych w spółkach osobowych. *Przegląd Ustawodawstwa Gospodarczego*, *10*, 9–17.

Maxwell, D., Speed, C., & Pschetz, L. (2017). Story blocks: Reimagining narrative through the blockchain. *Convergence: The International Journal of Research into New Media Technologies*, *23*(1), 79–97.

Michalski, M. (2021). Dematerializacja akcji a realizacja uprawnień akcyjnych przez akcjonariuszy. In M. Michalski (Ed.), *Powszechna dematerializacja akcji. Modernizacja konstrukcji spółki akcyjnej* (pp. 231–271). Wolters Kluwer Polska.

Mizerski, D. (2022). Ustanowienie zastawu zwykłego oraz rejestrowego na akcjach w świetle przepisów o przymusowej dematerializacji. *Przegląd Ustawodawstwa Gospodarczego*, *10*, 46–51.

Mmereole, J. (2023). Zawarcie umowy przez inteligentne oprogramowanie – smart kontrakty. *Prawo Nowoczesnych Technologii*, *1*, 30–35.

Obrist, T., & Pfister, R. A. (2019). Tax treatment of cryptocurrency holders and miners in the era of virtual currencies from a multijurisdictional and Swiss perspective. In D. Kraus, T. Obrist, & O. Hari (Eds.), *Blockchains, smart contracts, decentralised autonomous organisations and the law* (pp. 299–348). Edward Elgar.

Opalski, A. (2019). Prosta spółka akcyjna – nowy typ spółki handlowej (część I). *Przegląd Prawa Handlowego*, *11*, 5–15.

Pabis, R. (2022). Commentary to Article 328(4). In Z. Jara (Ed.), *Kodeks spółek handlowych. Komentarz* (pp. 1680–1750). C. H. Beck.

Panisi, F., Buckley, R. P., & Arner, D. (2019). Blockchain and public companies: A revolution in share ownership transparency, proxy-voting and corporate governance? *Stanford Journal of Blockchain Law & Policy*, *2*(2), 1–32.

Pecyna, M., & Behan, A. (2020). Smart contracts – Nowa technologia prawa umów? *Transformacje Prawa Prywatnego*, *3*, 187–216.

Pinior, P., & Langer, M. (2024). Tokenizacja akcji i innych praw udziałowych w spółkach kapitałowych. *Przegląd Ustawodawstwa Gospodarczego*, *10*, 2–9.

Popiołek, W. (2020). Rozporządzanie akcjami rejestrowymi spółek niepublicznych. *Przegląd Ustawodawstwa Gospodarczego*, *5*, 2–13.

Popiołek, W. (2024). Commentary to Article 328(4). In P. Pinior and J. A. Strzępka (Eds.), *Kodeks spółek handlowych. Komentarz* (pp. 867–869). C. H. Beck.

Priam, R. (2022). A European distributed ledger technology pilot regime for market infrastructures: Finding a balance between innovation, investor protection and financial stability. *Journal of Financial Regulation and Compliance*, *30*(3), 371–390.

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review*, *1*(2), 305–341.

Sejm of Poland. (1966). Civil Code of 23 April 1964 (consolidated text, Journal of Laws of 2024, item 1061, as amended).

Sejm of Poland. (1996). Act on Registered Pledges and Register of Pledges of 6 December 1996 (consolidated text, Journal of Laws of 2018, item 2017, as amended).

Sejm of Poland. (2000). Commercial Companies Code of 15 September 2000 (consolidated text, Journal of Laws of 2024, item 18, as amended).

Sejm of Poland. (2005). Act on Trading in Financial Instruments of 29 July 2005 (consolidated text, Journal of Laws of 2024, item 722, as amended).

Sejm of Poland. (2019). Act Amending the Commercial Companies Code Act and Certain Other Acts of 30 August 2019 (consolidated text, Journal of Laws of 2019, item 1798, as amended).

Sejm of Poland, 2019. (2019). Justification of the government's draft act amending the Commercial Companies Code and certain other acts, print no. 3541. Retrieved 18 November 2024, from URL: https://orka.sejm.gov.pl/Druki8ka.nsf/0/38BFA72164FE8069C125841D00436FE7/%24File/3541.pdf

Sobociński, F. (2022). Zastaw rejestrowy na akcjach spółki niepublicznej – problem konfliktu wpisów konstytutywnych. *Przegląd Prawa Handlowego*, *8*, 30–36.

Sójka, T. (2020). Obrót akcjami prostej spółki akcyjnej. *Przegląd Prawa Handlowego*, *1*, 5–11.

Sójka, T. (2021). Rejestr akcjonariuszy w postaci rozproszonej i zdecentralizowanej bazy danych. *Przegląd Ustawodawstwa Gospodarczego*, *4*, 26–33.

Stocker, P. (2023). The potential of blockchain technology for share transfers in nonlisted companies in Switzerland and the United Kingdom. *European Business Organization Law Review*, *24*, 439–470.

Szabo. N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9).

Szczerbowski, J. J. (2018). Sprytne kontrakty a prawo umów – wprowadzenie. *Edukacja Prawnicza*, *2*, 5–9.

Szostek, D. (2018). *Blockchain a prawo*, C. H. Beck.

Van der Elst, C., & Lafarre, A. (2018). *Blockchain technology for corporate governance and shareholder activism* [Law working paper 390]. European Corporate Government Institute.

Van der Elst, C., & Lafarre, A. (2019). Blockchain and smart contracting for the shareholder community. *European Business Organization Law Review*, *20*, 111–137.

Verstappen, J. (2023). *Legal agreements on smart contract platforms in European systems of private law*. Springer.

Załucki, M. (2024). Technologia blockchain i smart contracts a perspektywa prawa prywatnego międzynarodowego jako wyzwanie dla ustawodawcy. *Przegląd Prawa Publicznego*, *11*, 20–37.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.02

Received: 6.01.2025
Accepted: 3.07.2025

Bartłomiej Gliniecki
Uniwersytet Gdański, Polska
bartlomiej.gliniecki@ug.edu.pl
ORCID ID: https://orcid.org/0000-0003-0231-4903

Charakter prawny umowy o prowadzenie rejestru akcjonariuszy oraz obowiązek zapewnienia bezpieczeństwa i integralności danych zawartych w rejestrze

The Legal Nature of the Agreement on Maintaining the Register of Shareholders and the Obligation to Ensure the Security and Integrity of the Data Contained in the Register

Abstract: The content of the obligation to ensure the security of data contained in the register of shareholders, emphasized by the legislature, the implementation of which rests with the entity maintaining the register, has not been developed in the provisions of the Commercial Companies Code. In the context of the potential liability of this entity for improper performance of the agreement to maintain the shareholder register, it is therefore necessary to determine the features that are important for this issue and the legal nature of such an agreement, as well as which sources of normative law specify orders or prohibitions of specific conduct, so as to ensure the security of digital data contained in the shareholder register.

Keywords: register of shareholders, joint-stock companies, simple joint-stock companies, data security, contracts, services
Słowa kluczowe: rejestr akcjonariuszy, spółka akcyjna, prosta spółka akcyjna, bezpieczeństwo danych, umowa, usługa

Wprowadzenie

Przepisy Kodeksu spółek handlowych (Sejm RP, 2000), dalej jako KSH, przewidują – w przeciwieństwie do księgi udziałów prowadzonej samodzielnie przez zarząd spółki z ograniczoną odpowiedzialnością – wymóg prowadzenia rejestru akcjonariuszy niepublicznej spółki akcyjnej, prostej spółki akcyjnej, spółki komandytowo-akcyj-

© 2025 Bartłomiej Gliniecki published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

nej oraz spółki europejskiej przez podmiot zewnętrzny. Powodów słuszności takiego rozwiązania jest kilka. Przede wszystkim jest nim powierzenie tej istotnej dla akcjonariuszy czynności podmiotowi cechującemu się niezależnością i profesjonalizmem, w szczególności takiemu, który ma gwarantować bezpieczeństwo i wiarygodność danych zawartych w rejestrze, co stanowi fundament dla wykonywania przez akcjonariuszy ich praw udziałowych i właściwego funkcjonowania spółki. Ponadto nie bez znaczenia jest odciążenie zarządu (rady dyrektorów) spółki od potencjalnie absorbujących, a na pewno odpowiedzialnych czynności związanych z dokonywaniem wpisów do rejestru akcjonariuszy czy udzielaniem informacji o jego treści. Takie rozwiązanie należy uznać za istotne również ze względu na dążenie do zachowania neutralności podmiotu prowadzącego rejestr wobec akcjonariuszy, co może mieć istotne znaczenie w przypadku sporów korporacyjnych.

Treść akcentowanego przez ustawodawcę obowiązku zapewnienia bezpieczeństwa danych zawartych w rejestrze akcjonariuszy, którego realizacja spoczywa na podmiocie prowadzącym rejestr, nie została rozwinięta w przepisach KSH. W kontekście ewentualnej odpowiedzialności tego podmiotu za nienależyte wykonanie umowy o prowadzenie rejestru akcjonariuszy, ustalenia wobec tego wymagają istotne dla tej kwestii cechy określające charakter prawny takiej umowy, a także to, jakie źródła normatywne precyzują nakazy lub zakazy określonego zachowania w celu zapewnienia bezpieczeństwa danych cyfrowych zawartych w rejestrze akcjonariuszy.

1. Cechy umowy o prowadzenie rejestru akcjonariuszy wyznaczające jej charakter prawny

Nałożony na niepubliczne spółki akcyjne, spółki europejskie, proste spółki akcyjne oraz spółki komandytowo-akcyjne obowiązek rejestrowania akcji oraz zmian ich stanu prawnego w rejestrze akcjonariuszy, który prowadzony byłby przez podmiot inny niż sama spółka, realizowany jest poprzez zawarcie przez spółkę umowy z podmiotem, który ustawa kwalifikuje jako uprawniony do prowadzenia rejestru akcjonariuszy. Przepisy KSH odnoszące się do umowy o prowadzenie rejestru akcjonariuszy nie są rozbudowane. Ustawa wskazuje na nazwę umowy oraz określa jej strony (art. 328^{2} § 1, art. 328^{1} § 2, art. 300^{32} § 1, art. 300^{31} § 1 KSH). Zdecydowanie najwięcej przepisów odnosi się do tego, w jaki sposób rejestr akcjonariuszy powinien być prowadzony przez podmiot, który podejmie się tego obowiązku. Z powyższych względów sposób normowania treści stosunku zobowiązaniowego wynikającego z umowy o prowadzenie rejestru akcjonariuszy należałoby określić jako wyspowy, zbliżony do sposobu, w jaki ustawodawca poddaje regulacji niektóre umowy o świadczenie usług finansowych zawierane przez firmy inwestycyjne, które zostały wskazane w przepisach ustawy o obrocie instrumentami finansowymi (Sejm RP, 2005), np. umowa

o wykonywanie funkcji agenta emisji – art. 7a, umowa o świadczenie usług brokerskich – art. 73, umowa o prowadzenie rachunku papierów wartościowych – art. 121.

Prowadzenie rejestru akcjonariuszy stanowi zespół czynności faktycznych[1] będących usługą, która – biorąc pod uwagę, iż prowadzenie rejestru następuje w ramach działalności gospodarczej prowadzonej przez podmiot prowadzący rejestr – zazwyczaj świadczona jest odpłatnie. Składają się na nią przede wszystkim utrzymywanie rejestru akcjonariuszy w sposób zapewniający bezpieczeństwo i integralność zawartych w nim danych (art. 328^1 § 4 KSH), niezwłoczne dokonywanie wpisów na wniosek uprawnionych osób (art. 328^4 § 1 KSH), dokonywanie zawiadomień właściwych osób w związku z dokonaniem wpisu (art. 328^4 § 7 KSH), udzielanie uprawnionym osobom informacji na temat danych zawartych w rejestrze oraz wystawianie dokumentów je potwierdzających (art. 328^5 § 3, art. 328^6 § 1 KSH), a także pośredniczenie w dokonywaniu rozliczeń pomiędzy spółką a akcjonariuszami (art. 328^2 § 3, art. 328^{10} KSH). W mojej ocenie czynności podmiotu prowadzącego rejestr akcjonariuszy w swej zdecydowanej większości mają charakter czynności faktycznych, a jednocześnie wątpliwe jest występowanie wśród nich czynności prawnych z uwagi na brak spełnienia konstytutywnego dla nich oświadczenia woli podmiotu prowadzącego rejestr (np. przy czynności dokonywania wpisu do rejestru). Umowa o prowadzenie rejestru akcjonariuszy stanowi zatem typologicznie umowę o świadczenie usługi, do której odpowiednie zastosowanie znajdą przepisy Kodeksu cywilnego o zleceniu na podstawie odesłania zawartego w art. 750 KC (Leśniak, 2022, s. 399–400; Pabis, 2023, nb. 1; Popiołek, 2022, s. 562 i nast.; Pinior & Strzępka, 2024, nb. 2–3). W szczególności należy podkreślić, że istniejących przepisów KSH, które odnoszą się do umowy o prowadzenie rejestru akcjonariuszy, nie można określić mianem pełnej, wyczerpującej regulacji prowadzącej do normatywnej indywidualizacji takiej umowy. Ich treść ani szczegółowość w wyznaczeniu elementów stosunku zobowiązaniowego nie pozwala na porównanie względem przepisów Kodeksu cywilnego czy przepisów ustaw szczególnych normujących wybrane umowne stosunki zobowiązaniowe stanowiące umowy nazwane (Radwański, 1977, s. 209; Romanowski, 2009, s. 131–132). Z tego względu umowa o prowadzenie rejestru akcjonariuszy stanowi nienazwaną umowę o świadczenie usług, która nie jest uregulowana innymi przepisami, co uzasadnia stosowanie do niej również przepisów o zleceniu (art. 750 KC).

Taką kwalifikację charakteru prawnego umowy o prowadzenie rejestru akcjonariuszy wspiera również argumentacja odwołująca się do treści art. 328^2 § 2 oraz art. 300^{32} § 2 KSH, które stanowią o możliwości rozwiązania umowy przez podmiot prowadzący rejestr akcjonariuszy jedynie z ważnych powodów, z zachowaniem terminu wypowiedzenia nie krótszego niż trzy miesiące. Dostrzegalne jest w nich wy-

1 Odmiennie, akcentując w świadczeniu podmiotu prowadzącego rejestr akcjonariuszy współwystępowanie czynności faktycznych oraz czynności prawnych, postrzega to W. Popiołek (2022, s. 564 i nast.).

raźne podobieństwo do treści normy wyrażonej w art. 746 § 2 KC, poprzez odwołanie do kryterium „ważnych powodów" jako przesłanki wypowiedzenia umowy, a także przesądzenie, iż umowa może zostać rozwiązana jednostronnie poprzez złożenie oświadczenia o jej wypowiedzeniu. Jednocześnie wskazane przepisy KSH wyrażają normy szczególne wobec art. 746 § 2 KC w kontekście możliwości wypowiedzenia umowy o prowadzenie rejestru akcjonariuszy.

Usługa prowadzenia rejestru akcjonariuszy, obejmująca także obowiązki związane z dokonywaniem wpisów w rejestrze czy udzielaniem informacji na temat zawartości rejestru, świadczona jest na rzecz spółki. Brak jest podstaw do stwierdzenia, aby świadczenie podmiotu prowadzącego rejestr spełniane było na rzecz np. akcjonariuszy, nawet przy uwzględnieniu posiadania przez nich interesu prawnego w związku z dokonywaniem wpisów w rejestrze czy przyznaniem im uprawnień informacyjnych dotyczących treści rejestru[2].

Powyżej przedstawiona charakterystyka umowy o prowadzenie rejestru akcjonariuszy pozwala na stwierdzenie, że ma ona charakter obustronnie zobowiązujący, wzajemny i odpłatny[3], przynajmniej co do zasady wynikającej z zarobkowego charakteru czynności prowadzenia rejestru akcjonariuszy. Należy jednak zauważyć, że przepisy KSH nie przesądzają o treści zobowiązania spółki w stosunku do podmiotu prowadzącego rejestr. Ponadto jest to umowa konsensualna (Izdebski, 2021a, s. 53), ponieważ do powstania stosunku zobowiązaniowego nie jest wymagana zmiana władztwa nad żadną rzeczą, w szczególności nie jest wymagane dokonanie żadnej czynności faktycznej mającej za przedmiot np. rejestr akcjonariuszy, dokumenty mogące stanowić podstawę wpisu do rejestru czy inne dokumenty z nim związane, a wystarczy złożenie odpowiednich oświadczeń woli przez strony umowy (Radwański, 2002, s. 182; Radwański, 2005, s. 223–224). Stosunkowo uboga treść przepisów KSH mających zastosowanie do powstania i ustania tego stosunku zobowiązaniowego oraz wynikających z niego praw i obowiązków stron skłania do uznania, iż umowa o prowadzenie rejestru akcjonariuszy stanowi *contractus innominatus*, nawet wobec ustawowego określenia unikatowej nazwy takiej umowy.

Zobowiązanie podmiotu prowadzącego rejestr ma charakter ciągły (trwały) (Izdebski, 2021a, s. 52; 2021b, s. 20), wobec czego może ono wygasnąć m.in. wskutek upływu czasu, na który została zawarta umowa, rozwiązania umowy za zgodą obu stron bądź dokonania jednostronnej czynności wypowiedzenia umowy z ważnych powodów przez podmiot prowadzący rejestr, przy czym oświadczenie to będzie wywoływało skutek *ex nunc* (Wyrok Sądu Najwyższego, 2004; Wyrok Sądu Najwyższego, 2007). Natomiast zobowiązanie spółki – jeśli przyjmiemy, że na podstawie umowy

2 Pogląd stanowiący, że umowa o prowadzenie rejestru akcjonariuszy stanowi umowę o świadczenie na rzecz osoby trzeciej, wyraził Izdebski (2021a, s. 54–56; 2021b, s. 18).

3 Por. ogólną charakterystykę nienazwanych umów o świadczenie usług przedstawioną w Wyroku Sądu Apelacyjnego w Warszawie (2012) oraz Izdebski (2021a, s. 54).

spółka zobowiązana jest płacić określone wynagrodzenie za prowadzenie rejestru – ma charakter pieniężny i okresowy, przynajmniej w istotnej części. Nie jest bowiem wykluczone, aby część wynagrodzenia należnego podmiotowi prowadzącemu rejestr miała charakter jednorazowy lub aby spółka zobowiązana była dodatkowo do określonych świadczeń niepieniężnych na rzecz podmiotu prowadzącego rejestr, które nie stanowiłyby wynagrodzenia za prowadzenie rejestru (np. polegających na przekazaniu informacji dotyczących spółki lub akcjonariuszy).

Z uwagi na ustawowo wymaganą charakterystykę jej stron, umowa o prowadzenie rejestru akcjonariuszy ma charakter dwustronnie profesjonalny (Izdebski, 2021a, s. 53). Co do zasady obie jej strony są przedsiębiorcami, wyjąwszy potencjalne przypadki, w których spółka nie prowadziłaby działalności gospodarczej. Ponadto umowa ta jest dwustronnie kwalifikowana podmiotowo, albowiem możliwość jej zawarcia została zawężona z jednej strony do niepublicznej spółki akcyjnej lub europejskiej, prostej spółki akcyjnej oraz spółki komandytowo-akcyjnej, a z drugiej strony ograniczona do podmiotów, które na podstawie art. 4 ust. 1 ustawy o obrocie instrumentami finansowymi są uprawnione do prowadzenia rachunków papierów wartościowych, oraz – jedynie w przypadku prostej spółki akcyjnej – do notariusza prowadzącego kancelarię notarialną na terytorium Rzeczypospolitej Polskiej (art. 328^{1} § 2 oraz art. 300^{31} § 1 KSH).

2. Zasady prowadzenia rejestru akcjonariuszy

Dość uboga regulacja normatywna dotycząca umowy o prowadzenie rejestru akcjonariuszy swym zakresem koncentruje się między innymi na określeniu, w jaki sposób swoje świadczenie powinien spełnić podmiot prowadzący rejestr. Pod względem formalnym rejestr powinien być prowadzony w formie elektronicznej (art. 328^{1} § 3, art. 300^{31} § 3 KSH) – bazy danych utrzymywanej przez podmiot prowadzący rejestr i przechowywanej przez ten podmiot (np. baza danych znajdująca się na urządzeniu notariusza prowadzącego rejestr[4]) albo przez osobę trzecią działającą na jego zlecenie (np. baza danych przechowywana na serwerze usługodawcy hostingowego, z którego usług korzysta podmiot prowadzący rejestr) (Leśniak, 2022, s. 400–401). Rejestr może również funkcjonować w oparciu o zdecentralizowaną i rozproszoną bazę danych działającą np. z wykorzystaniem technologii *blockchain*[5], aczkolwiek również w takim przypadku podmiot prowadzący rejestr powinien posiadać wy-

4 Zob. szerzej na temat dokonywania wpisów w rejestrze akcjonariuszy prowadzonym przez notariusza: (Wrzecionek, 2021, s. 52–54).

5 Zob. szerzej na temat wątpliwości dotyczących możliwości wykorzystania tej technologii w kontekście jej uwarunkowań technologicznych oraz wymaganej kwalifikacji podmiotowej podmiotu prowadzącego rejestr: Czaplicki (2023, s. 26–28); zob. też: Dyrduł (2024, s. 67–70); Sójka (2021, s. 28–31).

łączne prawo odczytywania jego zawartości oraz dokonywania wpisów, ich modyfikacji i usuwania.

Fundamentalnymi zasadami, które determinują w sposób materialny prowadzenie rejestru akcjonariuszy, są zapewnienie przez podmiot go prowadzący bezpieczeństwa i integralności danych znajdujących się w rejestrze (art. 328^{1} § 4, art. 300^{31} § 4 KSH). Warto zauważyć, że te właściwości określające jakość świadczenia podmiotu prowadzącego rejestr zostały przez ustawodawcę wyrażone *explicite* w pierwszych przepisach normujących rejestr akcjonariuszy odpowiednio dla spółki akcyjnej oraz prostej spółki akcyjnej. Ponadto *in principio* w tych przepisach pojawia się sformułowanie: „Niezależnie od formy rejestru akcjonariuszy podmiot prowadzący ten rejestr prowadzi go w sposób, który zapewnia bezpieczeństwo i integralność zawartych w nim danych". Okoliczności te uzasadniają uznanie, że zachowanie bezpieczeństwa i integralności danych zawartych w rejestrze akcjonariuszy stanowią najważniejsze wartości wyznaczające sposób spełnienia świadczenia wynikającego z umowy o prowadzenie rejestru akcjonariuszy przez podmiot prowadzący ten rejestr.

Ponadto rejestr akcjonariuszy powinien być prowadzony w sposób zapewniający szybkie dokonywanie w nim wpisów, a więc tym samym w sposób minimalizujący czas trwania rozbieżności pomiędzy stanem faktycznym a stanem prawnym odzwierciedlonym w treści rejestru[6]. Konkretyzacją tej powinności jest wskazanie, że wpisy powinny zostać dokonywane niezwłocznie po zgłoszeniu żądania, nie później jednak niż w ciągu tygodnia (art. 328^{4} § 1 KSH), względnie siedmiu dni (art. 300^{34} § 4 KSH). Zapewnieniu realizacji tej zasady służy ograniczony zakres obowiązku badania przez podmiot prowadzący rejestr legalności i autentyczności dokumentów stanowiących podstawę wniosku o wpis (art. 328^{4} § 5 KSH, art. 300^{34} § 5 KSH).

Czwartą zasadą wyznaczającą sposób prowadzenia rejestru akcjonariuszy jest zapewnienie poufności zawartych w nim danych. Można ją postrzegać również jako zasadę ograniczonej jawności danych zawartych w rejestrze, której beneficjentami mogą być wyłącznie spółka oraz jej akcjonariusze (art. 328^{5} § 1 KSH, art. 300^{35} § 1 KSH). Na pewien sposób z prawa tego, aczkolwiek w zakresie ograniczonym treścią świadectwa rejestrowego, korzystać mogą zastawnicy i użytkownicy uprawnieni do wykonywania prawa głosu z akcji (328^{6} § 1 KSH).

Zasady prowadzenia rejestru akcjonariuszy wyznaczone zostały normami o charakterze imperatywnym[7], przez co wyznaczają one treść zobowiązania podmiotu prowadzącego rejestr, które wynika z umowy o prowadzenie rejestru akcjonariuszy, bez względu na treść takiej umowy. Uzasadnienie takiej oceny stanowi po pierwsze treść przywołanych powyżej przepisów, które w sposób konkretny i bezwzględny wyrażają

6 Zob. szerzej: Godlewski & Sójka (2023, s. 22–24).

7 Tak również: Popiołek (2022, s. 560–561). Odmienny, lecz nieuzasadniony w żaden sposób, pogląd o względnie obowiązującym charakterze norm prawnych Kodeksu spółek handlowych kształtujących zasady prowadzenia rejestru akcjonariuszy wyraził Izdebski (2021b, s. 20).

nakazy odpowiedniego zachowania się przez podmiot prowadzący rejestr oraz nie dopuszczają odmiennego uregulowania jego obowiązków przez treść umowy o prowadzenie rejestru akcjonariuszy. Po drugie na bezwzględny charakter norm wyznaczających sposób prowadzenia rejestru akcjonariuszy wskazują rezultaty funkcjonalnej wykładni wyżej przywołanych przepisów prawnych. Z uwagi na rolę rejestru akcjonariuszy w zapewnieniu właściwego funkcjonowania spółki oraz ochrony interesów akcjonariuszy, powinien on działać w każdej spółce w sposób analogiczny, z uwzględnieniem istotnych właściwości preferowanych przez ustawodawcę, które zostały wyrażone w treści przepisów prawnych. Wobec tego efektywne zapewnienie takiego sposobu prowadzenia rejestru akcjonariuszy może nastąpić wyłącznie w oparciu o normy o charakterze bezwzględnie obowiązującym lub semiimperatywnym.

W mojej ocenie brak jest jakichkolwiek podstaw do przyjęcia semiimperatywnego charakteru norm prawnych wynikających z przepisów m.in. art. 328^{1} § 3, art. 328^{1} § 4, art. 300^{31} § 3 KSH, art. 300^{31} § 4 KSH, co jednak nie wyklucza umownego rozszerzenia obowiązków podmiotu prowadzącego rejestr akcjonariuszy dotyczących sposobu jego prowadzenia. Można natomiast rozważać jednostronnie modyfikowalny charakter norm wynikających z przepisów art. 328^{4} § 1 oraz art. 300^{34} § 4 KSH w zakresie wyznaczenia maksymalnego terminu, w ciągu którego podmiot prowadzący rejestr akcjonariuszy powinien dokonać wpisu w rejestrze na żądanie osoby uprawnionej. Generalnie jednak liczba przepisów regulujących prowadzenie rejestru akcjonariuszy, których treść dawałaby asumpt do twierdzenia o semiimperatywnym charakterze wynikających z nich norm prawnych (i to zapewne jedynie w pewnym zakresie), jest ograniczona. Ponadto twierdzenie takie musiałoby zostać skonfrontowane z ryzykiem naruszenia interesów spółki lub interesów akcjonariuszy wskutek częściowej umownej modyfikacji treści obowiązków podmiotu prowadzącego rejestr, które określone zostały przez ustawę.

Z uwagi na tematykę niniejszego opracowania, bliższego przedstawienia wymaga obowiązek zapewnienia bezpieczeństwa i integralności danych zawartych w rejestrze przez podmiot prowadzący rejestr. Został on wyrażony w art. 328^{1} § 4 oraz art. 300^{31} § 4 KSH w sposób bardzo ogólny i przez to wymagający wypełnienia go treścią. Biorąc pod uwagę stwierdzony charakter prawny umowy o prowadzenie rejestru akcjonariuszy, podmiot prowadzący rejestr zobowiązany jest do stałego wykonywania czynności faktycznych dotyczących prowadzenia rejestru i dokonywania w nim wpisów, bez ponoszenia odpowiedzialności za określony, skonkretyzowany efekt tych działań. Nie stanowi go *per se* abstrakcyjny obowiązek dokonywania wpisów w rejestrze akcjonariuszy – treść zobowiązania nie przewiduje obowiązku dokonania określonej liczby wpisów o konkretnej treści, a tylko w takim wypadku moglibyśmy mówić o określonym rezultacie wynikającym z wykonania zobowiązania przez podmiot prowadzący rejestr. Zatem ponosi on odpowiedzialność odszkodowawczą wobec spółki w przypadku wyrządzenia szkody wskutek niezachowania należytej – profesjonalnej – staranności przy

prowadzeniu jej rejestru akcjonariuszy[8]. Określenie, na czym polega obowiązek zapewnienia bezpieczeństwa i integralności danych znajdujących się w rejestrze akcjonariuszy, stanowi zatem niezbędny element procesu zmierzającego do ustalenia wzorca oceny oczekiwanego zachowania podmiotu prowadzącego rejestr akcjonariuszy, co z kolei jest potrzebne do stwierdzenia, czy podmiot ten odpowiedzialny jest za szkodę wyrządzoną wskutek prowadzenia rejestru bez zachowania należnego bezpieczeństwa i integralności zawartych w nim danych[9].

Pojęcia „bezpieczeństwa danych" oraz „integralności danych" nie zostały normatywnie zdefiniowane, aczkolwiek stanowią określenia o fundamentalnym znaczeniu dla współczesnej informatyki[10]. Nie są one synonimami, jednak treści obu pojęć są w pewien sposób wobec siebie komplementarne poprzez zaakcentowanie stałego, pewnego i niezakłóconego przez czynniki zewnętrzne dostępu do danych przez te osoby, które zgodnie z intencją ich właściciela powinny móc je odczytywać, zapisywać, modyfikować lub usuwać.

Pierwsze pojęcie oznacza strategie i procesy, które pomagają chronić poufne dane przed nieuprawnionym dostępem, uszkodzeniem i utratą (Wikipedia, 2024). Typowe technologie wykorzystywane w celu zapewnienia bezpieczeństwa danych to szyfrowanie danych, zapewnienie dostępu do danych tylko dla autoryzowanych użytkowników (np. poprzez odpowiednio skomplikowane hasło, klucze algorytmiczne, dane biometryczne itd.), maskowanie danych wrażliwych i wykonywanie kopii zapasowych. Przykładem zdarzenia powodującego naruszenie bezpieczeństwa danych będzie np. ich odczytanie lub skopiowanie przez osoby niepowołane – inne niż podmiot prowadzący rejestr, spółka lub akcjonariusze (potocznie zwane „kradzieżą da-

8 Na marginesie należy zauważyć, że odpowiedzialność spółki wobec akcjonariuszy za szkodę wyrządzoną np. utratą lub uszkodzeniem danych zawartych w rejestrze bądź uzyskaniem do nich dostępu przez osoby trzecie jest w zasadzie wyłączona w myśl art. 429 Kodeksu cywilnego i zawartą w tym przepisie przesłankę powierzenia wykonywania czynności związanych z prowadzeniem rejestru akcjonariuszy podmiotowi profesjonalnemu. Nie dotyczy to sytuacji, w których winę za wyrządzenie szkody akcjonariuszowi przypisać można spółce, co może prowadzić do odpowiedzialności odszkodowawczej spółki opartej o art. 415 Kodeksu cywilnego np. w razie udostępnienia danych potrzebnych do uzyskania dostępu do rejestru akcjonariuszy osobie trzeciej albo nienależytego zabezpieczenia takich danych przed dostępem osób trzecich. Wykluczone nie jest również ponoszenie odpowiedzialności odszkodowawczej wobec akcjonariusza przez podmiot prowadzący rejestr akcjonariuszy na podstawie art. 415 Kodeksu cywilnego, jeżeli bezprawne – w kontekście naruszenia np. zasad prowadzenia rejestru akcjonariuszy przedstawionych powyżej – i zawinione zachowanie podmiotu prowadzącego rejestr doprowadzi do wyrządzenia szkody akcjonariuszowi (por.: Izdebski, 2021b, s. 20; Pabis, 2023, nb. 4). Za możliwe w pewnych sytuacjach należy uznać ponadto ponoszenie przez podmiot prowadzący rejestr akcjonariuszy równoległej – opartej o ten sam czyn – odpowiedzialności kontraktowej wobec spółki i deliktowej wobec akcjonariusza.

9 Na temat odpowiedzialności podmiotu prowadzącego rejestr akcjonariuszy zob.: Popiołek (2022, s. 566 i nast.).

10 Powszechnie przyjęte znaczenie tych pojęć określa treść normy ISO/IEC 27000.

nych") albo zaszyfrowanie lub usunięcie danych przez osobę trzecią lub algorytm (tzw. szkodliwe lub złośliwe oprogramowanie).

Z kolei „integralność danych" powszechnie rozumiana jest jako właściwość danych stanowiąca o ich dokładności, kompletności i prawdziwości, dzięki czemu dane możemy określić jako wiarygodne, a ich treść (wartość) jako zgodną z intencją osoby, która je wprowadziła (Wikipedia, 2024). W pewnych przypadkach naruszenie integralności danych może stanowić efekt naruszenia bezpieczeństwa danych, jeśli nieintencjonalna zmiana treści (wartości) danych została dokonana wskutek nieautoryzowanego dostępu do nich. Częstymi powodami naruszenia integralności danych są błędy podczas ich odczytywania, zapisywania lub transmisji, a także awarie sprzętowe. Zapewnienie „integralności danych" oznacza dokonanie czynności zapobiegających ich nieintencjonalnej modyfikacji, która może doprowadzić do zniekształcenia danych lub może uniemożliwiać ich odczytanie, np. jeśli akcjonariusz X posiada 100 akcji spółki, a w rejestrze akcjonariuszy znajduje się informacja o przypisanej mu liczbie akcji 1010 albo wpis o treści bn#34!*. Do najczęściej stosowanych środków zapobiegawczych należą algorytmy wykrywające lub korygujące błędy (np. w oparciu o sumy kontrolne danych lub zgromadzone dane naprawcze) oraz przechowywanie kopii zapasowych danych.

3. Standardy zapewnienia bezpieczeństwa danych zawartych w rejestrze akcjonariuszy

Przepisy Kodeksu spółek handlowych, ani żadnego powiązanego z tą ustawą aktu prawnego (np. rozporządzenia albo innej ustawy przez odesłanie), nie precyzują tego, na jakich działaniach podmiotu prowadzącego rejestr akcjonariuszy miałoby polegać zapewnienie bezpieczeństwa danych zawartych w tym rejestrze. Szczegółowego określenia wymagań związanych z zapewnieniem bezpieczeństwa danych, które w bezpośredni sposób miałyby zastosowanie do rejestru akcjonariuszy, nie zawierają normy żadnego aktu prawnego rangi ustawowej. Ze względu na zawartość rejestru akcjonariuszy oraz jego ustawowo określony sposób prowadzenia wydaje się, że nie stanowi on – ocieniając to z perspektywy realizacji obowiązku zapewnienia bezpieczeństwa – zbioru danych *sui generis*, który wymagałby opracowania i wdrożenia indywidualnych środków w zakresie bezpieczeństwa. Przeciwnie, wykazuje on funkcjonalne podobieństwo do innych zbiorów danych w postaci cyfrowej gromadzonych i przetwarzanych między innymi przez domy maklerskie, banki, firmy inwestycyjne czy *sensu largo* podmioty świadczące usługi na rynku finansowym, co będzie uzasadniało zastosowanie wspólnych, bardziej uniwersalnych zasad w zakresie zapewnienia bezpieczeństwa czy integralności danych zawartych w rejestrze akcjonariuszy. W tych okolicznościach za dopuszczalne wydaje się, aby treść umowy o prowadzenie rejestru akcjonariuszy wska-

zywała na działania lub środki, które podmiot prowadzący rejestr będzie musiał podjąć w celu zachowania bezpieczeństwa danych zawartych w rejestrze.

Istotną aktywnością legislacyjną w obszarze cyberbezpieczeństwa, w tym zapewnieniem bezpieczeństwa danych w postaci cyfrowej, w ostatnich latach wykazują się natomiast organy Unii Europejskiej. Jakkolwiek w pierwszej kolejności koncentrują się one na stworzeniu systemów współpracy pomiędzy państwami członkowskimi w zakresie cyberbezpieczeństwa oraz zapewnieniu niezawodności działania usług publicznych (Parlament Europejski i Rada UE, 2016 – obowiązywała do 17 października 2024 r. i została uchylona przez: Parlament Europejski i Rada UE, 2022b; Parlament Europejski i Rada UE, 2019), podmiotowy i przedmiotowy zakres unijnych aktów prawnych w tym zakresie coraz odważniej rozszerzany jest na przedsiębiorców świadczących usługi czy produkujących towary krytycznie istotne dla funkcjonowania rynku wewnętrznego (Parlament Europejski i Rada UE, 2022b) oraz produkty wykorzystujące oprogramowanie cyfrowe (Parlament Europejski i Rada UE, 2024). Aktualnie obowiązującym aktem prawa powszechnego, który miałby zastosowanie do części podmiotów prowadzących rejestr akcjonariuszy, m.in. banków, firm inwestycyjnych czy domów maklerskich, jest Rozporządzenie 2022/2554 (Parlament Europejski i Rada UE, 2022a), którego art. 5–15 w sposób kierunkowy wskazują na konieczność podjęcia określonych działań w celu zapewnienia bezpieczeństwa teleinformatycznego m.in. związanego z utrzymywaniem baz danych, które polegają m.in. na wykorzystywaniu aktualnych i niezawodnych systemów i narzędzi teleinformatycznych czy tworzeniu kopii zapasowych danych.

Wobec braku czy niedostatecznie określonych wzorców normatywnych definiujących sposób wykonania obowiązków ustawowych lub umownych, zachowanie należytej staranności przy wykonywaniu zobowiązania polega m.in. na wykonywaniu go w sposób zgodny z powszechnymi w danych stosunkach (branży) standardami, choćby te nie wynikały z aktów prawa powszechnie obowiązującego. W oparciu o nie można skonstruować wzorzec należytego postępowania, który będzie stanowił podstawę oceny tego, czy podmiot prowadzący rejestr akcjonariuszy spełnił swoje zobowiązanie w sposób właściwy. Z uwagi na ograniczenia objętościowe niniejszego opracowania, a także treści poniżej przywoływanych dokumentów koncentrujące się na zagadnieniach związanych z zarządzaniem oraz systemami teleinformatycznymi, nie będę analizował szczegółowo ich treści.

Najbardziej fundamentalne standardy należytego postępowania w zakresie zapewnienia bezpieczeństwa danych cyfrowych zawierają normy opracowane przez Międzynarodową Organizację Normalizacyjną. Podstawową normą, która swym szerokim zakresem obejmuje również zasady postępowania z danymi w celu zapewnienia ich bezpieczeństwa, jest ISO 9001:2015, określająca wymagania, które powinien spełniać system zarządzania jakością w organizacji. O wiele bardziej szczegółowe i ukierunkowane na zapewnienie bezpieczeństwa działania systemów teleinformatycznych są normy ISO/IEC 27001 oraz ISO/IEC 27002. Podczas gdy pierwsza

z nich ma za zadanie standaryzować systemy zarządzania bezpieczeństwem informacji i można ją określić mianem systemotwórczej w tym zakresie (Łuczak & Tyburski, 2009, s. 4–5), druga z powołanych norm określa szczegółowe wytyczne związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem Systemu Zarządzania Bezpieczeństwem Informacji. Stanowi merytoryczne i opisowe rozwinięcie normy ISO/IEC 27001, a cele stosowania zabezpieczeń omówione w tej drugiej normie są powszechnie uznawanymi praktykami zarządzania bezpieczeństwem informacji (Disterer, 2013, s. 97–98). Na podstawie obu wskazanych norm Polski Komitet Normalizacyjny opracował i opublikował odpowiednie Polskie Normy np. PN-EN ISO/IEC 27002.

Kolejną grupę standardów związanych z zapewnieniem bezpieczeństwa danych cyfrowych, które adresowane są do podmiotów świadczących usługi finansowe, stanowią akty normatywne Komisji Nadzoru Finansowego. Kierowana do banków Rekomendacja D (Komisja Nadzoru Finansowego, 2013) zawiera szczegółowe wytyczne związane z zapewnieniem bezpieczeństwa danych cyfrowych, w szczególności ochroną przed nieuprawnionym dostępem, działaniem szkodliwego oprogramowania czy zapewnieniem ciągłości działania systemów teleinformatycznych oraz wykonywania kopii zapasowych danych. Szczegółowe obowiązki o podobnej treści dotyczące m.in. zapewnienia bezpieczeństwa danych przetwarzanych przez firmy inwestycyjne zawierają wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych (Komisja Nadzoru Finansowego, 2014).

W przedmiocie ustalenia wzorca należytej staranności podmiotu prowadzącego rejestr akcjonariuszy znaczenie mogą również odgrywać standardy zapewnienia bezpieczeństwa danych osobowych – z uwagi na potencjalne ich umieszczenie w rejestrze akcjonariuszy. Norma ISO/IEC 27701 stanowi rozwinięcie przywołanej wyżej normy ISO/IEC 27001 w zakresie ochrony prywatności. Oprócz niej standardy bezpiecznego przetwarzania danych osobowych może wyznaczać np. norma ISO/IEC 27018, która dotyczy ochrony danych osobowych znajdujących się w chmurze.

Aktem normatywnym prawa krajowego o najbardziej konkretnej treści w zakresie wytyczenia treści obowiązku zapewnienia bezpieczeństwa danych cyfrowych jest rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Rada Ministrów RP, 2024). Ponieważ adresatem tego aktu prawnego są podmioty wykonujące zadania publiczne, może on stanowić wzorzec należytej staranności podmiotu prowadzącego rejestr akcjonariuszy co najwyżej w drodze analogii. Szczegółowe zasady dotyczące zapewnienia bezpieczeństwa informacji (danych) zawiera § 19 rozporządzenia, przy czym w jego treści ustawodawca odwołuje się do norm PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 27002 jako kryteriów referencyjnych, co potwierdza wskazaną powyżej wiodącą rolę tych norm, łącznie z ich pierwowzorami opracowa-

nymi przez Międzynarodową Organizację Normalizacyjną, w określeniu powszechnie przyjętych standardów w dziedzinie bezpieczeństwa danych cyfrowych.

Szczegółowych zasad zapewnienia bezpieczeństwa danych przez notariusza prowadzącego rejestr akcjonariuszy prostej spółki akcyjnej nie zawierają przepisy ustawy Prawo o notariacie (Sejm RP, 1991), w szczególności jej art. 108a oraz 108b. Treści takich nie zawierają również publicznie dostępne dokumenty opracowane przez Krajową Radę Notarialną, które dotyczą funkcjonowania usługi rejestru akcjonariuszy prostej spółki akcyjnej dostępnego w systemie teleinformatycznym Rejestry Notarialne (Krajowa Rada Notarialna, 2024).

Wnioski

Do kluczowych obowiązków podmiotu prowadzącego rejestr akcjonariuszy należy zapewnienie bezpieczeństwa i integralności zawartych w nim danych. Z uwagi na zobowiązanie do świadczenia usług polegających na szeregu czynności faktycznych związanych z wprowadzaniem danych do rejestru i udostępnianiem danych w nim zawartych, podmiot prowadzący rejestr akcjonariuszy ponosi odpowiedzialność za nienależyte wykonanie tego obowiązku m.in. polegające na niezapewnieniu bezpieczeństwa danych zawartych w rejestrze.

Zarówno bezpieczeństwo, jak i integralność danych stanowią pojęcia z zakresu informatyki, a ustalenie szczegółowych nakazów czy zakazów wyznaczających treść tych obowiązków musi nastąpić z odwołaniem się do pozasystemowych źródeł normatywnych, w szczególności dokumentów normalizacyjnych. W najbliższym czasie należy spodziewać się wzrostu roli aktów normatywnych w kreowaniu szczegółowych treści wytyczających standardy zapewnienia bezpieczeństwa danych cyfrowych, w tym danych zawartych w rejestrze akcjonariuszy. Wektor zmian oraz inicjatywa w tym zakresie aktualnie kreowane są przez organy Unii Europejskiej, za którymi podążają krajowe podmioty wyposażone w kompetencje prawodawcze.

W przeciwieństwie do innych podmiotów mogących prowadzić rejestr akcjonariuszy, brak jest szczegółowych wytycznych w zakresie realizacji obowiązku zapewnienia bezpieczeństwa oraz integralności danych w odniesieniu do notariuszy. Wziąwszy pod uwagę na ogół odmienne doświadczenia związane z administrowaniem zbiorami danych podobnymi do rejestru akcjonariuszy, a także zdecydowanie skromniejsze możliwości organizacyjne notariuszy, bezpieczeństwo i integralność danych zawartych w rejestrach akcjonariuszy, które prowadzą lub prowadzić będą notariusze, mogłyby zostać skuteczniej osiągnięte wówczas, gdyby szczegółowe obowiązki związane z zapewnieniem tych wartości zostałyby normatywnie określone przez organy samorządu notarialnego lub ustawodawcę.

BIBLIOGRAFIA

Czaplicki, P. (2023). Prowadzenie rejestru akcjonariuszy w formie rozproszonej i zdecentralizowanej bazy danych – uwagi na tle art. 328(1) kodeksu spółek handlowych, *IKAR*, *12*(6), 24–30.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management, *Journal of Information Security*, *4*(2), 92–100.

Dyrduł, P. (2024). Wykorzystanie Distributed Ledger Technology do prowadzenia rejestru akcjonariuszy prostej spółki akcyjnej, *Palestra*, (1), 60–71.

Godlewski, M. & Sójka, T. (2023). Zasady dokonywania wpisów w rejestrze akcjonariuszy, *Przegląd Ustawodawstwa Gospodarczego*, (9), 20–26.

Izdebski, P. (2021a). Umowa o prowadzenie rejestru akcjonariuszy – wybrane uwagi konstrukcyjno-prawne, *Przegląd Prawa Handlowego*, (2), 51–58.

Izdebski, P. (2021b). Cywilnoprawna odpowiedzialność podmiotu prowadzącego rejestr akcjonariuszy – wybrane zagadnienia, *Przegląd Prawa Handlowego*, (5), 8–25.

Komisja Nadzoru Finansowego. (2013). Uchwała nr 7/2013 z dnia 8 stycznia 2013 r. Komisji Nadzoru Finansowego w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Dziennik Urzędowy KNF z 2013 r., poz. 5.

Komisja Nadzoru Finansowego. (2014). Uchwała Nr 410/2014 z dnia 16 grudnia 2014 r. Komisji Nadzoru Finansowego w sprawie wydania „Wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w firmach inwestycyjnych", Dziennik Urzędowy KNF z 2015 r., poz. 51.

Krajowa Rada Notarialna. (2024). *Rejestry Notarialne*, https://rejestry-notarialne.pl

Leśniak, M., (2022). *Czynności notarialne dotyczące prowadzenia rejestru akcjonariuszy prostej spółki akcyjnej*. w: J. Haberko, J. Grykiel & K. Mularski (red.) *Ius civile vigilantibus scriptum est. Księga jubileuszowa Profesora Adama Olejniczaka*, (ss. 395–403), C.H. Beck.

Łuczak, J. & Tyburski, M. (2009). *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

Pabis, R. (2023). Komentarz do art. 3282. w: Z. Jara (red.), *Kodeks spółek handlowych. Komentarz,* wyd. 27, Warszawa, C.H. Beck.

Parlament Europejski i Rada UE. (2016). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dziennik Urzędowy UE, seria L, nr 194.

Parlament Europejski i Rada UE. (2019). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dziennik Urzędowy UE, seria L, nr 151.

Parlament Europejski i Rada UE. (2022a). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, Dziennik Urzędowy UE, seria L, nr 333.

Parlament Europejski i Rada UE. (2022b). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dziennik Urzędowy UE, seria L, nr 333.

Parlament Europejski i Rada UE. (2024). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności), Dziennik Urzędowy UE, seria L, nr 2024/2847.

Pinior, P. & Strzępka, J. A., (2024). Komentarz do art. 3282. w: P. Pinior & J. A. Strzępka (red.), *Kodeks spółek handlowych. Komentarz*, Warszawa, C.H.Beck.

Popiołek, W. (2022). Podmiot prowadzący rejestr akcjonariuszy jako strona umowy ze spółką akcyjną w: J. Haberko, J. Grykiel & K. Mularski (red.) *Ius civile vigilantibus scriptum est. Księga jubileuszowa Profesora Adama Olejniczaka*, (ss. 559–569), C.H. Beck.

Rada Ministrów Rzeczypospolitej Polskiej. (2024). Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dziennik Ustaw z 2024 r., poz. 773.

Radwański, Z. (2002). w: Z. Radwański (red.), *System prawa prywatnego. Tom 2. Prawo cywilne – część ogólna*, Warszawa, 182, C.H. Beck.

Radwański, Z. (2005). *Prawo cywilne – część ogólna*, C.H. Beck.

Radwański, Z. (1977). *Teoria umów*, Państwowe Wydawnictwo Naukowe.

Romanowski, M. (2009). Czy należy regulować umowy nienazwane?, *Studia Prawa Prywatnego*, *4*(2), 117–138.

Sejm Rzeczypospolitej Polskiej. (1991). Ustawa z dnia 14 lutego 1991 r. Prawo o notariacie, tekst jednolity: Dziennik Ustaw z 2024 r. poz. 1001.

Sejm Rzeczypospolitej Polskiej. (2000). Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych, tekst jednolity: Dziennik Ustaw z 2024 r., poz. 18.

Sejm Rzeczypospolitej Polskiej. (2005). Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, tekst jednolity: Dziennik Ustaw z 2024 r., poz. 722.

Sójka, T. (2021). Rejestr akcjonariuszy w postaci rozproszonej i zdecentralizowanej bazy danych, *Przegląd Ustawodawstwa Gospodarczego*, *74*(4), 26–33.

Wikipedia. (2024). Data integrity, https://en.wikipedia.org/wiki/Data_integrity

Wikipedia. (2024). Data security, https://en.wikipedia.org/wiki/Data_security

Wrzecionek, R. (2021). Wpis notarialny nabycia akcji prostej spółki akcyjnej do rejestru akcjonariuszy, *Przegląd Ustawodawstwa Gospodarczego*, *74*(2), 50–56.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 14 września 2012 r., I ACa 222/12, Legalis nr 730800.

Wyrok Sądu Najwyższego z dnia 15 lutego 2007 r., II CSK 484/06, Legalis nr 164747.

Wyrok Sądu Najwyższego z dnia 8 października 2004 r., V CK 670/03, Legalis nr 69976.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.03

Received: 30.12.2024
Accepted: 3.07.2025

Katarzyna Szczepańska
Uniwersytet im. Adama Mickiewicza w Poznaniu, Polska
katarzyna.szczepanska@amu.edu.pl
ORCID ID: https://orcid.org/0000-0002-3852-5078

Karol Ryszkowski
Uniwersytet Ekonomiczny w Krakowie, Polska
karol.ryszkowski@uek.krakow.pl
ORCID ID: https://orcid.org/0000-0003-2744-3533

Problem adekwatności rozwiązań prawnych przyjętych przez polskiego ustawodawcę dla zgromadzeń online wspólników spółek kapitałowych – ze szczególnym uwzględnieniem regulacji dotyczących prostej spółki akcyjnej

The Problem of the Adequacy of Legal Solutions Adopted by the Polish Legislator for Online Shareholder Meetings in Companies, with Particular Emphasis on the Regulation of Simple Joint-Stock Companies

Abstract: The aim of this article is to discuss the use of digital technologies to conduct online shareholder meetings in limited liability companies, joint-stock companies, and simple joint-stock companies under Polish law. The authors rely on a dogmatic analysis of amendments in this area introduced in the Polish Commercial Companies Code before and after the COVID-19 pandemic, supported by a comparative method with German and Austrian law. It is argued that the regulation of simple joint-stock companies is not compatible with the regulation of limited liability companies and joint-stock companies, and therefore three *de lege ferenda* postulates have been formulated: (1) online shareholder meetings in a simple joint-stock company should be foreseen by default as *ex lege*, not as up-to-date *ex contractu*, which will constitute a unification with the *ex lege* model already existing in limited liability companies and joint-stock companies, (2) the prerequisite of secrecy in voting should also be maintained in a simple joint-stock company, (3) more generally, due to the rapid changes in technology and the development of artificial intelligence systems, the regulation of online shareholder meetings in all types of companies should be regularly revised at certain time intervals, and these revisions should be programmed by law.

© 2025 Katarzyna Szczepańska, Karol Ryszkowski published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

Keywords: general meetings, shareholder meetings, online general/shareholder meetings, new technologies, digitalization, company law, simple joint-stock companies, joint-stock companies, limited liability companies, comparative law
Słowa kluczowe: walne zgromadzenie, zgromadzenie wspólników, zgromadzenia zdalne, nowoczesne technologie, cyfryzacja, prawo spółek, prosta spółka akcyjna, spółka z ograniczoną odpowiedzialnością, spółka akcyjna, komparatystyka prawnicza

Wprowadzenie[1,2,3,4,5]

Przedmiotem artykułu jest zagadnienie zastosowania nowych technologii w spółkach kapitałowych w aspekcie możliwości odbywania tzw. zgromadzeń *online*, co jest aktualnie dopuszczalne, w odpowiednim zakresie, w przepisach k.s.h. (Sejm RP, 2024), ze szczególnym uwzględnieniem wybranych rozwiązań przyjętych w Prostej Spółce Akcyjnej.

Przez zgromadzenia *online* (zdalne) należy rozumieć zgromadzenia, które nie odbywają się całkowicie w sposób stacjonarny (fizyczny) ani też nie odbywają się całkowicie (w pełni) w sposób wirtualny. Chodzi więc o takie zgromadzenia, dla których ustawodawca posługuje się określeniem dot. uczestnictwa w zgromadzeniach spółek kapitałowych przy wykorzystaniu środków komunikacji elektronicznej.

Problematyka odpowiedniej regulacji tego typu zgromadzeń w spółkach kapitałowych pojawiła się z całą mocą w trakcie trwania pandemii COVID-19 (dalej jako: „pandemia"), która *de facto* zmusiła do zmiany modelu odbywania posiedzeń (przynajmniej w jej trakcie) z posiedzeń (prawie wyłącznie) odbywanych w sposób stacjonarny (z udziałem osobistym) na model odbywania z wykorzystaniem nowych technologii – *online* / „zdalnie" (bez, czy też przy bardzo ograniczonej, jednoczesnej fizycznej obecności uczestników takich zgromadzeń w miejscu odbywania się zgromadzenia).

---

1 Artykuł stanowi wybraną część problematyki dotyczącej zgromadzeń *online* w spółkach kapitałowych zaprezentowaną przez Autorów w formie referatu pt. *Problem adekwatności rozwiązań prawnych przyjętych przez polskiego ustawodawcę dla zgromadzeń online wspólników spółek kapitałowych* podczas XIV Ogólnopolskiego Zjazdu Katedr Prawa Handlowego 2024 zorganizowanego w dniach 26–27 września 2024 r. przez Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.

2 Publikacja prezentuje wyniki badań naukowych przeprowadzonych w ramach projektu nr 061/WPC/2025/POT finansowanego ze środków subwencji przyznanej Uniwersytetowi Ekonomicznemu w Krakowie.

3 Badania zostały dofinansowane w ramach projektu Inicjatywa Doskonałości – Uczelnia Badawcza na Uniwersytecie im. Adama Mickiewicza w Poznaniu, numer projektu 146/07/POB5/0026, Autorka dziękuje Bibliotece Europejskiego Instytutu Uniwersyteckiego we Florencji (EUI Library) za udostępnienie zbiorów.

4 Przy przygotowaniu artykułu korzystano ze słowników języków obcych dostępnych pod adresem: https://pl.pons.com. Wszystkie tłumaczenia to tłumaczenia własne.

5 Przy przygotowaniu artykułu nie korzystano z narzędzi sztucznej inteligencji.

Było to „wymuszone" środkami sanitarnymi i ułatwione tymczasowymi rozwiązaniami legislacyjnymi, tj. przepisami szczególnymi, które obowiązywały w czasie pandemii (a częściowo także wprowadzonymi zmianami w k.s.h., które nie miały charakteru tymczasowego).

Zadaniem artykułu jest wskazanie na kierunek postulowanych, racjonalnych zmian ustawodawczych głównie w obrębie regulacji PSA, po części opierając się na argumentacji już przedstawionej w Niemczech i Austrii, mając na uwadze, że regulacji podlega w zasadzie ten sam problem czy zjawisko społeczne, co uwidoczniła pandemia, która nie tylko w UE, lecz praktycznie na całym świecie uniemożliwiła, a wręcz łączyła się z odgórnym zakazem stykania się z innymi osobami w ramach większych skupisk ludzkich oraz w zamkniętych przestrzeniach. Wpisuje się to w kierunek obrany przez ustawodawcę europejskiego postulującego digitalizację tych wszystkich dziedzin życia czy aktywności, w których jest to możliwe, pamiętając jednak przy tym, by nie doprowadzać tym samym do tzw. wykluczenia cyfrowego – wskazuje na to priorytet poprzedniej Komisji Europejskiej na lata 2019–2024 *A Europe fit for the digital age* (Komisja Europejska, 2019) oraz Komunikacja Komisji Europejskiej z dnia 19 lutego 2020 r., *Shaping Europe's digital future* (Komisja Europejska, 2020). Priorytet związany z zastosowaniem nowych technologii jest obecny również w agendzie strategicznej UE na lata 2024–2029 jako postulat *Making success of the digital transition* w ramach priorytetu *A prosperous and competitive Europe* (Rada Europejska, 2024).

1. Zagadnienia ogólne regulacji zgromadzeń online – oraz określenie luki badawczej

Na wstępie należy zaznaczyć, że artykuł dotyczy tzw. zgromadzeń *online* (zdalnych) – czyli odbywanych z wykorzystaniem środków komunikacji elektronicznej, nie będą zaś jego przedmiotem tzw. zgromadzenia w pełni wirtualne. Wyłączenie z zakresu przedmiotowego problematyki zgromadzeń w pełni wirtualnych jest związane z tym, że choć w polskiej literaturze kwestia ta była już przedmiotem opracowań, to jednak, aby dokonać jej dalszego pogłębienia, wymagane byłyby ramy objętościowe kolejnego artykułu. Z analizy wyłączona została też problematyka spółki publicznej.

W prawie polskim zasadniczym celem nowelizacji (Sejm RP, 2020) podjętej w marcu 2020 r. (dalej jako: nowelizacja 2020) było umożliwienie funkcjonowania organów spółek kapitałowych w trybie zdalnym albo zbliżonym do trybu zdalnego (Sejm RP, 2020a).

W uzasadnieniu projektu nowelizacji 2020 wskazano, że rozprzestrzenianie się koronawirusa oraz stosowane środki ochrony mające na celu ograniczenie związanego z tym zagrożenia powodują istotne ryzyko paraliżu decyzyjnego dla blisko 500 tys. spółek kapitałowych tworzących polską gospodarkę (Sejm RP, 2020a, s. 98).

Problematyka zgromadzeń odbywanych *online*, po przyjęciu nowelizacji 2020, w bardzo krótkim czasie stała się przedmiotem wypowiedzi (dość licznych) doktryny (Szczurowski, 2020, s. 46–54). Wypowiedzi te miały postać artykułów o charakterze analizującym zagadnienia przeważnie w aspekcie systemowym (jak i typowo dogmatyczne analizy komentatorskie).

Generalnie, wypowiedzi te można zaklasyfikować w dwóch nurtach: jeden z nich dotyczył zgromadzeń (m.in. Jerzmanowski, 2020, s. 337; Leśniak, 2020a, s. 20; Leśniak, 2020b, s. 753; Mazgaj, 2022, s. 140; Modrzejewski, 2021, s. 5; Pyka, 2022, s. 346–347; Szumański, 2020, s. 4; Szymański, 2020, s. 496; Wach-Pawliczak, 2020, s. 163; Żaba, 2020, s. 13), a drugi zarządów i rad nadzorczych (Baszczyk, 2022, s. 26; Nalazek & Letolc, 2020, s. 12; Starczewska, 2020, s. 856; Osajda, 2020, s. 18; Ostrowski, 2020, s. 32).

Trzeci zaś – poboczny – nurt dotyczył organów kolegialnych podmiotów uregulowanych poza k.s.h.: spółdzielni (Żaba, 2021, s. 962) czy organów banku spółdzielczego (Lenio & Srokosz, 2022, s. 74).

Natomiast, dla porządku, odnotować należy również, że problematyka była też przedmiotem analiz przy „poprzednich" nowelizacjach k.s.h. (przykładowo m.in.: Kappes, 2009, s. 11; Kocot, 2011, s. 4; Krukowska-Korombel, 2010, s. 36; Wrzecionek, 2014, s. 51), tj. po wprowadzeniu do regulacji SA w 2009 r. możliwości wykorzystania środków komunikacji elektronicznej.

W trakcie analizy zagadnienia zgromadzeń *online* w spółkach kapitałowych wyłoniły się w zasadzie trzy główne grupy kwestii bardziej przekrojowych, czy też w pewnym sensie o zakresie systemowym: kwestia spójności/niespójności regulacji spółki z o.o. i SA z regulacją PSA; kwestie prawnoporównawcze, a także kwestie dotyczące formalnych aspektów związanych z udziałem w zgromadzeniu notariusza. Łamy tego artykułu pozwolą jedynie na uwypuklenie najistotniejszych zagadnień w ramach pierwszej osi (niespójności regulacji sp. z o.o. i SA, a regulacji PSA). Dlatego wybrany został do analizy aspekt, który wymaga najpilniejszego rozwiązania, przemyślenia, przepracowania i opracowania przez prawodawcę. Jedynie punktowo przedstawione zostaną w tym artykule odniesienia prawnoporównawcze na kanwie niespójności między przepisami sp. z o.o. i SA a PSA, albowiem na takie pozwalają ramy tego opracowania i porównanie będzie wystarczające, by wskazać uzasadnienie dla wysuwanych postulatów *de lege ferenda*.

Sytuacja *lockdownu* doprowadziła do konieczności zmodyfikowania i uelastycznienia dotychczasowego modelu (zasad) odbywania zgromadzeń, wprowadzając możliwość odbywania ich w sposób zdalny (*online*), co umożliwiły również istniejące już rozwiązania technologiczne. Z drugiej strony należy mieć na uwadze, że pandemia znacznie przyśpieszyła, najprawdopodobniej i tak nieuchronnie zbliżające się, zmiany przepisów zezwalające na – w coraz szerszym zakresie – korzystanie z nowych technologii do odbywania zgromadzeń, które były zgłaszane przez praktykę już przed pandemią.

Jak wskazano powyżej, pewien element „nowości" i świeżości w ujęciu zagadnienia zgromadzeń *online* w spółkach kapitałowych, którego próby uchwycenia dokonuje artykuł, dotyczy, jak się wstępnie wydaje, niekompatybilności czy też niespójności systemowej pomiędzy uregulowaniami przewidzianymi dla spółki z o.o. i SA a uregulowaniem przewidzianym dla PSA. Problematyka wskazanej niekomp tybilności nie była jeszcze dotąd szerzej w literaturze poruszana (pewne wzmianki zawarto w: Mazgaj, 2022, s. 140). Próbę uzupełnienia tej luki podejmie artykuł, wskazując po przeprowadzeniu analizy na trzy postulaty *de lege ferenda* uspójniające regulację zgromadzeń online w PSA z regulacjami w sp. z o.o. oraz w SA

2. Ewolucja podejścia polskiego ustawodawcy odnośnie do możliwości podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej (w tym odbywania zgromadzeń online) wraz z odniesieniami prawnoporównawczymi

Należy odnotować ewolucję podejścia polskiego ustawodawcy do możliwości podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej (w tym odbywania zgromadzeń *online*) w spółkach kapitałowych.

Mamy tu do czynienia z dwoma pojęciami: po pierwsze – podejmowaniem uchwał przy wykorzystaniu środków komunikacji elektronicznej, po drugie – odbywaniem zgromadzeń przy wykorzystywaniu środków komunikacji elektronicznej (odbywanie zgromadzeń *online*). Na potrzeby niniejszego artykułu przez odbywanie zgromadzeń przy wykorzystywaniu środków komunikacji elektronicznej (odbywanie zgromadzeń *online*) rozumiemy zgromadzenia, które nie są w pełni wirtualne, tylko mają fizyczne miejsce zgromadzenia, a część uczestników bierze w nich udział przy wykorzystaniu środków komunikacji elektronicznej. Natomiast poprzez podejmowanie uchwał przy wykorzystaniu środków komunikacji elektronicznej rozumiemy podejmowanie uchwał w taki sposób (przy użyciu środków komunikacji elektronicznej), zarówno na zgromadzeniach spółek kapitałowych, jak i poza zgromadzeniami spółek w przypadkach, gdy przepisy k.s.h. na to pozwalają (obecnie jest to dopuszczalne w przypadku sp. z o.o. oraz PSA).

Nowelizacja z 2009 r. to pierwsza chronologicznie regulacja, która dała możliwości wykorzystania środków komunikacji elektronicznej. Pojawiła się ona na gruncie spółki akcyjnej w ramach przepisów art. 406^5 k.s.h. na mocy nowelizacji k.s.h. z 5.12.2008 r., która weszła w życie 3.08.2009 r. Stanowiła ona wykonanie art. 8 dyrektywy 2007/36/WE Parlamentu Europejskiego i Rady z 11.07.2007 r. w sprawie wykonywania niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym. Pomimo tego, że dyrektywa ta odnosiła się jedynie do spółek publicznych, to jednak polski legislator rozszerzył zakres podmiotowy norm implementowanych do prawa

polskiego z prawa europejskiego na wszystkie spółki akcyjne, a więc również na spółki akcyjne prywatne (niepubliczne) (Szumański, 2020, s. 6).

Z punktu widzenia dalszych rozważań istotnym jest, że sposób udziału w walnym zgromadzeniu spółki akcyjnej (w formie zdalnej) działał wtedy tylko z mocy statutu spółki (*ex contractu*).

Następnie nastąpiła nowelizacja przepisów sp. z o.o. z 2019 r. (czyli jeszcze przed pandemią), która wtedy „przeniosła" niemal dosłownie treść przepisów z SA na grunt sp. z o.o. Wprowadzono przepis art. 234^1 k.s.h., zasadniczo wzorowany na art. 406^5 k.s.h. W ten sposób zrealizowano w obrębie spółek kapitałowych jako taką spójność systemową w stosunku do zgromadzeń odbywanych *online* (Sejm RP, 2019). W 2020 r. w ramach nowelizacji z marca 2020 (Sejm RP, 2020) ustawodawca zmodyfikował zasady wynikające z art. 234^1 k.s.h. oraz art. 406^5 k.s.h. w ten sposób, że w wyniku zmiany przepisów rozwiązaniem *ex lege* w spółkach z o.o. i w spółkach akcyjnych stała się możliwość zdalnego uczestnictwa w zgromadzeniach, zaś jedynie wyłączenie tej możliwości wymaga od wspólników (akcjonariuszy) aktywnego działania w postaci modyfikacji umowy spółki bądź statutu (Mazgaj, 2020, s. 140). Istotnym jest, że ta modyfikacja przepisów w wymienionych wyżej dwóch spółkach kapitałowych nie była jedynie modyfikacją k.s.h. na czas obowiązywania pandemii.

W odniesieniu do PSA – w momencie dokonania nowelizacji k.s.h. w marcu 2020 r. w związku z pandemią przepisy o PSA co prawda były już przygotowane, lecz jeszcze nie weszły w życie. W dniu 19 lipca 2019 roku uchwalono nowelizację, na mocy której do polskiego porządku prawnego wprowadzono PSA (Sejm RP, 2019), lecz obowiązywanie tych przepisów, pierwotnie zaplanowane na 1 marca 2020 r., zostało odłożone w czasie i rozpoczęło się ono „dopiero" z dniem 1 lipca 2021 r., czyli ponad rok od nowelizacji k.s.h. z 2020 r.

Odnośnie więc do spółek akcyjnych oraz spółek z o.o. – najpierw przepisy k.s.h. nie dopuszczały możliwości odbywania zgromadzeń *online*, następnie odpowiednio od dnia 3 sierpnia 2009 roku dla spółek akcyjnych oraz od dnia 3 września 2019 roku dla spółek z ograniczoną odpowiedzialnością uzależniały ją od przewidzenia takiej możliwości odpowiednio w statucie bądź umowie spółki aż do teraz, gdy – jak to ma miejsce w obecnym brzmieniu – dopuszcza się taką możliwość *ex lege*, o ile odpowiednio w statucie bądź w umowie spółki nie znajdą się postanowienia tego zabraniające.

Dla porównania techniki legislacyjnej związanej z wprowadzaniem na coraz szerszą skalę rozwiązań związanych z wykorzystaniem środków komunikacji elektronicznej do odbywania zgromadzeń *online* przeprowadzić można punktowe porównanie do systemów prawa niemieckiego oraz prawa austriackiego. Uwaga prawnoporównawcza opiera się na założeniu dotyczącym tego, że identyczny problem wystąpił w różnych systemach prawnych w tym samym czasie (tzn. niemożność fizycznego spotykania się w ramach zgromadzenia spowodowana pandemią i *lockdownami*). Za wyborem tych systemów prawnych przemówiły: ich bliskość do polskiego porządku prawnego oraz fakt, że oba zagraniczne systemy prawne mają

bardzo silnie zakorzenioną tradycję pewności prawa i jako wartość stawiają pewność obrotu, co ma istotne znaczenie dla funkcjonowania spółek kapitałowych. W Niemczech ustawodawca w kontekście pandemii ustawą (już nieobowiązującą) z dnia 27 marca 2020 r. o środkach z zakresu prawa spółek, spółdzielczości, stowarzyszeń, fundacji i nieruchomości mieszkalnych, mających na celu zwalczanie skutków pandemii (GesRuaCOVBekG) stworzył w krótkim czasie i po raz pierwszy możliwość odbycia wirtualnych walnych zgromadzeń (Walch & Häuslmeier, 2023, s. 106). Aby w ogóle umożliwić odbycie walnych zgromadzeń w związku z ograniczeniami w zakresie zgromadzeń spowodowanymi pandemią, ustawodawca niemiecki ekspresowo wprowadził w ustawie tymczasowej szczególne zasady przeprowadzania walnych zgromadzeń w spółkach akcyjnych – z uwagi na działanie pod presją czasu – bez wcześniejszych szczegółowych konsultacji z doktryną i praktyką. Tymczasowa ustawa umożliwiła odbycie walnego zgromadzenia w całości jako wirtualnego walnego zgromadzenia bez fizycznej obecności akcjonariuszy. Do tego czasu (pandemii) oprócz bezpośredniego osobistego walnego zgromadzenia dostępna była jedynie hybrydowa forma zgromadzenia z możliwością uczestnictwa fizycznego i internetowego, w której forma uczestnictwa *online* mogła być wymienialna na formę uczestnictwa fizycznego, jednakże w zakresie prawa do fizycznego uczestnictwa w miejscu odbycia walnego zgromadzenia nie były dopuszczalne żadne ograniczenia, takie jak ograniczenie liczby uczestników (Franzmann & Rothweiler, 2022, s. 809–810).

Następnie w Niemczech poprzez ustawę (Bundestag, 2022) wprowadzającą walne zgromadzenia zdalne (*online*), która weszła w życie 27 lipca 2022 r. (niemiecka nowelizacja z lipca 2022 r.) dla spółek akcyjnych (oraz zmiany w prawie spółdzielczym i upadłościowym i przepisów restrukturyzacyjnych), do ustawy o spółkach akcyjnych wprowadzono nowe regulacje na wzór wyżej wymienionych przepisów (GesRuaCOVBekG). W dniu 31 sierpnia 2022 roku ostatecznie przestała obowiązywać tymczasowa ustawa, a zdalne walne zgromadzenie pozostało na stałe w ustawie o spółkach akcyjnych i, co ważniejsze, w realiach życia gospodarczego i obrotu (Hoppe, 2023, s. 587). Za pomocą nowelizacji z lipca 2022 r. ustawodawca niemiecki próbuje więc trwale zakotwiczyć, w bardziej rozwiniętej formie niż przed pandemią, w prawie spółek akcyjnych zdalne (*online*) walne zgromadzenie, które zrodziło się w sytuacji nadzwyczajnej (Franzmann & Rothweiler, 2022, s. 809). Centralnym przepisem regulującym tę materię jest obecnie art. 118a niemieckiej ustawy o spółkach akcyjnych – AktG (Bundestag, 2024b; Walch & Häuslmeier, 2023, s. 108).

Wbrew temu, co na pierwszy rzut oka sugeruje termin „wirtualne walne zgromadzenie", nie odbywa się ono wyłącznie w przestrzeni wirtualnej, ale nadal odbywa się w fizycznym miejscu. Zgodnie z § 118a ust. 2 AktG w posiedzeniu muszą uczestniczyć zarząd, rada nadzorcza i przewodniczący zgromadzenia, a także, w stosownych przypadkach, biegli rewidenci i pełnomocnicy.

Mimo odmienności walnego zgromadzenia prowadzonego w formie niestacjonarnej ustawodawca niemiecki twierdzi, że nie ustępuje ono podstawowej formie

zgromadzenia (stacjonarnej), a w szczególności nie stanowi zgromadzenia „drugiej kategorii" (Walch & Häuslmeier, 2023, s. 109).

W Niemczech w przepisach przyjętych po okresie obowiązywania przepisów tymczasowych – nowelizacja z lipca 2022 r. – powrócono do reguły, że odbycie walnego zgromadzenia w trybie zdalnym (*online*) zgodnie z § 118a ust. 1 zdanie 1 AktG wymaga podstawy statutowej (Walch & Häuslmeier, 2023, s. 110).

Nawiasem mówiąc, w prawie niemieckim, jeśli chodzi zaś o spółkę z ograniczoną odpowiedzialnością (GmbH), od 1 sierpnia 2022 r. wprowadzono uproszczenia w przeprowadzaniu wirtualnych spotkań. Zgromadzenia wspólników spółki z ograniczoną odpowiedzialnością (GmbH) wirtualne (w pełni wirtualne) są możliwe na podstawie przepisów ustawy o spółkach z o.o. – GmbHG (Bundestag, 2024a) i nie będzie potrzeby wskazywania tego w umowie spółki (Bundesministerium der Justiz, 2024). Przepis § 48 (*Gesellschafterversammlung*) GmbHG wskazuje od 2022 roku w sposób oczywisty (co wcześniej mogło być uregulowane w umowie spółki), że zgromadzenie wspólników może odbywać się w sposób „wirtualny" – w pełni wirtualny (Altmeppen, 2023, Rn. 52).

Z podobnej techniki legislacyjnej jak w Niemczech, tj. wprowadzenia najpierw ustawy tymczasowej na czas pandemii, a następnie nowelizacji, której czas obowiązywania nie był powiązany z okresem obowiązywania stanu epidemii czy też stanu zagrożenia epidemicznego, skorzystał również ustawodawca austriacki (Nauer, 2023, s. 771). W Austrii na okres pandemii ustawodawca dokonał nowelizacji na mocy ustawy tymczasowej, w której umożliwił odbywanie zgromadzeń przy użyciu technicznych środków komunikacji elektronicznej, zwłaszcza przez wideokonferencję (w tym tzw. w pełni „wirtualnych zgromadzeń"), a z uwagi na to, że taki tryb sprawdził się w praktyce, dokonano nowelizacji wprowadzenia form zgromadzeń *online* (dotyczy to wszystkich spółek kapitałowych) już nie za pomocą przepisów tymczasowych, a ustawą o zgromadzeniach wirtualnych (VirtGesG), która weszła w życie 14.07.2023 r. (Der National Rat Österreich, 2023; Parlament Österreich, 2023) i nadal obowiązuje. Z tym jednak zastrzeżeniem, że – podobnie jak w Niemczech – odwrócona została obowiązująca w pandemii zasada, że zgromadzenia *online* w sytuacji związanej z pandemią były dozwolone *ex lege*, obecnie zaś jedynie wówczas, gdy będzie to określone w umowie spółki lub statucie (§ 1 ust. 2 VirtGesG).

3. Niespójność regulacji zgromadzeń online w PSA w stosunku do uregulowań sp. z o.o. i SA

Na tle uwag prawnoporównawczych i polskiej regulacji spółek kapitałowych SA oraz z o.o. przejść należy do wspomnianej analizy niespójności rozwiązań przewidzianych dla PSA, w ramach wybranych 3 kwestii szczegółowych: dopuszczalności

zgromadzeń *online ex lege* a *ex contractu*, tajności głosowania, konieczności wprowadzenia regulaminów dla odbywania zgromadzeń *online*.

Wśród zalet prostej spółki akcyjnej wskazywano, że „Wszystkie organy prostej spółki akcyjnej mogą podejmować decyzje na tradycyjnych posiedzeniach lub przy wykorzystaniu środków komunikacji elektronicznej (na odległość) czyli np. poczty elektronicznej czy komunikatorów internetowych" (Biznes.gov.pl, 2024).

Prosta spółka akcyjna ostatecznie, po odłożeniu w czasie terminu wejścia jej w życie przez ustawodawcę, m.in. ze względu na pandemię, występuje więc w polskim porządku prawnym od 1.07.2021 r., a w szczególności przepisy dotyczące podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej (w tym odbywania zgromadzeń *online*) przez akcjonariuszy prostych spółek akcyjnych, w tym art. 300^{80} oraz art. 300^{92} k.s.h. Tym bardziej może dziwić odmienność regulacji zastosowanej odnośnie do prostej spółki akcyjnej, w szczególności różnica w zakresie konieczności przewidzenia w umowie prostej spółki akcyjnej odbywania zgromadzeń *online*, w tym wykonywania prawa głosu, a więc podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej, co jest dopuszczalne zarówno na zgromadzeniu, jak i poza zgromadzeniem, o ile umowa spółki na to zezwala. Alternatywnie jest to dopuszczalne także poza zgromadzeniem, w przypadku, gdy wszyscy akcjonariusze wyrazili zgodę na taki tryb głosowania w formie dokumentowej.

W przypadku walnego zgromadzenia PSA zastosowanie środków komunikacji elektronicznej do udziału w tym zgromadzeniu jest uprawnione – w świetle art. 300^{92} § 1 k.s.h. – z mocy umowy spółki, podobnie jak to było w spółce z o.o. czy też spółce akcyjnej przed nowelizacją z marca 2020 r.

Rozbieżne daty wejścia w życie przepisów obecnej regulacji odbywania zgromadzeń *online*, w tym podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej przez wspólników spółek kapitałowych, mogą w pewnym zakresie wyjaśniać, choć jednocześnie nie usprawiedliwiają obecnego stanu normatywnego.

Wspomniana powyżej konieczność przewidzenia w umowie prostej spółki akcyjnej odbywania zgromadzeń *online* – w tym wykonywania prawa głosu, a więc podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej, co jest dopuszczalne zarówno na zgromadzeniu, jak i poza zgromadzeniem, o ile umowa spółki na to zezwala, alternatywnie jest to dopuszczalne także poza zgromadzeniem, w przypadku, gdy wszyscy akcjonariusze wyrazili zgodę na taki tryb głosowania w formie dokumentowej – wprowadzona na podstawie art. 300^{80} i art. 300^{92} k.s.h. nie jest jedynym mankamentem obecnej regulacji. Wątpliwości interpretacyjne wzbudza także brzmienie art. 300^{80} § 1 k.s.h., wedle którego to przepisu: „Uchwały akcjonariuszy są podejmowane na walnym zgromadzeniu albo poza walnym zgromadzeniem na piśmie albo przy wykorzystaniu środków komunikacji elektronicznej". Unormowanie to nawiązuje po części do regulacji zasad podejmowania uchwał przez uczestników pozostałych spółek kapitałowych, przede wszystkim do odnoszącego się do spółki z ograniczoną odpowiedzialnością art. 227 § 2 k.s.h., który przewi-

duje, że uchwały wspólników mogą być podjęte również poza posiedzeniem organu właścicielskiego tej spółki, tj. poza zgromadzeniem wspólników, w przypadku, gdy wszyscy wspólnicy wyrażą na piśmie zgodę na postanowienie, które ma być powzięte, albo na głosowanie pisemne. Unormowania przepisów art. 393 i nast. k.s.h. dotyczące uchwał akcjonariuszy w SA nie przewidują natomiast możliwości ich podjęcia poza posiedzeniem organu właścicielskiego tej spółki, tj. poza walnym zgromadzeniem (Kozieł, 2020a). Warto w tym miejscu wskazać na kolejną rozbieżność pomiędzy regulacjami odnoszącymi się z jednej strony do spółek z ograniczoną odpowiedzialnością oraz prostych spółek akcyjnych, a spółek akcyjnych z drugiej, gdyż art. 406^5 § 1 k.s.h. dopuszcza możliwość udziału w walnym zgromadzeniu przy wykorzystaniu środków komunikacji elektronicznej, a więc jedynie na zgromadzaniu.

Kwestie związane z wprowadzeniem zgromadzeń *online ex contractu* a nie *ex lege* w PSA są po części łagodzone przez to, że proste spółki akcyjne mogą być tworzone za pomocą systemu S24, czyli z wykorzystaniem wzorca umowy spółki określonego w rozporządzeniu Ministra Sprawiedliwości (Minister Sprawiedliwości, 2021), zawierającego w paragrafie 16 możliwość udziału w walnych zgromadzeniach PSA przy wykorzystaniu środków komunikacji elektronicznej. Zatem utworzenie PSA przy wykorzystaniu tego wzorca w pewien sposób minimalizuje analizowany problem, gdyż od samego początku umowa spółki będzie „zaprogramowana" na model zgromadzenia *online*, acz całkowicie go nie eliminuje, w dalszym ciągu pozostawiając ogólną zasadę *ex lege*.

4. Kwestia tajności głosowania w PSA

Przepisy k.s.h. dotyczące udziału w zgromadzeniu wspólników (walnym zgromadzeniu) przy wykorzystaniu środków komunikacji elektronicznej w zakresie dotyczącym spółek z o.o. oraz SA nie odnoszą się do wymogu tajności głosowania (szerzej o wymogu tajności głosowania por.: Modrzejewski, 2021, s. 5). Należy zatem przyjąć, że w przypadku głosowań dokonywanych na zgromadzeniu wspólników (walnym zgromadzeniu) zorganizowanym zdalnie nie został uchylony wymóg tajności głosownia wynikający z art. 247 § 2 zd. 1 i art. 420 § 2 zd. 1 k.s.h. oraz wymóg przeprowadzania głosowania tajnego na żądanie wspólnika i akcjonariusza. Z powyższego wynika, że urządzenia służące do elektronicznego głosowania muszą nie tylko zapewnić prawidłowość głosowania w tym znaczeniu, że wola głosującego powinna być zinterpretowana jednoznacznie w sposób przez niego wybrany oraz umożliwiać oddanie właściwej liczy głosów w każdym głosowaniu, ale ponadto umożliwić tajność głosowania w sytuacji, kiedy przewidują to przepisy k.s.h. (Leśniak, 2020c, s. 14).

Tymczasem kolejną odmiennością występującą jedynie w przypadku zastosowania środków komunikacji elektronicznej poza zgromadzeniami PSA jest wyłączenie tajności głosowania w przypadkach objętych hipotezą art. 300^{99} § 2 k.s.h., gdyż

na podstawie art. 300^{80} § 3 k.s.h. do uchwał podejmowanych poza walnym zgromadzeniem PSA zastosowania nie znajdują przepisy o głosowaniu tajnym, zawarte w art. 300^{99} § 2 k.s.h. Przepis ten jednoznacznie pozwala uznać, iż w głosowaniu pisemnym oraz w głosowaniu przy wykorzystaniu środków komunikacji elektronicznej mogą być podjęte także uchwały, dla których art. 300^{99} § 2 k.s.h. wymaga zachowania tajności głosowania (Bieniak, 2024; tak też: Dumkiewicz, 2024a; Dumkiewicz, 2024b; Kawalec, 2021); podczas gdy w przypadku pozostałych spółek kapitałowych niezależnie, czy na zgromadzeniu spółek z o.o. oraz SA, czy też poza zgromadzeniem w spółkach z o.o., obowiązuje w analogicznych sytuacjach tajność głosowania.

5. Kwestia obowiązku przyjęcia regulaminów w PSA

Kolejnym obowiązkiem ciążącym na spółkach kapitałowych jest obowiązek przyjęcia regulaminu określającego szczegółowe zasady dotyczące sposobu uczestnictwa w zgromadzeniu przy wykorzystaniu środków komunikacji elektronicznej. Legislator nałożył na spółki, które chcą zapewnić zdalny udział w zgromadzeniu wspólników (walnym zgromadzeniu), obowiązek określenia w formie regulaminu szczegółowych zasad udziału w zgromadzeniu wspólników (walnym zgromadzeniu) przy wykorzystaniu środków komunikacji elektronicznej. W spółce z o.o. zgodnie z art. 234^{1} § 3 k.s.h. kompetencje do uchwalenia tego rodzaju regulaminu przyznano radzie nadzorczej, a gdy spółka jej nie posiada – wspólnikom. Natomiast w SA stosowny regulamin przyjmuje rada nadzorcza – art. 406^{5} § 3 k.s.h. (Leśniak, 2020c, s. 3) – podczas gdy w PSA na podstawie art. 300^{92} § 2 k.s.h. kompetencję przyznano walnemu zgromadzeniu akcjonariuszy. Jest to zatem kolejna rozbieżność pomiędzy spółkami kapitałowymi, jednakże w pewien sposób zrozumiała ze względu na nieobligatoryjność występowania rady nadzorczej w prostych spółkach akcyjnych.

W przepisach dotyczących walnego zgromadzenia PSA, jak też w innych unormowaniach odnoszących się do tej spółki nie przewidziano trybu przyjmowania (w tym uchwalania) związanego z tym trybem statusu prawnego, a ponadto treści regulaminu walnego zgromadzenia – inaczej niż w stosunku do regulaminów pozostałych organów tej spółki (np. zarządu czy rady dyrektorów), których dotyczy art. 300^{57} k.s.h. Wobec tego należy przyjąć, iż regulamin walnego zgromadzenia jest przyjmowany (uchwalany) w drodze uchwały akcjonariuszy podjętej na zasadach ogólnych, tj. bezwzględną większością głosów, niezależnie od liczby akcjonariuszy podejmujących uchwałę na walnym zgromadzeniu lub poza nim zgodnie z art. 300^{80} k.s.h. (Kozieł, 2020b).

We wszystkich przypadkach spółek kapitałowych powołane przepisy określają wprost, iż regulamin nie może określać wymogów oraz ograniczeń, które nie są niezbędne do identyfikacji wspólników (akcjonariuszy), a także zapewnienia bezpieczeństwa komunikacji elektronicznej. Należy przyjąć, iż regulamin tego typu powinien koncentrować się na regulacji kwestii technicznych dotyczących funkcjonalności środ-

ków komunikacji elektronicznej służących zdalnemu uczestnictwu w obradach zgromadzenia oraz zachowań uczestników związanych z obsługą środków komunikacji elektronicznej służących zdalnemu uczestnictwu w obradach zgromadzenia oraz ich funkcjonalności (tak odnośnie do sp. z o.o. oraz SA: Leśniak, 2020c, s. 3).

Warto zaznaczyć, że brak regulaminu jako uchybienie formalne może stanowić podstawę do zaskarżenia i stwierdzenia nieważności uchwał podjętych podczas zgromadzenia, w którym część wspólników brała udział przy wykorzystaniu środków komunikacji elektronicznej (odpowiednio art. 252 k.s.h. w zakresie spółki z o.o. oraz art. 425 k.s.h. w zakresie SA, a ponadto art. 300^{101} k.s.h. w zakresie PSA), tylko wówczas, gdy takie uchybienie miało – bądź mogło mieć – wpływ na treść takiej uchwały (Sarkowicz, 2023). Pogląd ten jest zbieżny z wyrokiem SN z 12.10.2012 r., IV CSK 186/12: „Badanie zgodności z ustawą uchwały zgromadzenia spółki handlowej obejmuje nie tylko stwierdzenie uchybień popełnionych przy zwoływaniu zgromadzenia i podjęciu uchwały, lecz także wpływ tych uchybień na treść tej uchwały" (Wyrok Sądu Najwyższego, 2012).

6. Definicja środków komunikacji elektronicznej w PSA

Następną kwestią, w której także występuje odmienność regulacji dotyczącej PSA, jest definicja środków komunikacji elektronicznej.

Brak wskazania w przepisach k.s.h. *stricte* środków komunikacji elektronicznej możliwych do zastosowania przez wspólników spółek kapitałowych w przedmiocie prawidłowego podejmowania uchwał sprawia, że właściwym zachowaniem wspólników jest posłużenie się definicją ustawową wskazanego pojęcia zawartą w Ustawie z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Sejm RP, 2002), zgodnie z którą (art. 2 pkt 5 ww. ustawy) wskazane środki to „rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną" (tak odnośnie do PSA: Kawalec, 2021).

Jednocześnie w przepisach dotyczących wszystkich spółek kapitałowych (art. 234^{1} § 1 i 2 k.s.h., art. 300^{92} § 1 oraz w art. 406^{5} § 1 i 2 k.s.h.) wskazano przykładowy sposób „udziału" w zgromadzeniu polegający na technicznej możliwości dwustronnej komunikacji w czasie rzeczywistym wszystkich osób uczestniczących w zgromadzeniu, w ramach której mogą one wypowiadać się w toku jego obrad, przebywając w innymi miejscu niż miejsce obrad zgromadzenia, a ponadto na zapewnieniu możliwości wykonywania osobiście lub przez pełnomocnika prawa głosu przed lub w toku zgromadzenia (tak odnośnie do sp. z o.o. oraz SA: Leśniak, 2020c, s. 3–4). Ponadto w art. 300^{92} § 1 k.s.h. zawarto dodatkowy przykład, tj. transmisję obrad walnego zgromadzenia w czasie rzeczywistym. Posłużenie się wyliczeniem przykłado-

wym należy ocenić pozytywnie, gdyż nie jest konieczna jego każdorazowa zmiana przy ciągłym rozwoju technologii, a ujednolicenie przepisów z pozostałymi spółkami kapitałowymi w tym zakresie nie jest z tego względu konieczne.

Wnioski i postulaty *de lege ferenda*

Należy zauważyć, że w k.s.h. nie ma jednolitej regulacji podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej (w tym odbywania zgromadzeń *online*) przez wspólników spółek kapitałowych. Jest to spowodowane wchodzeniem w życie w różnym czasie zmian k.s.h. w przedmiotowym zakresie. Obecna sytuacja normatywna nie jest do pogodzenia z zasadą bezpieczeństwa obrotu gospodarczego, gdyż w pewnym zakresie powoduje swoisty chaos normatywny.

Obecny stan normatywny można określić jako swoisty paradoks, gdyż to właśnie prosta spółka akcyjna miała być „łatwa w obsłudze", „elastyczna" oraz „idąca z duchem czasu" – tymczasem to właśnie w regulacji tej spółki istnieją pewne utrudnienia i rozbieżności w uregulowaniu odbywania zgromadzenia *online* w stosunku do pozostałych spółek kapitałowych, które mogą negatywnie rzutować na obrót gospodarczy.

Stąd wysunąć należy następujące postulaty o charakterze *de lege ferenda*, które miałyby na celu uspójnienie modeli sp. z o.o. i SA oraz PSA, tj. zmiany w regulacji PSA Wydaje się bowiem, że już samo dokonanie jedynie w zasadzie drobnych korekt istniejącej regulacji, które – należy mieć nadzieję – mogłyby się znaleźć w kręgu i polu zainteresowania Komisji Kodyfikacyjnej Prawa Cywilnego, bez „opcji atomowej", mogłoby znacząco wpłynąć na uspójnienie modelu zgromadzeń *online* w ramach wszystkich trzech spółek kapitałowych, a tym samym przełożyć się istotnie na poprawę, usprawnienie funkcjonowania zgromadzeń w PSA.

Postulaty *de lege ferenda* wedle założenia ujednolicenia regulacji poprzez punktowe korekty uspójniające, bez „obalania systemu", są następujące:

1) W PSA – wprowadzenie zasady zgromadzenia *online ex lege*, chyba że umowa spółki stanowi inaczej.
   Należy dokonać zmiany art. 300^{80} § 2 oraz art. 300^{92} § 1 k.s.h. w taki sposób, żeby *ex lege* dopuszczał możliwość podejmowania uchwał przy wykorzystaniu środków komunikacji elektronicznej (w tym odbywania zgromadzeń *online*) przez akcjonariuszy prostych spółek akcyjnych, o ile umowa spółki nie będzie stanowić inaczej.
   Uspójnienie przepisów PSA, tzn. wprowadzenie modelu *ex lege* odbywania się zgromadzeń *online* w PSA zamiast modelu *ex contractu*, uzasadnić można tym, że regulacja PSA niejako „nie nadążyła" w okresie *vacatio legis* za zmianami wprowadzonymi w spółce z o.o. i spółce akcyjnej. Ponadto, należy podkreślić, że zgromadzenia *online* zachowują ekwiwalencję funkcjonalną ze zgromadzeniami odbywanymi stacjonarnie, a więc w przypadku PSA nie

będą one stanowiły „zagrożenia", a wręcz ich *ex lege* egzystencja w pełniejszy sposób odpowiada założeniom systemowym, na których konstrukcja PSA została oparta, tj. elastyczności i „wychodzeniu naprzeciw" akcjonariuszom PSA. Ekwiwalencja funkcjonalna zakłada, że podkreśla się, że zgromadzenie prowadzone *online* ma stanowić odwzorowanie (ekwiwalentność) ze zgromadzeniem odbywanym w formie stacjonarnej. Jako ekwiwalentność/odwzorowanie należy rozumieć, że środki komunikacji elektronicznej stwarzają możliwość do komunikowania się w czasie rzeczywistym, nie wymagając, by uczestniczący (akcjonariusze) spotkali się w tym samym miejscu fizycznym. Polega to więc na tym, że rezygnuje się zatem tylko z tego, że wszyscy uczestnicy mają być obecni w jednym miejscu (w szczególności w jednym pomieszczeniu). Natomiast we wszelkich innych aspektach (w szczególności wykonywaniu uprawnień) zgromadzenie odbywane *online* powinno przebiegać „tak jak" zgromadzenie stacjonarne. Dlatego zasadny wydaje się wysuwany postulat uspójniający regulację k.s.h. w obszarze wszystkich trzech spółek kapitałowych w ten sposób, że również w PSA zastosuje się na wzór sp. z o.o. i SA regułę dla odbywania zgromadzenia *online ex lege*.

2) W PSA występuje w pewnych przypadkach brak tajności głosowania. Chodzi tu o relację między art. 380^{80} § 3 k.s.h. a art. 300^{99} k.s.h.
Wydaje się, że w PSA wymóg tajności również powinien być zachowany– na wzór przepisów regulujących sp. z o.o. i SA.
Ponieważ, jak wskazano wyżej, w przypadku pozostałych spółek kapitałowych – niezależnie, czy na zgromadzeniu w przypadku spółek z ograniczoną odpowiedzialnością oraz spółek akcyjnych, czy też poza zgromadzeniem w przypadku spółek z ograniczoną odpowiedzialnością – obowiązuje tajność głosowania. Wobec powyższego, w celu zachowania spójności przepisów dotyczących możliwości podejmowania uchwał, głosowania w sposób tajny za pomocą zastosowania środków komunikacji elektronicznej, postuluje się wykreślenie art. 380^{80} § 3 k.s.h.

3) Należy dokonać rewizji, po pewnym okresie obowiązywania, przepisów wprowadzonych do k.s.h. w czasie pandemii, mimo tego, że były w zamyśle wprowadzane nie jedynie tymczasowo, i oceny, jak funkcjonują, wraz z ewentualnymi zmianami czy dalszymi dostosowaniami (na wzór prawa niemieckiego i prawa austriackiego).
Wedle paragrafu 8 ust. 2[6] austriackiej ustawy o wirtualnych zgromadzeniach (VirtGesG), a dotyczy ona nie tylko całkowicie wirtualnych zgromadzeń, ale też zgromadzeń *online* (Der National Rat Österreich, 2023; Parlament Ös-

6 *§ 8. (1) Dieses Bundesgesetz tritt mit 14. Juli 2023 in Kraft. (2) Die Bundesministerin für Justiz hat im Jahr 2028 auf der Grundlage der Auswirkungen der Durchführung von virtuellen und hybriden Gesellschafterversammlungen nach diesem Bundesgesetz und der Erfahrungen in anderen vergleich-*

terreich, 2023), rewizja została przewidziana na rok 2028 (ustawa austriacka weszła w życie 14 lipca 2023 r.) – a więc miałaby nastąpić po 5 latach i ma ją przeprowadzić austriackie Ministerstwo Sprawiedliwości. Kryteria, które mają być brane pod uwagę, to: skutki, jakie wywołało wprowadzenie możliwości przeprowadzania zgromadzeń wirtualnych i hybrydowych, doświadczenia dotyczące wprowadzenia podobnych rozwiązań w innych Państwach Członkowskich UE, celowość wprowadzenia możliwości przeprowadzania zgromadzeń w tej formie.

Podobnie, w prawie niemieckim wraz z wprowadzeniem nowelizacji (Walch & Häuslmeier, 2023, s. 106) niemieckiej ustawy o spółce akcyjnej poprzez ustawę z 2022 r. (Bundestag Deutschland, 2022) przyjęto, że czas, na jaki statut spółki akcyjnej może przewidywać dopuszczanie zgromadzeń *online*, to 5 lat (§ 118a ust. 3–5 AktG). Decyzja akcjonariuszy musi zatem być odnawiana w regularnych odstępach czasu, co ma na celu szczególnie uwzględnienie zmian strukturalnych w grupie akcjonariuszy (Hoppe, 2023, s. 588).

O ile więc w prawie niemieckim inna jest zasada – albowiem zgromadzenie *online* może odbywać się nie *ex lege*, lecz *ex contractu* (*ex statuto*) – to jednak cały czas należy zwrócić uwagę, że ustawodawca zawarł ograniczenie czasowe i choć dotyczy ono nie samej rewizji ustawy a jedynie aktu wewnętrznego (umowy/spółki, statutu), to jednak można przyjąć, że jest to również argument za postulatem (wspierający), że w związku z ultraszybkim i często nieprzewidywalnym rozwojem techniki takie rewizje przepisów, jak postulowana, powinny być systematycznie przez ustawodawcę krajowego prowadzone.

Postulat kierowany do polskiego ustawodawcy dotyczący rewizji i oceny funkcjonowania przepisów odnoszących się do zgromadzeń *online* wydaje się uzasadniony, szczególnie z tego względu, że postęp technologiczny następuje obecnie w bardzo szybkim tempie (w szczególności zmiany technologiczne związane ze sztuczną inteligencją) i choćby z tego powodu należałoby postulować rewizję regulacji w okresie kilkuletnim od jej wprowadzenia. Taka procedura rewizji przypominać by mogła (choć z pewnością nie będzie identyczna) znaną prawu europejskiemu tzw. procedurą *recast* (por.: The European Parliament, The Council of the European Union and the Commission of the European Communities, 2001), poza tym można czerpać do niej wzorce z doświadczeń innych Państw Członkowskich, oczywiście nie na zasadzie jeden do jeden, a na zasadzie takiego doboru rozwiązań, by uwzględniał on specyfikę polskiego systemu prawnego.

baren EU-Mitgliedstaaten die Zweckmäßigkeit der Möglichkeit zur Durchführung solcher Versammlungen zu prüfen und darüber dem Nationalrat zu berichten.

BIBLIOGRAFIA

Altmeppen, H. (2023). GmbHG § 48 Gesellschafterversammlung. w: H. Altmeppen, *GmbHG Kommentar*, 11. Auflage. BECK-Online.

Baszczyk, M. (2022). Funkcjonowanie rady nadzorczej spółki z o.o. w kontekście najnowszych nowelizacji Kodeksu spółek handlowych – zagadnienia wybrane. *Monitor Prawa Handlowego*, (3), 26–34.

Bieniak, M. (2024). Komentarz do art. 300^{80} k.s.h. w: J. Bieniak, M. Bieniak, G. Nita-Jagielski, K. Oplustil, R. Pabis, A. Rachwał, M. Spyra, G. Suliński, M. Tofel, M. Wawer & R. Zawłocki, *Kodeks spółek handlowych. Komentarz*, wyd. 9. Legalis.

Biznes.gov.pl – Serwis informacyjno – usługowy dla przedsiębiorcy. (2024). *Prosta spółka akcyjna – nowa forma prowadzenia działalności.* https://www.biznes.gov.pl/pl/portal/00168

Bundesministerium der Justiz. (2024). Virtuelle Gesellschafterversammlung, https://www.bmj.de/DE/themen/wirtschaft_finanzen/handels_gesellschaftsrecht/gmbh-recht/gmbh-recht_artikel.html

Bundestag. (2022). Gesetz zur Einführung virtueller Hauptversammlungen von Aktiengesellschaften und Änderung genossenschafts – sowie insolvenz – und restrukturierungsrechtlicher Vorschriften Vom 20. Juli 2022, Bundesgesetzblatt Jahrgang 2022 Teil I Nr. 27, ausgegeben zu Bonn am 26. Juli 2022.

Bundestag. (2024a). Gesetz betreffend die Gesellschaften mit beschränkter Haftung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4123–1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 21 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323) geändert worden ist.

Bundestag. (2024b). Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), das zuletzt durch Artikel 18 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323) geändert worden ist

Der National Rat Österreich. (2023). Bundesgesetz über die Durchführung virtueller Gesellschafterversammlungen (VirtGesG), BGBl I 2023/79.

Dumkiewicz, M. (2024a). Komentarz do art. 300^{80} k.s.h. w: A. Kidyba & M. Dumkiewicz, *Komentarz aktualizowany do art. 1–300 Kodeksu spółek handlowych*, Lex el.

Dumkiewicz, M. (2024b). Komentarz do art. 300^{80} k.s.h. w: M. Dumkiewicz, *Kodeks spółek handlowych. Komentarz*, wyd. II, Lex el.

Franzmann, G. & Rothweiler S. (2022). Das Auskunfts – und Rederecht nach dem Gesetz zur dauerhaften Einführung virtueller Hauptversammlungen von Aktiengesellschaften, *Die Aktiengesellschaft*, (22), 809–820.

Hoppe, A. (2023). Die Transposition der virtuellen Hauptversammlung in die Satzung der AG. *Neue Zeitschrift für Gesellschaftsrecht*, 587–593.

Jerzmanowski, J. (2020). The growing popularity of remotely held meetings of management boards, supervisory boards and general meetings (shareholder meetings) as a manifestation of a digital revolution in company law: the case of amendments to polish law in response to the covid-19 pandemic. w: Appolloni A. et al. (eds). *Journal of Economics, Business & Organization Research. Proceedings of the Third Economics, Business and Organization Research (EBOR) Conference*, (ss. 337–350). EBOR Academy Ltd.

Kappes, A. (2009). Elektroniczne głosowania na walnych zgromadzeniach akcjonariuszy. *Przegląd Prawa Handlowego*, (6), 11–15.

Kawalec, G. (2021). Komentarz do art. 300^{80} k.s.h. w: R. Adamus & P. Malinowski (red.), *Prosta spółka akcyjna. Komentarz*, Lex el.

Kocot, W. J. (2011). Korzystanie z sieci teleinformatycznych w stosunkach korporacyjnych spółek akcyjnych. *Przegląd Prawa Handlowego*, (2), 4–15.

Komisja Europejska. (2019). Priorytet Komisji Europejskiej na lata 2019–2024 *A Europe fit for the digital age* https://commission.europa.eu/strategy-and-policy/priorities-2019–2024/europe-fit-digital-age_en

Komisja Europejska. (2020). Komunikacja Komisji Europejskiej z dnia 19 lutego 2020 r., *Shaping Europe's digital future*. https://commission.europa.eu/document/download/84c05739–547a-4b86–9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future-feb2020_en.pdf

Kozieł, G. (2020a). Komentarz do art. 300^{80} k.s.h. w: G. Kozieł, *Prosta spółka akcyjna*, Legalis.

Kozieł, G. (2020b). Komentarz do art. 300^{92} k.s.h. w: G. Kozieł, *Prosta spółka akcyjna*, Legalis.

Krukowska-Korombel, J. (2010). Prawa akcjonariuszy wykonywane za pośrednictwem środków elektronicznych w świetle przepisów kodeksu spółek handlowych. *Przegląd Prawa Handlowego*, (9), 36–43.

Lenio, P. & Srokosz, W. (2022). Funkcjonowanie organów banku spółdzielczego w sytuacjach i stanach nadzwyczajnych z wykorzystaniem środków bezpośredniego porozumiewania się na odległość. *Monitor Prawa Bankowego,* (1), 74–85.

Leśniak, M. (2020a). Udział w zgromadzeniu spółki kapitałowej za pomocą środków komunikacji elektronicznej po zmianach Kodeksu spółek handlowych dokonanych w ramach tzw. tarczy antykryzysowej. *Prawo Mediów Elektronicznych*, (2), 12–24.

Leśniak, M. (2020b). Udział w zgromadzeniu wspólników spółki z ograniczoną odpowiedzialnością i walnym zgromadzeniu spółki akcyjnej za pomocą środków komunikacji elektronicznej – wybrane aspekty regulacji po nowelizacji z 31.03.2020 r. w: M. Dumkiewicz, J. Szczotka & K. Kopaczyńska-Pieczniak, *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie*, t. 1, (ss. 753–766). Wolters Kluwer.

Leśniak, M. (2020c). Rekomendacja dobrych praktyk notarialnych na zgromadzeniach wspólników spółek z ograniczoną odpowiedzialnością i walnych zgromadzeniach spółek akcyjnych w których udział możliwy jest za pomocą środków komunikacji elektronicznej po zmianie przepisów Kodeksu spółek handlowych wynikających z ustawy z dnia 31.03.2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw. https://www.gov.pl/web/aktywa-panstwowe/rekomendacja-dobrych-praktyk-notarialnych-podpisana

Mazgaj, M. (2022). Wirtualne zgromadzenia w spółkach kapitałowych. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Cultura*, (1), 140–149.

Minister Sprawiedliwości. (2021). Rozporządzenie Ministra Sprawiedliwości z dnia 30 czerwca 2021 r. w sprawie określenia wzorców dotyczących prostej spółki akcyjnej udostępnionych w systemie teleinformatycznym (Dz.U. z 2021 r., poz. 1191).

Modrzejewski, J. (2021). Tajne głosowanie w spółkach kapitałowych w świetle przepisów Kodeksu spółek handlowych po ostatnich nowelizacjach – problemy wybrane. *Przegląd Prawa Handlowego*, (11), 5–13.

Nalazek, A. & Letolc, P. (2020). Nowelizacja k.s.h. dotycząca odbywania posiedzeń organów menedżerskich z wykorzystaniem środków bezpośredniego porozumiewania się na odległość. *Monitor Prawa Handlowego*, (2), 12–16.

Nauer, Ch. (2023). Virtuelle Gesellschafterversammlungen-Gesetz Österreichischer Kompromiss oder Schaden für die Aktionärskultur? *Recht der Wirtschaft*, (11), 771.

Osajda, K. (2020). Zarząd spółki kapitałowej (nowelizacja Kodeksu spółek handlowych w związku z pandemią). *Przegląd Prawa Handlowego*, (6), 18–29.

Ostrowski, F. (2020). Nowa regulacja posiedzeń zarządów i rad nadzorczych odbywanych przy wykorzystaniu środków komunikacji elektronicznej. *Przegląd Prawa Handlowego*, (5), 32–38.

Parlament Österreich. (2023). Virtuelle Gesellschafterversammlungen-Gesetz MinisterialentwurfErläuterungen 271/ME XXVII. GP https://www.parlament.gv.at/dokument/XXVII/ME/271/fname_1555993.pdf

Pons – słownik internetowy (2024). https://pl.pons.com

Pyka, M. (2022). Udział w walnym zgromadzeniu niepublicznej spółki akcyjnej. w: K. Małysa-Sulińska, M. Spyra & A. Szumański (red.), *Księga jubileuszowa Profesora M. Steca,* t. II, (ss. 346–347). Wolters Kluwer.

Rada Europejska. (2024). *EU Strategic Agenda 2024–2029* https://www.consilium.europa.eu/media/yxrc05pz/sn02167en24_web.pdf

Sarkowicz, J. (2023). *Sposób podejmowania uchwał zgromadzenia wspólników. Udział w zgromadzeniu przy wykorzystaniu środków komunikacji elektronicznej, Beckdirect praktyczne przewodniki*, Legalis.

Sejm Rzeczypospolitej Polskiej (2019). Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy – Kodeks spółek handlowych oraz niektórych innych ustaw (Dz. U. 2019 poz. 1655).

Sejm Rzeczypospolitej Polskiej. (2002). Ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204).

Sejm Rzeczypospolitej Polskiej. (2020). Ustawa tzw. „tarcza antykryzysowa" z 31.03.2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 i innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych i niektórych innych ustaw, (Dz.U. poz. 568).

Sejm Rzeczypospolitej Polskiej. (2020a). Druk Sejmu IX Kadencji nr 299, Rządowy projekt ustawy o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw, punkt 2.135 Zmiany ustawy – k.s.h.

Sejm Rzeczypospolitej Polskiej. (2024). Kodeks spółek handlowych z dnia 15 września 2000 r. (Dz.U. 2000 Nr 94, poz. 1037, t.j. z dnia 7 grudnia 2023 r., Dz.U. z 2024 r. poz. 18).

Starczewska, M. (2020). Podejmowanie uchwał rad nadzorczych spółek kapitałowych po zmianach dokonanych ZmKoronawirusU20. *Monitor Prawniczy*, (16), 856–863.

Szczurowski, T. (2020). Nowelizacja kodeksu spółek handlowych w dobie COVID-19. *Przegląd Ustawodawstwa Gospodarczego*, (11), 46–52.

Szumański, A. (2020). Nowa regulacja udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej. *Przegląd Prawa Handlowego*, (5), 4–14.

Szymański, K. M. (2020). Nowy model udziału w zgromadzeniach właścicielskich spółek kapitałowych przy wykorzystaniu środków komunikacji elektronicznej. *Monitor Prawniczy*, (10), 496–506.

The European Parliament, The Council of the European Union and the Commission of the European communities. (2001*). Interinstitutional Agreement of 28 November 2001 on a more structured use of the recasting technique for legal acts* (OJ C 77, 28.3.2002, s. 1–3).

Wach-Pawliczak, M. (2020). Nowe zasady uczestnictwa w zgromadzeniach wspólników w spółce z o.o. z wykorzystaniem środków komunikacji elektronicznej. w: A. Bielecki, D. Szafrański & T. Gąsior (red.), *Problemy prawa polskiego i obcego w ujęciu historycznym, praktycznym i teoretycznym, cz. 11*., (ss. 163–174). Wydawnictwo C.H. Beck.

Walch, A. & Häuslmeier S. (2023). Die „neue" virtuelle Hauptversammlung – Ein Überblick zum Gesetz zur Einführung virtueller Hauptversammlungen von Aktiengesellschaften und Änderung genossenschafts – sowie insolvenz – und restrukturierungsrechtlicher Vorschriften. *Deutsche Notar-Zeitschrift*, (2), 106–128.

Wrzecionek, R. (2014). Uczestnictwo akcjonariusza w walnym zgromadzeniu przy wykorzystaniu środków komunikacji elektronicznej a czynność notarialna spisania protokołu. *Przegląd Prawa Handlowego*, (3), 51–54.

Wyrok Sądu Najwyższego z dnia 12 października 2012 r., sygn. akt IV CSK 186/12.

Żaba, M. (2020). Uczestnictwo i głosowanie na zgromadzeniu wspólników przy wykorzystaniu środków komunikacji na odległość. *Przegląd Ustawodawstwa Gospodarczego*, (3), 13–20.

Żaba, M. (2021). Podejmowanie uchwał przez organy spółdzielni przy wykorzystaniu środków bezpośredniej komunikacji na odległość. *Monitor Prawniczy*, (18), 962–969.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.04

Received: 28.12.2024
Accepted: 4.07.2025

Marcin Tomasz Mazgaj
Uniwersytet Komisji Edukacji Narodowej w Krakowie, Polska
marcin.t.mazgaj@gmail.com
ORCID: https://orcid.org/0000-0001-7544-8414

Cyfrowe pole bitwy: strona internetowa spółki jako miejsce publikacji ogłoszeń a spory domenowe i korporacyjne

The Digital Battlefield: Company Websites as a Place to Publish Advertisements and Domain and Corporate Disputes

Abstract: In Article 5 § 5 of the Commercial Companies Code, the legislature imposes on joint-stock companies and limited joint-stock partnerships the obligation to maintain their own websites and to publish on them announcements required by law and the statutes of the companies. However, a number of detailed issues related to the determination of the address of such a website and its functioning have not been regulated, including such a fundamental issue as the method to determine what is or is not a company's website within the meaning of the above-mentioned provision. In practice, shareholders generally assume that the website will be the one located at the address appearing in the National Court Register. Although such a conclusion seems logical, it does not clearly result from the applicable legal regulations. However, this circumstance takes on particular significance in cases where a corporate dispute overlaps with a dispute over the company's internet domain. Such cases provoke questions such as what requirements (e.g. in terms of hosting, domain registration, actual control, etc.) must be met for a website to be considered the company's 'own' within the meaning of Article 5 § 5 ; whether a company can maintain (and alternatively use) more than one website for the publication of advertisements; from when a change of a company's website address is effective; and what the corporate consequences are of a company losing control over the content of its website. The subject of this article is analysis of the above issues and an attempt to provide answers to the questions presented. The entire discussion is crowned with conclusions *de lege ferenda*.

Keywords: companies, websites, advertisements, joint-stock companies, limited joint-stock partnerships

Słowa kluczowe: spółka, strona internetowa, ogłoszenia, spółka akcyjna, spółka komandytowo akcyjna

© 2025 Marcin Tomasz Mazgaj published by Sciendo.
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

1. Wprowadzenie[1]

Wykorzystanie stron internetowych w praktyce korporacyjnej nie jest zjawiskiem nowym – np. przepisy Kodeksu spółek handlowych[2] (Sejm RP, 2000) przewidujące możliwość użycia strony spółki jako miejsca publikacji planów połączenia (art. 500 § 2^1 k.s.h.) czy planów podziału (art. 535 § 3 zd. 2 k.s.h.) obowiązują już od 2011 r., stanowiąc wyraz tendencji dostrzegalnych także w prawie unijnym[3]. Tym niemniej jednym z przejawów postępującej elektronizacji w prawie spółek w ostatnich latach jest szersze zastosowanie stron internetowych spółek w praktyce biznesowej. Stanowi to przede wszystkim konsekwencję wejścia w życie z dniem 1 stycznia 2020 r. przepisu art. 5 § 5 k.s.h., przewidującego obowiązek prowadzenia przez spółki akcyjne oraz spółki komandytowo-akcyjne własnych stron internetowych, na których publikowane są ogłoszenia pochodzące od tych spółek (co ma miejsce oprócz, a nie zamiast, dotychczas już wymaganej publikacji ogłoszeń w innych miejscach, tj. przede wszystkim w Monitorze Sądowym i Gospodarczym). Zmiana ta była o tyle rewolucyjna, że dotknęła znaczną liczbę spółek i jednocześnie wprowadzała obowiązek wykorzystywania strony internetowej, podczas gdy wcześniej obowiązujące przepisy albo jedynie dawały możliwość takiego wykorzystania (*vide* wspomniane już wcześniej art. 500 § 2^1 i art. 535 § 3 zd. 2 k.s.h., które nie nakładały obowiązku publikacji dokumentów na stronach internetowych), albo dotyczyły relatywnie niewielkiego kręgu spółek (czego przykładami są chociażby art. 402^1 § 1 k.s.h. czy art. 402^3 k.s.h., odnoszące się jedynie do spółek publicznych).

W uzasadnieniu projektu nowelizacji wprowadzającej art. 5 § 5 k.s.h. wskazano między innymi, że: „Wprowadzenie rozwiązania przewidującego prowadzenie przez wszystkie spółki akcyjne (a nie tylko publiczne) strony internetowej zwiększy efektywność ochrony praw akcjonariuszy mniejszościowych, ograniczy ryzyka informowania w taki sposób, aby w praktyce nie poinformować akcjonariuszy, co szczególnie często występuje w sytuacjach konfliktów w spółkach (z udziałem akcjonariuszy i zarządów), oraz będzie sprzyjać stabilności i bezpieczeństwu obrotu, co jest wartością o charakterze systemowym" (Sejm RP, 2019, s. 12). Z argumentacją tą trudno się nie zgodzić. Przy okazji wprowadzania art. 5 § 5 k.s.h. polski ustawodawca ograniczył

---

1 Dziękuję Recenzentom niniejszego artykułu za wnikliwe komentarze, które przyczyniły się do ulepszenia tekstu, w szczególności w zakresie zagadnień odnoszących się do prawa unijnego. Wszelkie błędy i uchybienia pozostają wyłącznie odpowiedzialnością autora.

2 Ustawa z dnia 15 września 2000 r. – Kodeks spółek handlowych (tekst jedn.: Dz.U. z 2024 r., poz. 18; dalej: „k.s.h.").

3 Zob. np. motyw 6 preambuły dyrektywy Parlamentu Europejskiego i Rady 2007/36/WE z dnia 11 lipca 2007 r. w sprawie wykonywania niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym (Dz.U. UE.L z 2007 r., nr 184, poz. 17; dalej: „dyrektywa 2007/36") czy motyw 74 preambuły dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/1132 z dnia 14 czerwca 2017 r. w sprawie niektórych aspektów prawa spółek (Dz.U.UE.L z 2017 r., nr 169, poz. 46; dalej: „dyrektywa 2017/1132").

się jednak tylko do nałożenia obowiązku prowadzenia stron (i publikowania na nich ogłoszeń), nie regulując natomiast szeregu kwestii szczegółowych związanych z tymi czynnościami. Takie podejście legislacyjne niekoniecznie musi być prawidłowe, a kwestia ta zostanie poddana analizie w niniejszej publikacji.

Celem niniejszego artykułu jest ocena obecnie obowiązujących unormowań prawnych dotyczących obowiązku prowadzenia przez spółki akcyjne (i komandytowo-akcyjne) stron internetowych (jak również unormowań przewidujących możliwość wykorzystywania przez inne spółki stron internetowych do wykonywania obowiązków publikacyjnych), a w razie zidentyfikowania niedoskonałości tych unormowań – zaproponowanie mechanizmu usunięcia tych niedoskonałości. Do realizacji tego celu przyczyni się udzielenie odpowiedzi na następujące pytania badawcze:

- Co jest, a co nie jest stroną internetową spółki? W jaki sposób ustala się adres tej strony?
- Czy spółka może mieć więcej niż jedną stronę służącą do publikacji ogłoszeń, o której mowa w art. 5 § 5 k.s.h.?
- Jakie są skutki braku publikacji ogłoszenia na stronie internetowej spółki?
- Od kiedy zmiana adresu strony internetowej spółki jest prawnie skuteczna?
- Czy implementacja dyrektyw 2007/36 i 2017/1132 została – w zakresie kwestii odnoszących się do realizacji obowiązków informacyjnych za pośrednictwem stron internetowych – dokonana prawidłowo przez polskiego ustawodawcę?

Dotąd bowiem pytania te (poza trzecim z nich) nie doczekały się pogłębionej analizy w doktrynie, mogą one natomiast odgrywać kluczową rolę zwłaszcza w sytuacji istniejącego w spółce sporu korporacyjnego, względnie w razie powstania sporu, którego przedmiotem jest prawo do korzystania przez spółkę z jej domeny internetowej. Udzielenie odpowiedzi na przytoczone wyżej pytania badawcze pozwoli przy tym na dokonanie oceny zasadności nowelizowania obecnie obowiązujących unormowań.

Wyżej określony cel niniejszego artykułu realizowany będzie przy użyciu metody dogmatycznej, a w ograniczonym zakresie przy użyciu metody komparatystycznej (co jest o tyle zasadne, że niektóre z powoływanych w niniejszym tekście unormowań k.s.h. stanowią implementację dyrektywy 2007/36 oraz dyrektywy 2017/1132, co otwiera przestrzeń do porównania polskich uregulowań z unormowaniami innych porządków prawnych). Na potrzeby niniejszego artykułu analizie poddano prawo niemieckie oraz prawo brytyjskie, którego aktualne brzmienie – pomimo Brexitu – w omawianym tutaj zakresie ukształtowane zostało jeszcze pod wpływem prawa unijnego, w czasie gdy Zjednoczone Królestwo wciąż było państwem członkowskim Unii Europejskiej.

2. Źródła i zarys ewolucji obowiązku prowadzenia strony internetowej

Obowiązek prowadzenia przez spółkę strony internetowej wprowadzony został pierwotnie jedynie w odniesieniu do publicznych spółek akcyjnych, co nastąpiło z chwilą wejścia w życie przepisu art. 402^3 k.s.h., tj. z dniem 3 sierpnia 2009 r. Unormowanie to zostało uchwalone w ramach implementacji do polskiego porządku prawnego postanowień dyrektywy 2007/36. Na niepubliczne spółki akcyjne oraz spółki komandytowo-akcyjne wspomniany obowiązek został natomiast rozciągnięty z dniem 1 stycznia 2020 r., z chwilą wejścia w życie nowelizacji k.s.h. uchwalonej w dniu 30 sierpnia 2019 r.[4], w ramach której wprowadzono do k.s.h. przepis art. 5 § 5. Z kolei powołane na wstępie niniejszej publikacji unormowania art. 500 § 2^1 i art. 535 § 3 zd. 2 k.s.h. stanowią obecnie wyraz implementacji dyrektywy 2017/1132 (a wcześniej dyrektywy 2009/109[5]) i weszły w życie z dniem 27 października 2011 r.[6]

Pomiędzy dyrektywą 2007/36 a dyrektywą 2017/1132 zachodzi jednak zasadnicza różnica. O ile bowiem unormowania tej pierwszej nakładają na spółki publiczne obowiązek prowadzenia stron internetowych (*vide* ostatnie zdanie motywu 6 dyrektywy 2007/36, gdzie wskazano iż: „Niniejsza dyrektywa zakłada, że wszystkie notowane spółki mają już swoje strony internetowe"), o tyle dyrektywa 2017/1132 wprowadza stosowanie strony internetowej jako miejsca publikacji dokumentacji korporacyjnej jedynie jako rozwiązanie opcjonalne. Z kolei ustawodawca polski, rozszerzając obowiązek prowadzenia strony internetowej na spółki niepubliczne, wykroczył poza wymogi prawa unijnego (prawo Unii Europejskiej nie wprowadza bowiem w odniesieniu do tych spółek takiego obowiązku).

3. Co jest stroną internetową spółki?

Art. 5 § 5 k.s.h. nakłada na spółki akcyjne i komandytowo-akcyjne obowiązek prowadzenia „własnych" stron internetowych. Z kolei art. 500 § 2^1 i art. 535 § 3 zd. 2 k.s.h. wspominają o udostępnianiu przez spółkę dokumentacji na „swojej" stronie internetowej. Żadne z tych pojęć nie zostało jednak zdefiniowane, przez co mogą one być rozumiane na kilka różnych sposobów. Pojawia się bowiem w tym kontekście

4 Ustawa z dnia 30 sierpnia 2019 r. o zmianie ustawy – Kodeks spółek handlowych oraz niektórych innych ustaw (Dz.U. z 2019 r., poz. 1798 z późn. zm.).

5 Tj. dyrektywy Parlamentu Europejskiego i Rady 2009/109/WE z dnia 16 września 2009 r. zmieniającej dyrektywy Rady 77/91/EWG, 78/855/EWG i 82/891/EWG oraz dyrektywę 2005/56/WE w odniesieniu do wymogów dotyczących sprawozdawczości i dokumentacji w przypadku połączeń i podziałów (Dz.U. UE.L z 2009 r., nr 259, poz. 14).

6 Co do ewolucji obowiązku prowadzenia przez spółki stron internetowych zob. również Opalski (2024, Nb 7), który poddaje tam krytyce obowiązek prowadzenia stron internetowych przez spółki niepubliczne.

pytanie – czy stroną internetową spółki, o której mowa w przytoczonych unormowaniach, będzie:

- dowolna strona internetowa, z której spółka faktycznie korzysta?
- dowolna strona internetowa opublikowana pod domeną internetową, której spółka jest abonentem?
- strona internetowa dostępna pod adresem www widniejącym w Krajowym Rejestrze Sądowym?
- strona internetowa określona w uchwale zarządu?
- strona internetowa faktycznie wskazana akcjonariuszom?
- główny adres www spółki wykorzystywany biznesowo?

W dotychczasowej literaturze wskazuje się, że pod pojęciem strony internetowej spółki należy rozumieć „korporacyjną stronę WWW (*homepage*), której adres należy do spółki, a nie jakąkolwiek inną stronę w Internecie (np. na portalu społecznościowym czy na ogólnym portalu informacyjnym" (Oplustil, 2024, Nb 8), jak również, że „przesłanka prowadzenia «własnej» strony internetowej jest spełniona, jeżeli podmiotem uprawnionym z tytułu rejestracji domeny internetowej (abonentem) jest spółka, a uprawnienia administratora zawartych na niej danych przysługują jej zarządowi" (Herbet, 2013, Nb 16). Żadne z tych wyjaśnień nie rozwiązuje jednak w pełni istoty analizowanego problemu. Pierwsza z przytoczonych wypowiedzi posługuje się nie do końca precyzyjnym sformułowaniem *homepage*, natomiast druga nie wskazuje wprost, czy posiadanie przez spółkę statusu abonenta domeny jest jedynym kryterium wymaganym do uznania strony widniejącej pod tą domeną za „własną" stronę internetową spółki.

Rozwiązania wyżej opisanego problemu nie dostarcza również prawo unijne. Motyw 6 dyrektywy 2007/36 wskazuje bowiem, iż dyrektywa ta „zakłada, że wszystkie notowane spółki mają już swoje strony internetowe", nigdzie jednak nie precyzując, jak należy ustalać, czy konkretna strona internetowa może być przez spółkę uznana za „swoją" stronę internetową. Problem staje się jeszcze bardziej złożony po zestawieniu polskiej wersji językowej dyrektywy z np. wersją anglojęzyczną czy niemieckojęzyczną. Te ostatnie bowiem w analizowanym tutaj fragmencie w ogóle nie operują przymiotnikiem „swoje", wymagając jedynie, by spółki „miały" lub „posiadały" stronę internetową (ang.: *This Directive presupposes that all listed companies already have an Internet site*, niem.: *Mit dieser Richtlinie wird vorausgesetzt, dass alle börsennotierten Gesellschaften bereits über eine Internetseite verfügen*).

Także na gruncie prawa niemieckiego brak jest klarownego rozwiązania omawianego problemu – w niemieckiej ustawie normującej funkcjonowanie spółek akcyjnych (*Aktiengesetz*) niemiecki prawodawca po prostu posługuje się pojęciem „strony internetowej spółki" (*die Internetseite der Gesellschaft*), nie precyzując ani nie definiując omawianego pojęcia. W przeciwieństwie do polskiego ustawodawcy, prawodawca niemiecki wyraźnie odróżnia jednak stronę internetową spółki od stron

podmiotów trzecich, na których udostępniana jest dokumentacja korporacyjna (czego wyrazem jest dotyczący „wirtualnych walnych zgromadzeń" art. 118a[6] Aktiengesetz, nakazujący udostępnienie dokumentacji związanej z danym „wirtualnym walnym zgromadzeniem" poprzez „stronę internetową spółki lub stronę podmiotu trzeciego, która jest dostępna za pośrednictwem strony internetowej spółki" (*die Internetseite der Gesellschaft oder eine über diese zugängliche Internetseite eines Dritten zugänglich zu machen*).

Odmiennie natomiast podszedł do tego zagadnienia prawodawca brytyjski, który w wybranych przepisach tamtejszego *Companies Act 2006* (np. sec. 353[2], sec. 430[2], sec. 940A[1]) wprowadza wymaganie, by strona internetowa, na której spółka publikuje dokumenty i informacje:

– po pierwsze, była „utrzymywana przez spółkę lub w jej imieniu" (*is maintained by or on behalf of the company*);
– po drugie, „identyfikowała przedmiotową spółkę" (*identifies the company in question*).

W praktyce obrotu w Polsce nierzadko przyjmuje się po prostu, że stroną internetową spółki jest strona internetowa, której adres www ujawniony jest we wpisie danej spółki w Krajowym Rejestrze Sądowym (ustawodawca przewidział bowiem umieszczanie stosownej informacji w tym zakresie w Dziale 1, Rubryce 2 wpisu spółki w KRS). Należy jednak mieć na uwadze, że:

– po pierwsze, brak jest przepisu nadającego wpisowi adresu www strony internetowej spółki do KRS charakter konstytutywny (a co za tym idzie – wpis ten jest jedynie wpisem deklaratoryjnym);
– po drugie, nie wszystkie spółki mają obowiązek ujawnienia w KRS adresu swojej strony internetowej – art. 47 ust. 1 ustawy o Krajowym Rejestrze Sądowym[7] nakłada bowiem ten obowiązek jedynie na spółki akcyjne i spółki komandytowo-akcyjne, podczas gdy w pozostałych przypadkach wskazanie adresu strony internetowej spółki ma jedynie charakter fakultatywny (co wprost wynika z treści art. 38 pkt. 1a ustawy o KRS).

Odpowiedź na pierwsze z postawionych pytań („Co jest stroną internetową spółki?") zależna będzie jednak od odpowiedzi na pytanie drugie („Czy spółka może mieć więcej niż jedną stronę służącą do publikacji ogłoszeń, o której mowa w art. 5 § 5 k.s.h.?"). Stąd też do pierwszego z analizowanych problemów należy powrócić dopiero po rozwiązaniu drugiego z nich.

7 Ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (tekst jedn.: Dz.U. z 2024 r., poz. 979), dalej: „ustawa o KRS".

4. Ile spółka może mieć stron internetowych, o których mowa w art. 5 § 5 k.s.h.?

Nie ulega wątpliwości, że spółka może publikować swoje ogłoszenia korporacyjne jednocześnie na więcej niż jednej stronie internetowej. Istota problemu sprowadza się jednak do tego, czy spółka będzie działać zgodnie z prawem, wykorzystując w celach publikacyjnych swoje różne strony alternatywnie, np. niektóre ogłoszenia publikując na jednej, a inne na drugiej. Tytułem przykładu, można rozważyć, czy wymagania prawne zostaną spełnione, jeśli spółka w celu publikacji planu połączenia (a tym samym wypełnienia wymogu z art. 500 § 2^1 k.s.h.) wykupi odrębną domenę internetową (inną od tej, która jest wskazana w KRS, i tej, pod którą spółka na ogół publikuje swoje ogłoszenia) i tylko pod adresem dostępnym dzięki tej nowej domenie udostępni wspomniany plan.

De lege lata trudno znaleźć podstawy do uznania takiego działania za sprzeczne z prawem. K.s.h. wymaga dokonania przez spółkę publikacji na „swojej" stronie internetowej i brak jest argumentów prawnych, by uznać, że publikacja na takiej alternatywnej stronie nie jest publikacją, którą spółka dokonała na swojej stronie internetowej. To, czy adres takiej alternatywnej strony internetowej został ujawniony w KRS, nie jest w tym przypadku kluczowe, gdyż – jak już wskazano – wpis tego adresu w KRS jest wpisem jedynie deklaratoryjnym. Innymi słowy, nawet publikacja przez spółkę ogłoszenia wyłącznie na takiej stronie internetowej, której adres nie jest znany akcjonariuszom, i której adres nie jest opublikowany w KRS, w obecnym stanie prawnym jest zgodna z prawem (jeśli tylko spółka dysponuje faktyczną kontrolą nad treścią tej strony). Takie działanie może jedynie być rozpatrywane co najwyżej jako sprzeczne z dobrymi obyczajami, co – w realiach korporacyjnych – może dawać asumpt do skutecznego zaskarżenia uchwał walnego zgromadzenia (podjętych w oparciu o takie ogłoszenia) w trybie powództwa o uchylenie uchwały, na podstawie art. 422 § 1 k.s.h. Samo dokonanie publikacji ogłoszenia w opisany powyżej sposób nie będzie jednak wystarczające do skutecznego zaskarżenia uchwał w trybie powództwa o stwierdzenie nieważności, opisane działanie nie jest bowiem – jak już wskazano powyżej – sprzeczne z ustawą.

Nie jest jednak również tak, że wpis adresu strony internetowej w KRS pozostaje zupełnie bez znaczenia. Wiąże się z nim bowiem zarówno domniemanie prawdziwości (art. 17 ustawy o KRS), jak i – przede wszystkim – domniemanie znajomości tego wpisu (a co za tym idzie – adresu strony) przez m.in. akcjonariuszy (art. 15 ust. 1 zd. 1 ustawy o KRS). Kwestia znajomości lub nieznajomości adresu strony internetowej spółki przez akcjonariusza ma jednak obecnie znaczenie jedynie w kontekście zgodności działań spółki z dobrymi obyczajami, a nie w kontekście zgodności tych działań z prawem (gdyż – jak już wskazano – brak jest wymogu prawnego, by ogłoszenia pochodzące od spółki publikowane były na stronie internetowej, której adres znany jest akcjonariuszom). Okoliczność ta w sposób szczególny uwidacznia się w przy-

padku publikacji, o których mowa w art. 500 § 2^1 i art. 535 § 3 zd. 2 k.s.h. – podmiotem dokonującym tych publikacji może bowiem być przecież także spółka niebędąca spółką akcyjną czy komandytowo-akcyjną (a zatem niemająca obowiązku ujawnienia jakiegokolwiek adresu strony internetowej w KRS), a nawet spółka, która jeszcze nie została wpisana do KRS (zgodnie z poglądem dominującym w doktrynie [zob. Rodzynkiewicz, 2016, Nb 14 i dokonany tam przegląd literatury w tym zakresie], spółka w organizacji ma bowiem zdolność połączeniową i podziałową oraz może uczestniczyć w fazie menedżerskiej i w fazie właścicielskiej połączenia lub podziału; wpis tej spółki do KRS warunkuje jedynie możliwość rejestracji połączenia lub podziału).

Podsumowując, stwierdzić należy, że spółka może prowadzić więcej niż jedną stronę internetową służącą publikacji ogłoszeń. Wniosek ten jest dodatkowo – choć, jak trzeba przyznać, w ograniczonym zakresie – wspierany brzmieniem dyrektywy 2017/1132. Art. 28 tego aktu prawnego nakłada bowiem na państwa członkowskie obowiązek wprowadzenia sankcji na wypadek – między innymi – „nieumieszczenia na dowolnej ze stron internetowych spółki" informacji przewidzianych w art. 26 tej dyrektywy. Siła tego argumentu jest jednak, jak już zasygnalizowano powyżej, ograniczona. Wspomniany art. 26 dyrektywy 2017/1132 odnosi się bowiem nie tylko do stron internetowych spółki, lecz również do pism i formularzy zamówień spółki (wobec czego nie można jego zakresu zastosowania, a w konsekwencji również zakresu zastosowania art. 28 tej dyrektywy, utożsamiać z zakresem zastosowania przepisów normujących obowiązki spółek w zakresie publikowania ogłoszeń i dokumentów korporacyjnych na stronach internetowych)[8].

Tym niemniej wobec faktu, iż *de lege lata* na gruncie prawa polskiego dopuszczalne jest prowadzenie przez spółkę więcej niż jednej strony internetowej służącej publikacji ogłoszeń, publikacja na choćby tylko jednej spośród prowadzonych stron internetowych będzie działaniem zgodnym z prawem, i to również w przypadku, gdy publikacji dokonano na stronie internetowej, której adres nie jest ujawniony w KRS. Takie działanie ze strony spółki może jedynie być uznane za sprzeczne z dobrymi obyczajami (a przez to – jeśli np. w oparciu o publikację dokonaną na stronie internetowej przeprowadzono walne zgromadzenie – uzasadnić zaskarżenie uchwał podjętych na takim walnym zgromadzeniu, jednak wyłącznie w trybie powództwa o uchylenie, nie zaś w trybie powództwa o stwierdzenie nieważności).

To z kolei prowadzi do konkluzji, że stroną internetową, o której mowa w art. 5 § 5 k.s.h., jest każda strona internetowa, nad której treścią spółka ma faktyczną kon-

8 Co więcej, pewną przeciwwagą dla powołanego argumentu jest to, iż w angielskiej oraz w niemieckiej wersji językowej przytoczonego już w niniejszej publikacji motywu 6 dyrektywy 2007/36 prawodawca unijny posługuje się zwrotem „strona internetowa" w liczbie pojedynczej (co stoi w pewnym kontraście do polskiego brzmienia dyrektywy, gdzie sformułowanie to w motywie tym pojawia się w liczbie mnogiej).

trolę, a która przeznaczona została przez zarząd spółki[9] do publikacji ogłoszeń. Nie jest przy tym zasadne formułowanie wymogu, iż to spółka musi być abonentem domeny, pod którą dostępna jest ta strona (co czyni Herbet [2013, Nb 16]) – wywodzenie tego wymogu z posłużenia się przez ustawodawcę w art. 5 § 5 k.s.h. słowem „własnej" wydaje się zbyt daleko idącym zabiegiem (równie dobrze można by w oparciu o ten zwrot próbować stwierdzić, że strona powinna być dostępna z serwera należącego do spółki – które to wymaganie jednak także Herbet [2013, Nb 16] trafnie uznaje za zbyt daleko idące). Jeżeli spółka opublikuje ogłoszenie na stronie internetowej, nad którą ma faktyczną kontrolę, lecz która dostępna jest pod domeną, której abonentem formalnie nie jest sama spółka (może nim również być np. wspólnik czy członek zarządu spółki), to takie działanie uznać należy za wypełnienie wymogu wynikającego z art. 5 § 5 k.s.h.

Co przy tym istotne, stroną internetową, o której mowa w art. 5 § 5 k.s.h., nie jest każda strona, którą spółka faktycznie włada, lecz jedynie taka, którą spółka zarówno faktycznie włada, jak i która została przeznaczona przez zarząd do publikacji ogłoszeń. Publikacja ogłoszenia jest bowiem czynnością, za której wykonanie – zgodnie z ogólną zasadą domniemania kompetencji – odpowiedzialny jest zarząd. Zarząd działa natomiast *in corpore*, w drodze podejmowanych przez siebie uchwał. Z tego względu o przeznaczeniu konkretnej strony internetowej do publikacji ogłoszeń (a zatem o nadaniu jej statusu, o którym mowa w art. 5 § 5 k.s.h.) powinien zdecydować zarząd w podjętej przez siebie uchwale.

Jednocześnie stwierdzić należy, że obecny stan prawny jest wysoce niezadowalający. Wymóg publikacji ogłoszeń na stronie internetowej spółki służy, jak wiadomo, przede wszystkim celowi zapewnienia odpowiedniego dostępu do informacji korporacyjnych interesariuszom spółki. Cel ten obecnie nie jest (a przynajmniej nie musi być) należycie realizowany, skoro *de lege lata* dopuszczalne jest publikowanie ogłoszeń nawet na specjalnie utworzonej przez spółkę, nieujawnionej w KRS i nieznanej akcjonariuszom stronie internetowej. Słusznym krokiem było natomiast nałożenie na spółki akcyjne i komandytowo-akcyjne wynikającego z art. 47 ust. 1 ustawy o KRS wymogu ujawniania w KRS adresów stron internetowych. Ustawodawca powinien jednak pójść o krok dalej, tj.:

– po pierwsze, uzależnić – w przypadkach gdy korzystanie ze strony internetowej jako miejsca publikacji ma charakter fakultatywny (np. art. 500 § 2^1, art. 535 § 3 zd. 2 k.s.h.) – możliwość publikacji dokumentów na stronie internetowej spółki od uprzedniego ujawnienia w KRS adresu tej strony internetowej;

9 W przypadku spółki komandytowo-akcyjnej – przez komplementariuszy. Dla zapewnienia większej przejrzystości wywodu, w dalszej części niniejszego artykułu autor będzie posługiwał się terminologią właściwą dla spółki akcyjnej.

– po drugie, wprost wskazać, iż spółka może mieć w danym czasie tylko jedną stronę internetową służącą publikacjom, o których mowa w art. 5 § 5 k.s.h.;
– po trzecie, nadać wpisowi adresu strony internetowej spółki w KRS charakter konstytutywny.

Ostatnia z powyższych propozycji może w pewnych sytuacjach doprowadzić do przejściowej niemożliwości podejmowania niektórych czynności korporacyjnych (np. zwołania walnego zgromadzenia) w sposób zgodny z prawem, w razie utraty przez spółkę faktycznej kontroli nad stroną internetową, której adres wskazano w KRS (do momentu ujawnienia w KRS nowego adresu www, publikacja ogłoszenia pod takim nowym adresem nie byłaby bowiem równoznaczna ze spełnieniem wymagań prawnych). Przypadek, w którym ze względu na utrudnienia o charakterze faktycznym przejściowo nie da się skutecznie zwołać walnego zgromadzenia, nie jest jednak zjawiskiem nieznanym praktyce obrotu (zachodzi on również np. gdy z uwagi na rezygnację członków organów spółki organy te mają charakter kadłubowy bądź pozbawione są jakichkolwiek członków). Z drugiej jednak strony, nadanie wpisowi adresu strony internetowej spółki w KRS charakteru konstytutywnego pozwoli na uniknięcie sporów dotyczących kwestii fundamentalnej, tj. sporów o to, co jest, a co nie jest stroną internetową spółki. Przyczyni się zatem pozytywnie do bezpieczeństwa obrotu prawnego oraz ochrony interesariuszy spółek, a właśnie tej kwestii służą przepisy regulujące obowiązki informacyjne spółek. Ponadto wspomnianemu wyżej problemowi można przeciwdziałać poprzez wprowadzenie klauzuli generalnej umożliwiającej spółce dokonanie czynności korporacyjnej pomimo braku publikacji ogłoszenia na stronie internetowej, jeśli spółka dochowała należytej staranności, by zainteresowane podmioty zostały poinformowane o treści ogłoszenia również w inny sposób (zob. proponowany niżej nowy art. 5 § 8 k.s.h.).

Pierwsza z przedstawionych trzech propozycji *de lege ferenda* uniemożliwi stosowanie dopuszczalnej obecnie praktyki polegającej na publikowaniu np. planu połączenia czy planu podziału na specjalnie w tym celu utworzonej (a nieznanej wierzycielom spółki ani jej wspólnikom) stronie internetowej. Drugi z przedstawionych postulatów pozwoli natomiast na uniknięcie opisywanego w niniejszej publikacji problemu wielości stron internetowych spółki, który to problem wynika po części z posłużenia się przez ustawodawcę w aktualnym brzmieniu art. 5 § 5 k.s.h. liczbą mnogą („spółka akcyjna i spółka komandytowo-akcyjna prowadzą własne strony internetowe i zamieszczają także na tych stronach […]") zamiast liczbą pojedynczą („spółka akcyjna i spółka komandytowo-akcyjna prowadzi własną stronę internetową i zamieszcza także na tej stronie […]"). Z kolei trzeci ze sformułowanych postulatów pozwoli na jednoznaczne określenie, czy konkretna strona internetowa jest stroną, której treść powinna być monitorowana przez interesariuszy spółki w celu pozyskania wiążących informacji korporacyjnych.

5. Skutki braku publikacji ogłoszenia na stronie internetowej spółki

Jak już wskazano powyżej, problem skutków braku wymaganej prawem publikacji pochodzącego od spółki ogłoszenia na stronie internetowej tej spółki jest – wśród wszystkich problemów rozpatrywanych w niniejszym artykule – problemem, którego rozstrzygnięcie napotyka relatywnie najmniej przeszkód. Taki brak jest bowiem równoznaczny z naruszeniem ustawy (a konkretnie art. 5 § 5 k.s.h., ewentualnie innego przepisu wprowadzającego wymóg publikacji na stronie internetowej, jak np. art. 402^3 § 1 k.s.h.) i w konsekwencji czynność prawna zdziałana w sytuacji takiego naruszenia (np. uchwała walnego zgromadzenia podjęta na walnym zgromadzeniu zwołanym jedynie poprzez ogłoszenie w Monitorze Sądowym i Gospodarczym, bez publikacji ogłoszenia na stronie internetowej spółki), jako sprzeczna z prawem, może zostać uznana za nieważną[10] (tak również: Matraszek & Wojciechowska, 2020, s. 33). Jednocześnie, jak wynika z dotychczasowego orzecznictwa Sądu Najwyższego (np. Wyrok Sądu Najwyższego, 2007), w przypadku uchwał walnego zgromadzenia brak publikacji będzie stanowił podstawę do stwierdzenia nieważności jedynie, jeżeli wywarł wpływ na treść uchwały (a zatem np. gdy w wyniku braku publikacji ogłoszenia na stronie internetowej na zgromadzeniu nie stawił się akcjonariusz dysponujący pulą głosów wystarczającą do „zablokowania" podjęcia uchwały).

6. Od kiedy zmiana adresu strony internetowej spółki jest skuteczna?

Odpowiedź na pytanie o moment, od którego zmiana adresu strony internetowej spółki staje się skuteczna, stanowi wypadkową odpowiedzi na pytania postawione w pkt. 3 („Co jest stroną internetową spółki?") i pkt. 4 („Ile spółka może mieć stron internetowych, o których mowa w art. 5 § 5 k.s.h.?") niniejszego artykułu. Skoro bowiem uznano, że:

1. stroną internetową spółki jest każda strona, którą spółka faktycznie włada, a która została wskazana w uchwale zarządu jako służąca publikacji ogłoszeń;
2. spółka może mieć więcej niż jedną stronę internetową, o której mowa w art. 5 § 5 k.s.h.; a ponadto skoro wpis zmiany adresu strony internetowej spółki w KRS ma – *de lege lata* – charakter jedynie deklaratoryjny, stwierdzić należy, że w obecnym stanie prawnym:
   - po pierwsze, strona internetowa spółki traci status strony, o której mowa w art. 5 § 5 k.s.h., z chwilą podjęcia przez zarząd spółki uchwały, z której wynikać będzie taka decyzja zarządu;

10 W przypadku uchwał walnych zgromadzeń – na zasadzie art. 425 § 1 k.s.h.; w przypadku uchwał innych organów – na zasadzie art. 58 § 1 Kodeksu cywilnego w zw. z art. 2 k.s.h., choć możliwość stosowania art. 58 k.c. do uchwał organów spółek stanowi przedmiot dyskusji w doktrynie – zob. w tej kwestii: Opalski & Wiśniewski, 2024, Nb 30–33.

– po drugie, podjęcie przez zarząd uchwały, w której status strony, o której mowa w art. 5 § 5 k.s.h., nadany zostanie nowej (innej niż dotychczas) stronie internetowej, nie skutkuje utratą tego statusu przez inne strony, którym ten status nadano we wcześniejszych uchwałach.

Jak już przy tym wskazano, pomimo powyższego, nie jest tak, że wpis adresu strony internetowej w KRS pozostaje bez znaczenia, albowiem dane widniejące w KRS cechują się domniemaniem prawdziwości wpisów (art. 17 ust. 1 ustawy o KRS) oraz jawnością materialną (art. 15 ust. 1 ustawy o KRS). Hipotetycznie można więc wyobrazić sobie sytuację, w której zarząd publikuje w Monitorze Sądowym i Gospodarczym ogłoszenie o zwołaniu walnego zgromadzenia, następnie jednak (np. w wyniku podjęcia decyzji o rezygnacji z przeprowadzania tego zgromadzenia) rezygnuje z publikacji ogłoszenia na stronie internetowej (co czyni, mając na celu zapobieżenie odbyciu się owego walnego zgromadzenia). Jeśli, pomimo tej rezygnacji, na ujawnionej w KRS stronie internetowej spółki widniałoby ogłoszenie o zwołaniu walnego zgromadzenia (która to publikacja nastąpiłaby np. w wyniku samowolnych działań jednego z członków zarządu), zarząd nie mógłby skutecznie zaskarżyć uchwał podjętych na takim zgromadzeniu głosami akcjonariuszy działających w dobrej wierze, co wynika przede wszystkim z treści art. 14 i art. 17 ust. 1 ustawy o KRS.

7. Ocena prawidłowości polskiej implementacji dyrektyw 2007/36 oraz 2017/1132 w zakresie wykonywania obowiązków i uprawnień publikacyjnych poprzez stronę internetową spółki

Pomimo dokonanej w niniejszym artykule krytyki polskich rozwiązań legislacyjnych w zakresie omawianej tematyki, przyznać należy, iż obecny kształt polskich unormowań prawnych dotyczących tej materii stanowi konsekwencję równie nieprecyzyjnego jej uregulowania na poziomie prawa unijnego. Jak przy tym trafnie wskazuje się w literaturze anglojęzycznej, prawodawca unijny także dość niedbale posługuje się terminologią – np. z niewiadomych przyczyn w angielskiej wersji językowej dyrektywy 2007/36 pierwotnie posłużono się zwrotem *Internet site*, ale już w przepisach wprowadzonych do tej dyrektywy na mocy dyrektywy 2017/828[11] – zwrotem *website* (na co zasadnie wskazują Lieder & Bialluch [2021, s. 898–899]). Co jednak istotne, żadna z analizowanych dyrektyw nie precyzuje, jak należy rozumieć wspomniane sformułowania i co konkretnie się pod nimi kryje. W tym kontekście nie sposób oprzeć się wrażeniu, iż polska (jak również niemiecka) implementacja dyrektyw 2007/36 i 2017/1132, w omawianym tutaj zakresie, sprowadziła się w du-

11 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/828 zmieniająca dyrektywę 2007/36/WE w zakresie zachęcania akcjonariuszy do długoterminowego zaangażowania (Dz.U. UE.L z 2017 r., nr 132, poz. 1).

żej mierze do prostego skopiowania treści dyrektyw. Dlatego – jakkolwiek dokonana przez polskiego ustawodawcę implementacja jest formalnie prawidłowa (tj. prawo krajowe, w zakresie kwestii analizowanych w niniejszym artykule, nie jest sprzeczne z treścią dyrektyw) – budzi ona zastrzeżenia merytoryczne. Dyrektywa unijna jest bowiem ze swej istoty aktem o charakterze ramowym, który obliguje ustawodawców krajowych do osiągnięcia pewnego rezultatu, pozostawiając tym ustawodawcom pewien luz decyzyjny co do mechanizmu realizacji tego celu. Z tego względu siłą rzeczy unormowania dyrektywy z zasady nie muszą być w pełni precyzyjne. Z uwagi na wskazane powyżej niedoskonałości prawa unijnego, omawianych w niniejszym artykule problemów nie da się usunąć w drodze prounijnej wykładni prawa krajowego, lecz wymagają one interwencji legislacyjnej (której propozycja przedstawiona jest w pkt. 8 niniejszego artykułu).

Przykładem porządku prawnego, w którym – pomimo braku obowiązku wynikającego z dyrektyw – ustawodawca podszedł do omawianego tematu znacznie bardziej kompleksowo, jest prawo brytyjskie (którego obecna treść, w analizowanym tutaj zakresie, w zdecydowanej większości powstała jeszcze pod wpływem prawa unijnego, albowiem powstała w czasie, gdy Zjednoczone Królestwo było państwem członkowskim Unii Europejskiej), gdzie ustawodawca:

- po pierwsze, dookreślił, jakie kryteria muszą być spełnione, by strona internetowa mogła być przez spółkę wykorzystywana w celach publikacyjnych (zob. pkt. 3 niniejszego artykułu powyżej);
- po drugie, wyłączył negatywne skutki prawne nieudostępnienia informacji bądź dokumentów na stronie internetowej, jeśli nieudostępnienie to wyniknęło z okoliczności, których zapobieżenia lub uniknięcia nie można było od spółki rozsądnie oczekiwać (zob. np. art. 353(5) czy 940A(1) Companies Act 2006[12]);
- po trzecie, niejednokrotnie wyraźnie wskazuje, przez jaki dokładnie okres informacje muszą być dostępne na stronie internetowej (zob. np. art. 353(4)(b) czy art. 430(1)(b) Companies Act 2006[13]).

12 Zgodnie z tymi unormowaniami nieudostępnienie informacji na stronie internetowej nie jest brane pod uwagę, jeżeli: (a) informacje są udostępniane na stronie internetowej przez część wymaganego prawem okresu, oraz (b) wspomniane nieudostępnienie jest w całości spowodowane okolicznościami, których zapobieżenie lub uniknięcie przez spółkę nie byłoby uzasadnione.

13 Pierwszy z przytoczonych przepisów wprowadza wymóg utrzymania na stronie internetowej niektórych spółek publicznych informacji o wynikach głosowań na walnym zgromadzeniu przez okres co najmniej dwóch lat. Z kolei drugi wprowadza wymóg udostępniania sprawozdań finansowych niektórych spółek publicznych na ich stronach internetowych aż do czasu udostępnienia na tej stronie takich sprawozdań za kolejny rok obrotowy.

8. Postulaty de lege ferenda. Podsumowanie

Przedstawione w odniesieniu do prawa polskiego konkluzje *de lege lata* nie prowadzą do realizacji celu w postaci zapewnienia wśród interesariuszy spółki odpowiedniego poziomu poinformowania o zachodzących w niej zdarzeniach korporacyjnych. Problem ten zostałby jednak usunięty w razie zrealizowania przez ustawodawcę postulatów *de lege ferenda* zgłoszonych w pkt. 4 niniejszego artykułu, przede wszystkim zaś postulatu nadania wpisowi adresu strony internetowej spółki w KRS charakteru konstytutywnego. Realizacja tych postulatów mogłaby nastąpić w drodze:

– po pierwsze, dodania nowego art. 4 § 6 k.s.h. o następującym brzmieniu:
„Ilekroć w ustawie mowa jest o «własnej stronie internetowej» spółki lub «swojej stronie internetowej» spółki, bądź o «stronie internetowej spółki», należy przez to rozumieć stronę internetową, której adres jest wpisany do rejestru, a która jest utrzymywana przez spółkę lub przez podmiot trzeci, który utrzymuje tę stronę w imieniu spółki za jej zgodą.";
– po drugie, zmiany brzmienia art. 5 § 5 k.s.h. na następujące:
„Spółka akcyjna i spółka komandytowo-akcyjna prowadzi własną stronę internetową i zamieszcza także na tej stronie, w miejscu wydzielonym na komunikację z akcjonariuszami, wymagane przez prawo lub statut ogłoszenia pochodzące od spółki.";
– po trzecie, dodania w art. 5 k.s.h. nowych § 6, § 7 i § 8 o następującym brzmieniu:
„§ 6. Spółka niebędąca spółką akcyjną i spółką komandytowo-akcyjną może, w przypadkach przewidzianych w przepisach szczególnych, wykorzystywać własną stronę internetową w celu publikowania na niej, w miejscu wydzielonym na komunikację ze wspólnikami lub akcjonariuszami, wymaganych przez prawo dokumentów i ogłoszeń pochodzących od spółki.
§ 7. Ogłoszenia i dokumenty uznaje się za należycie opublikowane na stronie internetowej, jeśli są one na tej stronie ogólnodostępne bez ponadprzeciętnych utrudnień oraz bez konieczności uiszczania opłat.
§ 8. Ogłoszenia i dokumenty uznaje się za należycie opublikowane na stronie internetowej spółki nawet pomimo ich przejściowej niedostępności na tej stronie internetowej, jeśli niedostępność ta wynika wyłącznie z okoliczności, których zapobieżenia lub uniknięcia nie można było od spółki rozsądnie oczekiwać, a spółka dołożyła należytej staranności, by jej wspólnicy lub akcjonariusze, a także inne znane spółce zainteresowane podmioty, zostali w inny sposób poinformowani o treści danego ogłoszenia lub dokumentu."

Proponowane zmiany nie tylko pozwoliłyby na wyeliminowanie większości spośród opisanych w niniejszym artykule wątpliwości, lecz również byłyby zgodne

z celem dyrektywy 2007/36, jakim jest zapewnienie odpowiedniego poziomu informowania akcjonariuszy spółek (*vide* motywy 5 i 6 tej dyrektywy).

Dotychczasowe rozszerzanie przez ustawodawcę zakresu wykorzystania stron internetowych spółek w praktyce korporacyjnej ocenić należy przy tym ze wszech miar pozytywnie. Praktyka obrotu pokazywała bowiem, że utrzymywanie dotychczasowego założenia znajomości przez interesariuszy spółek treści ogłoszeń publikowanych w Monitorze Sądowym i Gospodarczym było utrzymywaniem fikcji. Stan ten wymagał modyfikacji i zasadniczy kierunek obrany przez ustawodawcę jest słuszny. Poprzestanie przez ustawodawcę na wprowadzeniu obowiązku dokonywania publikacji na stronach internetowych, przy jednoczesnym braku unormowania szczegółowych kwestii związanych z określaniem przez spółki adresów tych stron internetowych i funkcjonowaniem wspomnianych stron, zrodziło jednak kolejne wątpliwości, które aktualizować się będą przede wszystkim w sytuacji sporu korporacyjnego, względnie w przypadkach sporu domenowego dotyczącego strony internetowej wykorzystywanej przez spółkę do publikacji ogłoszeń. Realizacja przedstawionych w niniejszym artykule postulatów *de lege ferenda* (w tym przede wszystkim postulatu nadania wpisowi adresu strony internetowej spółki charakteru konstytutywnego) pozwoliłaby na znaczące ograniczenie wspomnianych problemów, z korzyścią dla poziomu świadomości interesariuszy spółek o zdarzeniach korporacyjnych, i w konsekwencji z korzyścią dla bezpieczeństwa obrotu prawnego.

BIBLIOGRAFIA

Herbet, A. (2013). Komentarz do artykułu 402[3], w: S. Sołtysiński i in. (red.), *Kodeks spółek handlowych. Komentarz*, C.H. Beck (Legalis).

Lieder, J. & Bialluch, M. (2021). Directive 2007/36/EC of the European Parliament and of the Council of 11 July 2007 on the exercise of certain rights of shareholders in listed companies (Shareholder Rights Directive), w: P. Kindler & J. Lieder (red.), *European Corporate Law. Article-by-Article Commentary*, Nomos & Beck & Hart.

Matraszek, J. & Wojciechowska, Z. (2020). Wpływ przepisów wprowadzających obowiązkową dematerializację na zaskarżanie uchwał organów „właścicielskich" spółek akcyjnych, *Przegląd Prawa Handlowego,* (10), 30–38.

Opalski, A. (2024), Komentarz do artykułu 5, w: A. Opalski (red.), *Kodeks spółek handlowych. Komentarz*, C.H. Beck (Legalis).

Opalski, A. & Wiśniewski, A. (2024), Komentarz do artykułu 2, w: A. Opalski (red.), *Kodeks spółek handlowych. Komentarz*, C.H. Beck (Legalis).

Oplustil, K. (2024), Komentarz do artykułu 500, w: M. Bieniak i in., *Kodeks spółek handlowych. Komentarz*, C.H. Beck (Legalis).

Rodzynkiewicz, M. (2016), Komentarz do artykułu 491, w: A. Opalski (red.), *Kodeks spółek handlowych. Komentarz*, C.H. Beck (Legalis).

Sejm Rzeczypospolitej Polskiej. (2000). Ustawa z dnia 15 września 2000 r. – Kodeks spółek handlowych (tekst jedn.: Dz.U. z 2024 r., poz. 18).

Sejm Rzeczypospolitej Polskiej (2019). Uzasadnienie projektu ustawy o zmianie ustawy – Kodeks spółek handlowych oraz niektórych innych ustaw. https://orka.sejm.gov.pl/Druki8ka.nsf/0/38BFA72164FE8069C125841D00436FE7/%24File/3541-uzas.DOCX

Wyrok Sądu Najwyższego z dnia 5 lipca 2007 r., sygn. akt II CSK 163/07, LEX.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.05

Received: 31.12.2024
Accepted: 30.04.2025

Przemysław Katner
Uniwersytet Szczeciński, Polska
przemyslaw.katner@usz.edu.pl
ORCID ID: https://orcid.org/0000-0003-4059-5216

Prawo do jednostki kryptowaluty – uwagi *de lege lata*, prawnoporównawcze i *de lege ferenda*

The Right to a Cryptocurrency Unit: *de lege lata,* Comparative Law and *de lege ferenda* Considerations

Abstract: Despite the fact that cryptocurrency trading has been taking place in Poland for a dozen or so years, the issue of the existence and nature of the right to cryptocurrency units has not been resolved in civil law doctrine and case law. The legislature has also not taken any action in this regard, including in the draft act on the cryptoasset market currently in process. Meanwhile, this issue is of significant theoretical and practical importance. This article therefore examines the currently presented views together with their indicated consequences, and then supplements the ongoing discussion with comparative legal remarks usually omitted in Polish literature. In this respect, solutions proposed or in force in European Union, German, British and Chinese law are taken into account. This provides an opportunity to comment on existing concepts, in particular the rejection of the proposal to adopt in Polish law *de lege lata* the right to a unit of cryptocurrency, effective *erga omnes* (although with the submission of a *de lege ferenda* application), and the view that there is no substantive right in this respect. In conclusion, it is considered that currently in Poland, the right to a unit of cryptocurrency is of a relative nature.

Keywords: right to a cryptocurrency unit, cryptocurrency, cryptoassets, property rights to cryptocurrencies, virtual currency, MiCA regulation
Słowa kluczowe: prawo do jednostki kryptowaluty, kryptowaluta, kryptoaktywo, prawo własności kryptowaluty, waluta wirtualna, rozporządzenie MiCA

Wprowadzenie

Obrót kryptowalutami w Polsce ma relatywnie długą tradycję. Pierwsze na świecie przeniesienie bitcoina miało miejsce w styczniu 2009 r., a już w 2011 r. powstała pierwsza polska giełda kryptowalut – Bitomat.pl. Na początku 2014 r. pojawiły się

© 2025 Przemysław Katner published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

też pierwsze polskie kryptowaluty, m.in. Polcoin (PLC), PolishCoin (PCC) i PLNcoin (PLNc) (Woźnicki, 2014). W 2014 r. jedna z polskich „kopalń" kryptowalut zajmowała piątą pozycję na świecie pod względem wartości mocy obliczeniowej (Ministerstwo Finansów, 2019, s. 131).

Rozwój rynku kryptowalut w Polsce odbywał się pomimo początkowego braku jakichkolwiek rozwiązań prawnych, które by się do nich wprost odnosiły. Podobnie jak i w innych państwach można było także zaobserwować ostrożne podejście do kryptowalut przez podmioty nadzorujące rynek finansowy. Przykładem w tej mierze może być komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego (2017) lub ostrzeżenie Urzędu KNF (2021)[1].

Choć obrót kryptowalutami jest w Polsce bez wątpienia dopuszczalny, w przypadku dotyczących ich zdarzeń cywilnoprawnych pojawia się wiele pytań, które wynikają w znacznej mierze z problemu z określeniem charakteru prawa podmiotowego do jednostek kryptowaluty. Jego rozwiązanie na gruncie prawa cywilnego staje się obecnie naglące, ponieważ – ze względu na szeroką dostępność kryptowalut w Polsce oraz coraz częstsze ich występowanie jako składników majątku (Łukasik, 2023, s. 6) – ma znaczenie nie tylko teoretyczne, ale również praktyczne. Ustalenie, czym jest kryptowaluta z punktu widzenia prawa prywatnego oraz czy – i jeśli tak, to jakie – przysługuje do niej prawo, jest kluczowe dla wskazania m.in. przepisów znajdujących zastosowanie do jej przeniesienia i do umowy zobowiązującej do dokonania takiej czynności rozporządzającej, zakresu uprawnień osób dysponujących jednostkami kryptowaluty oraz roszczeń służących ochronie tytułu do nich, a także do prawidłowego posługiwania się aparatem pojęciowym, np. czy możemy mówić o istnieniu „prawa" do jednostek kryptowaluty, w szczególności prawa własności, o ich „posiadaniu", „sprzedaży", „pożyczce" itp.

Z tego też względu celem niniejszego artykułu jest określenie charakteru prawa podmiotowego do jednostek kryptowalut w Polsce *de lege lata* i *de lege ferenda*. Nastąpi krytyczne przyjrzenie się występującym obecnie w polskiej doktrynie i orzecznictwie propozycjom i ich konsekwencjom na gruncie prawa prywatnego. Istotne uzupełnienie dyskusji będą stanowić – pomijane zazwyczaj w polskim piśmiennictwie – rozwiązania prawne proponowane lub obowiązujące w innych porządkach prawnych, a także prezentowana w tej mierze argumentacja. Artykuł oprze się na metodzie dogmatycznej, prawnoporównawczej oraz elementach analizy *de lege ferenda*.

1. Stanowiska dotyczące kwalifikacji prawa do jednostki kryptowaluty w polskim prawie cywilnym

W polskim piśmiennictwie panuje dotąd dość zgodne stanowisko, że kryptowaluty nie stanowią pieniądza w rozumieniu prawnym (m.in. Dybowski & Pyrzyń-

1 Odnośnie do rozwoju rynku kryptowalut w Polsce zob. szerzej P. Katner (2022, s. 159–162).

ska, 2019, s. 271; zob. jednak Dudek, 2016, s. 43 w związku z wyrokiem TSUE, 2015)[2] oraz nie są walutą (m.in. Grabowski, 2020, s. 291; NBP & KNF, 2017, s. 1). Zauważa się również, że nie są instrumentem finansowym (m.in. Kruszewski, 2017; NBP & KNF, 2017, s. 1), środkiem płatniczym (m.in. NBP & KNF 2017, s. 1; Zacharzewski, 2014, s. 1135), pieniądzem elektronicznym (m.in. Górniak, 2019, s. 567; NBP & KNF, 2017, s. 1)[3], nie podlegają też przepisom ustawy o usługach płatniczych (Zacharzewski, 2015, s. 194; Srokosz, 2015, s. 73, 79). Pewne zmiany w tym spojrzeniu są jednak konieczne w związku z obowiązywaniem od dnia 30 czerwca 2024 r. art. 48 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 (Parlament Europejski i Rada, 2023; dalej: Rozporządzenie MiCA), zgodnie z którym rodzaj kryptoaktywa, który ma utrzymywać stabilną wartość dzięki temu, że jest powiązany z jedną walutą urzędową, został uznany za pieniądz elektroniczny (zob. Michna, 2024)[4].

Choć w polskim prawie publicznym istnieje obecnie pewne ujęcie kryptowaluty (a właściwie waluty wirtualnej[5]) w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Sejm RP, 2018)[6], w doktrynie prawa cywilnego od początku istnienia kryptowalut nie było i nadal nie ma zgody, czym jest kryptowaluta, oraz – jeżeli w ogóle – jakie przysługuje do niej prawo. Uwagi sporej części autorów były odnoszone przy tym wprost lub pośrednio do bitcoina, stanowiącego jednak jedynie jeden z wielu typów kryptowalut (zob. Urząd KNF, 2020; Wnęk, 2023, s. 12–32). Można zatem wskazać, że K. Zacharzewski (2014, s. 1133) uznał kryptowalutę (bitcoina) za rodzaj mienia, niebędącego rzeczą, stanowiącego zbywalne względne prawo majątkowe, które nie może być w rozumieniu technicznoprawnym przedmiotem własności i może wchodzić do majątku osoby tylko jako wierzytelność. Z kolei K. Górniak (2019, s. 566–567) przyjął, że „kryptowaluty są dobrem (przedmiotem) niematerialnym, a jego dysponentom przysługuje bezwzględne prawo majątkowe do takiego dobra. Istnienie i treść prawa do waluty cyfrowej należy wyprowadzić z analogicznego stosowania do kryptowalut

2 Choć zasadne są stanowiska w doktrynie widzące w nich pieniądz w rozumieniu ekonomicznym (m.in. Michna, 2018, s. 7–13). Osobną kwestią jest ewentualna możliwość zastosowania do zobowiązań wyrażonych w kryptowalucie ogólnych przepisów normujących zobowiązania pieniężne; w tej mierze zob. m.in. F. Zoll (2023, s. 1144–1145); K. Zagrobelny (2022, s. 1674–1689); Ł. Mazur (2024, s. 213–214, 220–224).

3 W dokumencie Ostrzeżenie Urzędu KNF (2021, s. 7–8) wskazano jednak, że przy spełnieniu dodatkowych warunków tzw. *stable coins* mogą spełniać definicję pieniądza elektronicznego.

4 Szerzej odnośnie do Rozporządzenia MiCA zob. m.in. Hrabčák & Štrkolec (2024, s. 27–45).

5 Pojęcia te nie są synonimami. Każda kryptowaluta jest walutą wirtualną (choć i tu można spotkać inne stanowiska), ale nie odwrotnie. Artykuł posługuje się terminem waluty wirtualnej w sytuacji, gdy jest on użyty przez przytaczane źródło. Szerzej odnośnie do rozwiązań dotyczących kryptowalut w polskim prawie publicznym zob. P. Katner (2022, s. 162–172).

6 Do definicji tej odwołują się: ustawa o podatku dochodowym od osób fizycznych (Sejm RP, 1991) oraz o podatku dochodowym od osób prawnych (Sejm RP, 1992); zgodnie z obecnym brzmieniem projektu ustawy o rynku kryptoaktywów (Minister Finansów, 2024) po jej wejściu w życie definicja ta nadal będzie obowiązywać we wskazanych ustawach podatkowych.

przepisów o rzeczach, co prowadzi do wniosku, że kryptowaluty stanowią przedmiot prawa własności (art. 140 k.c. *per analogiam*)"[7]. M. Michna (2018, s. 45–46) uznaje, że „bitcoin stanowi jedynie przedmiot świadczenia w stosunku zobowiązaniowym – jest więc samoistnym (samodzielnym) przedmiotem świadczenia". J. Szewczyk (2018, s. 247) podnosi, że bitcoin nie stanowi składnika mienia (w rozumieniu art. 44 k.c.), natomiast dysponowanie określonym adresem publicznym, jak również kluczem prywatnym, pozwalającym na posługiwanie się bitcoinem, niewątpliwie stanowi korzystną sytuację faktyczną o wymiernej wartości majątkowej i może być uznane za składnik mienia. W. Srokosz (2017) przyjął, że jak na razie legalna definicja kryptowalut nie jest co do zasady potrzebna w obszarze regulacji cywilnoprawnej. Prawo cywilne, dzięki rozbudowanym narzędziom wykładni i zasadzie swobody umów powiązanej z zasadą równorzędności (równości) stron w stosunku cywilnoprawnym, radzi sobie z technologicznymi nowinkami, w tym z technologią blockchainu. Natomiast T. Dybowski i A. Pyrzyńska (2019, s. 271) uznali, że ze względu na funkcję, jaką w obrocie prawnym pełni pieniądz, w systemie prawa prywatnego należy posługiwać się definicją kryptowalut (walut wirtualnych) przyjętą w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z 2018 r., implementującej m.in. dyrektywę AML V (Parlament Europejski i Rada, 2018).

Przyjęcie określonego rozwiązania ma oczywiście daleko idące konsekwencje. Tytułem przykładu, K. Górniak opowiadający się za analogicznym stosowaniem do kryptowalut przepisów o rzeczach (art. 45 k.c.) i uznający je w drodze analogii za przedmiot prawa własności przyjmuje, że prawo własności kryptowalut jest prawem majątkowym, zbywalnym, bezwzględnym (skutecznym *erga omnes*). Kryptowaluty mogą być też przedmiotem faktycznego władztwa, a więc – przez analogię – posiadania (2019, s. 586–614). W tym ujęciu przeniesienie prawa własności kryptowaluty następuje co do zasady na podstawie przepisów o przeniesieniu własności rzeczy oznaczonych co do gatunku (art. 155 § 2 k.c. i wyjątkowo art. 155 § 1 k.c. w przypadku kryptowalut indywidualnie oznaczonych), przy czym odpowiednikiem wymagania przeniesienia posiadania jest zarejestrowanie zmiany dysponenta w ramach rozproszonej księgi transakcji funkcjonujących w ramach blockchaina i przypisanie jednostek kryptowaluty do adresu skojarzonego z kluczem publicznym nabywcy. W przypadku wykopania kryptowalut prawo własności do nich jest nabywane pierwotnie, można je też nabyć od osoby nieuprawnionej w przypadkach, gdy to możliwe względem rzeczy ruchomej, a także w drodze zasiedzenia. Uprawnionemu w zależności od sytuacji przysługiwałaby teoretycznie ochrona petytoryjna, względnie roszczenie posesoryjne. Większe znaczenie miałaby jednak ochrona na podstawie przepisów o czynach niedozwolonych oraz o bezpodstawnym wzbogaceniu. Egze-

7 Podobnie P. Machnikowski (2020, s. 30) przyjmuje, że do kryptowalut należy podchodzić podobnie jak w przypadku energii, co daje możliwość stosowania do nich przepisów o własności z niezbędnymi modyfikacjami; zob. też A. Weber-Elżanowska (2021, s. 586).

kucja ze świadczenia opiewającego na jednostki waluty cyfrowej – z przyczyn technologicznych, uniemożliwiających odebranie kryptowaluty – musiałaby natomiast nastąpić w trybie właściwym dla świadczeń niepieniężnych polegających na czynnościach, których inna osoba nie może wykonać za dłużnika i których wykonanie zależy wyłącznie od jego woli (Górniak, 2019, s. 614–642).

Z kolei K. Zacharzewski, proponujący uznanie bitcoina za wierzytelność, wskazuje, że jest on zbywalnym względnym prawem majątkowym, którym rozporządzenie jest dokonywane w drodze przelewu na podstawie art. 510 § 1 k.c. oraz dodatkowego aktu przewłaszczenia poprzez użycie klucza prywatnego. Zobowiązanie do zbycia bitcoina może wynikać z umowy sprzedaży (której przedmiotem świadczenia zgodnie z art. 555 k.c. mogą być prawa) lub zamiany (w sytuacji, gdy w zamian za bitcoina ma nastąpić przeniesienie mienia), przy której odpowiednio są stosowane przepisy o umowie sprzedaży. Na skutek szerokiej analogii z art. 140 k.c. kryptowaluta daje uprawnionemu prawo do korzystania z niej oraz do rozporządzania. Autor przyjmuje, że przeniesienie tytułu do bitcoina nie jest przeniesieniem posiadania, choć władztwo faktyczne można wykonywać względem klucza prywatnego, zaś prawo podmiotowe osoby utytułowanej w tym zakresie ma charakter wyłączny. Zakaz naruszeń klucza prywatnego ma charakter powszechny (*erga omnes*). W przypadku naruszenia wierzytelności nie przysługuje ochrona windykacyjna, choć jest ona dopuszczalna w razie utraty klucza prywatnego do momentu jego użycia (Zacharzewski, 2014, s. 1132–1139). Bitcoiny mogą być przedmiotem pożyczki, można też umówić się co do jej oprocentowania w bitcoinach. Będą one również mogły stanowić składnik majątku wspólnego lub osobistego małżonków, stanowiąc w tym pierwszym przypadku przedmiot jego podziału w razie rozwodu. Bitcoiny wchodzą także do spadku (Zacharzewski, 2015, s. 187–191).

Natomiast autorzy uznający kryptowaluty za samoistny, niematerialny przedmiot świadczenia w stosunku zobowiązaniowym wskazują, że w relacji do kryptowalut nie istnieje prawo podmiotowe (ani bezwzględne, ani względne). Samo przeniesienie kryptowaluty stanowi zazwyczaj czynność czysto faktyczną z wykorzystaniem klucza prywatnego, względnie np. związaną z przegraniem tego klucza na nośnik należący do nowego podmiotu lub przeniesieniem na inny podmiot własności nośnika fizycznego, na którym znajduje się klucz prywatny. Umowa, w której jedna ze stron w zamian za przeniesienie własności rzeczy lub praw zobowiązuje się do przeniesienia kryptowaluty, nie stanowi umowy sprzedaży (przedmiotem świadczenia nie jest rzecz lub prawo), ale jest to umowa nienazwana, której cel ekonomiczny jest jednak bardzo zbliżony do celu umowy sprzedaży. Dlatego przez analogię *legis* powinno się tu odpowiednio stosować przepisy o sprzedaży. Jeżeli zapłata w kryptowalucie byłaby dokonywana w zamian za usługę, zastosowanie znajdowałby art. 750 k.c. nakazujący odpowiednie stosowanie przepisów o umowie zlecenia. Można też wprost stosować przepisy o umowie najmu (w której czynsz będzie określony w kryptowalucie) oraz dotyczące darowizny w sytuacji nieodpłatnego przeniesienia na inną osobę jednostek

kryptowaluty W przypadku pożyczenia jednostek kryptowaluty nie będziemy mieć do czynienia z umową pożyczki (ze względu na jej przedmiot wskazany w art. 720 k.c. definiującym tę umowę), ale *per analogiam* będziemy stosować przepisy o umowie pożyczki (Michna, 2018, s. 75–82).

Na tym tle ciekawie wygląda sytuacja w orzecznictwie. W tym przypadku sądy zdają się wychodzić z założenia, że w odniesieniu do kryptowaluty mamy do czynienia z odnoszącym się do niej podmiotowym prawem majątkowym, bez określania jego charakteru, które stanowi składnik mienia, a także może być przedmiotem obrotu. Tytułem przykładu, w wyroku z dnia 10 lutego 2021 r. Naczelny Sąd Administracyjny wskazał, że „wymiana kryptowalut, czyli jednego niematerialnego prawa majątkowego na inne tego rodzaju prawo, stanowi umowę zamiany w rozumieniu art. 603 w zw. z art. 555 ustawy z 23 kwietnia 1964 r. Kodeks cywilny" (wyrok NSA, 2021). Stanowisko takie zajął także Naczelny Sąd Administracyjny w wyroku z dnia 27 kwietnia 2022 r. (wyrok NSA, 2022). Kierując się tym założeniem, sądy dokonują też np. podziału majątku wspólnego małżonków, uwzględniając jednostki kryptowaluty.

Na zakończenie powyższych uwag warto zauważyć, że Rada Ministrów pracuje nad projektem ustawy o rynku kryptoaktywów (Minister Finansów, 2024)[8], która pierwotnie miała wejść w życie, z zastrzeżeniem wyjątków, z dniem 30 czerwca 2024 r. Ma ona w szczególności na celu zapewnienie stosowania Rozporządzenia MiCA. Zgodnie z projektowanym art. 1 ustawy, jej przedmiotem mają być szczegółowe zasady prowadzenia działalności w zakresie kryptoaktywów, zasady odpowiedzialności cywilnej w związku z dokumentem informacyjnym dotyczącym kryptoaktywa oraz zmienionym dokumentem informacyjnym dotyczącym kryptoaktywa, a także organizacja i wykonywanie nadzoru nad rynkiem kryptoaktywów. Niestety, projekt ustawy – pierwotnie nazwanej ustawą o kryptoaktywach – w żaden sposób nie odnosi się jednak do problemu kwalifikacji prywatnoprawnej kryptowalut. Z tego też względu – niezależnie od tego, kiedy wpłynie on pod obrady Sejmu, zaś ustawa zostanie uchwalona – w obecnym kształcie nie ma wpływu na prowadzone rozważania.

2. Uwagi prawnoporównawcze

2.1. Prawo Unii Europejskiej

Problem kwalifikacji prywatnoprawnej kryptowalut oraz prawa przysługującego do ich jednostek nie stał się przedmiotem przyjętego niedawno Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Parlament Europejski

8 Pierwszy projekt ustawy nosił datę 22 lutego 2024 r.

i Rada, 2023)[9], które nie zawiera nawet ujęcia kryptowalut, będących najbardziej znaną postacią kryptoaktywów[10]. Wskazuje jedynie w art. 3 ust. 1 pkt 5, że to ostatnie pojęcie oznacza cyfrowe odzwierciedlenie wartości lub prawa, które da się przenosić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii. Warto jednak zauważyć, że zgodnie z art. 48 ust. 2 w zw. z art. 3 ust. 1 pkt 7 rozporządzenia rodzaj kryptoaktywa, który ma utrzymywać stabilną wartość dzięki temu, że jest powiązany z jedną walutą urzędową, został uznany za pieniądz elektroniczny i jest określany w treści rozporządzenia jako token będący pieniądzem elektronicznym lub token będący e-pieniądzem.

Problemu prywatnoprawnego ujęcia kryptowalut nie rozwiązała także wcześniej wydana dyrektywa (UE) 2015/849 (Parlament Europejski i Rada, 2015), która – w wyniku jej nowelizacji tzw. dyrektywą AML V (Parlament Europejski i Rada, 2018) – do dnia 29 grudnia 2024 r. definiowała waluty wirtualne. Zgodnie z art. 3 pkt 18 tej dyrektywy oznaczały one cyfrowe wyznaczniki wartości, które nie są emitowane ani gwarantowane przez bank centralny lub organ publiczny, nie muszą być powiązane z walutą prawnie obowiązującą i nie posiadają prawnego statusu waluty lub pieniądza, lecz są akceptowane przez osoby fizyczne lub prawne jako środek wymiany i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną[11]. Od dnia 30 grudnia 2024 r. pojęcie walut wirtualnych zostało natomiast w tej dyrektywie zastąpione pojęciem kryptoaktywa, zasadniczo zgodnego z definicją w Rozporządzeniu MiCA.

2.2. Podejście do kryptowalut w prawie chińskim

W związku z tym, że Chiny przyjęły w 2020 roku nowy Kodeks cywilny (Narodowy Kongres Ludowy, 2020), można byłoby się spodziewać, że kwestie dotyczące kryptowalut powinny zostać w nim unormowane. Niemniej jednak prawo chińskie nadal nie podaje konkretnej definicji kryptowalut, a doktryna nie jest w tej mierze zgodna. Najważniejsze obwieszczenia i komunikaty dotyczące kryptowalut wydane przez rząd chiński nie definiują szczegółowo ani walut wirtualnych, ani kryptowalut, ale raczej odwołują się do ich określonych rodzajów jako przykładów. W niektórych przypadkach wskazują one także tylko pewne cechy walut wirtualnych (zob. Ludowy Bank Chin et al., 2021).

---

9 Zgodnie z art. 1 ust. 1 Rozporządzenia MiCA ustanawia ono jednolite wymagania dotyczące oferty publicznej i dopuszczania do obrotu na platformie obrotu określonymi kryptoaktywami oraz wymagania w odniesieniu do dostawców usług w zakresie kryptoaktywów.

10 Odnośnie do wyróżnionych przez Rozporządzenie MiCA rodzajów kryptoaktywów zob. Hrabčák & Štrkolec (2024, s. 34–35).

11 Ujęcie to w zmodyfikowanej postaci zostało przyjęte przez ustawę o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Sejm RP, 2018). Po zmianie w tym zakresie tej ustawy – w razie przyjęcia projektu ustawy o rynku kryptowalut (Minister Finansów, 2024) – postać ta będzie nadal obowiązywać w ustawie o podatku dochodowym od osób fizycznych (Sejm RP, 1991) i osób prawnych (Sejm RP, 1992).

Z punktu widzenia prawa cywilnego warto zauważyć, że Bitcoin został określony w Obwieszczeniu w sprawie zapobiegania niebezpieczeństwu związanemu z Bitcoinem wydanym przez Ludowy Bank Chin, Ministerstwo Przemysłu i Technologii Informacyjnych, Komisję ds. Regulacji Bankowości, Komisję ds. Regulacji Papierów Wartościowych i Komisję ds. Regulacji Ubezpieczeń w grudniu 2013 roku jako swoisty towar wirtualny (XXIst International Congress of Comparative Law, 2022, s. 17–19; Hu, 2024, s. 57–58). Z tego powodu, na gruncie chińskiego kodeksu cywilnego kryptowaluty powinny być uznane za sieciowe mienie wirtualne, konstrukcję wprowadzoną do kodeksu w art. 127 (zob. też Hu, 2024, s. 59). Kodeks nie precyzuje jednak jej natury. W doktrynie charakter sieciowego mienia wirtualnego budzi natomiast kontrowersje, zaś poglądy wahają się od teorii prawa rzeczowego, zgodnie z którą uprawniony dysponuje prawem rzeczowym do sieciowego mienia wirtualnego, do teorii wierzytelności, która przyznaje uprawnionemu wierzytelność wobec emitenta aktywa wirtualnego online. Wyrażane jest też stanowisko, że w sytuacji, gdy sieciowe mienie wirtualne jest emitowane przez scentralizowanego zarządcę i uprawniony nie może z niego korzystać lub nim rozporządzać bez współpracy z emitentem, teoria wierzytelności jest bardziej odpowiednia. Nie może jednak mieć zastosowania w przypadku, gdy brak jest emitenta, co ma miejsce w przypadku wielu kryptowalut (XXIst International Congress of Comparative Law, 2022, s. 7; zob. też Hu, 2024, s. 67–69).

Obecnie kwestia charakteru prawa do jednostek kryptowaluty wydaje się jednak mieć w Chinach drugorzędne znaczenie. Dzieje się tak, ponieważ rząd chiński poczynił wiele kroków ograniczających obrót kryptowalutami – takich jak zamknięcie platform umożliwiających wymianę kryptowalut i ograniczenie wydobycia kryptowalut – poprzez wspólne wydawanie przez organy administracji aktów resortowych w postaci obwieszczeń lub komunikatów (Norton Rose Fulbright, 2017). Wreszcie w obwieszczeniu z 2021 r. (Ludowy Bank Chin et al., 2021) wskazano, że „Działalność związana z walutami wirtualnymi stanowi nielegalną działalność finansową" oraz „W przypadku, gdy jakakolwiek osoba prawna, jednostka organizacyjna nieposiadająca osobowości prawnej lub osoba fizyczna narusza porządek publiczny i dobre obyczaje, inwestując w waluty wirtualne lub powiązane z nimi instrumenty pochodne, związana z tym czynność prawna jest nieważna, zaś wynikające stąd straty podmiot taki ponosi samodzielnie". Obwieszczenie to nie jest wprawdzie wydane przez ustawodawcę i w teorii nie ma mocy, by unieważnić czynności prawne dotyczące kryptowalut – ponieważ stanowi jedynie akt resortowy – niemniej jednak zgodnie z art. 153 § 2 chińskiego Kodeksu cywilnego: „Czynność prawna godząca w porządek publiczny i dobre obyczaje jest nieważna". Natomiast w 2019 r. Sąd Najwyższy wskazał w protokole z Konferencji sądów krajowych poświęconej postępowaniom sądowym w sprawach cywilnych i handlowych, że naruszenie aktów resortowych nie wpływa na ważność umów jako takich, ale jeżeli akty takie dotyczą porządku publicznego i dobrych obyczajów, np. bezpieczeństwa finansowego, porządku na rynku lub krajowej polityki makroekonomicznej, umowy powinny zostać uznane za nie-

ważne (XXIst International Congress of Comparative Law, 2022, s. 8). W rezultacie, w zdecydowanej większości spraw rozpoznawanych przez sądy czynności prawne dotyczące kryptowalut (np. umowy sprzedaży, umowy zlecenia inwestycji) są uznawane za nieważne (XXIst International Congress of Comparative Law, 2022, s. 8–14; i wskazane tam rozstrzygnięcia sądów chińskich).

2.3. Kryptowaluty w niemieckim prawie prywatnym

W prawie niemieckim brak jest spójnych ram prawnych służących kwalifikacji kryptowalut, a także kompleksowych rozwiązań dotyczących ich traktowania w prawie prywatnym, np. w prawie umów, prawie rzeczowym, spadkowym, postępowaniu cywilnym. Wprawdzie implementacja dyrektywy AML V w 2019 r. doprowadziła do wyróżnienia kryptoaktywów w niemieckim Prawie bankowym (Bundestag, 1961; dalej: KWG), gdzie są one obecnie zdefiniowane w § 1 ust. 11 zdaniu czwartym i piątym KWG i na podstawie § 1 ust. 11 zdanie 1 pkt 10 KWG, dla celów tej ustawy zostały w sposób wyraźny uznane za instrumenty finansowe. Niemniej jednak KWG nie odróżnia kryptowalut od innych rodzajów kryptoaktywów. Ujęcie kryptoaktywów w KWG jest także mało przydatne dla wskazania podejścia do kryptowalut w niemieckim prawie prywatnym, ponieważ nie pomaga w wyjaśnieniu ich usytuowania wśród tradycyjnych kategorii prawa prywatnego. Stąd też, w obliczu braku szczególnej regulacji[12], rozwiązywanie problemów dotyczących kryptowalut następuje w oparciu o stosowanie zasad ogólnych. Można przy tym zaobserwować rosnącą liczbę rozstrzygnięć sądowych odnoszących się do walut wirtualnych, niemniej jednak – jak dotąd – ograniczają się one do orzeczeń sądów niższych instancji, co pozostawia znaczny stopień niepewności prawnej (Binder, 2022, s. 2).

Podobnie jak w innych państwach członkowskich strefy euro, kryptowaluty nie są uznawane w Niemczech za prawny środek płatniczy. Wynika to z art. 128 ust. 1 zd. 3 Traktatu o funkcjonowaniu Unii Europejskiej. Większość przedstawicieli doktryny uważa także, że nie można zakwalifikować kryptowalut jako pieniędzy lub waluty (zob. m.in. Omlor, 2019, s. 307–308). W konsekwencji, skoro nie uznaje się ich za prawny środek płatniczy, to – przynajmniej bez modyfikacji – nie można do nich stosować zasad prawa cywilnego dotyczących zobowiązań pieniężnych (m.in. Grundmann, 2019, pkt 13–24).

W doktrynie niemieckiej dość jednolicie reprezentowany jest także pogląd, zgodnie z którym kryptowaluty co do zasady nie mogą być uznane za wierzytelności (niem. *Forderungen*) ze względu na to, że nie odzwierciedlają stosunków dwustron-

12 Ponieważ definicja produktów cyfrowych (obejmująca treści cyfrowe i usługi cyfrowe) znajdująca się w § 327 ust. 2 niemieckiego Kodeksu cywilnego (Reichstag, 1896; dalej: BGB) nie obejmuje kryptowalut, nie dotyczą ich także § 327–327u oraz § 475a BGB. Można wprawdzie zauważyć, że zgodnie z § 327 ust. 1 zd. 2 BGB cyfrowe odwzorowanie wartości może na podstawie umowy stanowić cenę, jaką należy zapłacić za produkty cyfrowe. Stwierdzenie to nie pomaga jednak przy klasyfikacji jednostek kryptowaluty dla celów prawa rzeczowego lub prawa umów.

nych, w ramach których wierzyciel dysponuje skutecznym względem dłużnika prawem żądania spełnienia świadczenia (m.in. Skauradszun, 2021, s. 365–366). Toczy się natomiast dyskusja, czy mogą być kwalifikowane jako wierzytelności takie kryptowaluty, które są emitowane przez centralnego emitenta (np. Libra) (Langenbucher et al., 2020, s. 791).

Niektórzy autorzy proponują, by kryptoaktywa zakwalifikować jako rzeczy (przedmioty materialne, niem. *Sachen*), co wyjaśniłoby tytuł prawny do takich aktywów oraz ułatwiło stosowanie do nich zasad prawnych dotyczących obrotu rzeczami (m.in. John, 2020, s. 76; Walter, 2019, s. 3613, opowiada się za stosowaniem zasad odnoszących się do dóbr materialnych *per analogiam*). Takie rozwiązanie jest jednak odrzucane przez większość przedstawicieli doktryny ze względu na brzmienie oraz tradycyjną wykładnię definicji rzeczy znajdującej się w § 90 BGB, zgodnie z którą jako rzeczy kwalifikowane są tylko przedmioty materialne (fizyczne) (zob. m.in. Langenbucher et al., 2020, s. 790; Skauradszun, 2021, s. 361–363; Spindler & Bille, 2014, s. 1359). Tokeny kryptowalut nie są także uznawane za przedmioty prawa własności intelektualnej w rozumieniu niemieckiej ustawy o prawie autorskim i prawach pokrewnych (zob. m.in. Beck & König, 2015, s. 131; Kütük & Sorge, 2014, s. 644; Schlund & Pongratz, 2018, s. 600). Stąd też większość autorów kwalifikuje kryptowalutę jako inne prawo majątkowe (zob. m.in. Langenbucher, 2018, s. 407; Schlund & Pongratz, 2018, s. 600; Skauradszun, 2021, s. 468–69; Spindler & Bille, 2014, s. 1360), chociaż są i tacy, którzy kwestionują takie rozwiązanie (zob. m.in. Kütük & Sorge, 2014, s. 644; Paulus & Matzke, 2018, s. 451; Rückert, 2016, s. 296).

Przyjęcie takiego stanowiska nie usuwa jednak problemów z kwalifikacją czynności prawnych dotyczących kryptowalut w prawie rzeczowym i prawie umów. W rezultacie sposób ich traktowania w prawie rzeczowym w ogólności, a szczególnie kwalifikacji prawnej przeniesienia tytułu do nich (jako przeniesienia własności, przelewu, jednego z powyższych *per analogiam*, faktycznego przeniesienia tytułu prawnego na skutek działania stron [niem. *Realakt*]), pozostaje dotychczas w znacznej mierze nierozstrzygnięty (Binder, 2022, s. 27–30). W prawie umów sytuacja wygląda lepiej, między innymi ze względu na dość pojemną treść § 453 ust. 1 zd. 1 i § 480 BGB, które umożliwiają odpowiednie stosowanie przepisów normujących umowę sprzedaży np. do nabycia kryptowaluty w zamian za zapłatę dokonaną prawnym środkiem płatniczym lub wymiany jednej kryptowaluty na inną. Budzi już jednak wątpliwości, czy można zastosować do kryptowalut np. przepisy dotyczące umowy pożyczki pieniężnej (§ 488-490 BGB) lub umowy pożyczenia rzeczy (§ 607-609 BGB) (Binder, 2022, s. 23–24).

2.4. Prawo do jednostek kryptowaluty w prawie brytyjskim

W prawie brytyjskim brak jest ogólnej definicji legalnej kryptowalut. Zazwyczaj określa się je jako tokeny wymienialne lub krypto-tokeny stanowiące jeden z rodzajów kryptoaktywów (Urząd Podatkowy i Celny Jej Królewskiej Mości, 2023; Komisja ds. Prawa, 2023; 2024). Natomiast termin „kryptoaktywo" został zdefiniowany dla

celów ustawy w sprawie prania pieniędzy, finansowania terroryzmu i transferu środków pieniężnych (informacji o płatniku) z 2017 r. w jej art. 14A ust. 3 lit. a w związku z implementacją dyrektywy AML V. Definicja wskazuje, że „kryptoaktywo oznacza kryptograficznie zabezpieczoną cyfrową reprezentację wartości lub praw wynikających z umowy, która korzysta z technologii rozproszonego rejestru i może być przenoszona, przechowywana lub zbywana elektronicznie" (Izba Gmin, 2017). W 2023 r. wprowadzono też nową, szerszą definicję kryptoaktywów w art. 417 ustawy o usługach i rynkach finansowych z 2000 r., która nie wymaga korzystania z technologii rozproszonego rejestru (Izba Gmin, 2000). Kryptoaktywa – a zatem także i kryptowaluty – nie są jednak uznawane w Wielkiej Brytanii za prawny środek płatniczy, pieniądz lub walutę (zob. m.in. Held et al., 2022, pkt 1.1–1.3; Skarb Państwa et al., 2018, s. 12; Bank Anglii & Skarb Państwa, 2023, s. 21–23).

Jeśli chodzi o prawo prywatne, to nie ma – póki co – ani kompleksowej ustawy dotyczącej majątkowych aspektów kryptoaktywów, ani autorytatywnej decyzji Sądu Najwyższego Zjednoczonego Królestwa w sprawie znajdujących do nich zastosowanie zasad ogólnych. Przez długi okres można było spotkać jedynie różne rozstrzygnięcia sądów pierwszej instancji oparte na założeniu, że kryptowaluty stanowią „przedmiot własności", wydane na potrzeby rozpoznania wniosków tymczasowych dotyczących jurysdykcji, udzielania zabezpieczeń i wydania nakazów dotyczących majątku. Nie stanowią one jednak ani wiążących precedensów, ani stanowisk przekonujących siłą autorytetu (Held et al., 2022, pkt 4.1.1). Dopiero w 2023 r. w sprawie Tulip Trading v. Van Der Laan Sąd Apelacyjny przyjął szerszą zasadę, zgodnie z którą „kryptoaktywo takie jak bitcoin stanowi przedmiot własności" w prawie Anglii i Walii (Wyrok Sądu Apelacyjnego, 2023; zob. też Komisja ds. Prawa, 2023, s. 44; 2024, s. 7).

Zauważa się jednak, że kryptowaluty nie można w prosty sposób zakwalifikować do żadnej z tradycyjnie wyróżnianych kategorii praw majątkowych skutecznych względem osób trzecich. W tej mierze raport *Digital Assets: Final report* przygotowany przez Komisję ds. Prawa – opublikowany w czerwcu 2023 r. – wskazuje, że „od momentu wydania wyroku w sprawie AA v. Persons Unknown w 2019 r. sądy w co najmniej 14 z 24 spraw, w tym Sąd Apelacyjny, przytaczały to orzeczenie na poparcie stanowiska, że rozważane aktywo cyfrowe stanowi przedmiot, którego mogą dotyczyć prawa majątkowe o charakterze bezwzględnym odnoszące się do przedmiotów nie będących nieruchomością [*personal property rights* – PK]. W sprawie AA v. Persons Unknown sędzia Bryan stwierdził, że „błędne" byłoby postępowanie oparte na założeniu, że prawo Anglii i Walii uznaje jedynie podział na ruchomości [*things in possession* – PK] oraz prawa przysługujące na podstawie obowiązujących przepisów i wierzytelności zaskarżalne [*things in action* – PK]. Wyraźnie dostrzegł trudność w kwalifikacji krypto-tokenów, które na pierwszy rzut oka nie są ani jednym, ani drugim. Cytując pełne uzasadnienie w tej kwestii Stanowiska Prawnego Zespołu

Zjednoczonego Królestwa ds. Jurysdykcji[13], stwierdził, że krypto-token może stanowić przedmiot praw majątkowych skutecznych względem osób trzecich dotyczących przedmiotów, które nie są nieruchomością [*personal property rights* – PK], nawet jeżeli nie jest prawem przysługującym na podstawie obowiązujących przepisów lub wierzytelnością zaskarżalną w wąskim znaczeniu.

Biorąc to pod uwagę, orzecznictwo wskazuje, że sądy w Anglii i Walii wyróżniają obecnie krypto-tokeny jako odrębne przedmioty, które mogą stanowić przedmiot praw majątkowych skutecznych względem osób trzecich dotyczących przedmiotów innych niż nieruchomości. Idąc dalej, poprzez konsekwentne stosowanie rozwiązania przyjętego w sprawie AA v. Persons Unknown […] sądy rozmyślnie postępowały w sposób, który wyodrębnił trzecią opartą na orzecznictwie kategorię przedmiotów innych niż nieruchomości, do której mogą odnosić się prawa majątkowe skuteczne względem osób trzecich" (Komisja ds. Prawa, 2023, s. 45–46).

Oprócz powyższego, raport stwierdza, że „pogląd, że krypto-tokeny mogą być przedmiotami lub rzeczami samymi w sobie (i najlepiej można je opisać w ten sposób) jest obecnie szeroko rozpowszechniony w komentarzach prawnych i akademickich tak dalece, że jest standardowo prezentowany w autorytatywnych tekstach i podręcznikach praktyków" (Komisja ds. Prawa, 2023, s. 45, przypis 170 z zamieszczonym tam piśmiennictwem). W konkluzji zaleca jednak potwierdzenie przez ustawę, że taki przedmiot jak krypto-token (np. bitcoin) nie zostanie pozbawiony statusu przedmiotu praw majątkowych skutecznych względem osób trzecich dotyczących przedmiotów innych niż nieruchomości tylko z tego powodu, iż nie jest ani ruchomością, ani prawem przysługującym na podstawie obowiązujących przepisów lub wierzytelnością zaskarżalną. Podaje też wiele przykładów na to, w jaki sposób takie ustawowe potwierdzenie zwiększy pewność prawa i pozwoli na jego rozwój w oparciu o mocną i jasną podstawę. Autorzy raportu nie widzą natomiast potrzeby ustawowego definiowania sztywnych przesłanek, jakie muszą spełniać przedmioty należące do takiej trzeciej kategorii przedmiotów (niekoniecznie cyfrowych, np. wskazują tu kwoty mleczne), ponieważ prawo zwyczajowe jest lepszym narzędziem dla ich uznania jako przedmiotów praw majątkowych skutecznych względem osób trzecich (Komisja ds. Prawa, 2023, s. 19, 53–55).

Następstwem raportu było opublikowanie w lutym 2024 r. przez Komisję ds. Prawa dokumentu *Digital assets as personal property. Short consultation on draft clauses*. Potwierdza on stanowisko zajęte w raporcie *Digital Assets: Final report* oraz zawiera krótki projekt ustawy dotyczącej prawa angielskiego i walijskiego – służącej potwierdzeniu, że przedmiot (rzecz) może być przedmiotem praw majątkowych skutecznych względem osób trzecich, nie będąc ani ruchomością, ani prawem przysługującym na podstawie obowiązujących przepisów lub wierzytelnością zaskarżalną

13 Dotyczy to stanowiska Zespołu Zjednoczonego Królestwa ds. Jurysdykcji (2019).

– i kieruje go do konsultacji przed przekazaniem rządowi w celu podjęcia decyzji co do potrzeby wdrożenia (Komisja ds. Prawa, 2024)[14].

Wnioski

Poczynione uwagi dotyczące rozwiązań przyjmowanych w dość różnych porządkach prawnych potwierdzają, że występujący w Polsce problem z kwalifikacją prawa do kryptowaluty w prawie prywatnym ma charakter powszechny. Nie budzi przy tym zastrzeżeń sama potrzeba ochrony tytułu do uzyskanych jednostek kryptowaluty prawem podmiotowym, wątpliwości dotyczą natomiast tego, czy chroniące prawo ma charakter względny, bezwzględny (i jeżeli, to na jakiej podstawie), czy też zależy to od właściwości konkretnej kryptowaluty. Wątpliwości te są zrozumiałe, mając na uwadze różne rodzaje kryptowalut, w tym emitowane przez określony podmiot, bez współpracy z którym uprawniony nie może z nich korzystać lub nimi rozporządzać, a także przyjmowany w poszczególnych porządkach prawnych różny katalog przedmiotów praw skutecznych względem osób trzecich.

Spoglądając na proponowane w polskiej doktrynie rozwiązania dotyczące prawa do jednostek kryptowaluty, jest raczej wątpliwe – ze względu na to, czym w istocie są kryptowaluty (choć i w tym zakresie istnieją różne podejścia) – by *de lege lata* można było je uznać za przedmiot prawa własności[15]. Sytuacja jest podobna, jak w prawie niemieckim. Z pewnością rozwiązywałoby to niektóre problemy jurydyczne, mając pewien wymiar praktyczny, niemniej jednak brzmienie art. 45 k.c. definiującego rzecz oraz art. 140 k.c. odnośnie do przedmiotu prawa własności jest dość jednoznaczne. Co najwyżej można przychylić się do zastosowania do prawa do jednostek kryptowaluty samego art. 140 k.c. *per analogiam* w zakresie, w jakim wskazuje on treść prawa własności. Warto w tym miejscu przypomnieć, że nawet w przypadku prawa angielskiego i walijskiego – pomimo odmiennego sposobu normowania prawa rzeczowego, orzecznictwa zmierzającego w stronę umożliwienia kwalifikacji prawa do kryptowaluty jako skutecznego względem osób trzecich oraz braku przeszkód natury ustawowej – za celowe uznano rozstrzygnięcie wątpliwości w tej mierze w drodze ustawy i przygotowano odpowiedni projekt. Tym bardziej takie działanie powinno mieć zatem miejsce w takim porządku prawnym, jak polski, w którym przyjmuje się zamknięty katalog praw bezwzględnych i wobec tego taka przeszkoda występuje. Byłoby ono jednocześnie jak najbardziej celowe, biorąc pod uwagę możliwą do zaob-

14 Odnośnie do różnych stanowisk dotyczących prawa do kryptowaluty w prawie szkockim zob. m.in. (Held et al., 2022, pkt 4.1.2.; MacPherson & Ripley, 2022; Fox, 2021).

15 Można natomiast rozważyć na gruncie prawa własności intelektualnej, jakie znaczenia dla stawianego problemu ma okoliczność, że dana kryptowaluta (a zatem i jej poszczególne jednostki) powstaje w wyniku z góry założonego działania programu komputerowego stworzonego przez człowieka (programistę).

serwowania w świetle poczynionych uwag prawnoporównawczych przychylność do chronienia jednostek przynajmniej niektórych kryptowalut prawem bezwzględnym. Należałoby jednak od razu wskazać właściwości, które kryptowaluta musiałaby spełniać, by jej jednostki stanowiły przedmiot prawa bezwzględnego, a także rozważyć, czy – zgodnie z rysującą się tendencją, znajdującą odzwierciedlenie choćby w Rozporządzeniu MiCA – przyjęte rozwiązanie nie powinno odnosić się także do innych rodzajów kryptoaktywów, a nawet szerzej – aktywów cyfrowych.

Nie należy jednocześnie mylić kryptowaluty z materialnym nośnikiem zawierającym klucz prywatny umożliwiający dysponowanie nią, co zdają się czynić niektórzy autorzy, oraz z samym kluczem prywatnym. Materialnych nośników zawierających ten sam klucz (jego kopie) może być zresztą wiele, jak również nośnik taki może w ogóle nie istnieć.

Jeżeli zatem przyjmiemy za orzecznictwem, że w polskim prawie w odniesieniu do jednostek kryptowaluty mamy do czynienia z prawem majątkowym, to – w przypadku odrzucenia *de lege lata* koncepcji prawa skutecznego *erga omnes* – pozostanie nam przyjęcie istnienia prawa względnego. To nie jest jednolita kategoria. Stanowisko uznające prawo do jednostki kryptowaluty za względne nie znajduje wprawdzie w doktrynie szerszej aprobaty, m.in. ze względu na problemy ze wskazaniem osoby dłużnika. W tej mierze można jednak zauważyć, że z jednej strony problem z ustaleniem konkretnej osoby dłużnika nie neguje istnienia prawa względnego (choć oczywiście utrudnia jego dochodzenie), z drugiej – istnieją różne kryptowaluty, stąd w przypadku niektórych można bez problemu dostrzec istnienie wierzytelności względem osoby (osób) wydającej daną kryptowalutę lub zarządzającej nią. Nie powinno budzić także zastrzeżeń istnienie wierzytelności wobec podmiotów będących uczestnikami systemu danej kryptowaluty (w szczególności zarządzających jego węzłami i mających wpływ na jego działanie), której przedmiotem jest znoszenie istnienia danego adresu (klucza) publicznego, powiązania z nim jednostek kryptowaluty wynikającego z rejestru blockchain i dostępu doń z wykorzystaniem określonego klucza prywatnego (zob. Górniak, 2019, s. 583) oraz powstrzymanie się od działań mogących wpłynąć na ten stan rzeczy (np. poprzez zmianę algorytmu danej kryptowaluty). Można też mówić o związaniu tych podmiotów zasadami dotyczącymi funkcjonowania danej kryptowaluty.

Niezależnie jednak od tego, które z prezentowanych w doktrynie stanowisk przyjmiemy *de lege lata*, związane z jednostką kryptowaluty prawo podmiotowe (lub stan faktyczny polegający na powiązaniu jej z określonym rachunkiem [adresem publicznym] będącym w dyspozycji danej osoby) stanowi składnik mienia, a także składnik majątku rozumianego jako „składniki mienia, dające się wyodrębnić jako zespół aktywów (nieraz i pasywów), będących przedmiotem dziedziczenia, obrotu, zabezpieczenia wierzytelności, podstawą odpowiedzialności za zobowiązania, itp." (Katner, 2012, 1297–1298; odnośnie do pojęcia mienia).

BIBLIOGRAFIA

Bank Anglii & Skarb Państwa. (2023). The digital pound: A new form of money for households and businesses? Consultation Paper. https://www.bankofengland.co.uk/-/media/boe/files/paper/2023/the-digital-pound-consultation-working-paper.pdf

Beck, B., & König, D. (2015). Bitcoin: Der Versuch einer vertragstypologischen Einordnung von kryptographischem Geld. *Juristenzeitung*, *70*(3), 130–138.

Binder, J. H. (2022). *Cryptocurrencies – Country Report: Germany*. XXIst International Congress of Comparative Law.

Bundestag. (1961). Ustawa z dnia 10 lipca 1961 r. Prawo bankowe ze zm. https://www.gesetze-im-internet.de/kredwg/KWG.pdf

Dudek, M. D. (2016). Waluta bitcoina – glosa do wyroku Trybunału Sprawiedliwości z 22.10.2015 r. w sprawie C-264/14 Skatteverket przeciwko Davidowi Hedqvistowi, *Europejski Przegląd Sądowy* (6), 38–43.

Dybowski, T., & Pyrzyńska, A. (2019). Świadczenia pieniężne. w: K. Osajda (red.), *System Prawa Prywatnego. Tom 5. Prawo zobowiązań – część ogólna* (wyd. 3), (ss. 261–307). C.H. Beck.

Fox, D. (2021). Digital Assets in Scots Private Law. *Edinburgh School of Law Research Paper*. No. 2021/17, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3914228&download=yes

Górniak, K. (2019). Prawo własności jednostek waluty kryptograficznej. *Kwartalnik Prawa Prywatnego*, *28*(3), 561–642.

Grabowski, M. (2020). Ustawa o usługach płatniczych. C.H. Beck.

Grundmann, S. (2019). Komentarz do § 245 BGB. w: W. Krüger (red.) *Münchener Kommentar zum Bürgerlichen Gesetzbuch.* C.H. Beck. beck-online.beck.de

Held, A., MacPherson, A. & Ripley, B. Y. (2022). *United Kingdom (UK) Report with a focus on the law of England and Wales and the law of Scotland*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4543838

Hrabčák, L. & Štrkolec M. (2024). EU Regulation of the Crypto-Assets Market. *Białostockie Studia Prawnicze*, *29*(1), 27–45. https://bsp.uwb.edu.pl/bialostockie-studia-prawnicze-zeszyt-29-nr-1/

Hu, J. (2024). The Regulation of Cryptocurrency in China. *International Journal of Digital Law and Governance*, *1*(1), 53–79.

Izba Gmin. (2000). Ustawa o usługach i rynkach finansowych z 2000 r., (Dz.U. poz. 8 ze zm.). https://www.legislation.gov.uk/ukpga/2000/8/section/417

Izba Gmin. (2017). Ustawa w sprawie prania pieniędzy, finansowania terroryzmu i transferu środków pieniężnych (informacji o płatniku) z 2017 r. (Dz.U. poz. 692 ze zm.). https://www.legislation.gov.uk/uksi/2017/692/contents

John, D. (2020). Zur Sachqualität und Eigentumsfähigkeit von Kryptotoken. *Zeitschrift für Bank – und Kapitalmarktrecht*, (2), 76–81.

Katner, P. (2022). Cryptocurrencies: The Impossible Domestic Law Regime? w: B. Lewaszkiewicz-Petrykowska & D. Skupień (red.), *Rapports polonaise. XXI Congrès international de droit compare. Asunción 23–28 X 2022* (ss. 169 –180). Wydawnictwo Uniwersytetu Łódzkiego.

Katner, W. J. (2012). Przedmiot stosunku cywilnoprawnego. w: M. Safjan (red.), *System Prawa Prywatnego. Tom 1. Prawo cywilne – cześć ogólna*, (ss. 1291 – 1384). C.H. Beck.

Komisja ds. Prawa. (2023). *Digital Assets: Final report*, https://s3-eu-west-2.amazonaws.com/cloud-platform-e218f50a4812967ba1215eaecede923f/uploads/sites/30/2023/06/Final-digital-assets-report-FOR-WEBSITE-2.pdf

Komisja ds. Prawa. (2024). *Digital assets as personal property. Short consultation on draft clauses*, https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/02/Feb-2024-digital-assets-and-personal-property-CP.pdf

Kruszewski, A. (2017). Polskie regulacje dotyczące walut cyfrowych. w: W. Rogowski (red.), *Regulacje finansowe. Fintech – nowe instrumenty finansowe – resolution*. Instytut Allerhanda.

Kütük, M. E. & Sorge, C. (2014). Bitcoin im deutschen Vollstreckungsrecht – Von der "Tulpenmanie" zur "Bitcoinmanie". *Multimedia und Recht*, (10), 643–646.

Langenbucher, K. (2018). Digitales Finanzwesen. *Archiv für die civilistische Praxis*, (218), 385–429.

Langenbucher, K., Hoche, M. & Wentz, J. (2020). Virtuelle Währungen. w: K. Langenbucher, D. H. Bliesener & G. Spindler (red.), *Bankrechtskommentar* (3 wyd.) (ss. 782–800). C.H. Beck.

Ludowy Bank Chin, Chińska Administracja Cyberprzestrzeni, Najwyższy Sąd Ludowy, Najwyższa Prokuratura Ludowa, Ministerstwo Przemysłu i Technologii Informacyjnych, Ministerstwo Bezpieczeństwa Publicznego, Państwowa Administracja ds. Regulacji Rynku, Chińska Komisja ds. Regulacji Bankowości i Ubezpieczeń, Chińska Komisja ds. Regulacji Papierów Wartościowych, Państwowy Urząd Wymiany Walut. (2021). *Notice on Further Preventing and Resolving the Risks of Virtual Currency Trading and Speculation.* http://www.pbc.gov.cn/en/3688253/3689012/4353814/index.html

Łukasik, K. (2023, 13 lipca). Jak Polacy inwestują w kryptowaluty. *Tygodnik Gospodarczy PIE*, 28, 6–7. https://pie.net.pl/wp-content/uploads/2023/07/Tygodnik-PIE_28–2023.pdf

Machnikowski, P. (2020). Przedmioty podmiotowych praw rzeczowych. w: E. Gniewek (red.), *System Prawa Prywatnego. Tom 3. Prawo rzeczowe*, (ss. 27–33). C.H. Beck.

MacPherson, A. & Ripley, B. Y. (2022). *Digital Assets Law Reform in England and Wales and Prospects for Scotland.* Aberdeen Law School Blog. https://www.abdn.ac.uk/law/blog/digital-assets-law-reform-in-england-and-wales-and-prospects-for-scotland/

Mazur, Ł. (2024). Kryptowaluty jako środek umarzania zobowiązań. w: J. Gołaczyński (red.), *Prawo umów elektronicznych. Zarys systemu*, (ss. 205–224). C.H. Beck.

Michna, M. (2018). Bitcoin jako przedmiot stosunków cywilnoprawnych. C.H. Beck.

Michna, M. (2024). Tokeny będące e-pieniądzem jako nowa forma pieniądza elektronicznego. *Monitor Prawa Bankowego*, (10), 78–195.

Minister Finansów. (2024). Projekt ustawy o rynku kryptoaktywów. https://legislacja.rcl.gov.pl/projekt/12382311/katalog/13040399#13040399

Ministerstwo Finansów. (2019). Krajowa ocena ryzyka prania pieniędzy oraz finansowania terroryzmu. https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu

Narodowy Bank Polski & Komisja Nadzoru Finansowego. (2017). Komunikat Narodowego Banku Polskiego i Komisji Nadzoru Finansowego z dnia 7 lipca 2017 r. w sprawie „walut" wirtualnych.

https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_NBP_KNF_w_sprawie_walut_wirtualnych_7_07_2017_57361.pdf

Narodowy Kongres Ludowy. (2020). Ustawa z dnia 28 maja 2020 r. Kodeks cywilny, https://english.www.gov.cn/archive/lawsregulations/202012/31/content_WS5fedad98c6d0f72576943005.html

Norton Rose Fulbright. (2017). *China issues announcement to ban fundraising through token offering*. https://www.nortonrosefulbright.com/en/knowledge/publications/aa676f71/china-issues-announcement-to-ban-fundraising-through-token-offerings

Omlor, S. (2019). Kryptowährungen im Geldrecht, *ZHR – Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht*, *183*, 294–345.

Parlament Europejski i Rada. (2015, 20 maja). Dyrektywa (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. UE L 141, 05.06.2015).

Parlament Europejski i Rada. (2018, 30 maja). Dyrektywa (UE) 2018/843 zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz.U. UE L 156, 19.06.2018).

Parlament Europejski i Rada. (2023, 31 maja). Rozporządzenie (UE) 2023/1114 w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U. UE L 150, 09.06.2023).

Paulus, D. & Matzke, R. (2018). Smart Contracts und das BGB – Viel Lärm um nichts?. *Zeitschrift für die gesamte Privatrechtswissenschaft*, (4), 431–466.

Reichstag. (1896). Ustawa z dnia 18 sierpnia 1896 r. Kodeks cywilny ze zm. https://www.gesetze-im-internet.de/bgb/BJNR001950896.html

Rückert, C. (2016). Vermögensabschöpfung und Sicherstellung bei Bitcoins. *Multimedia und Recht*, (5), 295–300.

Schlund, A. & Pongratz, H. (2018). Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung. *Deutsches Steuerrecht*, (12), 598–604.

Sejm Rzeczypospolitej Polskiej. (1991). Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (tj. z 2024, poz. 226 ze zm).

Sejm Rzeczypospolitej Polskiej. (1992). Ustawa z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (tj. z 2023, poz. 2805 ze zm).

Sejm Rzeczypospolitej Polskiej. (2018). Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tj. z 2023, poz. 1124 ze zm).

Skarb Państwa, Urząd ds. Postępowania Finansowego & Bank Anglii. (2018). *Cryptoassets Taskforce: final report.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

Skauradszun, D. (2021). Kryptowerte im Bürgerlichen Recht. *Archiv für die civilistische Praxis*, (221), 353–398.

Spindler, G. & Bille, M. (2014). Rechtsprobleme von Bitcoins als virtuelle Währung. *Wertpapiermitteilungen*, (29), 1357–1369.

Srokosz, W. (2015). Istota prawna kryptowaluty a odpowiedzialność prawna jej użytkownika. w: D. Szostek & J. Gołaczyński (red.), *Płatności elektroniczne: prawne finansowe i ekonomiczne ujęcie walut wirtualnych i cyfrowych*, (ss. 69–79). Wykładnia.

Srokosz, W. (2017). Legalna definicja kryptowaluty. w: W. Rogowski (red.), *Regulacje finansowe. Fintech – nowe instrumenty finansowe – resolution*, (ss. 37–47). Instytut Allerhanda.

Szewczyk, J. (2018). O cywilnoprawnych aspektach bitcoina. *Monitor Prawniczy* (5), 243–251.

Urząd Komisji Nadzoru Finansowego. (2020). Stanowisko Urzędu Komisji Nadzoru Finansowego w sprawie wydawania i obrotu kryptoaktywami. https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_71794.pdf

Urząd Komisji Nadzoru Finansowego. (2021). Ostrzeżenie Urzędu KNF o ryzykach związanych z nabywaniem oraz z obrotem kryptoaktywami (w tym walutami wirtualnymi oraz kryptowalutami). https://www.knf.gov.pl/knf/pl/komponenty/img/Ostrzezenie_UKNF_o_ryzykach_zwiazanych_z_nabywaniem_oraz_z_obrotem_kryptoaktywami_72241.pdf

Urząd Podatkowy i Celny Jego Królewskiej Mości. (2023). *Cryptoassets Manual. CRYPTO10100 – Introduction to cryptoassets: what are cryptoassets*. https://www.gov.uk/hmrc-internal-manuals/cryptoassets-manual/crypto10100

Walter, A. (2019). Bitcoin, Libra und sonstige Kryptowährungen aus zivilrechtlicher Sicht. *Neue Juristische Wochenschrift*, (50), 3609–3614.

Weber-Elżanowska, A. (2021). Zapłata w bitcoinach za przeniesienie własności rzeczy lub praw – uwagi na tle wybranych instytucji prawa obligacyjnego. w: K. Bilewska, W. J. Kocot & D. Krekora-Zając (red.), *Wykonywanie zobowiązań. Księga jubileuszowa dedykowana profesorowi Adamowi Brzozowskiemu* (ss. 581–590). C.H. Beck.

Wnęk, M. (2023). Natura prawna kryptowaluty. C.H. Beck.

Woźnicki, Ł. (2014, 28 marca). PolishCoin, PolCoin i PLNc. W Polsce są już aż trzy narodowe kryptowaluty. Dlaczego? *Gazeta Wyborcza*. https://wyborcza.pl/7,75398,15707096,polishcoin-polcoin-i-plnc-w-polsce-sa-juz-az-trzy-narodowe.html

Wyrok NSA z dnia 10 lutego 2021 r., sygn. akt II FSK 2870/18, https://orzeczenia.nsa.gov.pl/doc/8889489BE0

Wyrok NSA z dnia 27 kwietnia 2022 r., sygn. akt II FSK 2181/19, https://orzeczenia.nsa.gov.pl/doc/DC967F7AE0

Wyrok Sąd Apelacyjnego z dnia 3 lutego 2023 r. w sprawie Tulip Trading v Van der Laan, [2023] EWCA Civ 83.

Wyrok TSUE z dnia 22 października 2015 r. w sprawie Skatteverket v. David Hedqvist, C 264/14.

XXIst International Congress of Comparative Law. (2022). *Cryptocurrencies: The Impossible Domestic Law Regime? China*.

Zacharzewski, K. (2014). Bitcoin jako przedmiot stosunków prawa prywatnego. *Monitor Prawniczy* (21), 1132–1139.

Zacharzewski, K. (2015). Praktyczne znaczenie bitcoina na wybranych obszarach prawa prywatnego. *Monitor Prawniczy* (4), 187–195.

Zagrobelny, K. (2022). Komentarz do artykułu 358. w: P. Machnikowski (red.), *Zobowiązania. Tom I. Przepisy ogólne i powiązane przepisy Księgi I KC. Komentarz* (ss. 1674–1689). C.H. Beck.

Zespół Zjednoczonego Królestwa ds. Jurysdykcji. (2019). *Legal Statement on cryptoassets and smart contracts*, UK Jurisdiction Taskforce. https://www.blockchain4europe.eu/wp-content/uploads/2021/05/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119–1.pdf

Zoll, F. (2023). Wykonanie zobowiązań przez spełnienie świadczenia. w: A. Olejniczak (red.), *System Prawa Prywatnego. Tom 6. Prawo zobowiązań – część ogólna*, (wyd. 4), (ss. 1123–1207). C.H. Beck.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.06

Received: 16.12.2024
Accepted: 10.04.2025

Konrad Zacharzewski
Akademia Leona Koźmińskiego, Polska
kancelaria@zacharzewski.pl
ORCID ID: https://orcid.org/0000-0002-9850-6020

Model i środki bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy kryptoaktywów w prawie polskim

The Model and Means of Direct Protection of the Individual Rights of Buyers and Holders of Cryptoassets in Polish Law

Abstract: The legal basis for investigations into the model and means of direct protection of the subjective rights of buyers and holders of cryptoassets in Polish law is the provisions of the MiCA Regulation and the provisions of the Polish Act on Cryptoassets, assuming that the draft law will be adopted in the form known on 31 December 2024. Summarizing the normative solutions already in force and planned in Polish law which are devoted to the means of direct protection for the subjective rights of purchasers and holders of cryptographic assets is a source of limited optimism. In the current legal situation, the model of protecting the subjective rights of buyers and holders of cryptographic assets is not effective, and the means of direct protection of these subjective rights are not sufficient or fully effective.

Keywords: protection of buyers and holders of cryptoassets, model for the protection of buyers and holders of cryptoassets, measures for the direct protection of buyers and holders of cryptoassets
Słowa kluczowe: ochrona nabywców i posiadaczy kryptoaktywów, model ochrony nabywców i posiadaczy kryptoaktywów, środki bezpośredniej ochrony nabywców i posiadaczy kryptoaktywów

Wprowadzenie

Podstawę prawną dociekań na temat modelu i środków bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy kryptoaktywów w prawie polskim stanowią przepisy rozporządzenia MiCA oraz przepisy polskiej ustawy o kryptoaktywach, przy założeniu, że projekt ustawy zostanie przyjęty w kształcie znanym w dniu

© 2025 Konrad Zacharzewski published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

31 grudnia 2024 roku[1]. Zsumowanie już obowiązujących oraz projektowanych w prawie polskim rozwiązań normatywnych poświęconych środkom bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych jest źródłem umiarkowanego entuzjazmu. W aktualnym stanie prawnym model ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych nie jest efektywny, a środki bezpośredniej ochrony tych praw podmiotowych nie są wystarczające i w pełni skuteczne. Składają się na to liczne uwarunkowania normatywne, które uzasadniają zajęcie się tytułowym zagadnieniem.

Rozważania opierają się na założeniu, że w obecnym stanie wiedzy prawniczej nie zachodzi już potrzeba wyjaśniania pojęć podstawowych związanych z technologią blockchain oraz aktywami kryptograficznymi, w tym walutami cyfrowymi. Ponadto treść przepisów prawa została przytoczona z poszanowaniem ich oryginalnego zapisu gramatycznego.

1. Uwagi wstępne na temat potrzeby ochrony uczestników rynku kryptoaktywów

W trakcie prac legislacyjnych projekt polskiej ustawy o kryptoaktywach był wzorowany na regulacjach europejskich, spośród których najważniejszą rolę odgrywa właśnie rozporządzenie MiCA. Jednakże polski ustawodawca nie uwzględnił w treści tego długo oczekiwanego i dyskutowanego aktu prawnego dwóch ważnych rozwiązań przewidzianych na poziomie prawa europejskiego, a mianowicie prawa żądania wykupu posiadanych tokenów powiązanych z aktywami (art. 39 rozporządzenia MiCA) oraz będących e-pieniądzem (art. 49 rozporządzenia MiCA), a także prawa odstąpienia przez nabywcę kryptoaktywów od umowy stanowiącej prawną podstawę nabycia (art. 13 rozporządzenia MiCA). Prawo żądania wykupu posiadanych tokenów oraz prawo odstąpienia od umowy w terminie 14 dni bez podania przyczyny będą mogły być wykonywane przez nabywców i posiadaczy kryptoaktywów, ale bezpośrednio na podstawie wspomnianych przepisów art. 39, art. 49 albo art. 13 rozporządzenia MiCA.

Ten znaczący niedostatek regulacyjny, polegający na braku bezpośrednio w prawie polskim prawnej podstawy skorzystania z przysługujących uprawnień, skłania do postawienia pytania o to, w jaki sposób polski system prawny będzie chronił obywateli Rzeczpospolitej Polskiej po wejściu w życie polskiej ustawy o kryptoaktywach (prognozowany początkowo termin upłynął dnia 30 czerwca 2024 roku; art. 111 projektu ustawy o kryptoaktywach) oraz po rozpoczęciu bezpośredniego stosowania

1 Uwaga Autora: rozważania opierają się na projekcie ustawy o kryptoaktywach z dnia 22 lutego 2024 roku (numer w wykazie prac legislacyjnych i programowych Rady Ministrów: UC2) z uwzględnieniem stanu zaawansowania prac na dzień 31 grudnia 2024 roku; dalej: polska ustawa o kryptoaktywach.

przepisów rozporządzenia MiCA od dnia 30 grudnia 2024 roku (art. 149 ust. 2 rozporządzenia MiCA). Porównawcza analiza rozwiązań przewidzianych na poziomie obu aktów prawnych daje wynik w postaci ukształtowania modelu ochrony oraz katalogu przyjętych środków ochronnych.

Sprawa jest ważna z trzech podstawowych punktów widzenia.

Po pierwsze, popularność aktywów cyfrowych nieustannie wzrasta wśród publiczności, a wzrosty popularności następują skokowo. Wraz ze wzrostem kursów najpopularniejszych kryptowalut rozwija się gorączka spekulacyjna i powiększa skłonność do ryzyka, zwłaszcza pod wpływem silnych bodźców psychologicznych (szansa na uzyskanie łatwego zarobku bez pracy).

Po drugie, w tych okolicznościach powiększa się obszar działania przedsiębiorców prowadzących swoją działalność gospodarczą za pomocą łączności internetowej w sposób legalny, ale poza zakresem jurysdykcji prawa polskiego oraz prawa Unii Europejskiej. Wśród publiczności zasady prowadzenia tej działalności częstokroć nie są powszechnie zrozumiałe, jeżeli chodzi o szczegóły, a nawet o ogóły. Otoczenie prawne branży kryptowalutowej jest skomplikowane, podobnie jak konfiguracja i przedmiot powiązań pomiędzy różnymi osobami i dokonywanymi pomiędzy nimi czynnościami, z czego nie zdają sobie sprawy osoby, których wiedza na temat kryptowalut wywodzi się głównie z internetowych reklam. Niezależnie od tego wraz ze wzrostem masowej popularności kryptowalut wzrasta też skala oszustw.

Po trzecie, organy administracji publicznej nie są w stanie skutecznie zabezpieczyć przed utratą środków przeznaczonych na nabycie aktywów kryptograficznych ani również nie są w stanie zapewnić bezpieczeństwa osobom z własnej woli dokonującym czynności, których skutków prawnych nie zrozumiały, a nawet padły ofiarą oszustów. Natomiast poszukiwanie ochrony przed organami wymiaru sprawiedliwości często bywa nieskuteczne, zwłaszcza w przypadku postępowań karnych przygotowawczych w fazie *ad rem*, które nie przechodzą w fazę *ad personam* ze względu na niewykrycie sprawcy przestępstwa na szkodę nabywcy kryptoaktywów. Dochodzenie roszczeń w procesie cywilnym trwa zaś niewymownie długo, o ile w ogóle sprawcę szkody uda się zindywidualizować i będzie nad nim rozciągała się jurysdykcja prawa polskiego. W praktyce najsprawniej działają organy administracji publicznej, nakładając sankcje na animatorów przedsięwzięć nielegalnych – ale ten fakt nie daje satysfakcji osobom pokrzywdzonym i poszkodowanym, skoro nie mogą one liczyć w wyobrażalnej perspektywie czasowej na odzyskanie pieniężnego ekwiwalentu środków zainwestowanych w utracone aktywa kryptograficzne.

Te wszystkie względy sprawiają, że podjęcie tytułowej tematyki modelu i środków bezpośredniej ochrony praw podmiotowych nabywców oraz posiadaczy kryptoaktywów w prawie polskim jest aktualne i należy poświęcić jej właściwą porcję uwagi.

2. Zagadnienia terminologiczne

2.1. Aspekt podmiotowy

Obowiązujące przepisy poświęcone obrotowi aktywami kryptograficznymi nie posługują się pojęciem konsumenta, lecz pojęciami równoznacznymi z punktu widzenia kryterium celowościowego. Uwagi szczegółowe należy rozpocząć od wyjaśnienia podstawowych kwestii terminologicznych. Prawo polskie recypowało rozwiązania unijne. Odpowiednikiem znanego w prawie powszechnym pojęcia „konsument" na obszarze obrotu aktywami kryptograficznymi jest pojęcie „posiadacz detaliczny" oraz nieco ogólniejsze pojęcie „klient". Takimi sformułowaniami posługują się obowiązujące źródła prawa.

Pojęcie „konsumenta" pojawia się właściwie tylko w kilku miejscach preambuły rozporządzenia MiCA, na ogół z wyraźnym rysem publicznoprawnym. Jest ono m.in. wspomniane w kontekście „stowarzyszeń konsumentów reprezentujących posiadaczy tokenów powiązanych z aktywami" w przepisie art. 31 ust. 1 rozporządzenia MiCA oraz w kontekście „organizacji konsumenckich" w przepisie art. 108 ust. 1 rozporządzenia MiCA. W sensie publicznoprawnym słowo „konsument" zostało użyte jako podstawa cyklicznej ewaluacji przyjętych rozwiązań normatywnych, należącej do kompetencji ESMA (art. 103 ust. 6 rozporządzenia MiCA) oraz należącej do kompetencji EUNB (art. 104 ust. 6 rozporządzenia MiCA).

Z perspektywy bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych istotniejsze znaczenie ma przepis art. 108 ust. 1 rozporządzenia MiCA. W świetle jego brzmienia właściwe organy [państw członkowskich Unii Europejskiej – uwaga k.z.] określają procedury umożliwiające klientom i innym zainteresowanym stronom, w tym organizacjom konsumenckim, składanie do nich skarg dotyczących domniemanych naruszeń niniejszego rozporządzenia przez oferujących, osoby ubiegające się o dopuszczenie do obrotu, emitentów tokenów powiązanych z aktywami lub tokenów będących e-pieniądzem lub przez dostawców usług w zakresie kryptoaktywów. Skargi przyjmuje się w formie pisemnej, w tym elektronicznej, oraz w języku urzędowym państwa członkowskiego, w którym złożono skargę, lub w języku akceptowanym przez właściwe organy tego państwa członkowskiego.

Z przepisu art. 113 ust. 2 pkt 2 rozporządzenia MiCA wynika zaś, że organizacje konsumenckie mające uzasadniony interes w ochronie posiadaczy kryptoaktywów mogą być uprawnione – w interesie konsumentów i zgodnie z prawem krajowym – do wszczęcia postępowania przed sądem lub właściwym organem administracyjnym w celu zapewnienia stosowania niniejszego rozporządzenia.

Jak zatem okazuje się, przepisy rozporządzenia MiCA nie przewidują odpowiednika pojęcia „konsument" charakterystycznego dla prawa polskiego (i europejskiego) ze względu na postulat poszerzonej ochrony prawnej tej kategorii podmiotów prawa cywilnego (szerzej nt. statusu konsumenta na rynku kapitałowym zob. Jastrzębski, 2022, s. 45; Osajda, 2021, s. 22; Osajda, 2022, s. 41; Rydz, 2023, s. 101; Kukuryk, 2014,

s. 18) i zdefiniowanego jako osoba fizyczna dokonująca z przedsiębiorcą czynności prawnej niezwiązanej bezpośrednio z jej działalnością gospodarczą lub zawodową (art. 22^1 kodeksu cywilnego; dalej k.c.). Odpowiednikiem takiego pojęcia posługuje się jednak prawodawca europejski i jest nim „posiadacz detaliczny".

„Posiadacz detaliczny" został zdefiniowany jako osoba fizyczna działająca w celach, które nie mieszczą się w ramach jej działalności handlowej, gospodarczej, rzemieślniczej lub zawodowej (art. 3 ust. 1 pkt 37 rozporządzenia MiCA). Co ciekawe – polska ustawa o kryptoaktywach nie recypowała pojęcia „posiadacza detalicznego". Dlatego powinno być ono rozumiane w sposób bezpośrednio unormowany na poziomie rozporządzenia MiCA.

Polska ustawa recypowała jednak pojęcie nieco szersze zakresowo, a mianowicie pojęcie „klient". W świetle przepisu art. 2 pkt 8 polskiej ustawy o kryptoaktywach przez klienta rozumie się klienta w rozumieniu art. 3 ust. 1 pkt 39 rozporządzenia MiCA. W tym najszerszym rozumieniu „klient" oznacza osobę fizyczną lub prawną, na rzecz której dostawca usług w zakresie kryptoaktywów świadczy usługi w zakresie kryptoaktywów.

Na potrzeby niniejszego opracowania nabywca i posiadacz kryptoaktywów będzie rozumiany w sposób najbardziej zbliżony do ujęcia przewidzianego w przepisie art. 22^1 k.c., czyli jako osoba fizyczna działająca w celach, które nie mieszczą się w ramach jej działalności handlowej, gospodarczej, rzemieślniczej lub zawodowej (art. 3 ust. 1 pkt 37 rozporządzenia MiCA). Uzasadnienie takiego zabiegu metodologicznego, być może nawet uważanego za pewne uproszczenie, jest właściwie oczywiste i opiera się na dwóch argumentach.

Po pierwsze, właśnie osoby fizyczne działające „jako" osoby fizyczne (we własnym imieniu i na własny rachunek) są w polskiej praktyce najczęstszymi nabywcami aktywów kryptograficznych. To właśnie osoby fizyczne są podatne na reklamy internetowe i pod ich wpływem albo z własnej inicjatywy zakładają portfele kryptowalutowe bądź zakładają konta na platformach handlowych, aby później wpłacać tam pieniądze, a na ogół nieco później – z różnych względów – nie móc ich odzyskać. Właśnie ta kategoria podmiotów zasługuje na wzmożoną ochronę.

Po drugie, w polskiej praktyce znanym zjawiskiem jest dokonywanie czynności w obrocie aktywami kryptograficznymi przez osoby prawne działające przez swoje organy – ale takie osoby prawne nie zasługują *ex lege* na wzmożoną ochronę. Dlatego poszerzona analiza dogmatyczna zagadnienia ochrony osób prawnych dokonujących czynności w obrocie aktywami kryptograficznymi nie wydaje się w obecnym stanie prawnym potrzebą najpilniejszą. Panują tutaj zasady ogólne.

Takie założenie metodologiczne, wraz z zaprezentowanym uzasadnieniem zajętego stanowiska, usprawiedliwia ujęcie tytułu niniejszego opracowania. Jest ono po prostu najistotniejsze z praktycznego punktu widzenia, ponieważ jest poświęcone modelowi i środkom bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy kryptoaktywów w prawie polskim. Przyjęcie tej formuły jest tym bardziej

usprawiedliwione w świetle ugruntowanego w doktrynie ustalenia – które należy podzielić – że inwestor indywidualny działający na rynku kapitałowym, spełniający wymogi określone w art. 22^1 k.c., jest konsumentem (Jastrzębski, 2022, s. 48) i że każdy inwestor indywidualny będący osobą fizyczną może i powinien zostać uznany za konsumenta, o ile nie prowadzi działalności gospodarczej związanej z inwestowaniem na rynkach finansowych (Osajda, 2021, s. 25).

Na marginesie rozważań należy zauważyć, że w konkretnej sytuacji konkretna osoba fizyczna działająca we własnym imieniu i na własny rachunek może zostać pozbawiona ochrony, zwłaszcza wówczas, gdy z obrotu aktywami kryptograficznymi uczyni sobie przedmiot regularnej działalności zarobkowej, spełniając jednocześnie przesłanki wystarczające do zakwalifikowania jej jako przedsiębiorcy w rozumieniu przepisu art. 4 ust. 1 Prawa przedsiębiorców z 2018 roku. Należy o tym wspomnieć tylko dla porządku, ponieważ omawianie zagadnień, których kwalifikacja prawna jest uzależniona od konkretnego stanu faktycznego, leży poza obszarem głównego nurtu niniejszych rozważań.

2.2. Aspekt przedmiotowy

Krótkie wyjaśnienie terminologiczne należy także wystosować pod adresem przedmiotu czynności prawnych dokonywanych przez osoby zainteresowane w obrocie kryptoaktywami. Już na pierwszy rzut oka można dostrzec dywergencję pomiędzy tytułem aktu prawnego unijnego, który został poświęcony „rynkowi aktywów kryptograficznych", oraz tytułem aktu prawa polskiego, który został poświęcony „kryptoaktywom". Nad tą różnicą można właściwie przejść do porządku, wskazując jednak na to, że atrybut „kryptograficzny" nie jest jedynym występującym w praktyce i w mowie codziennej (potocznej). Tutaj bogactwo ujęć językowych jest znaczne i obejmuje także atrybuty „wirtualne" (zob. np. Europejski Bank Centralny, 2012; Wyczik, 2022; Karkut, 2018, s. 31) oraz atrybuty „cyfrowe" (zob. np. Rezolucja Parlamentu Europejskiego [2016] w sprawie wirtualnych walut; pismo Izby Skarbowej w Katowicach [2013]). Są one konkurencyjne względem siebie, mają ustalone znaczenia normatywne i są poddawane rozkładowi na czynniki pierwsze w literaturze przedmiotu oraz orzecznictwie. Przepisy o przeciwdziałaniu praniu pieniędzy oraz przepisy prawa podatkowego, w odróżnieniu od przepisów ustawy o kryptowalutach, posługują się pojęciem „walut wirtualnych" (zob. art. 2 ust. 2 pkt 26 ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu [2018] oraz przepis art. 5a pkt 33a ustawy o podatku dochodowym od osób fizycznych [1991]). W celu zredukowania płaszczyzn problemowych można jednak na nasze potrzeby przyjąć, że występujące pojęcia prawne mają analogiczne znaczenie na potrzeby prowadzonych rozważań, biorąc jednak pod uwagę kilka okoliczności towarzyszących.

Po pierwsze, w świetle przepisów rozporządzenia MiCA podstawowym pojęciem jest ogólne pojęcie „kryptoaktywo". Token jest rodzajem kryptoaktywu.

Tokeny jako rodzaje kryptoaktywów są reprezentowane przez trzy kategorie partykularne, a mianowicie przez tokeny inne niż tokeny powiązane z aktywami lub będące pieniądzem elektronicznym, tokeny powiązane z aktywami oraz tokeny będące pieniądzem elektronicznym (tokeny będące e-pieniądzem). Każda z tych trzech kategorii doczekała się sobie właściwej regulacji, co pozostaje jednak bez znaczenia z punktu widzenia ogólnych rozważań na temat modelu i środków bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych.

Po drugie bowiem, środki ochronne przewidziane na poziomie rozporządzenia MiCA są – w pewnym uproszczeniu – analogiczne dla każdej kategorii nabywców i posiadaczy tokenów bez względu na rodzaj nabytych i posiadanych tokenów, jednakże ze wskazaniem, że tokeny niższej kategorii normatywnej są obwarowane regulacjami w mniejszym stopniu i *vice versa*. W rachubę wchodzą tutaj środki ochrony pośredniej, tj. głównie administracyjny nadzór emisji tokenów, licencjonowanie działalności usługowej, obowiązki informacyjne emitentów i oferujących, reglamentowany marketing, petryfikowanie odpowiedzialności za szkodę, zakaz *insider tradingu* i manipulacji kursem. W praktyce także i to pozostaje jednak bez znaczenia z punktu widzenia ogólnych rozważań na temat modelu i środków bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych.

Po trzecie bowiem, w praktyce międzynarodowego obrotu aktywami cyfrowymi za pomocą sieci Internet najistotniejsze znaczenie ma ochrona obywateli Unii Europejskiej przed naruszeniami ze strony podmiotów, których siedziba leży poza obszarem Unii Europejskiej.

Z tych trzech skonfrontowanych ze sobą względów drobiazgowa analiza typu nabytego albo posiadanego tokena nie ma znaczenia w procesie ustalania katalogu oraz charakterystyki prawnej środków ochrony przysługujących nabywcy lub posiadaczowi nabytego tokena. Dlatego można w pewnym uproszczeniu zuniwersalizować rozważania i przyjąć, że główne pojęcia „kryptoaktywów" oraz „aktywów kryptograficznych" są – albo mogą być – synonimami pojęć konkurencyjnych, a mianowicie „aktywów cyfrowych" czy też „aktywów wirtualnych" albo innych jeszcze ujęć o różnej wartości dogmatycznej ze względu na ich zakotwiczenie w publicystyce oraz przekazach popularnonaukowych, jak np. „wirtualna własność" (Karkut, 2018, s. 53). Skrupulatne uporządkowanie także tego obszaru terminologicznego wymagałoby poszerzenia rozważań w kierunku ich znacznego uszczegółowienia. Kierując się kolejnym uproszczeniem, można przyjąć, że nabywca i posiadacz aktywów kryptograficznych może zostać określony jako finalny nabywca kryptoaktywów (aktywów cyfrowych, aktywów wirtualnych), a idąc jeszcze dalej – jako niezawodowy uczestnik rynku aktywów kryptograficznych.

3. Aktualnie ukształtowany model ochrony

De lege lata model ochrony praw podmiotowych finalnego nabywcy oraz posiadacza aktywów kryptograficznych opiera się przede wszystkim na wzmożonym nadzorze administracyjnym. Taki punkt wyjścia narzuciły przepisy rozporządzenia MiCA i taki też kierunek został przyjęty przez polskiego ustawodawcę (zob. uzasadnienie projektu ustawy o kryptoaktywach [2024]). Oba akty prawne różnią się jednak od siebie pod względem treści, co można ustalić już nawet na podstawie ich przedmiotu i systematyki wewnętrznej. Rozłożenie akcentów pomiędzy tymi dwoma regulacjami prawnymi wpływa na katalog środków ochrony praw podmiotowych nabywcy i posiadacza aktywów kryptograficznych.

Z przepisu art. 1 rozporządzenia MiCA wynika, że w niniejszym rozporządzeniu ustanawia się jednolite wymogi dotyczące oferty publicznej i dopuszczania do obrotu na platformie obrotu kryptoaktywów innych niż tokeny powiązane z aktywami i tokeny będące e-pieniądzem, tokenów powiązanych z aktywami i tokenów będących e-pieniądzem, a także wymogi w odniesieniu do dostawców usług w zakresie kryptoaktywów.

Natomiast z przepisu art. 1 polskiej ustawy o kryptoaktywach wynika, że ustawa określa organizację i wykonywanie nadzoru nad oferującymi, osobami ubiegającymi się o dopuszczenie kryptoaktywów do obrotu, emitentami tokenów powiązanych z aktywami i tokenów będących e-pieniądzem oraz dostawcami usług w zakresie kryptoaktywów, zwanego dalej „nadzorem nad rynkiem kryptoaktywów".

Z tego krótkiego zestawienia przepisów otwierających oba akty prawne wynika, że regulacje polskie mają znacznie zawężony zakres. Przedmiotem regulacji unijnej jest rynek, a przedmiotem regulacji polskiej jest nadzór. W istocie tytuł polskiej ustawy jest nawet nieco mylący. Polska ustawa o kryptoaktywach – sądząc po kształcie projektu w grudniu 2024 roku – nie jest odpowiednikiem rozporządzenia MiCA, które zostało poświęcone rynkowi kryptoaktywów. Mamy więc właściwie do czynienia z częściową implementacją, a przedmiot polskiej regulacji obejmuje w swej najgłębszej istocie nadzór nad rynkiem kryptoaktywów i taki powinien być jej tytuł. Wynika to zresztą już z brzmienia przepisu art. 1 polskiej ustawy o kryptoaktywach, który jednoznacznie wskazuje na to, że jej przedmiotem jest nadzór, zwany dalej „nadzorem nad rynkiem kryptoaktywów". Taka optyka polskiego ustawodawcy w znacznym stopniu ogranicza efektywność bezpośredniej ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych.

Na model ochrony przewidziany na poziomie rozporządzenia MiCA składają się środki prawne o charakterze publicznoprawnym oraz prywatnoprawnym. Z przepisu art. 1 ust. 2 rozporządzenia MiCA wynika, że do tej pierwszej kategorii należą przede wszystkim licencjonowanie działalności dostawców usług w zakresie kryptoaktywów, czyli podmiotów świadczących usługi na rzecz klientów, a także nadzór administracyjny. Charakter publicznoprawny, ale ze skutkami w zakresie prawa pry-

watnego, można przypisać wymogom dotyczącym przejrzystości i ujawniania informacji, wymogom dotyczącym ochrony posiadaczy kryptoaktywów w ramach emisji, oferty publicznej i dopuszczania kryptoaktywów do obrotu, wymogom dotyczącym ochrony klientów dostawców usług w zakresie kryptoaktywów oraz środkom zapobiegającym wykorzystywaniu informacji poufnych, bezprawnemu ujawnianiu informacji poufnych i manipulacjom na rynku związanym z kryptoaktywami.

Podobnie w prawie polskim podstawowe znaczenie odgrywa licencjonowanie prowadzenia działalności w charakterze dostawców usług w zakresie kryptoaktywów, czyli podmiotów świadczących usługi na rzecz klientów, a także nadzór administracyjny. Model licencjonowania i nadzoru jest zbliżony do modelu licencjonowania i nadzoru rynku instrumentów finansowych (Zacharzewski, 2021, s. 195). Samo licencjonowanie opiera się na konkretnych podstawach prawnych przewidzianych w przepisach rozporządzenia MiCA, do którego polska ustawa o kryptoaktywach częstokroć odsyła w tym zakresie (np. w przepisie art. 40 pkt. 1 dotyczącym opłat za udzielenie zezwolenia). Na nadzór administracyjny składają się liczne kompetencje szczegółowe (Rozdział 5 ustawy jest najobszerniejszy ze wszystkich). Natomiast charakter publicznoprawny, ale z dalszymi skutkami w zakresie prawa prywatnego, można przypisać wymogom dotyczącym obowiązków informacyjnych (Rozdział 3) oraz odpowiedzialności cywilnej w związku z dokumentem informacyjnym (Rozdział 4). We wszystkich niemal sprawach kardynalnych polska ustawa o kryptoaktywach odsyła do rozporządzenia MiCA (takich odesłań jest znacznie ponad sto).

Jak zatem okazuje się, przepisy prawa polskiego nie obejmują wyraźnie wyodrębnionych w strukturze logicznej ustawy takich obszarów, jak ochrona posiadaczy kryptoaktywów w ramach emisji, oferty publicznej i dopuszczania kryptoaktywów do obrotu, wymogi dotyczące ochrony klientów dostawców usług w zakresie kryptoaktywów oraz środki zapobiegające wykorzystywaniu informacji poufnych, bezprawnemu ujawnianiu informacji poufnych i manipulacjom na rynku związanym z kryptoaktywami. Rozwiązania te – przynajmniej najważniejsze – są jednak przewidziane w prawie polskim, ale poza obszarem normatywnego oddziaływania przepisów ustawy o kryptoaktywach. Z jednej strony są to rozwiązania przewidziane wprost w przepisach rozporządzenia MiCA, stosowanego bezpośrednio w Rzeczpospolitej Polskiej (odesłania ustawowe mają tzw. charakter instrukcyjny), z drugiej zaś strony są to rozwiązania przewidziane w przepisach szczególnych.

Właśnie uporządkowanie tego rozległego arsenału środków ochronnych może doprowadzić do rozróżnienia środków ochrony pośredniej (publicznoprawnej, ogólnosystemowej) oraz bezpośredniej (prywatnoprawnej). Takie postawienie sprawy jest podstawą udzielenia odpowiedzi na pytanie, co konkretnie może zrobić nabywca lub posiadacz kryptoaktywów, którego prawa podmiotowe zostały naruszone albo przynajmniej zostały – lub mogą zostać – zagrożone naruszeniem. W dalszej części rozważań zostaną programowo pominięte środki prawne pośredniej ochrony praw podmiotowych nabywców i posiadaczy kryptoaktywów.

4. Środki prawne bezpośredniej ochrony przewidziane w rozporządzeniu MiCA

4.1. Prawo do odstąpienia

Najważniejszym środkiem prawnym bezpośredniej ochrony sytuacji prawnej nabywcy i posiadacza kryptoaktywów jest prawo do odstąpienia. To termin ustawowy (pojęcie prawne). W istocie chodzi o prawo do odstąpienia od umowy nabycia kryptoaktywów. Pod względem podstawowych elementów konstrukcji prawnej instytucja prawa do odstąpienia (art. 13 rozporządzenia MiCA) została ukształtowana analogicznie jak prawo odstąpienia od umowy zawartej na odległość, które przysługuje na podstawie przepisu art. 27 ust. 1 ustawy o prawach konsumenta 2014 (szerzej zob. Kocot & Kondek, 2014, s. 4; Czech, 2016, s. 47; Czech, 2020). Ta instytucja nie została przewidziana w prawie polskim, ponieważ pod względem przedmiotowym dotyczy tokenów innych niż tokeny powiązane z aktywami i tokeny będące e-pieniądzem. Prawo polskie nie obejmuje zaś przedmiotowym zakresem swojego unormowania tych tokenów, lecz inne tokeny, a mianowicie tokeny powiązane z aktywami oraz tokeny będące e-pieniądzem (art. 1 polskiej ustawy o kryptoaktywach).

W świetle przepisu art. 13 ust. 1 rozporządzenia MiCA posiadacze detaliczni, którzy nabywają kryptoaktywa inne niż tokeny powiązane z aktywami lub tokeny będące e-pieniądzem bezpośrednio od oferującego lub od dostawcy usług w zakresie kryptoaktywów dokonującego plasowania kryptoaktywów w imieniu tego oferującego, mają prawo do odstąpienia. Z przepisu art. 13 ust. 2 rozporządzenia MiCA wynika zaś, że posiadaczom detalicznym przysługuje okres 14 dni kalendarzowych na odstąpienie od umowy nabycia kryptoaktywów innych niż tokeny powiązane z aktywami lub tokeny będące e-pieniądzem bez ponoszenia jakichkolwiek opłat lub kosztów i bez konieczności podawania przyczyny. Okres, w którym można odstąpić od umowy, liczy się od dnia wyrażenia przez posiadacza detalicznego zgody na nabycie tych kryptoaktywów.

Skutki złożenia przez posiadacza detalicznego oświadczenia o odstąpieniu są typowe. Umowę uważa się za niezawartą, a przysporzenia uzyskane przez obie strony są pozbawione swojej przyczyny prawnej (*causae*) wynikającej ze zobowiązania do rozporządzenia (art. 155 § 1 k.c., art. 156 k.c., art. 510 § 1 i § 2 k.c.). Dlatego strony umowy zawartej i rozwiązanej w wyniku odstąpienia powinny zwrócić sobie to, co wzajemnie świadczyły (na zasadach ogólnie zbliżonych do tych określonych w przepisie art. 494 k.c.). Tej formule hołduje przepis art. 13 ust. 3 rozporządzenia MiCA. Mianowicie, wszystkie płatności otrzymane od posiadacza detalicznego, w tym – w przypadku, gdy ma to zastosowanie – wszelkie opłaty, muszą zostać zwrócone bez zbędnej zwłoki, czyli niezwłocznie w rozumieniu przepisu art. 494 § 2 k.c. (szerzej zob. Adamus, 2018, s. 11), a w każdym razie nie później niż w terminie 14 dni od dnia, w którym oferujący lub dostawca usług w zakresie kryptoaktywów dokonujący plasowania kryptoaktywów w imieniu tego oferującego został poinformowany o decyzji posiada-

cza detalicznego o odstąpieniu od umowy nabycia tych kryptoaktywów. Sposób zwrotu wszystkich płatności również został określony w przywołanym przepisie. Mianowicie, zwrotu płatności dokonuje się przy użyciu takich samych środków płatniczych, których użył posiadacz detaliczny w pierwotnej transakcji, chyba że posiadacz detaliczny wyraźnie zgodzi się na inne rozwiązanie i pod warunkiem, że posiadacz detaliczny nie zostanie obciążony żadnymi opłatami ani kosztami w związku z takim zwrotem.

Komentowana regulacja instytucji odstąpienia od umowy nie określiła jednak skutków odstąpienia w zakresie spoczywającego na posiadaczu detalicznym obowiązku zwrotu nabytych kryptoaktywów. Ze względu na ogólną zasadę zakazu wzbogacenia bez należytej podstawy prawnej oraz na ogólnej zasadzie określonej w przepisie art. 494 § 1 zdanie pierwsze k.c. (szerzej zob. Jabłoński, 2017, s. 73; Mleczak, 2017, s. 53) należy przyjąć, że nabywca kryptoaktywów powinien je przekazać (zwrócić) w to samo miejsce, z którego je otrzymał (zwrócić na ten sam adres, na ten sam portfel kryptoaktywów).

Powyższy środek bezpośredniej ochrony praw podmiotowych posiadaczy kryptoaktywów został ukształtowany z naciskiem na efektywne odzyskanie spełnionego świadczenia. Jeżeli posiadacz kryptoaktywów odstępuje od umowy, to powinien spełnione świadczenia odzyskać, a oświadczenie o odstąpieniu od umowy może złożyć samodzielnie i bez dodatkowych obwarowań administracyjnych.

4.2. Prawo do żądania wykupu tokenów

Prawo do żądania wykupu tokenów pod względem swoich ogólnych założeń konstrukcyjnych przypomina prawo żądania wykupu obligacji, przysługujące obligatariuszowi na wypadek popadnięcia emitenta w chociażby przejściową niewypłacalność na podstawie przepisu art. 74 ust. 2 ustawy o obligacjach 2015 (szerzej zob. Godlewski & Sójka, 2022; Ernt-Staniulis & Rudnicki, 2019). Na poziomie rozporządzenia MiCA prawo do żądania wykupu (pojęcie prawne) zostało przewidziane w dwóch przypadkach – dla posiadaczy tokenów powiązanych z aktywami (art. 39) oraz dla posiadaczy tokenów będących e-pieniądzem (art. 49). Trzeba powiedzieć, że analogiczne uprawnienia nie są przewidziane na poziomie polskiej ustawy o kryptoaktywach. Dlatego w polskiej praktyce będą one stosowane wprost, z racji bezpośredniego stosowania przepisów rozporządzenia MiCA.

Jeżeli chodzi o konstrukcję prawną prawa do żądania wykupu przysługującego posiadaczom tokenów powiązanych z aktywami, to w świetle przepisu art. 39 ust. 2 rozporządzenia MiCA na żądanie posiadacza tokena powiązanego z aktywami emitent takiego tokena dokonuje jego wykupu poprzez zapłatę kwoty środków pieniężnych innych niż pieniądz elektroniczny, odpowiadającej wartości rynkowej aktywów powiązanych z posiadanym tokenem powiązanym z aktywami, albo poprzez przekazanie aktywów powiązanych z tym tokenem. Przesłanką powstania tego roszczenia jest przynajmniej przejściowa niewypłacalność, ponieważ posiadaczom tokenów powiązanych z aktywami przysługuje w każdym momencie prawo do żądania wykupu wobec

emitentów tokenów powiązanych z aktywami oraz w odniesieniu do aktywów rezerwowych, jeżeli emitenci nie są w stanie wywiązać się ze swoich obowiązków (art. 39 ust. 1 rozporządzenia MiCA). Użyte w treści tego ostatniego przepisu sformułowanie „w każdym momencie" należałoby wykładać funkcjonalnie, z tym skutkiem, aby posiadaczowi tokenów powiązanych z aktywami przedmiotowe roszczenie przysługiwało od momentu powzięcia wiedzy o niewypłacalności albo zagrożeniu wypłacalności emitenta aż do momentu uzyskania faktycznego zaspokojenia poprzez spełnienie świadczenia ze skutkiem zwalniającym emitenta ze zobowiązania.

Wzmocnienie sytuacji prawnej posiadacza tokenów powiązanych z aktywami zostało osiągnięte za pomocą dwóch środków prawnych. Pierwszym z nich jest obowiązek opracowania przez emitenta „polityki dotyczącej stałego prawa do żądania wykupu" (art. 39 ust. 2 zdanie drugie rozporządzenia MiCA), w istocie sprowadzającej się do określenia zasad spełnienia przez emitenta świadczenia na żądanie posiadacza tokenów. Drugim środkiem jest zakaz świadczenia w miejsce wypełnienia (czyli zakaz *datio in solutum*), które może być dopuszczalne tylko po spełnieniu dodatkowych przesłanek (określonych w art. 39 ust. 2 zdanie trzecie rozporządzenia MiCA).

Dodatkowym środkiem wzmacniającym sytuację prawną posiadacza tokenów powiązanych z aktywami – o charakterze administracyjnym, czyli pośrednim – jest opracowanie planu wykupu (pojęcie prawne). Na podstawie przepisu art. 47 ust. 1 rozporządzenia MiCA emitent tokena powiązanego z aktywami sporządza i utrzymuje plan operacyjny z myślą o uporządkowanym wykupie każdego tokena powiązanego z aktywami, który to plan ma zostać wdrożony na podstawie decyzji właściwego organu stwierdzającej, że emitent nie jest lub prawdopodobnie nie będzie w stanie wypełnić swoich obowiązków, w tym w przypadku niewypłacalności lub w innych stosownych przypadkach (restrukturyzacja, uporządkowana likwidacji, cofnięcie zezwolenia udzielonego emitentowi). W świetle przepisu art. 47 ust. 2 rozporządzenia MiCA plan wykupu ma wykazywać zdolność emitenta tokena powiązanego z aktywami do dokonania wykupu pozostającego w obrocie wyemitowanego tokena powiązanego z aktywami bez narażania jego posiadaczy na nadmierne straty ekonomiczne oraz bez narażania stabilności rynków aktywów rezerwowych.

Jeżeli natomiast chodzi o konstrukcję prawną prawa do żądania wykupu przysługującego posiadaczom tokenów będących e-pieniądzem, to zostało ono ukształtowane analogicznie jak prawo posiadacza pieniądza elektronicznego do żądania wykupu w dowolnym momencie i według wartości nominalnej wartości pieniężnej posiadanego pieniądza elektronicznego na podstawie dyrektywy 2009/110/WE. W świetle przepisu art. 49 ust. 2 rozporządzenia MiCA posiadaczom tokenów będących e-pieniądzem przysługuje roszczenie wobec emitentów takich tokenów będących e-pieniądzem. Z przepisu art. 49 ust. 4 rozporządzenia MiCA wynika zaś, że na wniosek posiadacza tokena będącego e-pieniądzem emitent tego tokena będącego e-pieniądzem wykupuje go – w każdym czasie i według wartości nominalnej – poprzez zapłatę warto-

ści pieniężnej posiadanego tokena będącego e-pieniądzem jego posiadaczowi w środkach pieniężnych innych niż pieniądz elektroniczny.

Szczegółowe zasady wykupu nie zostały określone na poziomie rozporządzenia MiCA, ponieważ emitenci tokenów będących e-pieniądzem mają określić warunki wykupu w dokumencie informacyjnym (art. 49 ust. 5 rozporządzenia MiCA). Ta kategoria emitentów została jednak zobowiązana do opracowania planu wykupu, na zasadach analogicznych jak w przypadku emitentów tokenów powiązanych z aktywami, co wynika z wewnętrznego odesłania (art. 55 rozporządzenia MiCA).

Powyższe środki bezpośredniej ochrony posiadaczy kryptoaktywów zostały ukształtowane z naciskiem na efektywne uzyskanie świadczenia. Jeżeli posiadacz kryptoaktywów żąda spełnienia świadczenia (żąda wykupu tokena), to powinien świadczenie otrzymać, a z żądaniem spełnienia świadczenia (żądaniem wykupu tokena) może wystąpić samodzielnie i bez dodatkowych obwarowań administracyjnych.

5. Środki prawne bezpośredniej ochrony przewidziane w polskiej ustawie o kryptoaktywach

Przewidziany w prawie polskim model ochrony nabywcy lub posiadacza kryptoaktywów nie przewiduje wyżej scharakteryzowanych środków bezpośredniej ochrony naruszonych albo zagrożonych praw, lecz spiętrzenie obowiązków publicznoprawnych obciążających przedsiębiorców z sektora kryptowalutowego oraz wprowadzenie bardzo surowych sankcji administracyjnych i karnych. Najwyższa administracyjna kara pieniężna, którą może zostać obciążona osoba zawodowo pośrednicząca w zawieraniu transakcji lub realizująca transakcje związane z kryptoaktywami, została ustalona na poziomie 66 852 000 złotych. To niewątpliwie suma rekordowa. Pewnym problemem przy wykładni przepisu art. 65 ust. 1 pkt 1 polskiej ustawy o kryptoaktywach jest to, że pojęcie „osoba zawodowo pośrednicząca w zawieraniu transakcji lub realizująca transakcje związane z kryptoaktywami" jest zwrotem niedookreślonym, ponieważ nie zostało zdefiniowane – nawet na poziomie rozporządzenia MiCA, które mogłoby stanowić punkt odniesienia przy wykładni praktycznej w prawie polskim. To jeden z licznych niedostatków polskiej ustawy o kryptoaktywach.

Trzeba jednak przyznać, że taka formuła, czyli brak środków bezpośredniej ochrony, wynika z założeń legislacyjnych, ponieważ – jak już wskazano nieco wyżej – prawo polskie nie obejmuje przedmiotowym zakresem swojego unormowania tokenów innych niż tokeny powiązane z aktywami i tokeny będące e-pieniądzem, lecz tylko tokeny powiązane z aktywami oraz tokeny będące e-pieniądzem (art. 1 polskiej ustawy o kryptoaktywach). Dlatego w przepisach prawa polskiego brakuje regulacji prawnej instytucji prawa do odstąpienia przewidzianej w przepisie art. 13 rozporzą-

dzenia MiCA, ponieważ dotyczy ono nabycia tokenów innych (najniższej kategorii normatywnej).

Z założeń legislacyjnych wynika też, jak należy przyjąć, pominięcie unormowania wyżej scharakteryzowanego prawa do żądania wykupu tokenów – co wymaga krótkiego komentarza. Jeżeli bowiem chodzi o odpowiednik prawa do żądania wykupu tokenów przewidzianego w przepisie art. 39 rozporządzenia MiCA, to rzeczywiście taka instytucja nie została przewidziana, a polska ustawa o kryptoaktywach nie odsyła w żadnym zakresie do przepisu art. 39 rozporządzenia MiCA. Z tego wynika, że posiadacz tokenów powiązanych z aktywami nie może domagać się zaspokojenia swoich roszczeń na wypadek powzięcia informacji o niewypłacalności albo grożącej niewypłacalności emitenta na podstawie prawa polskiego. Trzeba przyznać, że to istotny niedostatek. Osoba uprawniona musi poszukiwać podstawy prawnej w bezpośrednio stosowanym przepisie art. 39 rozporządzenia MiCA.

Natomiast jeżeli chodzi o drugą kategorię tokenów objętych instytucją prawa do żądania wykupu tokenów, czyli o tokeny będące e-pieniądzem, to w tym przypadku również polska ustawa o kryptoaktywach nie odsyła do przepisów art. 49 rozporządzenia MiCA – ale przewiduje sankcje za naruszenie tego przepisu. Z tego wynika – chociaż wprawdzie pośrednio – że posiadaczowi tokenów będących e-pieniądzem przysługuje prawo do żądania wykupu tokenów tej kategorii normatywnej, ale z dwoma zastrzeżeniami.

Po pierwsze, podstawa prawna tej prerogatywy tkwi w bezpośrednio stosowanym przepisie art. 49 rozporządzenia MiCA. Po drugie, fakt przysługiwania tego uprawnienia wynika z objęcia sankcją faktu naruszenia tego obowiązku przez osobę zobowiązaną do jego przestrzegania. Stosowne odesłania ustawowe do przepisu art. 49 rozporządzenia MiCA zostały przewidziane w następujących przepisach sankcjonujących: art. 48 ust. 1, art. 49 ust. 1, art. 61 ust. 1, art. 67 pkt 1 polskiej ustawy o kryptoaktywach.

Wnioski

Przedstawione powyżej refleksje są podstawą umiarkowanie optymistycznej oceny aktualnego modelu ochrony praw podmiotowych nabywców i posiadaczy kryptoaktywów w prawie polskim. Przyjęte rozwiązania nie zapewniają ochrony w pełni efektywnej. Całkowite wyeliminowanie źródeł zagrożeń i nadużyć jest w praktyce niemożliwe, ponieważ czynności prawne dotyczące kryptoaktywów dokonywane są w przestrzeni internetowej i ponad granicami państwowymi. Przyjęty model ochrony może przyczynić się do wyeliminowania niektórych źródeł zagrożeń, ale tylko tych, które pozostają w granicach jurysdykcji prawa polskiego oraz prawa europejskiego.

Analiza stanu prawa obowiązującego wskazuje na to, że model ochrony nabywców i posiadaczy kryptoaktywów jest charakterystyczny dla dzisiejszych czasów, a środki ochrony bezpośredniej praw podmiotowych z pewnością są niewystarczające.

Przepisy polskiej ustawy o kryptoaktywach nie przewidują bezpośrednich uprawnień dla nabywców i posiadaczy kryptoaktywów. Odpowiedź na pytanie: „czy chronić?" – jest jednoznaczna. Nadal otwarte pozostaje jednak pytanie: „w jaki sposób?"

Trzeba z rezygnacją powiedzieć, że ochrona „konsumentów" w obrocie kryptoaktywami będzie iluzoryczna z poziomu rozwiązań przewidzianych w prawie polskim wszędzie tam, gdzie prawo polskie nie będzie mogło zostać zastosowane. Trudno tej praktycznej bolączce przeciwstawić się w dążeniu do roztoczenia ochrony praw podmiotowych nabywców i posiadaczy aktywów kryptograficznych w Polsce za pomocą radykalnych środków normatywnych o charakterze administracyjnym. Cóż przyjdzie bowiem z wyposażenia Komisji Nadzoru Finansowego w silne narzędzia licencyjne i nadzorczo-kontrolne, jeżeli krąg podmiotów nadzorowanych będzie znikomy? Cóż przyjdzie z dokonywania wpisów na listę ostrzeżeń publicznych prowadzoną przez KNF, jeżeli majątek osób wpisanych na tę listę nie będzie obejmował składników możliwych do późniejszego wyegzekwowania? Jakie praktyczne znaczenie może mieć zawiadomienie jednostki prokuratury o podejrzeniu popełnienia przestępstwa popełnionego przy użyciu zapewniającej anonimowość łączności internetowej? Do czego może doprowadzić wyśledzenie przez wyspecjalizowanego informatyka miejsca (portfela, adresu, *walleta*), do którego trafiły skradzione przez hakera kryptoaktywa wówczas, gdy nie da się ustalić tożsamości hakera ani tego, czy posiada rachunek bankowy? Jak wreszcie przeciwstawiać się klauzulom abuzywnym w regulaminach platform handlu internetowego wówczas, gdy siedziba podmiotu prowadzącego taką platformę znajduje się poza granicami Unii Europejskiej?

Te retoryczne pytania można mnożyć. W trakcie ogólnodostępnych społecznych konsultacji nad projektem polskiej ustawy o kryptoaktywach liczna rzesza podmiotów zainteresowanych zgłaszała różne uwagi szczegółowe (zob. tabele uwag do projektu ustawy o kryptoaktywach z 2024). Znamienne jest to, że tylko jeden organ stanowczo postulował wprowadzenie rozwiązań prowadzących do wzmocnienia sytuacji prawnej nabywcy i posiadacza aktywów kryptograficznych. Co ciekawe – nie była to Komisja Nadzoru Finansowego, lecz Rzecznik Finansowy. Nie można się łudzić co do tego, że środki prawne, którymi dysponuje Rzecznik Finansowy na podstawie ustawy o rozpatrywaniu reklamacji przez podmioty rynku finansowego, o Rzeczniku Finansowym i o Funduszu Edukacji Finansowej 2015, będą środkami wystarczającymi. Zbudowanie skutecznego systemu ochrony przed nadużyciami w obrocie aktywami kryptograficznymi nie jest zadaniem prostym. Aktualny jednak pozostaje postulat dbałości o własne sprawy. Od wielu lat jestem zwolennikiem powiedzenia, aby nie robić rzeczy, których się nie rozumie. Dlatego uważam, że podstawowym środkiem ochrony nabywców i posiadaczy aktywów kryptograficznych jest pogłębiona edukacja.

BIBLIOGRAFIA

Adamus, R. (2018). Kilka uwag o skutkach odstąpienia od umowy, *Rejent,* 7, 9-20.

Czech, T. (2016). Konsumenckie uprawnienie do odstąpienia od umowy zawartej na odległość lub poza lokalem przedsiębiorstwa, *Temidium* 3, 47–51.

Czech, T. (2020). Komentarz do art. 27 w: T. Czech (red.), *Prawa konsumenta. Komentarz*. Lex.

Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE, Dz. Urz. UE z 10.10.2009 r., L 267/7.

Ernt-Staniulis, K. & Rudnicki, S. (2019) Komentarz do art. 74 [w:] M. Wierzbowski (red.), *Ustawa o obligacjach. Komentarz*. Legalis.

Europejski Bank Centralny. (2012). *Virtual Currency Schemes*, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [wejście dnia 13 grudnia 2024 roku].

Godlewski, M. & Sójka, T. (2022). Komentarz do art. 74 w: T. Sójka (red.),*Ustawa o obligacjach. Komentarz*. Legalis.

Jabłoński, Z. (2017). Ustawowe prawo odstąpienia – skutki prawnorzeczowe, *Rejent,* 2, 73–87.

Jastrzębski, J. (2022). Czy inwestor indywidualny na rynku kapitałowym jest konsumentem? *PUG,* 4, 45–53.

Karkut, D. (2018). *Własność wirtualna w prawie polskim. Zagadnienia wybrane*, Wrocław.

Kocot, W. J. & Kondek, J. M. (2014). Nowe zasady zawierania umów z udziałem konsumenta, cz. II, *PPH,* 12, 4–10.

Kukuryk, P. (2014). Definicje konsumenta w kodeksie cywilnym (obecnym i przyszłym) w kontekście najnowszych unijnych dyrektyw konsumenckich, *PPH,* 5, 18–25.

Mleczak, J. (2017). Skutek rzeczowy odstąpienia od umowy. *Palestra, 62*(12), 53-62.

Osajda, K. (2021). Ochrona inwestora – konsumenta na rynku instrumentów finansowych (rynku kapitałowym), *PiP,* 4, 22–38.

Osajda, K. (2022). Granice statusu konsumenta w prawie cywilnym – perspektywa temporalna oraz kwestia niedokonania czynności prawnej, *PS,* 11/12, 41–53.

Izba Skarbowa w Katowicach. (2013). Pismo Izby Skarbowej w Katowicach z dnia 14 listopada 2013 r., IBPP2/443–762/13/ICz.

Projekt ustawy o kryptoaktywach z dnia 22 lutego 2024 roku (numer w wykazie prac legislacyjnych i programowych Rady Ministrów: UC2), uwzględniający stan zaawansowania prac na dzień 31 grudnia 2024 roku.

Rezolucja Parlamentu Europejskiego z dnia 26 maja 2016 r. w sprawie wirtualnych walut (2016/2007(INI), https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016IP0228&from=CS [wejście dnia 13 grudnia 2024 roku].

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz

dyrektyw 2013/36/UE i (UE) 2019/1937, Dz. Urz. UE z 9.6.2023 r., L 150/40 (rozporządzenie MiCA).

Rydz, K. (2023). Pozycja prawna wspólnika lub akcjonariusza spółki handlowej a status konsumenta. Analiza z uwzględnieniem koncepcji prezentowanych na tle prawa niemieckiego i austriackiego, TPP 1, 101–156.

Sejm Rzeczypospolitej Polskiej. (2018). Ustawa z dnia 1 marca 2018 roku o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu (tekst jedn. Dz.U. z 2024 r., poz. 850, 1222 ze zm.).

Sejm Rzeczypospolitej Polskiej. (1964). Ustawa z dnia 23 kwietnia 1964 roku – Kodeks cywilny (tekst jedn. Dz.U. z 2024 r., poz. 1061, 1237 ze zm.).

Sejm Rzeczypospolitej Polskiej. (1991). Ustawa z dnia 26 lipca 1991 roku o podatku dochodowym od osób fizycznych (tekst jedn. Dz.U. z 2024 r., poz. 226, 232, 854, 858, 859, 863, 1572, 1585, 1593, 1615, 1635 ze zm.).

Sejm Rzeczypospolitej Polskiej. (2018). Ustawa z dnia 6 marca 2018 roku – Prawo przedsiębiorców (tekst jedn. Dz.U. z 2024 r., poz. 236, 1222 ze zm.).

Uzasadnienie projektu ustawy o kryptowaktywach z dnia 22 lutego 2024 roku dostępne na https://legislacja.rcl.gov.pl/projekt/12382311/katalog/13040399 [wejście dnia 13 grudnia 2024 roku]; tabele uwag do projektu ustawy o kryptoaktywach dostępne na https://legislacja.rcl.gov.pl/projekt/12382311/katalog/13040399 [wejście dnia 13 grudnia 2024 roku].

Wyczik, J. (2022). Dobra wirtualne z perspektywy użytkowników i dostawców treści. Prawne uwarunkowania obrotu, Legalis [wejście dnia 13 grudnia 2024 roku].

Zacharzewski, K. (2021). Digital Asset Capital Market Law: A New Discipline of Private Law, *Krytyka Prawa, 2*(13), 195–208.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.07
Received: 22.06.2025
Accepted: 30.06.2025

Paweł Czaplicki
Uniwersytet w Białymstoku, Polska
p.czaplicki@uwb.edu.pl
ORCID ID: https://orcid.org/0000-0002-9782-7252

Stosowanie Rozporządzenia DLT Pilot Regime w polskim i francuskim porządku prawnym – analiza prawnoporównawcza

The Application of the DLT Pilot Regime in the Polish and French Legal Systems: A Comparative Analysis

Abstract: This article addresses the issue of applying the DLT Pilot Regime Regulation in the realities of national legal orders. The Polish and French legislation is analysed, using the dogmatic and comparative legal methods. The main objective of the article is to attempt to answer two questions: firstly, whether the scope of application of the DLT Pilot Regime Regulation allows the use of the potential of blockchain technology on the EU financial instruments markets, and secondly, to what extent it is possible to apply the solutions provided for in the DLT Pilot Regime Regulation in the realities of national legal orders. The following theses are put forward in the study: firstly, the scope of application of the Regulation has been excessively limited and does not allow the use of the full potential of distributed ledger technology on financial markets. Secondly, in the case of the Polish legal system, even the amendments to the legal provisions introduced in connection with the entry into force of the Regulation do not allow the full application of the solutions provided for therein. Solutions that guarantee the possibility of a wider use of tools available on the basis of the DLT Pilot Regime Regulation are provided for in the French legal system. The study shows that these are solutions that could be considered by the Polish legislature.

Keywords: blockchain, distributed ledger technology, DLT Pilot Regime, financial instruments, financial markets
Słowa kluczowe: blockchain, technologia rozproszonego rejestru, DLT Pilot Regime, instrumenty finansowe, rynki finansowe

© 2025 Paweł Czaplicki published by Sciendo. This work is licensed under the Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 License.

Wprowadzenie

Rozporządzenie DLT Pilot Regime, czyli rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/858 z dnia 30 maja 2022 r. w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, obowiązuje od dnia 23 marca 2023 r. Program został przewidziany na okres 3 lat, z możliwością przedłużenia lub odnowienia do łącznie 6 lat. Podstawowym założeniem rozporządzenia było umożliwienie dematerializacji, obrotu, rozliczania i rozrachunku określonych instrumentów finansowych w infrastrukturze systemów rejestrów rozproszonych z pominięciem wymogów MIFID, MIFIR oraz CSDR, czyli w realiach polskiego systemu prawnego wymogów stawianych przede wszystkim przez przepisy prawa ujęte w ustawie z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi. Rozporządzenie miało być ogromną szansą na popularyzację technologii rejestrów rozproszonych i wykorzystania ich do emisji tradycyjnych instrumentów finansowych. Pierwotnie dawało nadzieje na zrewolucjonizowanie rynków finansowych w aspekcie obracania na nich instrumentami finansowymi. Tym bardziej, że stanowiło element szerszych działań organów szczebla unijnego, które miały na celu uporządkowanie pod kątem prawnym rynku kryptowalut na terenie całej Unii Europejskiej (Hrabčák & Štrkolec, 2024, s. 27–45).

Podkreślenia wymaga również fakt, że możliwości, które daje rozporządzenie DLT Pilot Regime, i związane z nimi liczne obostrzenia oraz ograniczenia wymagały od ustawodawców krajowych dostosowania rodzimych regulacji do potrzeb wynikających z treści Rozporządzenia DLT Pilot Regime. Polski ustawodawca dokonał tego ustawą z dnia 16 sierpnia 2023 r. o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku. Stosowne rozwiązania w tym zakresie zostały również wprowadzone do francuskiego systemu prawa i przewiduje je przede wszystkim francuski *Code monétaire et financier*. Wyjaśnienia wymaga również to, że wybór prawa francuskiego jako materiału prawnoporównawczego był podyktowany przede wszystkim tym, że przewiduje ono bardziej elastyczne zasady stosowania rozporządzenia DLT Pilot Regime na gruncie krajowym w porównaniu z rozwiązaniami przewidzianymi przez polskiego ustawodawcę. Stąd też przepisy prawa francuskiego stanowiły dobry punkt odniesienia do przepisów obowiązujących w Polsce w kontekście rozważań nad potencjalną potrzebą ich nowelizacji.

Analiza treści rozporządzenia oraz wskazanych powyżej regulacji krajowych, która w szczegółowy sposób została zaprezentowana poniżej, uprawnia do postawienia dwóch podstawowych hipotez badawczych. Po pierwsze, iż zakres zastosowania rozporządzenia DLT Pilot Regime został nadmiernie ograniczony i nie pozwala na wykorzystanie w pełni potencjału technologii rejestrów rozproszonych na rynkach finansowych. Po drugie, że w przypadku polskiego sytemu prawa wprowadzone w związku z wejściem w życie rozporządzenia DLT Pilot Regime nowelizacje przepisów prawa nie pozwalają na pełne zastosowanie rozwiązań w nim przewidzianych.

Rozwiązania gwarantujące możliwości szerszego wykorzystania narzędzi przewidzianych w rozporządzeniu DLT Pilot Regime ustanowiono natomiast we francuskim porządku prawnym. W opracowaniu starano się wykazać, że są to rozwiązania, na których mógłby wzorować się polski ustawodawca.

1. Podstawowe założenia Rozporządzenia DLT Pilot Regime i ich ocena

W pierwszej kolejności należy zwrócić uwagę na słusznie podnoszony w piśmiennictwie fakt, że Rozporządzenie DLT Pilot Regime jedynie w bardzo ograniczonym zakresie pozwala na wykorzystanie zalet aktywów cyfrowych usytuowanych w środowisku rejestrów rozproszonych (Tomczak, 2024, s. 34–37). W oparciu o przedstawione przez przywołanego autora zestawienie przymiotów kryptoaktywów należy stwierdzić, iż w realiach rozporządzenia cechy, takie jak istnienie aktywów poza powszechnym systemem obrotu, anonimowość inwestorów czy też brak kosztów transakcji, nie funkcjonują w ogóle. Natomiast cechy kryptoaktywów, takie jak decentralizacja (brak pośredników), bezpieczeństwo obrotu, nieodwracalność transakcji, natychmiastowość transakcji, zostały przewidziane jedynie częściowo.

Kolejnym zasadniczym mankamentem Rozporządzenia DLT Pilot Regime jest to, że na mocy rozwiązań zastosowanych w rozporządzeniu możliwe jest wprowadzenie do obrotu i obracanie z wykorzystaniem infrastruktury systemów rejestrów rozproszonych jedynie akcjami, których kapitalizacja rynkowa lub niepewna kapitalizacja rynkowa jest niższa niż 500 mln euro, obligacjami, innymi formami sekurytyzowanego długu, w tym kwitami depozytowymi w odniesieniu do takich papierów wartościowych, lub instrumentami rynku pieniężnego, o wielkości emisji poniżej 1 mld euro, z wyłączeniem tych, które zawierają instrument pochodny lub które posiadają strukturę utrudniającą klientowi zrozumienie związanego z tym ryzyka, oraz jednostkami uczestnictwa w przedsiębiorstwach zbiorowego inwestowania, których wartość rynkowa zarządzanych aktywów jest niższa niż 500 mln euro. Zastosowane w rozporządzeniu rozwiązania zawierają więc dwa podstawowe ograniczenia. Po pierwsze, przewidziano ograniczenie w zakresie kategorii instrumentów finansowych, które mogą zostać wprowadzone do obrotu z wykorzystaniem technologii rejestrów rozproszonych. Po drugie, w stosunku do tych aktywów, które zostały objęte rozporządzeniem, ustalono przywołane powyżej limity kwotowe. Co więcej, również krąg podmiotów, które mogą zostać uprawnione do prowadzenia platform obsługi aktywów funkcjonujących w środowisku rejestrów rozporoszonych, został ograniczony do firm inwestycyjnych, depozytów i operatorów rynków regulowanych. Powyższe rozwiązania należy ocenić negatywnie z uwagi na to, że nie pozwalają wykorzystać w pełni możliwości technologii blockchain na rynku finansowym. Oczywiście należy mieć świadomość tego, że jest to program pilotażowy, jednakże

ograniczenie potencjału wykorzystania technologii rozproszonych rejestrów już na samym początku wdrażania go na rynki finansowe może spowodować nikłe zainteresowanie programem, a tym samym – nie przynieść wymiernych wyników w zakresie zbadania realnego zapotrzebowania na kompleksowe zastosowanie tego typu rozwiązań na rynkach finansowych. Słuszność tej tezy potwierdza fakt, że przez pierwszy rok obowiązywania rozporządzenia pilotażowego żaden podmiot na terenie całej Unii Europejskiej nie został uprawniony do przeprowadzenia emisji i wprowadzenia do obrotu aktywów w oparciu o zasady w nim przewidziane, zaś wniosków o wydanie stosownego zezwolenia było zaledwie kilka (Ledger Insights, 2024). Co więcej, dotychczas (stan na koniec czerwca 2025 r.) zarejestrowano łącznie jedynie trzy takie podmioty: dwa w Niemczech i jeden w Czechach (ESMA, 2025). Również na gruncie polskim możliwości zagwarantowane przez rozporządzenie DLT Pilot Regime spotkały się z negatywnym przyjęciem. Stanowisko to potwierdza choćby komunikat Krajowego Depozytu Papierów Wartościowych, zgodnie z którym z końcem 2022 r. podjęto decyzję o nieprzystępowaniu do programu, m.in. ze względu na jego ostatecznie bardzo konserwatywny charakter oraz ograniczony horyzont czasowy (Krajowy Depozyt Papierów Wartościowych, 2023).

Z uwagi na wskazane powyżej dwa elementy, tj. brak wykorzystania pełnego potencjału technologii rejestrów rozproszonych oraz ograniczony zakres zastosowania rozporządzenia, wprowadzenie go do unijnego porządku prawnego należy uznać za co prawda krok słuszny, ale zbyt zachowawczy.

2. Wdrożenie rozporządzenia DLT Pilot Regime do polskiego porządku prawnego

Mimo wskazanych powyżej ogólnych wad konstrukcyjnych rozporządzenia ustawodawcy krajowi musieli zmierzyć się z dostosowaniem przepisów krajowych do jego potrzeb. Wdrożenie rozporządzenia DLT Pilot Regime odbyło się na gruncie polskiego systemu prawa w oparciu o ustawę z dnia 16 sierpnia 2023 r. o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku. W artykule zostaną omówione trzy kluczowe aspekty funkcjonowania w obrocie aktywów emitowanych na bazie rozporządzenia DLT Pilot Regime, tj. warunki ubiegania się o zezwolenie na ich emisję i obrót, zasady ich rejestrowania oraz pośredniczenia w obrocie nimi.

W pierwszej kolejności należy zwrócić uwagę na treść art. 131za ustawy o obrocie instrumentami finansowymi, który przewiduje podmioty uprawnione do prowadzenia platform obrotu aktywami opartych na DLT. Zgodnie z regulacjami obowiązującymi w polskim prawodawstwie alternatywny system obrotu oparty na DLT albo TSS oparty na DLT, na zasadach określonych w rozporządzeniu DLT Pilot Regime, może prowadzić wyłącznie spółka prowadząca rynek regulowany, Krajowy Depozyt Papie-

rów Wartościowych, centralny depozyt papierów wartościowych oraz firma inwestycyjna. Natomiast w art. 131zb przewidziano, że podmioty wskazane w art. 8 ust. 2 (osoba prawna występująca o zezwolenie jako firma inwestycyjna lub o zezwolenie na prowadzenie rynku regulowanego), art. 9 ust. 2 (osoba prawna występująca o zezwolenie jako centralny depozyt papierów wartościowych) oraz art. 10 ust. 2 (osoba prawna występująca o zezwolenie jako firma inwestycyjna lub o zezwolenie na prowadzenie rynku regulowanego lub jako centralny depozyt papierów wartościowych) rozporządzenia DLT Pilot Regime mogą wystąpić do Komisji Nadzoru Finansowego o specjalne zezwolenie na prowadzenie platformy obrotu aktywami podlegającymi regulacji rozporządzenia. Jednocześnie zastrzeżono, że wraz z wnioskiem o jego udzielenie przywołane powyżej podmioty mają obowiązek złożenia do KNF wniosku o udzielenie zezwolenia na prowadzenie odpowiednio działalności maklerskiej, rynku regulowanego albo centralnego depozytu papierów wartościowych. Co istotne, Komisja – odmawiając udzielenia zezwolenia na prowadzenie działalności maklerskiej, rynku regulowanego albo centralnego depozytu papierów wartościowych – ma jednocześnie obowiązek odmówienia udzielenia specjalnego zezwolenia. Dodatkowo, przywołane powyżej regulacje nie wskazują dokładnie, jakie wymogi miałyby takie podmioty spełniać, ponieważ zostało to szczegółowo określone w treści samego rozporządzenia. W konsekwencji, wątpliwości odnośnie tego, w jakich właściwie sytuacjach Komisja Nadzoru Finansowego miałaby podstawy do odmowy udzielenia zezwolenia na prowadzenie działalności maklerskiej, rynku regulowanego albo centralnego depozytu papierów wartościowych, co musiałoby skutkować również odmową udzielenia specjalnego zezwolenia, należy również rozstrzygać na gruncie samego rozporządzenia. Biorąc pod uwagę to, że zgodnie z oczekiwaniami rozporządzenie DLT Pilot Regime miało dać możliwości korzystania z technologii rejestrów rozproszonych jak najszerszemu kręgowi podmiotów spoza tradycyjnego rynku kapitałowego, przedstawione powyżej rozwiązania zastosowane przez unijnego, a w konsekwencji polskiego ustawodawcę mogą w zasadzie w praktyce uniemożliwić osiągnięcie tego celu.

W kontekście zasad rejestrowania aktywów emitowanych w oparciu o rozwiązania przewidziane w rozporządzeniu DLT Pilot Regime trzeba wskazać, że polski ustawodawca jednoznacznie oddzielił instrumenty finansowe funkcjonujące w standardowym obrocie od tych pozostających w strukturze rejestru rozproszonego. W konsekwencji tego sprawił, że potencjalny rynek kryptoaktywów emitowanych na bazie rozporządzenia zostanie odseparowany od standardowego rynku kapitałowego – co wcale nie oznacza, że nie będzie podlegał wymogom stawianym na tym rynku. W myśl art. 131s ustawy o obrocie instrumentami finansowymi papiery wartościowe będące instrumentami finansowymi obsługiwanymi przez DLT są rejestrowane w SS opartym na DLT albo w TSS opartym na DLT na rachunkach DLT albo – jeżeli zezwolenie na prowadzenie SS opartego na DLT albo TSS opartego na DLT zwalnia podmiot prowadzący SS oparty na DLT albo TSS oparty na DLT z obowiązku prowadzenia rachunków DLT

– w ewidencji DLT. Co istotne, rachunek DLT oraz ewidencja DLT mogą być prowadzone wyłącznie przez podmiot posiadający zezwolenie na prowadzenie SS opartego na DLT albo TSS opartego na DLT. Słusznie w piśmiennictwie zwraca się uwagę na fakt, że definicja rachunku DLT nie została wprowadzona do rozporządzenia i pojęcie to jest dziełem wyłącznie polskiego ustawodawcy (DLKLegal, 2023). Co istotne, polski ustawodawca zastrzegł także, że zarówno rachunek DLT, jak i ewidencja DLT musi zapewniać jednoznaczną i nieodwracalną identyfikację papierów wartościowych zapisanych w tej ewidencji oraz osoby uprawnionej z tych papierów wartościowych, a także liczby papierów wartościowych przysługujących tej osobie. Oznacza to, że niezależnie od sposobu ewidencjonowania aktywów uczestnicy obrotu zostali pozbawieni możliwości zachowania anonimowości. W art. 131w ustanowiono natomiast zasadę autonomiczności poszczególnych rejestrów. Zgodnie z jego treścią akcje tej samej spółki nie mogą być jednocześnie zarejestrowane na rachunku DLT oraz w ewidencji DLT, co wydaje się być naturalną konsekwencją wskazanych powyżej rozwiązań. Natomiast dodatkowo, akcje tej samej spółki zarejestrowane na rachunku DLT albo w ewidencji DLT nie mogą być jednocześnie zarejestrowane w rejestrze akcjonariuszy, o którym mowa w art. 328^1 § 1 k.s.h. oraz w depozycie papierów wartościowych. Oznacza to, że spółka funkcjonująca w oparciu o akcje musi zdecydować o wyborze wyłącznie jednego reżimu prawnego – tradycyjnego lub w oparciu o technologię DLT – funkcjonowania jej praw udziałowych. Dotyczy to także akcji wyemitowanych już wcześniej, gdyż ustawodawca na gruncie art. 131z ustawy o obrocie instrumentami finansowymi dopuścił tzw. wtórną rejestrację akcji w strukturze rejestru rozproszonego. Przy czym od razu należy zauważyć, że zgodnie z treścią przywołanego przepisu przedmiotem wtórnej rejestracji DLT mogą być wyłącznie akcje spółki niebędącej spółką publiczną zarejestrowane w rejestrze akcjonariuszy. Tym samym ustawodawca wyłączył kolejne dwie istotne grupy podmiotów – wszystkie spółki publiczne i spółki niepubliczne, których akcje są zarejestrowane w depozycie – z możliwości skorzystania z rozwiązań przewidzianych w rozporządzeniu pilotażowym. Biorąc pod uwagę to, że rozporządzenie DLT Pilot Regime jest programem pilotażowym, jest to kolejny argument potwierdzający tezę, że szczegółowe rozwiązania stosowania rozporządzenia w Polsce zniechęcają, a czasami wręcz uniemożliwiają skorzystanie z przewidzianych w nim narzędzi. Po pierwsze, spółki, których funkcjonowanie oparte jest na akcjach, nie mogą przeprowadzić w ramach pilotażu konkretnej emisji akcji z wykorzystaniem technologii rejestru rozproszonego, co być może pozwoliłoby na przekonanie się do niej w pełnym wymiarze. Po drugie, dla wielu spółek całkowite przejście na funkcjonowanie w środowisku blockchain może wydawać się zbyt ryzykowne i kosztowne. Wynika to z tego, że rozporządzenie DLT Pilot Regime umożliwiające taki krok jest rozwiązaniem tymczasowym i nie wiadomo, jakie będzie podejście unijnego ustawodawcy do tej kwestii po zakończeniu programu. W przypadku wielu spółek może rodzić się obawa, czy po upływie czasu, na jaki został przewidziany program, nie będzie konieczny powrót do klasycznych zasad ewidencjonowania akcji funkcjonujących w spółce. Dodatkowo, biorąc

pod uwagę ograniczenia kwotowe, spod reżimu rozporządzenia wyłączone zostały największe przedsiębiorstwa, które rzeczywiście dysponowałyby zasobami zarówno ludzkimi, jak i finansowymi do przeprowadzenia tego typu transformacji technologicznej. Wskazane powyżej regulacje dotyczące konieczności wyboru wyłącznie jednej formy ewidencjonowania wyemitowanych papierów wartościowych stosuje się odpowiednio do obligacji tej samej serii. Oznacza to, że w przypadku obligacji emitent dysponuje już większą swobodą w podejmowaniu działań, ponieważ ograniczenia dotyczą wyłącznie emisji jednej serii obligacji, a nie wszystkich obligacji wyemitowanych przez określonego emitenta. Należy więc wysnuć wniosek, że jeden emitent może wyemitować obligacje zarówno korzystając z trybu standardowego, jak i z wykorzystaniem technologii rejestrów rozproszonych. Wyboru jednej ze ścieżek musi dokonać bowiem wyłącznie w ramach konkretnej emisji obligacji.

Biorąc pod uwagę specyfikę funkcjonowania instrumentów finansowych w środowisku rejestrów rozproszonych, zaskakujące jest to, że polski ustawodawca nie przewidział żadnych szczególnych zasad pośrednictwa w transakcjach, których przedmiotem są instrumenty finansowe wyemitowane i wprowadzone do obrotu w oparciu o regulacje rozporządzenia DLT Pilot Regime. Brakuje w polskim porządku prawnym reguł związanych choćby z udzielaniem dostępu do platform obsługi aktywów, w tym wydawania i posługiwania się kluczami kryptograficznymi. Polski ustawodawca nie przewidział także szczegółowych zasad przechowywania kryptoaktywów i odpowiedzialności za ich potencjalną utratę. W polskim prawodawstwie nie przewidziano żadnych szczególnych reguł dotyczących zapewniania bezpieczeństwa obrotu aktywami emitowanymi na bazie regulacji rozporządzenia DLT Pilot Regime, choć ich specyfika wskazywałaby na taką potrzebę. Nie uwzględniono w krajowych regulacjach również żadnych odrębnych reguł postępowania w przypadku naruszenia zasad dostępu do systemu i obrotu kryptoaktywami, podczas gdy ma to kluczowe znaczenie choćby dla ochrony danych osobowych uczestników systemu. Na potrzebę zwrócenia uwagi na ten aspekt funkcjonowania platform obrotu aktywami w oparciu o rozporządzenie DLT Pilot Regime i szczegółowego uregulowania zagadnień w tym zakresie zwracał uwagę m.in. Europejski Inspektor Ochrony Danych Osobowych (Wiewiórkowski, 2021).

3. Wdrożenie rozporządzenia DLT Pilot Regime do francuskiego porządku prawnego

Również francuski ustawodawca musiał przewidzieć stosowne ramy prawne do stosowania Rozporządzenia DLT Pilot Regime. Zostały one kompleksowo omówione w opracowaniu przygotowanym przez AMF (*Autorité des Marchés Financiers*)[1], tj. fran-

1 Na temat roli i miejsca AMF w dwufilarowym systemie nadzoru finansowego we Francji zobacz szerzej: Mariański (2016, s. 64–74) oraz Mariański (2023, s. 38–44).

cuski Urząd Nadzoru Finansowego (https://www.amf-france.org, 2025). Na uwagę zasługuje również fakt, że problematyka wdrażania technologii rejestrów rozproszonych na rynek finansowy jest przedmiotem rozważań także francuskiej doktryny prawa[2].

Pierwszym ważnym elementem wdrożenia rozporządzenia DLT Pilot Regime do francuskiego porządku prawnego są zasady uzyskiwania zezwolenia na obsługę emisji i obrót instrumentami finansowymi[3] w oparciu o zasady przewidziane w rozporządzeniu. Francuski ustawodawca przewidział w tym zakresie dwie ścieżki. Pierwsza obejmuje podmioty, które nie uzyskały wcześniej autoryzacji, zaś druga dotyczy podmiotów, które uzyskały uprzednio zezwolenia na prowadzenie działalności pośrednictwa na rynku finansowym i chciałyby skorzystać z możliwości przewidzianych w rozporządzeniu DLT Pilot Regime. W pierwszym przypadku wnioskodawcy, którzy nie posiadają jeszcze autoryzacji jako instytucja kredytowa świadcząca usługi inwestycyjne, firma inwestycyjna, operator rynku lub centralny depozyt papierów wartościowych, muszą złożyć wnioski do stosownych organów i przejść pełną procedurę autoryzacji. Natomiast podmioty, które są już upoważnione i chcą skorzystać z rozwiązań przewidzianych w rozporządzeniu DLT Pilot Regime, muszą jedynie uzyskać uprzednią zgodę właściwych organów na pośrednictwo w obrocie instrumentami finansowymi z wykorzystaniem technologii rejestrów rozproszonych. Co ciekawe, podmioty te mają m.in. obowiązek przedstawienia stosownym organom swojego projektu i przejścia procedury zbadania harmonogramu jego realizacji. Dopiero po realizacji wskazanego powyżej etapu możliwe jest złożenie formalnej aplikacji o wydanie zezwolenia. W końcu należy zauważyć w tym kontekście, że w dniu 8 marca 2023 r. Europejski Urząd Nadzoru Giełd i Papierów Wartościowych opublikował wytyczne dotyczące standardowych formularzy, formatów i szablonów do składania wniosków o zezwolenie na prowadzenie infrastruktury rynku DLT (ESMA, 2023), co znacząco ułatwia przejście procedur rejestracyjnych. Podsumowując, trzeba wskazać, że dwutorowość uzyskiwania uprawnień do emisji i obracania aktywami pod rządami rozporządzenia DLT Pilot Regime, jak już zostało to wykazane przy okazji omawiania polskiego porządku prawnego w tym zakresie, wynika z treści samego rozporządzenia, więc rozwiązania zastosowane przez polskiego i francuskiego ustawodawcę pozostają w tej materii co do zasady zbieżne.

Drugim istotnym elementem są zasady rejestrowania aktywów emitowanych w oparciu o zasady przewidziane w rozporządzeniu. Zgodnie z prawem francuskim tokeny lub instrumenty finansowe DLT dopuszczone do obrotu w infrastrukturze rynku DLT na mocy rozporządzenia DLT Pilot Regime mogą być rejestrowane na dwa spo-

2 Zobacz choćby Audit (2020, s. 669–694); Manzari & Wagner (2021, s. 7–10) oraz Sotiri (2024, s. 17–23).

3 Na temat systematyki pojęcia przedmiotu obrotu na rynku finansowym i zależności między określeniami: tytuł zbywalny, instrument finansowy, papier wartościowy, zobacz szerzej Lemonnier i in. (2011, s. 43–53) oraz Mariański & Lemonnier (2017, s. 181–191).

soby. Po pierwsze, jako „zarejestrowany instrument finansowy" zapisany w blockchainie na warunkach przewidzianych przez przepisy szczególne. W tej sytuacji podmiot odpowiedzialny za infrastrukturę danego rynku DLT zgodnie z rozporządzeniem DLT Pilot Regime jest zobowiązany do prowadzenia rejestru instrumentów finansowych DLT jako systemu rozliczeniowego DLT (DLT SS) lub systemu obrotu i rozliczeń DLT (DLT TSS) na rzecz emitenta. Drugim sposobem jest rejestracja aktywów jako „papieru wartościowego na okaziciela" zapisanego w blockchainie na warunkach określonych w rozporządzeniu DLT Pilot Regime. W każdym ze wskazanych powyżej dwóch przypadków infrastruktura rynku DLT (DLT SS lub DLT TSS) nie musi przechodzić autoryzacji w celu realizacji funkcji przechowywania danych użytkowników systemu. Pierwsze ze wskazanych powyżej rozwiązań nawiązuje do sposobu ewidencjonowania aktywów przyjętego również przez polskiego ustawodawcę. Drugi ze sposobów rejestrowania odbiega od standardów przewidzianych w prawie polskim, gdyż umożliwia uczestnikom obrotu posługiwanie się papierami wartościowymi na okaziciela, zamiast papierami wartościowymi imiennymi. W polskim systemie prawa niezależnie od tego, czy dla aktywów prowadzony jest rejestr DLT, czy ewidencja DLT, dane dotyczące inwestorów są gromadzone przez podmiot je prowadzący i dla niego dostępne. Wśród gromadzonych danych mają znajdować się również te jednoznacznie identyfikujące osobę uprawnioną do aktywów. Tym samym nie ma możliwości realnego posługiwania się instrumentami finansowymi na okaziciela tak, aby – jak to było niegdyś w przypadku dokumentowych papierów wartościowych – zapewniały one anonimowość uczestnikom rynku.

Trzecim kluczowym elementem stosowania rozporządzenia DLT Pilot Regime są zasady pośrednictwa w obrocie aktywami emitowanymi na jego mocy. W świetle prawa francuskiego pośrednictwo w zakresie papierów wartościowych dopuszczonych do obrotu w infrastrukturze rynku DLT na mocy rozporządzenia pilotażowego jest jedynie opcją oferowaną właścicielom papierów wartościowych, a nie obowiązkiem. Francuski *Code monétaire et financier* stanowi, że właściciel papierów wartościowych na okaziciela może zlecić depozytariuszowi rachunku powierniczego lub infrastrukturze rynku DLT przetwarzanie zdarzeń dotyczących tych papierów wartościowych i posiadanie środków dostępu do swoich papierów wartościowych, w tym w formie prywatnych kluczy kryptograficznych. Podobnie w przypadku papierów wartościowych zarejestrowanych na blockchainie, dla których infrastruktura rynku DLT została upoważniona przez emitenta do prowadzenia rejestru instrumentów finansowych DLT, właściciel papierów wartościowych może powierzyć pośrednikowi te same zadania. W obu przypadkach pośrednik działa jako administrator i nie odpowiada za przechowywanie instrumentów finansowych. Dlatego w przypadku utraty instrumentów finansowych infrastruktura rynku DLT ponosi odpowiedzialność na warunkach określonych w rozporządzeniu pilotażowym i francuskim kodeksie monetarnym i finansowym. Rozporządzenie ogólne AMF (https://www.amf-france.org, 2024) szczegółowo określa warunki tego pośrednictwa, w szczególności obowiązki, które muszą spełniać pośrednicy. W szczególności

pośrednik musi dokładać wszelkich starań, aby ułatwić wykonywanie praw związanych z tymi papierami wartościowymi. Ponadto, gdy oferuje posiadanie środków dostępu do papierów wartościowych, w tym za pomocą prywatnych kluczy kryptograficznych, musi prowadzić rejestr administrowanych pozycji, dokładać wszelkich starań, aby zapewnić posiadanie środków dostępu do papierów wartościowych, nie może korzystać ze środków dostępu do papierów wartościowych bez wyraźnej zgody ich właściciela oraz – gdy administrowanie papierami wartościowymi dobiega końca, w szczególności w przypadku zmiany administratora – ma obowiązek przekazać kontrolę nad środkami dostępu innemu administratorowi lub właścicielowi. Pośrednik musi również ustanowić i utrzymywać systemy operacyjne i procedury w celu ochrony bezpieczeństwa, integralności i poufności informacji, w tym środków dostępu do papierów wartościowych. Na uwagę zasługuje również fakt, że w zakresie, w jakim papiery wartościowe nie są przechowywane u pośrednika, działalność pośrednictwa w zakresie papierów wartościowych dopuszczonych do obrotu w infrastrukturze rynku DLT nie stanowi usługi przechowywania instrumentów finansowych, lecz stanowi usługę administrowania instrumentami finansowymi. Jest ona traktowana jako usługa powiązana, która może być przeniesiona do innego państwa członkowskiego w związku z usługą inwestycyjną. W rezultacie, ze względu na brak przechowywania papierów wartościowych finansowych przez pośrednika, odpowiedzialność administratora będzie ograniczona. Z drugiej strony, w zakresie, w jakim pośrednik posiada środki dostępu do papierów wartościowych, będzie on ponosił odpowiedzialność za szkody wyrządzone w przypadku utraty lub niedostępności środków dostępu do papierów wartościowych, z wyjątkiem przypadków siły wyższej. Ponadto w takich okolicznościach administrator musi pomóc właścicielowi papierów wartościowych lub infrastrukturze rynku DLT w łagodzeniu skutków takiej utraty lub niedostępności. Szczegółowych rozwiązań we wskazanych powyżej zakresach w odniesieniu bezpośrednio do aktywów podlegających reżimowi rozporządzenia DLT Pilot Regime brakuje natomiast w prawie polskim.

Wnioski

Podsumowując, należy w pierwszej kolejności wskazać, że rozporządzenie DLT Pilot Regime nie spełniło dotychczas pokładanych w nim pierwotnie nadziei. Przyczyn tego stanu rzeczy należy poszukiwać w uregulowaniu rozwiązań przewidzianych w rozporządzeniu w taki sposób, że nie pozwalają one na wykorzystanie w pełni potencjału tkwiącego w technologii rejestrów rozproszonych. Ponadto, unijny ustawodawca w znaczący sposób ograniczył zakres stosowania rozporządzenia zarówno w ujęciu podmiotowym, jak i przedmiotowym. Wykluczyło to z rynku bardzo wiele podmiotów, które nadal nie mają podstaw prawnych do emitowania i obracania instrumentami finansowymi z wykorzystaniem technologii blockchain. Dostępne dane statystyczne pokazują, że mogło mieć to bezpośredni wpływ na popularność

programu. Z pełną świadomością, że rozporządzenie DLT Pilot Regime miało być wyłącznie programem pilotażowym, należałoby postulować na przyszłość szersze i odważniejsze otwarcie możliwości wykorzystania systemów rejestrów rozproszonych na rynkach finansowych, aby w pełnym wymiarze zbadać zapotrzebowanie na tego typu rozwiązania i ich realny potencjał na rynkach finansowych.

Odnosząc się natomiast do rozwiązań zastosowanych w prawie polskim i francuskim w ramach poszczególnych aspektów funkcjonowania rozporządzenia DLT Pilot Regime, należy wskazać, że procedury certyfikacji podmiotów uprawnionych do prowadzenia platform obrotu aktywami w oparciu o rozwiązania przewidziane w rozporządzeniu są co do zasady analogiczne. Oba porządki prawne przewidują bowiem w oparciu o regulacje zawarte bezpośrednio w rozporządzeniu dwie ścieżki uzyskiwania uprawnień we wskazanym powyżej zakresie – jedną dla podmiotów, które dotychczas funkcjonowały już w wybranej formie na rynkach finansowych, drugą dla podmiotów, które łącznie z uzyskaniem specjalnego zezwolenia muszą ubiegać się jednocześnie o status podmiotu uprawnionego do prowadzenia działalności maklerskiej, rynku regulowanego albo centralnego depozytu papierów wartościowych.

W ramach drugiego aspektu stosowania rozporządzenia omawianego w artykule należy wskazać, że dzięki zastosowaniu dwóch trybów ewidencjonowania instrumentów finansowych emitowanych w oparciu o rozwiązania przewidziane w DLT Pilot Regime ustawodawca francuski zapewnił możliwość uzyskania rejestracji i posługiwania się przez inwestorów także papierami wartościowymi na okaziciela. Z uwagi na przyjęte przez polskiego ustawodawcę rozwiązania sprowadzające się do założenia, że zarówno rejestr DLT, jak i ewidencja DLT może być prowadzona wyłącznie przez podmiot uprawniony, który musi gromadzić ściśle określone dane, w tym dane jednoznacznie identyfikujące osobę uprawnioną do aktywów, posługiwanie się w polskich realiach papierami wartościowymi na okaziciela, w tradycyjnym rozumieniu tego pojęcia, nie jest w praktyce możliwe.

Przeprowadzona analiza prowadzi również do wniosku, że francuski ustawodawca w szerszym zakresie zadbał o bezpieczeństwo obrotu na rynkach prowadzonych w oparciu o rozwiązania przewidziane w rozporządzeniu DLT Pilot Regime. Ustanowił bowiem szczegółowe zasady pośrednictwa w obrocie aktywami emitowanymi na jego mocy. Z regulacji francuskich wynika również większa swoboda w kształtowaniu relacji między inwestorami a podmiotami świadczącymi usługi pośrednictwa. Francuski ustawodawca przewidział także szczegółowe zasady odpowiedzialności za realizację usług przechowywania kryptoaktywów emitowanych i wprowadzanych do obrotu na podstawie zasad przewidzianych w rozporządzeniu i jedynie ewidencjonowania transakcji dokonywanych z ich wykorzystaniem. Podobnych rozwiązań zabrakło natomiast w polskich regulacjach dostosowujących krajowe przepisy do potrzeb stosowania rozporządzenia.

Z powyższego podsumowania jednoznacznie wynika, że ustawodawstwo francuskie zostało dostosowane do potrzeb stosowania rozporządzenia DLT Pilot Re-

gime w sposób bardziej kompleksowy z jednej strony, z drugiej zaś – pozostawiający większą swobodę kształtowania relacji samym uczestnikom obrotu. W związku z tym rozwiązania zastosowane w prawie francuskim można zarekomendować polskiemu ustawodawcy, oczywiście z uwzględnieniem specyfiki obu systemów i różnic w nich występujących, co wymagałoby dostosowania rozwiązań francuskich do warunków polskiego porządku prawnego, jako wzorce do ewentualnej nowelizacji polskich przepisów wdrażających rozporządzenie do krajowego systemu prawa.

Przedstawiając konkretne rekomendacje dla polskiego ustawodawcy, oczywiście ze świadomością, jakie ograniczenia niesie ze sobą samo rozporządzenie DLT Pilot Regime w tym zakresie, trzeba zwrócić uwagę na potrzebę zastosowania w odniesieniu do aktywów emitowanych na bazie rozwiązań przewidzianych w rozporządzeniu instrumentu podobnego do znanych już w polskim ustawodawstwie rachunków zbiorczych, znanych też jako konta omnibusowe. To rachunki papierów wartościowych, na których mogą być rejestrowane papiery wartościowe należące do różnych osób, a nie tylko do posiadacza tego rachunku. Powyższe rozwiązanie pozwoliłoby na zachowanie większej anonimowości uczestników rynku finansowego. Ponadto, w ramach uelastycznienia polskich rozwiązań należałoby zarekomendować także rezygnację z zakazu *dual listingu*, tj. należałoby dopuścić możliwość częściowego emitowania akcji w reżimie tradycyjnym, zaś częściowego w ramach technologii rejestrów rozproszonych. Rozwiązanie umożliwiające skorzystanie z technologii rejestrów rozproszonych niejako „na próbę" zwiększyłoby z pewnością zainteresowanie programem i zachęciło większą liczbę podmiotów do zweryfikowania na własnym organizmie zalet i wad, jakie niesie on ze sobą. Obie wskazane powyżej zmiany polskich regulacji pozwoliłyby w pełniejszym wymiarze wykorzystać możliwości, jakie daje rynkom finansowym rozporządzenie DLT Pilot Regime.

BIBLIOGRAFIA

Audit, M. (2020). Le droit international privé confronté à la blockchain. *Revue critique de droit international privé*, *4*(4), 669–694.

Autorité des marchés financiers (AMF). (2024). https://www.amf-france.org/en/regulation/policy/doc-2024–07

Autorité des marchés financiers (AMF). (2025, 16 stycznia). https://www.amf-france.org/en/news-publications/depth/pilot-regime

DLKLegal. (2023, 23 marca). *Rozporządzenie pilotażowe DLT.* https://www.dlklegal.com/wiedza/rozporzadzenie-pilotazowe-dlt-2022/

Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA). (2023). *Wytyczne w sprawie standardowych formularzy, formatów i wzorów wniosków o wydanie zezwolenia na prowadzenie infrastruktury rynkowej opartej na DLT.* https://www.esma.europa.eu/sites/default/files/library/ESMA70–460-213_DLTR_GLs_on_application_standard_forms_formats_templates_PL.pdf

Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA). (2025). *DLT Pilot Regime*. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/dlt-pilot-regime

Hrabčák, L. & Štrkolec, M. (2024). EU Regulation of the Crypto-Assets Market. *Białostockie Studia Prawnicze*, *29*(1), 27–45. https://bsp.uwb.edu.pl/article/view/1005/837

Krajowy Depozyt Papierów Wartościowych. (2023). *Blockchain – Projekty badawcze*. https://www.kdpw.pl/pl/dlt-blockchain.html

Ledger Insights. (2024, 4 kwietnia). *ESMA explains why DLT Pilot Regime hasn't taken off.* https://www.ledgerinsights.com/esma-explains-why-dlt-pilot-regime-hasnt-taken-off/

Lemonnier, M., Mariański, M. & Zięty, J. J. (2011). Ewolucja koncepcji papieru wartościowego w prawie polskim i francuskim. *Przegląd Prawa Handlowego*, (8), 43-53.

Manzari, N. & Wagner, Z. (2021). The Digital Future for Financial Services. *Pin Code*, *7*(1), 7–10.

Mariański, M. & Lemonnier, M. (2017). Francuska koncepcja tytułu zbywalnego (titre négociable) a regulacje rynków finansowych. [w:] W. Rogowski (red.) *Regulacje finansowe. FinTech – nowe instrumenty finansowe – resolution* (ss. 181-191). Wydawnictwo C.H. Beck.

Mariański, M. (2016). Struktura wewnętrzna oraz podstawa funkcjonowania L'Autorité des marchés financiers (AMF) jako organu nadzoru nad rynkiem finansowym we Francji. *Monitor Prawa Bankowego*, (5), 64–74.

Mariański, M. (2023). Uprawnienia i kompetencje francuskiego pomocniczego organu nadzoru nad rynkiem finansowym Autorité de contrôle prudentiel et de résolution. *Przegląd Prawa Handlowego*, (4), 38–44.

Parlament Europejski i Rada (UE). (2014, 15 maja). Dyrektywa w sprawie rynków instrumentów finansowych (2014/65/UE) (Dz.U. L 173, 12.6.2014).

Parlament Europejski i Rada (UE). (2014, 15 maja). Rozporządzenie w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 (600/2014) (Dz.U. L 173, 12.6.2014).

Parlament Europejski i Rada (UE). (2014, 23 lipca). Rozporządzenie w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych (909/2014) (Dz.U. L 257, 28.8.2014).

Parlament Europejski i Rada (UE). (2022, 30 maja). Rozporządzenie w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, a także zmiany rozporządzeń (UE) nr 600/2014 i (UE) nr 909/2014 oraz dyrektywy 2014/65/UE (2022/858) (Dz.U. L 151, 02.06.2022).

Sejm Rzeczypospolitej Polskiej. (2005). Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. z 2024, poz. 722, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2023). Ustawa z dnia 16 sierpnia 2023 r. o zmianie niektórych ustaw w związku z zapewnieniem rozwoju rynku finansowego oraz ochrony inwestorów na tym rynku (Dz.U. 2023, poz. 1723, ze zm.).

Sotiri, E. (2024). A Comparative Analysis of Virtual Assets and Crypto-Assets and the Transition From Vasp to Casp. *Pin Code*, *20*(4), 17–23.

Tomczak, T. (2024). 'Advantages' of distributed ledger technology and the DLT Pilot Regime. *Przegląd Ustawodawstwa Gospodarczego*, (5), 32–39.

Wiewiórkowski, W. R. (2021). *Opinion of the European Data Protection Supervisor on the Proposal for a Pilot Regime for Market Infrastructures based on Distributed Ledger Technology (DLT).* https://www.kdpw.pl/uploads/attachments/opinia-europejskiego-inspektora-ochrony-danych.pdf

Zgromadzenie Narodowe. (1999). *Code monétaire et financier* z dnia 16 grudnia 1999 r. (JORF nr 0103 z dnia 2 maja 2025 r.), https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072026/

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.08
Received: 7.01.2025
Accepted: 3.07.2025

Tomasz Tomczak
Uniwersytet Opolski, Polska
tomasz.tomczak@uni.opole.pl
ORCID ID: https://orcid.org/0000-0002-8499-4553

Nadzór AML nad kryptoaktywami od 30.12.2024 r. – zmiany w Dyrektywie 2015/849 wprowadzone rozporządzeniem 2023/1113

AML Supervision of Cryptoassets since 30 December 2024: Changes to Directive 2015/849 Introduced by Regulation 2023/1113

Abstract: The aim of this article is to take a closer look at the most important changes to EU AML supervision of cryptoassets introduced to EU Directive 2015/849 by EU Regulation 2023/1113. The analysis leads to the thesis that as of 30 December 2024, this supervisory landscape has been significantly remodelled. There have been changes to the subject of supervision, the scope of supervised activity, entity modifications and licensing requirements. These changes are aimed at tightening AML supervision over cryptoassets. The considerations made also allow us to state that the EU legislation perceives the MiCA regulation as a legal act of a systemic nature for a new class of assets, i.e. cryptoassets.

Keywords: cryptoassets, Regulation EU 2023/1113, AML, CTF, money laundering, MiCAR
Słowa kluczowe: kryptoaktywa, rozporządzenie UE 2023/1113, AML, CTF, pranie brudnych pieniędzy, MiCAR

Wprowadzenie

Od dnia 30 grudnia 2024 r. stosuje się Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE)

© 2025 Tomasz Tomczak published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

2015/849[1] (dalej: Rozporządzenie 2023/1113). Ten akt prawny zawiera przepisy dotyczące m.in. informacji o inicjatorach i beneficjentach, które towarzyszą transferom kryptoaktywów, w celu zapobiegania przypadkom prania pieniędzy i fnansowania terroryzmu, wykrywania tych przypadków i prowadzenia postępowań przygotowawczych w ich sprawie, w sytuacji gdy co najmniej jeden z dostawców usług w zakresie kryptoaktywów biorących udział w danym transferze kryptoaktywów ma siedzibę w Unii lub – w stosownych przypadkach – ma siedzibę statutową w Unii[2].

Przedmiotem artykułu są nowe i wybrane przepisy dyrektywy (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE[3] (dalej: Dyrektywa 2015/849), które zostały dodane lub zmienione na mocy art. 38 Rozporządzenia 2023/1113. Analiza niektórych z tych modyfikacji pozwoli ukazać, jak od 30.12.2024 r., z perspektywy prawa unijnego i przeciwdziałania praniu pieniędzy (tzw. AML) oraz finansowaniu terroryzmu (tzw. CFT), zmieni się, nieco upraszczając, zakres nadzoru nad kryptoaktywami[4]. Co istotne, w ramach niniejszego opracowania nie zostaną omówione wszystkie zmiany wprowadzone przez art. 38 Rozporządzenia 2023/1113 i dotyczące krypoaktywów, a jedynie te najdonioślejsze i mające charakter systemowy. Kolejno zostaną przeanalizowane modyfikacje przedmiotu nadzoru, nadzorowanej aktywności, zmiany podmiotowe co do wymogów reglamentacyjnych, a także ewentualne modyfikacje odnośnie do organów nadzoru. Nie zostanie natomiast przeanalizowane wprowadzone do Dyrektywy 2015/849 bardzo istotne pojęcie „adresu niehostowanego" (zob. art. 38 pkt 2 lit. d Rozporządzenia 2023/1113). Omówienie tego narzędzia i problemów, jakie z nim się wiążą z punktu widzenia nadzoru AML, niestety wykracza poza ramy niniejszego artykułu i zasługuje na odrębne, obszerne opracowanie (Ciechoński, 2024).

Na koniec, przed przejściem do istoty niniejszego artykułu, należy jeszcze zwrócić uwagę na cztery kwestie. Po pierwsze, dzięki zmianie dyrektywy 2015/849 przez Dyrektywę 2018/843[5] (dalej: poprzednia zmiana dyrektywy 2015/849), kryptoaktywa, nieco

1 Dz.U. UE. L. z 2023 r. Nr 150, str. 1. Zob. Art. 40 tego rozporządzenia.

2 Dokładniej i szerzej zob. Art. 1 (Przedmiot) rozporządzenia UE 2023/1113.

3 Dz.U. UE. L. z 2015 r. Nr 141, str. 73 z późn. zm.

4 Nieco upraszczając, gdyż nadzór ma charakter podmiotowy, a nie przedmiotowy. Natomiast to, co jest przedmiotem aktywności danego podmiotu, będzie miało wpływ na to, czy jest on objęty nadzorem. Kwestie te zatem są ze sobą ściśle powiązane. Biorąc pod uwagę, że omawiane zmiany są wprowadzane zarówno co do podmiotu, jak i przedmiotu, trudno jest znaleźć idealne językowe rozwiązanie. Ze względu na powyższe, Czytelnik musi wybaczyć takie językowe skróty myślowe, jak: „nadzór nad kryptoaktywami" (tytuł artykułu), „objęcie kryptoaktywów nadzorem AML" (tytuł pierwszej części).

5 Dyrektywa Parlamentu Europejskiego i Rady (UE) z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pienię-

upraszczając i przynajmniej w pewnym stopniu, zostały już objęte nadzorem AML (Haffke et al., 2020, s. 125–138; Golonka, 2020)[6]. Po drugie, Rozporządzenie 2023/1113 stanowi część szerszego pakietu regulacyjnego, który ma za zadanie jeszcze bardziej wzmocnić unijny nadzór AML/CFT (Tomczak & Weck, 2024, Introduction; Golonka, 2024)[7]. Po trzecie, omawiane modyfikacje są zmianami wprowadzanymi do dyrektywy, a zatem wymagają one implementacji do krajowych porządków prawnych. Dokładna analiza ich wpływu na krajowe regulacje dotyczące przeciwdziałania praniu brudnych pieniędzy i finansowania terroryzmu zasługuje na odrębne opracowania. Na dzień pisania niniejszego artykułu zagadnienia w nim omówione spotkały się tylko z niewielkim zainteresowaniem w literaturze (zob. np. Janczak, 2023; Włoczka & Windak, 2024).

1. Objęcie kryptoaktywów nadzorem AML

Obecnie kryptoaktywa zostały wyodrębnione przez unijnego prawodawcę jako odrębna klasa aktywów (Tomczak & Weck, 2024, I. *Introduction*). Definiuje je i pośrednio reguluje m.in. Rozporządzenie UE 2023/1114[8] (tzw. Rozporządzenie MiCA lub MiCAR). Nie dotyczy ono jednak, przynajmniej bezpośrednio, nadzoru AML/CFT. Jak już zostało to wskazane, do regulacyjnego świata AML/CFT kryptoaktywa częściowo wkroczyły na mocy poprzedniej zmiany dyrektywy 2015/849[9]. Do artykułu 3 został wprowadzony nowy punkt 18, który definiował pojęcie waluty wirtualnej. W literaturze zwraca się uwagę, że dzięki tej zmianie mieliśmy do czynienia z pierwszym unijnym aktem prawnym, który przynajmniej do pewnego stopnia próbował zmierzyć się

dzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE.

6 Nieco upraszczając, gdyż nadzorem objęte zostały „waluty wirtualne". Jak zostanie jednak wykazane poniżej, pomiędzy definicjami kryptoaktywa i waluty wirtualnej zachodzi relacja krzyżowania się.

7 W skład tego pakietu wchodzi również: 1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (Dz.U. UE. L. z 2024 r. poz. 1624); 2) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca dyrektywę (UE) 2019/1937 oraz zmieniająca i uchylająca dyrektywę (UE) 2015/849 (Dz.U. UE. L. z 2024 r. poz. 1640) oraz 3) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1620 z dnia 31 maja 2024 r. w sprawie ustanowienia Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010 (Dz.U. UE. L. z 2024 r. poz. 1620). Powyższe w literaturze jest określane jako tzw. Pakiet AML (zob. Golonka, 2024).

8 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U. UE. L. z 2023 r. Nr 150, str. 40 z późn. zm.).

9 Częściowo, gdyż – jak zostało to wskazane w przypisie nr 6 – nadzorem objęte zostały „waluty wirtualne". Pojęcie to odsyła jednak do podobnej klasy aktywów. Szerzej na ten temat poniżej.

z tą nową klasą aktywów z perspektywy AML (Tomczak & Weck, 2024, I. *Introduction*), choć ciągle czynił to w sposób niedoskonały (Haffke et al., 2020, s. 125–138).

Natomiast art. 38 pkt 2 lit. c Rozporządzenia 2023/1113 zmienia brzmienie ww. art. 3 pkt 18 dyrektywy 2015/849 w ten sposób, że definicję „waluty wirtualnej" zastępuje pojęciem „kryptoaktywa". To drugie zostało zdefiniowane na gruncie Dyrektywy 2015/849 jako kryptoaktywo zgodnie z definicją art. 3 ust. 1 pkt 5 [MiCAR], z wyjątkiem sytuacji, gdy należy ono do kategorii wymienionych w art. 2 ust. 2, 3 i 4 MiCAR lub w inny sposób kwalifikuje się jako środki pieniężne.

W pierwszej kolejności warto zwrócić uwagę na wskazane w definicji wyjątki. Art. 2 ust. 2–4 MiCAR to wyłączenia z zakresu zastosowania MiCAR. Zostały one już do pewnego stopnia omówione w literaturze (Tomczak, 2023b; Korus, 2024). Różnica polega na tym, że o ile pewne aktywo na gruncie MiCAR będzie mogło być zakwalifikowane jako kryptoaktywo, to MiCAR nie będzie znajdowało do niego zastosowania ze względu właśnie na te wyłączenia. Natomiast na gruncie przepisów AML takiego aktywa w ogóle nie powinniśmy traktować jako kryptoaktywa. Różnica wydaje się być bardziej teoretyczna niż praktyczna (Tomczak & Weck, 2024, II. *Crypto-assets instead of virtual currencies*). Natomiast drugi wyjątek dotyczy kwalifikowania aktywa jako „środków pieniężnych". W literaturze zwraca się uwagę, że wyłączenie środków pieniężnych z definicji kryptoaktywa wydaje się dosyć oczywiste, gdyż na gruncie AML kryptoaktywa mają być, co do zasady, nową kategorią aktywów traktowaną nieco inaczej niż dotychczasowe aktywa, więc prawodawca chciał uniknąć podwójnej regulacji tego samego przedmiotu (tak: Tomczak & Weck, 2024, II. *Crypto-assets instead of virtual currencies*). Natomiast to, co może wydawać się na pierwszy rzut oka nielogiczne w takim zabiegu, to fakt, że MiCAR już wyłącza środki pieniężne ze swojego zakresu, chyba że kwalifikują się one jako tokeny pieniądza elektronicznego (art. 2 ust. 4 lit. c MiCAR). Takie dodatkowe brzmienie – zdaje się – zatem ma na celu traktowanie z perspektywy unijnych przepisów AML tokenów pieniądza elektronicznego, które kwalifikują się jako środki pieniężne, a nie jako kryptoaktywa (Tomczak & Weck, 2024, II. *Crypto-assets instead of virtual currencies*). Wydaje się, że powyższe ma na celu, nieco upraszczając i mówiąc obrazowo, przedmiotowe rozdzielenie na gruncie AML „tradycyjnych" środków pieniężnych, do których zaliczono tokeny pieniądza elektronicznego[10], od świata kryptoaktywów. Niestety nie jest to dokonane w sposób w pełni klarowny, gdyż nie tylko Dyrektywa 2015/849 nie zawiera definicji środków pieniężnych, ale co więcej polski ustawodawca, implementując dyrektywę PSD2, nie zdecydował się wprowadzić tej definicji do polskiego porządku prawnego (szerzej: Korus, 2024,

10 Warto wskazać, że zgodnie z art. 48 ust. 2 zd. 1 MiCAR tokeny będące e-pieniądzem uznaje się za pieniądz elektroniczny, a ten ostatni jest zaliczany do środków pieniężnych. Zob. art. 4 pkt 25 dyrektywy (UE) 2015/2366 (tzw. PSD 2, dalej: Dyrektywa PSD2).

s. 34–36)[11]. Powyższa analiza prowadzi do wniosku, że kryptoaktywa z perspektywy Dyrektywy 2015/849 zostały zdefiniowane w istocie bardzo podobnie jak na gruncie MiCAR i w istocie przez odesłanie do tego aktu prawnego. Zgodnie z art. 3 ust. 1 pkt 5 MiCAR „kryptoaktywo" oznacza cyfrowe odzwierciedlenie wartości lub prawa, które da się przenosić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii. Pojęcie to zostało omówione w doktrynie, a zatem należy odesłać do istniejących opracowań (Tomczak, 2022; Tomczak, 2023a; Wiącek, 2024, s. 24–25). Warto jednak porównać ww. pojęcie z dotychczasową definicją waluty wirtualnej (Srokosz, 2017), która wskazywała, że oznaczają one cyfrowe wyznaczniki wartości, które nie są emitowane ani gwarantowane przez bank centralny lub organ publiczny, nie muszą być powiązane z walutą prawnie obowiązującą i nie posiadają prawnego statusu waluty lub pieniądza, lecz które są akceptowane przez osoby fizyczne lub prawne jako środek wymiany i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną (dotychczasowy art. 3 pkt 18 Dyrektywy 2015/849). Obie definicje są niewątpliwie szerokie. Z jednej strony wymóg akceptowalności jako środka wymiany może na pierwszy rzut oka sugerować, że definicja waluty wirtualnej jest nieco węższa. Takiej przesłanki można jednak próbować doszukiwać się w przesłance „przenoszalności" występującej w definicji kryptoaktywów, gdyż trudno uznać, że coś jest przenoszalne, jeżeli nikt tego nie akceptuje. Oczywiście można twierdzić, że kryptoaktywo może pełnić też inne funkcje niż wymiany (np. inwestycyjną), ale wydaje się, że również na gruncie AML nie było problemu z kwalifikowaniem danego kryptoaktywa jako waluty wirtualnej, mimo że występowanie funkcji wymiany mogło być wątpliwe. Z drugiej strony wymóg technologii rozproszonego rejestru (tzw. DLT) lub podobnej technologii może sugerować, że definicja kryptoaktywa jest węższa, gdyż definicja waluty wirtualnej była neutralna technologicznie. Jednak zwrot „podobnej technologii" wydaje się być tak szeroki i niedookreślony, że trudno jest mówić o jakiejś praktycznej i rzeczywistej różnicy, a niewątpliwie to właśnie DLT doprowadziło do wyodrębnienia tej nowej klasy aktywów (pkt 1–2 wstępu do MiCAR). Natomiast sam zwrot „podobnej technologii" występujący w definicji „kryptoaktywa" słusznie spotkał się z krytyką w literaturze (Tomczak, 2022, s. 367–369; Wyżykowski, 2024, s. 87). Podsumowując, z formalnego punktu widzenia można zatem powiedzieć, że definicje te krzyżują się. Obecnie na gruncie AML/CFT będziemy mówić już o kryptoaktywach, a nie o walutach wirtualnych. Dzięki zdefiniowaniu tego pojęcia w istocie przez odesłanie do MiCAR w prawie unijnym wystąpi większa koherentność terminologiczna. Sam punkt 10 wstępu do rozporządzenia UE 2023/1113 zwraca uwagę, że ujednolicenie terminologii ma zapewnić spójność unijnego prawa w dziedzinie AML/CFT.

11 Powyższe zagadnienie może jednak być widziane jako sporne i zasługuje na odrębne opracowanie.

2. Zmiana w zakresie usług objętych nadzorem AML

Powyżej zostało omówione, jak zmienił się przedmiot objęty nadzorem AML. Obecnie, zamiast o nadzorze nad walutami wirtualnymi, będziemy mówić o nadzorze nad kryptoaktywami. Powstaje jednak pytanie: jaka aktywność związana z tego rodzaju aktywem objęta jest nadzorem AML? Czy zakres ten rzeczywiście się zmienia, czy znowu mamy do czynienia raczej jedynie ze zmianą terminologiczną?

Co interesujące, poprzednia zmiana dyrektywy 2015/849, choć wprowadziła definicję waluty wirtualnej, nie przyjęła – przynajmniej bezpośrednio – katalogu usług, które były objęte nadzorem AML (Tomczak & Weck, 2024, IV. *Services*). Odbyło się to jednak w pewnym stopniu pośrednio przez rozszerzenie katalogu podmiotów zobowiązanych, który znajduje się w art. 2 tego aktu prawnego. Szerzej i bardziej precyzyjnie mowa o tym będzie w części 3 niniejszego artykułu, gdzie zostanie omówiona zmiana zakresu podmiotowego nadzoru AML. Niewątpliwie jednak w dyrektywie 2015/849 próżno było szukać jakiejś samodzielnej definicji „usług związanych z walutami wirtualnymi".

Zmiany wprowadzone Rozporządzeniem 2023/1113 również nie wprowadziły jej bezpośrednio do dyrektywy 2015/849. Do zakreślenia katalogu usług ponownie doszło pośrednio, ale tym razem w sposób bardziej precyzyjny. Została wprowadzona definicja dostawcy usług w zakresie kryptoaktywów (o czym więcej poniżej), ale w niej możemy znaleźć odesłanie do usług w zakresie kryptoaktywów (zob. nowe brzmienie art. 3 punkt 19 Dyrektywy 2015/849). Nie są one jednak zdefiniowane na gruncie AML a znowu przez odesłanie do definicji znajdującej się w MiCAR, przy czym z zakresu nadzoru AML zostało wyłączone świadczenie wyłącznie usługi doradztwa w zakresie kryptoaktywów (art. 3 pkt 19 Dyrektywy 2015/849 w obecnym brzmieniu). Doradztwo w zakresie kryptoaktywów zostało zdefiniowane w MiCAR jako oferowanie, udzielanie lub zgodę na udzielanie klientowi spersonalizowanych zaleceń – na żądanie klienta albo z własnej inicjatywy dostawcy usług w zakresie kryptoaktywów świadczącego doradztwo – w odniesieniu do co najmniej jednej transakcji związanej z kryptoaktywami lub korzystania z usług w zakresie kryptoaktywów (art. 3 ust. 1 pkt 16 lit. h oraz pkt 24 MiCAR). Z przywołanej definicji wynika, dlaczego prawodawca zdecydował się wyłączyć ową usługę z zakresu nadzoru AML. Jej świadczenie nie sprawia, że dostawca ma bezpośredni kontakt z kryptoaktywami klienta, a zatem prawodawca unijny najprawdopodobniej uznał, że brak jest ryzyka prania brudnych pieniędzy czy finansowania terroryzmu (Tomczak & Weck, 2024, IV. *Services*). W tym miejscu należy zwrócić uwagę na jedną kwestię. Podmiot świadczący wyłącznie tę usługę będzie wyłączony z nadzoru AML. Natomiast gdy będzie ona połączona np. z przechowywaniem kryptoaktywów, to taki podmiot nie znajdzie się poza zakresem kontroli odpowiednich organów AML (zob. uwagi poniżej), choć sama usługa doradztwa nie będzie objęta obowiązkami AML.

Nie wliczając ww. usługi doradztwa w art. 3 ust. 1 pkt 16 MiCAR, znajdziemy jeszcze dziewięć (9) kryptousług, które są zdefiniowane w kolejnych punktach słowniczka i są objęte nadzorem AML. Wśród tych usług znajdziemy: a) zapewnianie przechowywania kryptoaktywów i administrowanie nimi w imieniu klientów (art. 3 ust. 1 pkt 17 MiCAR); b) prowadzenie platformy obrotu kryptoaktywami (art. 3 ust. 1 pkt 18 MiCAR); c) wymiana kryptoaktywów na środki pieniężne (art. 3 ust. 1 pkt 19 MiCAR); d) wymiana kryptoaktywów na inne kryptoaktywa (art. 3 ust. 1 pkt 20 MiCAR); e) wykonywanie zleceń związanych z kryptoaktywami w imieniu klientów (art. 3 ust. 1 pkt 21 MiCAR); f) plasowanie kryptoaktywów (art. 3 ust. 1 pkt 22 MiCAR); g) przyjmowanie i przekazywanie zleceń związanych z kryptoaktywami w imieniu klientów (art. 3 ust. 1 pkt 23 MiCAR); h) zarządzanie portfelem kryptoaktywów (art. 3 ust. 1 pkt 25 MiCAR); oraz i) świadczenie usług transferu kryptoaktywów w imieniu klientów (art. 3 ust. 1 pkt 26 MiCAR).

Należałoby porównać powyższy katalog z dotychczasowym. Do tej pory do grona podmiotów zobowiązanych zaliczane były, po pierwsze, podmioty zajmujące się świadczeniem usług wymiany walut pomiędzy walutami wirtualnymi a walutami fiducjarnymi (art. 2 ust. 1 pkt 3 lit. g Dyrektywy 2015/849 w dotychczasowym brzmieniu) oraz dostawcy kont walut wirtualnych (art. 2 ust. 1 pkt 3 lit. h Dyrektywy 2015/849 w dotychczasowym brzmieniu). Pierwsza z tych usług obecnie również objęta jest nadzorem AML (art. 3 ust. 1 pkt 19 MiCAR) i – co więcej – prawodawca unijny wyraźnie objął nadzorem również usługę wymiany kryptoaktywów na inne kryptoaktywa (art. 3 ust. 1 pkt 20 MiCAR)[12]. Jeden podmiot może świadczyć obie te usługi (co często ma miejsce w praktyce), ale z prawnego punktu widzenia nic nie stoi na przeszkodzie, aby świadczył tylko jedną z nich. Natomiast usługa zapewnienia kont walut wirtualnych ewoluowała w usługę zapewnienia przechowania kryptoaktywów i administrowania nimi w imieniu klientów (art. 3 ust. 1 pkt 17 MiCAR). Można zatem, w bardzo dużym uproszczeniu, stwierdzić, że obecnie unijnym nadzorem AML zostały wyraźnie objęte 2 dotychczasowe i 7 nowych usług związanych z kryptoaktywami (por. Tomczak & Weck, 2024, IV *Services*)[13].

3. Zmiany dotyczące podmiotu objętego nadzorem

Do tej pory zostały omówione zmiany przedmiotu oraz aktywności objętych nadzorem AML. Należy jednak pamiętać, że obowiązki ostatecznie są nakładane nie

12 Przy czym do tej pory była mowa o wymianie waluty wirtualnej (nie kryptoaktywów), a jak zostało to wykazane powyżej, nie są to pojęcia tożsame (zob. część 1).

13 W bardzo dużym uproszczeniu, gdyż nie można w pełni utożsamiać dotychczasowych usług wymiany walut wirtualnych na waluty fiducjarne oraz usługi konta z, odpowiednio, usługą wymiany kryptoaktywów na środki pieniężne oraz z usługą zapewnienia przechowywania i administrowania nimi. Szersze rozważania na ten temat wykraczają jednak poza ramy tego artykułu.

na przedmiot czy aktywność, a na podmiot, co było już częściowo widoczne w poprzedniej części niniejszego artykułu (część 2)[14].

Poprzednia zmiana dyrektywy 2015/849 do katalogu podmiotów zobowiązanych dodała wyżej wspomniane podmioty zajmujące się świadczeniem usług wymiany walut pomiędzy walutami wirtualnymi a walutami fiducjarnymi oraz dostawców kont walut wirtualnych (dodane lit. g i h w art. 2 ust. 1 pkt 3). Ci drudzy byli zdefiniowani jako podmioty świadczące usługi polegające na przechowywaniu prywatnych danych uwierzytelniających w imieniu swoich klientów na potrzeby posiadania, przechowywania i przekazywania walut wirtualnych (art. 3 pkt 19 Dyrektywy 2015/849 w dotychczasowym brzmieniu). W ten sposób, poprzez definicję podmiotową, doszło zatem również do dookreślenia usługi objętej nadzorem. Podmioty świadczące te usługi (wymiana lub portfel) były określane w praktyce jako VASPsy od ang. *virtual asset service providers* (Cegłowski, 2024, s. 65).

Natomiast Rozporządzenie 2023/1113:

1) usuwa z katalogu podmiotów zobowiązanych dwa wyżej wskazane podmioty (art. 38 pkt 1 tego rozporządzenia);
2) definicję dostawcy kont waluty wirtualnej zastępuje definicją dostawcy usług w zakresie kryptoaktywów (art. 38 pkt 2 lit. c); oraz
3) takiego dostawcę traktuje na gruncie AML jako instytucje finansową (zob. art. 38 pkt 2 lit. a).

Dostawców usług w zakresie kryptoaktywów określa się w praktyce jako CASPy, od ang. *crypto-asset service providers*. Można zatem w skrócie i nieco potocznie powiedzieć, że nadzór nad dotychczasowymi VASPami jest zastępowany przez nadzór nad CASPami (Tomczak & Weck, 2024, III *Crypto-assets service providers*).

Jak wynika z punktu 3 powyżej, owe CASPy nie będą traktowane jako odrębna kategoria, która wymaga szczególnego uregulowania, a będą objęte parasolem nadzorczym i wymogami AML dotyczącymi instytucji finansowych (zob. pkt 59 wstępu do Rozporządzenia 2023/1113 oraz EBA, 2024, s. 5). Oznacza to, że dotychczasowe rozróżnienie występujące na gruncie AML na tradycyjny świat finansów oraz świat kryptoaktywów, przynajmniej do pewnego stopnia, zniknie (Tomczak & Weck, 2024, *Crypto-assets service providers*).

Aby zatem wiedzieć, kto obecnie objęty jest unijnym nadzorem AML, należy bliżej przyjrzeć się wprowadzonej definicji CASPu, która stanowi, że „dostawca usług w zakresie kryptoaktywów" oznacza dostawcę usług w zakresie kryptoaktywów zgodnie z definicją w art. 3 ust. 1 pkt 15 [MiCAR], który świadczy co najmniej jeden

14 Przy czym przepisy mogą nakładać obowiązek na ściśle określony podmiot lub odnosić się do danego rodzaju aktywności. W tym drugim przypadku obowiązek również nakładany jest na podmiot, ale do ustalenia podmiotu zobowiązanego dochodzi w inny sposób (przez zbadanie jego aktywności, a nie statusu).

rodzaj usługi w zakresie kryptoaktywów zgodnie z definicją w art. 3 ust. 1 pkt 16 tego rozporządzenia, z wyjątkiem doradztwa w zakresie kryptoaktywów, o których mowa w art. 3 ust. 1 pkt 16 lit. h) tego rozporządzenia.

Termin „dostawcy usług w zakresie kryptoaktywów" został w istocie zdefiniowany ponownie przez odesłanie do MiCAR i poza wyłączeniem usługi doradztwa brak jest innych różnic. W MiCAR CASP został określony jako osoba prawna lub inne przedsiębiorstwo, których działalność zawodowa lub działalność gospodarcza polega na profesjonalnym świadczeniu co najmniej jednej usługi w zakresie kryptoaktywów na rzecz klientów i którym zezwolono na świadczenie usług w zakresie kryptoaktywów zgodnie z art. 59 (art. 3 ust. 1 pkt 15 MiCAR). Definicja ta wobec CASP stawia zatem następujące wymogi:

a) podmiotowe – os. prawna lub inne przedsiębiorstwo;
b) profesjonalizmu działania – profesjonalna działalność zawodowa lub gospodarcza;
c) uzyskania zezwolenia;
d) świadczenia odpowiedniej usługi (co najmniej jednej).

Zagadnienie świadczonych usług zostało już omówione powyżej. W tym miejscu można tylko zwrócić uwagę, że wyłączenie podmiotu świadczącego wyłącznie usługę krypto-doradztwa z nadzoru AML sprawia, że podmioty, które będą kwalifikowały się jako CASPy na gruncie MiCAR, niekoniecznie będą zaliczały się do CASPów na gruncie przepisów AML. Innymi słowy, że będziemy mogli mieć do czynienia z CASPem, który będzie musiał spełniać wymogi wynikające z MiCAR, ale już nie z przepisów AML. Biorąc jednak pod uwagę rozszerzony zakres usług objętych nadzorem AML, obecne CASPy stanowią szerszą kategorię niż dotychczasowe VASPy.

W literaturze zwraca się uwagę, że VASPy, które świadczyły usługi w zgodzie z obowiązującym je prawem przed 30.12.2024 r. i korzystają z okresu przejściowego, nie są traktowane jako CASPy na gruncie MiCAR tak długo, jak nie uzyskają odpowiedniego zezwolenia (ESMA, 2024; Tomczak & Weck, 2024, III *Crypto-assets service providers*). Taka sytuacja ma swoje zalety i wady. Zaletą jest to, że przez ww. okres nie są na nie nałożone obowiązki wynikające z MiCAR. Wadą natomiast to, że nie mogą korzystać z tzw. zasady jedego paszportu (zob. art. 59 ust. 7 MiCAR oraz Tomczak & Weck, 2024, III. *Crypto-assets service providers*).

Natomiast bardziej problematyczna jest kwestia, czy taki VASP musi od 30.12.2024 r. i do czasu uzyskania zezwolenia wypełniać obowiązki wynikające z rozporządzenia UE 2023/1113. Problematyczność zaznaczonej kwestii wynika z faktu, że wskazane rozporządzenie, inaczej niż MiCAR, co prawda nie przewiduje okresu przejściowego, ale reguluje nie tyle VASPy, co CASPy, a CASPy zostały zdefiniowane przez odesłanie do MiCAR. Problem ten wykracza poza ramy niniejszego artykułu, gdyż niniejsze opracowanie skupia się na zmianach do Dyrektywy 2015/849 wprowadzonych przez rozporządzenie UE 2023/1113, a nie na obowiązkach wynikających z tego

rozporządzenia i początku ich obowiązywania. Poza tym, problem ten został już dosyć szeroko omówiony w literaturze i została postawiona teza, że taki VASP musi od 30.12.2024 r. spełniać obowiązki wynikające z rozporządzenia UE 2023/1113 (zob. szerzej: Tomczak & Weck, 2024, VII. *Grandfathering period*).

Na koniec należy krótko zwrócić uwagę, że MiCAR dosyć obszernie reguluje wymogi w stosunku do CASPów. Można zatem zgodzić się ze stanowiskiem, że od czasu pełnego wejścia w życie w MiCAR w odniesieniu do CASPów w Unii powinniśmy mieć do czynienia z bardziej wiarygodnymi dostawcami krypto-usług, co powinno wpłynąć, przynajmniej do pewnego stopnia, na redukcję ryzyk związanych z praniem brudnych pieniędzy czy finansowaniem terroryzmu przez takie podmioty (Włoczka & Windak, 2024, s. 71–72).

4. Wymóg uzyskania zezwolenia

Powyżej zostały omówione zmiany w nadzorze AML dotyczące kategorii aktywów, działalności oraz podmiotów wprowadzone do Dyrektywy 2015/849 przez Rozporządzenie 2023/1113. Obecnie zostaną omówione zmiany w tzw. obowiązkach reglamentacyjnych.

Artykuł 47 ust. 1 dyrektywy 2015/849 wskazuje, jakie podmioty powinny podlegać rejestracji, uzyskać zezwolenie lub być regulowane. Poprzednia zmiana dyrektywy 2015/849 do katalogu podmiotów, które muszą co najmniej podlegać obowiązkowi rejestracji, wprowadziła podmioty świadczące usługi wymiany walut pomiędzy walutami wirtualnymi a fiducjarnymi i dostawców kont waluty wirtualnej, czyli wyżej wskazane VASPy. Natomiast art. 38 pkt 7 Rozporządzenia 2023/1113 usunął te dwie kategorie podmiotów ze wskazanego katalogu. Co na pierwszy rzut oka może wydawać się interesujące – nie zmienił on brzmienia art. 47 ust. 1 dyrektywy 2015/849 w taki sposób, aby wyraźnie wskazać, że CASPy powinny być np. podmiotami regulowanymi czy takimi, które muszą uzyskać zezwolenie. Innymi słowy, nie mamy do czynienia z zabiegiem, gdzie brzmienie przepisu zostało zmienione w taki sposób, że dotychczasowe podmioty zostały zastąpione nową kategorią. Jak zwraca się uwagę w doktrynie, miało to na celu uniknięcie powielania czy duplikowania wymogów licencyjnych (Tomczak & Weck, 2024, V. *Authorisation*). Obecnie obowiązek uzyskania zezwolenia przez CASPy będzie wynikał z MiCAR, a zatem nie ma potrzeby, aby był on nałożony również przez przepisy AML. Tylko na marginesie należy zwrócić uwagę, że pewnym podmiotom na gruncie MiCAR przysługuje tzw. przywilej notyfikacyjny i tym samym nie ciąży na nich obowiązek uzyskania zezwolenia na gruncie MiCAR (dokładniej: Cegłowski, 2024).

Mogłoby się wydawać, że na podstawie powyższego można stwierdzić, że dotychczasowy obowiązek rejestracji VASPów został zastąpiony przez wymóg uzyskania zezwolenia przez CASPy. Należy jednak zwrócić uwagę, że wynikający z Dyrektywy

2015/849 obowiązek rejestracji był minimalnym standardem i państwa członkowskie mogły nałożyć dalej idące wymogi licencyjne/regulacyjne. W literaturze zwrócono uwagę, że pomiędzy państwami członkowskimi zaczęły pojawiać się znaczne różnice w tym zakresie (Stolarski, 2023, s. 62). Przykładowo, jeszcze przed omawianą zmianą w Niemczech do świadczenia usług finansowych związanych z kryptoaktywami sama rejestracja była niewystarczająca i podmiot musiał uzyskać odpowiednie zezwolenia na gruncie niemieckiego prawa bankowego (dokładniej: Tomczak & Weck, 2024, VI. *Authorisation*). Powyższe oznacza, że dzięki omawianej zmianie występujące obecnie różnice reglamentacyjne/rejestracyjne powinny w przyszłości zniknąć. Podsumowując, na gruncie Dyrektywy 2015/849 wymóg rejestracji został zastąpiony wymogiem uzyskania zezwolenia. Obowiązek ten będzie wynikał z MiCAR, a nie przepisów AML.

5. Organy nadzoru

Art. 48 ust. 1 Dyrektywy 2015/849 stanowi, że państwa członkowskie zobowiązują właściwe organy do skutecznego monitorowania i podejmowania niezbędnych środków służących zapewnieniu przestrzegania niniejszej dyrektywy. Zarówno poprzednia zmiana dyrektywy 2015/849, jak i art. 38 Rozporządzenia 2023/1113 nie zmieniły brzmienia tego artykułu. Mogłoby się zatem wydawać, że niniejsza część artykułu jest niepotrzebna. Należy jednak zwrócić uwagę, jak zostało to już zaznaczone powyżej, że CASPy będą obecnie z punktu widzenia unijnych przepisów AML zaliczane do grona instytucji finansowych. Jeżeli dotychczas inny organ bezpośrednio nadzorował VASPy, a inny instytucje finansowe, to obecnie sytuacja się zmieni. Art. 93 ust. 1 MiCAR stanowi, że państwa członkowskie wyznaczają właściwe organy odpowiedzialne za wykonywanie funkcji i obowiązków przewidzianych w MiCAR. Podmiot ten będzie m.in. wydawał zezwolenia na świadczenie krypto-usług CASPom i m.in. w tym zakresie nadzorował CASPy. Tym samym omawiane w niniejszym artykule zmiany zapewne już doprowadziły – albo dopiero doprowadzą – do tego, że w państwach członkowskich dojdzie, przynajmniej do pewnego stopnia, do zmian w organach odpowiedzialnych za nadzór nad rynkiem kryptoaktywów. Przykładem może być Polska, gdzie najprawdopodobniej dotychczasowy nadzór nad VASPami przez Generalnego Inspektora Informacji Finansowej zostanie w dużym stopniu zastąpiony przez nadzór sprawowany przez Komisję Nadzoru Finansowego (dokładniej: Stolarski, 2023, s. 62–63 oraz Urząd Komisji Nadzoru Finansowego, 2025)[15].

15 Zob. również art. 20 projektu ustawy o kryptoaktywach (projekt z dnia 22 lutego 2024), który stanowi, że organem właściwym w rozumieniu art. 93 ust. 1 MiCAR jest Komisja Nadzoru Finansowego.

Wnioski

Celem niniejszego artykułu było przyjrzenie się najważniejszym zmianom odnośnie do unijnego nadzoru AML nad kryptoaktywami wprowadzonymi do dyrektywy UE 2015/849 przez rozporządzenie UE 2023/1113. Przeprowadzona analiza prowadzi do wniosku, że z dniem 30.12.2024 r. owy krajobraz nadzorczy został znacznie przemodelowany. Zmienia się przedmiot nadzoru (kryptoaktywa zamiast walut wirtualnych), rozszerzono zakres nadzorowanych usług, dodatkowo zamiast VASPów nadzorowane będą CASPy, które z perspektywy AML powinny być kwalifikowane jako instytucje finansowe, a minimalny wymóg rejestracji został zastąpiony wymogiem uzyskania zezwolenia. Zmiany te mają na celu uszczelnienie unijnego nadzoru AML/CFT nad kryptoaktywami.

Powyższa analiza prowadzi też do bardziej generalnych wniosków. Pojęcia kryptoaktywów, usług w zakresie kryptoaktywów oraz dostawców usług w zakresie kryptoaktywów zostały w istocie i jedynie z niewielkimi modyfikacjami zdefiniowane przez odesłanie do słowniczka zawartego w MiCAR. Takie podejście należy ocenić pozytywnie, gdyż ujednolicenie terminologii powinno zapewnić większą spójność unijnego prawa dotyczącego kryptoaktywów. Co więcej, przyjęta optyka pozwala postawić tezę, że unijny prawodawca postrzega rozporządzenie MiCA jako akt prawny o charakterze systemowym dla rynków kryptoaktywów. Wydaje się, że powoli kształtuje nam się nowa dziedzina prawa, tj. prawo kryptoaktywów.

BIBLIOGRAFIA

Cegłowski, M. (2024). Dopuszczalność i zasady świadczenia usług objętych Rozporządzeniem MiCA przez podmioty finansowe. *Monitor Prawa Bankowego*. (7–8), 61–79.

Ciechoński, T. (2024). Poślizg ustawy o kryptoaktywach grozi zamieszaniem z AML. https://www.prawo.pl/biznes/ustawa-o-rynku-kryptoaktywow-zmieni-ustawe-o-aml,530282.html

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1640 z dnia 31 maja 2024 r. w sprawie mechanizmów, które państwa członkowskie powinny wprowadzić w celu zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca dyrektywę (UE) 2019/1937 oraz zmieniająca i uchylająca dyrektywę (UE) 2015/849 (Dz.U. UE. L. z 2024 r. poz. 1640).

Dyrektywa Parlamentu Europejskiego i Rady (UE) z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz.U. UE. L. z 2018 r. Nr 156, str. 43).

Dyrektywy (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. UE. L. z 2015 r. Nr 141, str. 73 z późn. zm.).

EBA (2024). *Final Report EBA/GL/2024/01*, Paris: EBA Publishing. https://www.eba.europa.eu/sites/default/files/2024–01/a3e89f4f-fbf3–4bd6–9e07–35f3243555b3/Final%20Amending%20%20Guidelines%20on%20MLTF%20Risk%20Factors.pdf

ESMA (2024). *QA_2295*, https://www.esma.europa.eu/publications-data/questions-answers/

Golonka, A. (2020). Przeciwdziałanie praniu pieniędzy w obliczu zmian wprowadzonych IV i V dyrektywą AML. *Przegląd Ustawodawstwa Gospodarczego. 73*(4), 16–23.

Golonka, A. (2024). Unijny projekt "pakietu AML" – reforma czy rewolucja w zakresie przeciwdziałania praniu pieniędzy. *Ius Novum. 18*(2), 1–22.

Haffke, L., Fromberger, M. & Zimmermann, P. (2020) Cryptocurrencies and anti-money laundering: the shortcomings of the fifth AML Directive (EU) and how to address them, *Journal of Banking Regulation. 21*(2), 125–138.

Janczak, P. (2023). Planowane zmiany w europejskim systemie regulacji AML/CFT, *Monitor Prawniczy (dodatek)*. (9), 33–36.

Korus, K. (2024). Zakres przedmiotowy pojęcia kryptoaktywów w Rozporządzeniu MiCA, *Monitor Prawa Bankowego.* (7–8), 27–39.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (Dz.U. UE. L. z 2023 r. Nr 150, str. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U. UE. L. z 2023 r. Nr 150, str. 40 z późn. zm.)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1620 z dnia 31 maja 2024 r. w sprawie ustanowienia Urzędu ds. Przeciwdziałania Praniu Pieniędzy i Finansowaniu Terroryzmu oraz zmiany rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010 (Dz.U. UE. L. z 2024 r. poz. 1620).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1624 z dnia 31 maja 2024 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (Dz.U. UE. L. z 2024 r. poz. 1624).

Srokosz, W. (2017). Legalna definicja kryptowalut. w: W. Rogowski (ed.), *Regulacje finansowe: fintech – nowe instrumenty finansowe – resolution*. (ss. 37–47), C.H. Beck.

Stolarski, K. (2023). Wpływ MiCA na regulacyjnoprawne uwarunkowania prowadzenia działalności z wykorzystaniem kryptoaktywów w Polsce i UE. *Monitor Prawniczy (Dodatek)*. (9), 62–66.

Tomczak, T. (2022). Crypto-assets and crypto-assets' subcategories under MICA Regulation. *Capital Markets Law Journal. 3*, 367–372.

Tomczak, T. (2023a). Ewolucja definicji kryptoaktywów w projekcie rozporządzenia MiCA. *Przegląd Prawa Handlowego. 3*, 37–44.

Tomczak, T. (2023b). Substantive scope of the MiCA Regulation. *Przegląd Prawniczy Allerhanda 6*, 1 (11), poz. 4, 45–58.

Tomczak, T. & Weck, T. (2024). Change of the AML/CFT regulatory landscape for crypto-assets – EU, Polish and German perspectives. *Zeitschrift für das Recht der digitalen Wirtschaft 2024/7–8*.

UKNF. (2025). *Stanowisko UKNF ws. stosowania Rozporządzenia MiCA w okresie przejściowym*, Warszawa: Publikacje UKNF, https://www.knf.gov.pl/?articleId=91955&p_id=18 (dostęp: 3.01.2025).

Wiącek, T. (2024). Obrót prawny w Web3 – uwolnienie obrotu dobrami wirtualnymi. *Przegląd Prawa Handlowego.* (7), 20–27.

Włoczka, R. & Windak, F. (2024). Wpływ nowych regulacji na ryzyka związane z nawiązywaniem stosunków gospodarczych z dostawcami usług w zakresie kryptoaktywów. *Monitor Prawniczy (Dodatek).* (9), 70–75.

Wyżykowski, B. (2024). Crypto-assets and crypto-asset services excluded entirely or partly from the scope of the regulation on markets in crypto-assets (MiCAR). *Monitor Prawa Bankowego.* (7–8), 80–98.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.09

Received: 29.01.2025
Accepted: 29.04.2025

Michal Kozieł
Palacký University, Olomouc, Czech Republic
michal.koziel@upol.cz
ORCID ID: https://orcid.org/0000-0001-8561-0358

Martin Cahlík
Palacký University, Olomouc, Czech Republic
martin.cahlik01@upol.cz
ORCID ID: https://orcid.org/0009-0001-4025-8941

Michael Kohajda
Palacký University, Olomouc, Czech Republic
michael.kohajda@upol.cz
ORCID ID: https://orcid.org/0000-0001-7235-0921

Simona Kurtinová
Palacký University, Olomouc, Czech Republic
simona.kurtinova01@upol.cz
ORCID ID: https://orcid.org/0009-0003-4273-4635

Digital Currency in the Context of the Czech Financial System: Legal and Regulatory Challenges for a Two-Tier Banking System[1]

Abstract: Central bank digital currencies are a topic that is currently receiving increasing attention. It is a type of money that brings significant innovations to the financial system. Because of the development of cryptoassets and their alternatives, states are also considering the possible introduction of digital currencies into their legal systems. However, the very definition of digital currency by central banks and the variety of different types of currency are challenges to its introduction. In addition, many jurisdictions

1 This research was supported by Czech Science Foundation Grant no. 24–12864S, named 'Cryptoassets as a Threat to the Sovereign'.

© 2025 Michal Kozieł et al. published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

do not currently allow for the introduction of these digital currencies and require some revision. This article aims to assess the Czech legal framework around the possibility of introducing central bank digital currencies in the Czech Republic. The authors also address the legislative challenges associated with implementing central bank digital currencies in general and specifically concerning the Czech Republic. The stated objective is achieved through scholarly methods of primary and secondary data analysis, followed by a comparison of starting points in different countries.

Keywords: CBDCs, central bank digital currencies, Czech Republic, monetary law, cryptoassets, two -tier banking systems

Introduction

Society has witnessed intense technological development over the past few decades. Major milestones include the development of computers, the internet, mobile phones and, more recently, artificial intelligence. All these areas significantly impact the world around us, as we have suddenly transitioned from originally using purely material exchanges to being able to experience a substantial part of our lives in the digital world. One of the significant outcomes of this development is the gradual introduction of cryptoassets into everyday practice, which have become a major part of our lives over the last decade. However, public authorities see cryptoassets as a substantial risk, as they are entirely out of their reach and very difficult to regulate. Indeed, the separation of cryptoassets from public power is also one of their significant benefits.

However, public authorities do not want to be left behind in this area of technological development. Many states are considering introducing digital currencies to complement or completely replace legal money in a given territory. These digital currencies are called central bank digital currencies (CBDCs), and their potential is considerable. Indeed, many countries are intensively exploring the possibility of introducing CBDCs into their legal systems. One such country is the Czech Republic, which, according to an analysis prepared by the Czech National Bank (CNB) (Česká národní banka, 2022, p. 3), is considering the conditions under which a digital currency could be introduced.

This article aims to evaluate the Czech legislation concerning the possibility of the central bank introducing a digital currency in the Czech Republic. Analysis will be used to achieve the stated objective, where the definition of CBDC, its basic categories and its relation to the banking sector will be defined based on general knowledge of CBDCs. Subsequently, the situation in different countries with more or less experience with the introduction of CBDCs will be compared, using a comparative method. Finally, an analysis of the primary legislation in the Czech Republic will be carried out to verify whether the existing legal framework allows for the introduction of a CBDC, and, if we conclude that this legislative framework is insufficient, the challenges for the future introduction of a CBDC into the Czech legal system will be identified and appropriate solutions proposed.

For the comparative analysis of experience with CBDC implementation in different jurisdictions, countries with different degrees of progress in this area are considered, with the selection reflecting geographical and economic diversity, different stages of the development of CBDC projects and the potential relevance of their legislative solutions for the Czech context. Although comparative analysis is not the primary objective of this study, it is an important methodological tool for identifying general trends and approaches that may be useful in assessing the potential for CBDC implementation in the Czech Republic. In a situation where the Czech Republic decides that it wants to issue its own CBDC (e.g. a digital koruna), it is necessary to make legislative changes so that there is a basis in law for issuing such a currency. This is the hypothesis of this article, which will be disproved or confirmed at the conclusion.

1. Literature review

There is a consensus in the literature on the basic concept of CBDCs as a digital form of central bank money, where there is a direct relationship between the holder and the central bank or another government-designated entity. This concept is supported by the definitions of leading monetary institutions (Bank for International Settlements, 2020, p. 3; Caccia et al., 2024, p. 6). In categorising CBDCs, the key distinction between the two main models in terms of implementation is between wholesale CBDCs, designed for interbank transactions, and retail CBDCs, available to the general public (Česká národní banka, 2022, p. 5). From a technological perspective, Auer and Böhme (2020) distinguish different implementation approaches, including direct, indirect and hybrid models.

CBDCs represent a significant innovation in 21st-century monetary policy. However, it is essential to note that the motivation for central banks to introduce them is not primarily driven by a need to digitise public administration or tax systems but, as Kohajda and Moravec (2021) suggest, by a need to respond to the dynamic development of cryptoassets, especially stablecoins. These cryptoassets represent a potential threat to the monetary sovereignty of states, motivating central banks to develop their own digital currencies (Bossu et al., 2020, p. 9). In their study for the Bank for International Settlements, Barontini and Holden (2019, p. 12) conclude that although central banks have a clear understanding of the challenges associated with CBDC implementation, most do not yet see sufficiently compelling evidence that the benefits of this innovation outweigh the associated costs.

Research in the field of CBDCs has increased significantly in recent years. Central banks and international organisations are engaged in a thorough analysis of the benefits and risks associated with their introduction (Barontini & Holden, 2019; Bindseil et al., 2024b; Česká národní banka, 2022; Griffoli et al., 2018). Academia is also actively contributing to the debate through a variety of research studies (Bae-

riswyl et al., 2024; Infante et al., 2024; Morales-Resendiz et al., 2021; Náñez Alonso et al., 2020; Nieborak, 2024). Jozipović et al. (2024) point out that when a CBDC is classified as legal tender, the state is responsible for protecting the integrity of transactions. This commitment includes the obligation to establish a clear regulatory framework, legal mechanisms for dispute resolution, creditor protection and effective sanction mechanisms against fraud or theft. This confirms that implementing CBDCs is a technological challenge and requires a comprehensive legal and institutional approach to ensure its functionality and credibility in practice.

The CNB has been reticent about the development of a digital currency. Although it started research on the CBDC in 2016, its analysis from 2022 (Česká národní banka, 2022, p. 19) did not show any significant advantages for the Czech Republic due to the stable use of cash and the low importance of other potential benefits. However, as Vodrážka et al. (2022) state in their analysis of the Bank for International Settlements, despite the current lack of a compelling case for the introduction of a retail CBDC, the activities of other central banks need to be closely monitored given the dynamic developments in this area. It should be noted that the legal issues surrounding the possible introduction of a CBDC in the Czech Republic still need to be resolved.

2. Central bank digital currencies

Central bank digital currencies are an entirely new technology with the potential to become the technological successor to current legal tender. It should also be noted, however, that CBDCs represent an innovation in the financial system of legal money that has not occurred for decades. CBDCs are defined as 'a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank' (Bank for International Settlements, 2020, p. 3). More generally, the Czech National Bank defines them as '[d]igital money that represents a direct claim of the holder on the central bank' (Česká národní banka, 2022, p. 4). Caccia et al. (2024, p. 6) also take a similar view, but expand the terms by stating that it must be issued by a central bank.

By comparing the above definitions, it can be concluded that CBDCs are defined by the following three features of the digital form: they have (1) an existence in the digital (immaterial) world; (2) the function of a payment instrument; and (3) a direct claim by the holder on the central bank (or the liability of the central bank on the holder). The first two features will undoubtedly be fulfilled in any form of CBDC, regardless of the form chosen. A problem arises when an indirect form of CBDC involves an intermediary that issues a CBDC derivative that is subsequently released into circulation by that intermediary, which must hold a reserve of the CBDC issued by the central bank equal to the amount of the derivative. In this scenario, however, it can no longer be established that the CBDC is a direct claim by the holder on the central bank; rather, it is only a claim to the amount of the CBDC derivatives on

a specific intermediary. In general terms, it can no longer be said to be a direct claim, even if compensation mechanisms are set up in case the intermediary issuing the CBDC derivative cannot meet the claim. Therefore, it is a matter for consideration whether the third aspect should correspond to a different feature, e.g. issuance by a central bank.

3. Forms of central bank digital currencies

Distinguishing between the different forms of CBDC is crucial for assessing the legislative and regulatory implications and the impact on the duality of banking systems. Each form requires a different legislative arrangement that will precisely define the rights and obligations of the individual addressees, particularly as each form or combination of forms changes the meaning, purpose, use and substance of the CBDC payment instrument.

Currently, CBDCs can be categorised from different perspectives. Those that have the most significant impact on the legislative framework include in particular the categorisation according to the entity that is allowed to use the CBDC, namely retail and wholesale CBDCs (Lau, 2018, p. 51). A retail CBDC is accessible to the general public for everyday transactions; in contrast, a wholesale CBDC is only for a limited number of entities, usually financial institutions and securities dealers, and is mainly used for large-volume transactions, which may be the settlement of securities claims between financial institutions or the settlement of transactions from a country's monetary policy instruments.

CBDCs can be further categorised according to how a particular CBDC unit is defined, either account-based (Pocher & Veneris, 2021, p. 1), where all CBDC units are held only in the form of balances in individual accounts (a principle essentially identical to regular bank accounts), or token-based (Pocher & Veneris, 2021, p. 2), where individual units within a token-based CBDC are issued with unique identification digits that identify the particular unit. These units are then stored by the CBDC holder in a digital wallet (either in the form of a software application or a hardware wallet) and disposed of using this wallet.

An equally important categorisation is the role of the central bank (or monetary authority) and intermediaries, whereby CBDCs can be categorised into 'direct, indirect, and hybrid' (Auer & Böhme, 2020, p. 89) forms. In the case of the direct form, the entity that issues the CBDC (usually the central bank) is essential in the entire structure; the entity takes care of all the existing processes, implements Know Your Customer and Anti-Money Laundering regulations, communicates directly with the holders and carries out all transactions. In this form, the CBDC holder has a direct claim against the issuing entity. However, we believe that most central banks in developed countries do not have the staff substrate to be able to provide all these processes.

Our position finds strong empirical support in the current implementation practice of CBDC projects at the global level, where all CBDC initiatives in the entire deployment, pilot or advanced development phase appear to adopt the indirect model, without exception (Auer et al., 2020, p. 39).

In a hybrid form of CBDC, some of the rights and obligations of the issuing entity are delegated to intermediaries, who then provide some of the processes that the issuing entity is unable (or unwilling) to provide. However, the direct claim of the CBDC holder against the issuing entity remains the holder's right. The indirect form of CBDC then aims at entrusting a large number of competencies to intermediaries, who must hold the same number of CBDCs in the issuing entity's reserves, which will be offered to the public in the form of CBDC derivatives (Auer & Böhme, 2020, p. 89). Auer and Böhme (2020, p. 89) mention in this context that the CBDC holder does not have a direct claim on the issuing entity but only on the derivative issuer, i.e. the intermediary, which then has a direct claim on the issuing entity. In this context, it should be noted that although the CBDC holder does not have a direct claim on the issuing entity, it is possible to characterise this claim as at least indirect, as it is likely that in the event of the bankruptcy or insolvency of the intermediary, it is still possible to satisfy the derivative holder from the reserves that are on deposit with the issuing entity. However, how the reserves will be paid out to the holders seems problematic, because the issuing entity cannot provide these CBDC units to the derivative holders, as at that point, it would no longer be an indirect model but a direct model, which is very unlikely to be allowed by legislation. However, transferring the reserves to another intermediary or compensating through a different payment method remains an option.

CBDCs can be classified into those that use a decentralised registry technology (such as distributed ledger technology (DLT)) and those that do not (Bossu, 2020, p. 10). While DLT-based CBDCs can provide benefits such as increased transparency, resilience to outages and the ability to better connect systems, implementing this technology also presents some challenges, including the complexity of managing scalability, transaction speed and power consumption (Sasongko & Yazid, 2020). Using centralised systems, an alternative approach offers more straightforward implementation and control over monetary policy but may be less resilient to attacks and failures. Hybrid models combining elements of DLT and centralised systems are currently being explored as a solution to balance efficiency and security. For example, proposals based on two-layer systems (wholesale and retail CBDCs) show the potential for linking DLT at the interbank transaction level with traditional systems for retail use (Guo et al., 2024).

Territorial usage possibilities refer to whether the CBDC can only be used within the national territory or whether it has some cross-border overlap. These two forms can be characterised as national on the one hand and cross-border on the other.

4. A two-tier banking system: Coexistence, substitution or cooperation?

CBDCs are a type of public money that brings fundamental innovation to the financial system. As noted above, each form of CBDC brings different technological and legislative challenges that affect the financial system and banking. Therefore the question remains whether it is possible to create a symbiotic (mutually beneficial) two-tier banking system, which, in the context of this paper, distinguishes between a private banking system, represented by commercial banks that offer their banking products (notably bank accounts and transfers between these accounts, where all these processes are recorded within the bank's internal system, or shared in the case of international payments), and a public banking system, which if adopted would be an account-based CBDC system that would work with legal tender and which would be more or less the responsibility of the particular central bank. Although a CBDC is currently seen primarily as an option to offer public funds to a large group of actors in a given economy and to preserve the monetary sovereignty of states, many legislators believe that it could also have a negative effect on the financial system in general (Ahnert et al., 2023, p. 2).

In assessing the impact on private banking when a state CBDC is issued, it is necessary first to answer the question of the purpose of issuing a CBDC. The focus needs to be on whether it is intended to replace the existing private banking system, whether it is a supplementary payment instrument to existing payment accounts and e-money, or whether some private–public cooperation in the CBDC area is envisaged. If the purpose of the CBDC is to replace the existing banking system entirely, it is clear that a two-tier banking system cannot be sustained at this point, and private commercial banking will be entirely replaced by state CBDC through legislation. On the other hand, it can be said that when the purpose of the CBDC is to coexist with the current private banking system, the primary purpose will only be to create an alternative payment instrument that will be able to attract a group of subjects who are not comfortable with the current private system or who do not trust it. Moreover, this system may coexist without some functional connection, or there may be bridges through which the CBDC can be exchanged for bank account deposits and vice versa. It is therefore a kind of competition. This is also how the purpose of the digital euro is defined, with the main reasons for its introduction being to make the financial system more efficient and reduce costs for financial service providers, to increase competition with private forms of money, to provide easier access to the currency by foreign investors, and to reduce the environmental impact of the financial system (European Central Bank, 2020, pp. 10–15).

Cooperation can be described almost identically to coexistence, with one significant difference: in the case of cooperation, the private commercial bank is part of the CBDC infrastructure and participates in their processes, i.e. in the indirect and hybrid forms. In these cases, there is still the possibility of a functioning private banking system participating in the CBDC. It is also possible to think of a cooperative arrangement

where the private banking system no longer performs the services currently associated with it and becomes merely a service provider where the central bank does not have the staff or facilities. However, we do not consider this option very realistic, as it would mean that commercial banks would lose a substantial part of their business and would have to sell off a large part of their assets and eliminate much of their staff.

We believe that it is also essential to consider that were a state to issue its own CBDC and wanted to maintain a two-tier banking system, it would be forced to assess whether an unrestricted CBDC could adversely affect the financial system. Given the institution of legal money, which a CBDC is and which possesses greater credibility than private money, it could threaten the liquidity of private banks, not only in crises (Ahnert et al., 2024, p. 4) but also in the case of the issuance of an unrestricted CBDC at the earliest stage, as trust in the state and the central bank may force institutions and entities to withdraw their bank deposits and put them into the state's digital money. Similar concerns exist for banking institutions regarding adoption of the digital euro (Bindseil et al., 2024a). However, the European Central Bank completely dismisses such concerns and sees the solution as being a limit on the amount of digital euros that an entity will be allowed to hold and the number of digital euros in circulation (Bindseil et al., 2024a).

5. Legislative challenges related to the implementation of central bank digital currencies

The legislative challenges that may arise in implementing CBDCs can be classified into two basic groups, which are, however, linked by a fundamental criterion, namely that of time. It is necessary to distinguish between challenges that occur before the development of a specific CBDC project and those that occur after the incorporation of a CBDC into the legal order. Regarding the former, this has to be considered in the research about and the actual selection of the specific form of CBDC that a particular state could use. It is necessary at this stage to concentrate the research, as a rule, on two parts, namely what form of CBDC is appropriate for a given state in terms of existing legal provisions, both national and international obligations, which would be either difficult or impossible to change or abolish. This is likely the case in legislation governing anti-money laundering and counterterrorism financing measures. It is therefore necessary at this stage to define how to design the CBDC project and, on the basis of a comprehensive legal and technological search, to choose a legal form that does not conflict with any regulations to which the country is bound. The second part is what are the legislative changes that will need to be made in the case of an individual CBDC after its completion and the possibility of incorporation into the legal system. This needs to be assessed in the case of a specific project and a comprehensive preparation for a given change in the legislative environment

needs to be undertaken, as otherwise it may happen that the CBDC project is ready, but the legislation that would allow it to be used is not.

If a particular state concludes that the benefits of issuing a CBDC outweigh the pitfalls and chooses an appropriate form, then it is necessary to determine whether the legislative challenges that precede the project launch also threaten that particular state. The competence of the central bank or monetary authority to issue CBDCs seems to be a very problematic legislative challenge. Academic publications document the lack of competence of most central banks or monetary authorities either to issue certain types of currency or to open and maintain accounts for various entities and persons (Bossu et al., 2020, p. 16). Bossu et al.'s research shows that '[a]mong the 171 central banks of the IMF membership, 61% of central bank laws limit the authority of issuance of currency to banknotes and coins' (2020, p. 21). However, they also add that for a further 16% of these banks, it is not directly apparent from the law whether or not they can issue anything other than coins and banknotes (Bossu et al., 2020, p. 21). This implies that 77% of central banks cannot or do not know whether they can issue anything other than coins and banknotes and thus are not authorised to issue any form of CBDC, whether token – or account-based, precisely because the competence of a central bank to issue a particular CBDC (whether the digital dollar, euro, zloty or koruna) is a prerequisite for it to come into existence. Although a token-based CBDC is sufficient to enshrine this basic competence, the situation is somewhat more complex in the case of account-based CBDCs.

Account-based CBDCs are, as mentioned above, almost identical in operation to bank accounts. Therefore it is necessary that the central bank, in addition to having the competence to issue a particular CBDC, can also open accounts for all entities of a given country or for entities that are exhaustively defined if this will suit the chosen form of CBDC. In this context, it is essential to distinguish between CBDCs intended for retail or wholesale entities. The statistics for retail account-based CBDCs are inarguable, with 85% of the 171 central banks not opening accounts for entities that are not exhaustively defined by law (Bossu et al., 2020, p. 23). Moreover, for another 9%, it is unclear whether they have the authority to open accounts for entities other than those specified by law (Bossu et al., 2020, p. 23). Thus it is possible to assume a set of central banks will have the authority to issue account-based CBDCs (assuming, of course, that they have the general authority to issue CBDCs, as discussed above). Still, the vast majority will not have the authority to hold entity accounts, and thus it is clear that retail account-based CBDCs must be legislated for before they can be issued.

It should also be mentioned that another monetary issue that may arise is whether CBDCs become legal tender at the moment of issuance or whether a legislative change is required. The answer to this question cannot be presented without further discussion. The situation must be examined from the perspective of the particular state, as the question of legal money will vary from jurisdiction to jurisdiction (Bank for International Settlements, 2024, p. 5), and this area must be examined

using legal methodology, which in theory can bridge the lack of exact language and grammar by purposive interpretation or other methods of legal methodology. It must be said, however, that while it is not necessary to grant a CBDC the status of lawful money, it is clear beyond doubt that without that status, the particular CBDC will not be given credence by the public, nor will the obligation among merchants and/or the public to accept it be very enforceable. On the other hand, before a given CBDC is made legal tender, all aspects associated with it (security, legal framework, intermediaries, etc.) must be adequately and comprehensively analysed and accounted for; otherwise, the issuing entity risks causing overwhelming damage to the economy of the country in question (Jozipović et al., 2024, p. 79).

A problematic aspect can also be seen in the potential threat to user privacy at a fundamental level. In the current world, user data (whether personal or business) can be seen as a kind of commodity that has a fundamental economic value (Murphy et al., 2024, p. 1). This economic significance is overlooked in the CBDC system compared to other types of payment instruments (in the case of the direct CBDC model). Still, even though this fundamental problem of private payment instruments is overlooked, there may be a significant issue in the possibility of the CBDC being seen as a tool of state surveillance (Murphy et al., 2024, p. 2). However, this is only one of the pitfalls that may arise in this regard; as Schueffel argues, others may be the restriction and blocking of specific users or the restriction of the purchase of certain goods or, conversely, the promotion of other goods by the state or an adverse interest (Schueffel, 2023, pp. 52–53). However, a form of CBDC based on DLT and in an indirect or hybrid form can be viewed differently; in this respect, the threat to users by private actors is no less than that of conventional payment instruments. The solution to this problem, though, is technologically and legally complex, as also noted by Hrabčák and Štrkolec (2024, p. 41). Both technological and legal perspectives must be applied at the outset to prepare the technological infrastructure. The key is a model that ensures that all data is cyber-protected, not misused and used only to the extent necessary. It can be argued that the envisaged digital euro model is suitable for user privacy, as European Union legislation is robust regarding user data protection (e.g. GDPR). At the same time, however, it is assumed that digital euro data will be pseudonymised, that data in the system will only be available to the extent critical to the functioning of the currency, and that the data will also be under the complete control of the user (European Central Bank, 2023, pp. 38–39).

6. Analysis of the challenges in Czech legislation and possible solutions

Czech legislation also contains several legislative challenges, which have been mentioned above. The existing key legislation for the Czech Republic is Act no. 6/1993

Sb. on the Czech National Bank, as amended, which defines the Czech National Bank as the key institution in the area of banknote and coin issuance in the country. It follows from the provisions of Section 12 of this Act that the Czech National Bank is granted the right to issue coins, banknotes and commemorative coins and notes (Act on the Czech National Bank, 1993). Suppose we focus on the linguistic interpretation of this provision; in that case, it is necessary to conclude that the Czech National Bank is entitled to issue only the exhaustively specified monetary instruments and that it is not competent to issue any monetary instruments other than coins and banknotes. The conclusion, therefore, remains that the Czech National Bank is not authorised to issue CBDCs without a change in the law. We can then analyse the provisions of Section 14 of the Act on the Czech National Bank, which state that the Bank 'shall manage the stock of banknotes and coins and organise the supply of banknotes and coins from manufacturers by the requirements of money circulation', and Section 15: 'the Czech National Bank arranges for the printing of banknotes and the minting of coins and supervises the protection and security of banknotes and coins not issued for circulation and the safekeeping and destruction of printing plates, stamps, and invalid and scrapped banknotes and coins' (Act on the Czech National Bank, 1993). From these provisions, it is possible to identify the keywords used to confirm the above thesis. We conclude that the Czech National Bank manages the stock, custody and destruction of printing plates, stamps, and invalid and discarded banknotes and coins, and organises the supply of banknotes and coins from manufacturers. It follows that coins and banknotes are of a material nature, not digital; thus in a more metaphysical interpretation, we must conclude that they are only material, and not even apparently digital. Given that CBDC technology is relatively new, we consider it irrelevant to apply a subjective-historical interpretation, since it is clear that it could not have been the intention of the legislature at the time of the adoption of the Czech National Bank Act to cover these modern technologies as well. In conclusion, the Czech National Bank is not authorised to issue token-based CBDCs under the current legal framework.

Similar but different is the situation in the case of account-based CBDCs, where the Czech National Bank is very similar to other central banks of states that are members of the International Monetary Fund, in terms of the possibility of opening accounts for entities other than those specified in law. As can be seen from the provisions of Section 33 of Act no. 218/2000 Sb. on Budgetary Rules, the Czech National Bank is authorised to maintain 'Treasury accounts and accounts subordinate to the Treasury' (Act on Budgetary Rules, 2000). These specified entities are the state, organisational units of the state, the State Fund and the National Fund, contributory organisations established by the state, the Railway Administration, territorial self-government units, public research institutions, public universities, public health insurance companies, other legal entities with the consent of the Ministry of Finance, the Export Guarantee and Insurance Corporation, the Czech Export Bank and state enterprises. According to the provisions of Section 32 of the Act on the Czech Na-

tional Bank, the Bank is also authorised to maintain accounts for banks, foreign banks, savings and credit cooperatives and, according to the provisions of Section 34, for employees of the Bank. In conclusion, it is possible to say that although the Czech National Bank is not granted the competence to issue CBDCs in the general sense, if this competence existed, it would at least have a legislative basis for issuing wholesale account-based CBDCs that would be available to the above-mentioned entities. If the Bank were empowered to issue CBDCs and, in addition, were granted the competence to issue retail account-based CBDCs, the necessary legislative change would be minimal. It would essentially correspond to either an extension of the entities that are currently in the legislation in force or, on the contrary, a complete change in the provision could be made, granting the Czech National Bank the power to open and maintain accounts to all entities (i.e. including the general public).

It is evident that the problem of the Czech National Bank's lack of authority to issue CBDCs cannot be overcome by interpretation or analogy, and it is necessary to amend the wording of the Act. However, any change in the law cannot be made without defining what CBDCs really are. We assume defining what a CBDC means in Czech terms is initially necessary; we believe the ideal concept is 'a digital koruna is the digital equivalent of coins and banknotes'. However, this concept can only be applied to amending the Act on the Czech National Bank by extending the current wording of Section 12 of Act no. 6/1993 Sb. on the Czech National Bank to read: 'The Czech National Bank has the exclusive right to issue banknotes, coins, and the Digital Koruna.' However, it should be noted that this change in the law would allow the CNB to issue only token-based, not account-based, CBDCs. For the CNB to be empowered by law to issue account-based CBDCs, the definition of a 'digital koruna' would have to be changed, so that the new definition would read: 'The Digital Koruna is a representation of the Czech koruna that is held in the form of balances in a payment account that is maintained on the Digital Koruna network.' Of course, the provisions of Section 12 would have to be modified identically, as stated above. It would also be necessary to extend the provisions of Section 34 of Act No 6/1993 Sb. by adding a third paragraph, reading: 'The Czech National Bank is the exclusive entity that may open and manage bank accounts held on the Digital Koruna network or delegate this authority to another financial institution.' This amended provision of Section 34(3) of the Act also allows for the consideration of the possibility of a direct, indirect or hybrid CBDC model and in conjunction with Section 12 of the Act also allows the CNB to issue account-based CBDCs.

The issue of legal tender is also applicable in Czech law, specifically in the provisions of Section 16 of the Czech National Bank Act, which states that only '[v]alid banknotes and coins issued by the Czech National Bank are legal tender in their face value for all payments in the Czech Republic' (Act on the Czech National Bank, 1993). If the state wishes to have a CBDC enshrined as legal tender, it is necessary

to extend the wording of the Act to include CBDCs as a form of legal tender; otherwise, they cannot automatically become legal tender.

Conclusion

Although introducing CBDCs in the Czech environment might initially seem simple, the opposite is true. The very definition of the forms of CBDC brings us to a situation where each has its specificities and differences. The definition of CBDCs also appears to be complicated. In addition, each type of CBDC impacts the legislative environment and needs to be regulated differently, or legislative changes need to be applied to introduce them. This is similar to the case of the two-tier banking system, which is possible where the purpose of the CBDC is not to replace the private banking system, but the CBDC must then be issued in a phased manner. In addition, the total number of CBDCs must be limited to minimise the risk of jeopardising the stability of the monetary system.

In the event of an attempt to introduce CBDCs into the Czech legal system, the state has to deal with many challenges. The most pressing of these are legislative, where changes to legislation would need to be made to correspond with the chosen CBDC concept. The Czech National Bank, as the key authority in the area of the monetary system, will of course play a crucial role in this process. The legislative challenges must be dealt with both before the preparation of the CBDC project and before the implementation of the CBDC into the legal system. Our analysis of the Czech legislation showed the above results, where a solution was also outlined, which may not be applicable in all countries but is sufficient for the Czech Republic.

As follows from Czech legislation, in cases where a legislature (whether Czech or foreign) decides to issue a national CBDC, it is absolutely essential that the initial research is focused on a legislative assessment of whether the individual models are compatible with the current legislation and whether there is no need to change the law at a very basic level, as it is absolutely clear from the currently available statistics that most states do not have the legal basis to simply issue a CBDC and the powers to do so do not exist. In Sweden, for example, even if one spent several years on research and arrived at a successful or working prototype CBDC, one is not able to issue a CBDC without the active involvement of the legislature. It can therefore be concluded that legislation should have been prepared before the prototype was ready.

In conclusion, given the above, Czech legislation does not currently allow for the direct introduction of a CBDC in the Czech Republic. It is therefore evident that the hypothesis that was set out above has been confirmed, and it is obvious that each of the options considered here would ultimately lead to a need to change the laws in the Czech Republic, as they do not meet the requirements of a digital currency as defined by the Czech National Bank. On the other hand, it should be noted that no insur-

mountable obstacle would prevent the introduction of a CBDC. The Czech Republic should consider active research into and the possible initiation of CBDC prototypes, as such a payment system may be an interesting alternative to the current cash or non-cash system. Legislative pitfalls are only a political problem in the Czech Republic, since law is not that complicated to change.

REFERENCES

Act no. 6/1993 Sb., on the Czech National Bank, wording from 01.11.2024. https://www.e-sbirka.cz/sb/1993/6?zalozka=text

Act no. 218/2000 Sb., on Budgetary Rules and Amendments to Certain Related Acts (Budgetary Rules), wording from 19.02.2025. https://www.e-sbirka.cz/sb/2000/218/2025–02-19?zalozka=text

Ahnert, P., Leonello, A., & Procellacchia, D. (2023). *Central bank digital currency and financial stability*. European Central Bank. https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2783~0af3ad7576.en.pdf

Auer, R., & Böhme, R. (2020). *The technology of retail central bank digital currency*. BIS Quarterly Review. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561198

Auer, R., Cornelli, G., & Frost, J. (2020). *Rise of the central bank digital currencies: Drivers, approaches and technologies* [Working paper no. 880]. Bank for International Settlements. https://www.bis.org/publ/work880.pdf

Baeriswyl, R., Reynard, S., & Swoboda, A. (2024). Retail CBDC purposes and risk transfers to the central bank. *Swiss Journal of Economics and Statistics*, *160*(1). https://doi.org/10.1186/s41937–024-00124–3

Bank for International Settlements. (2020). *Central bank digital currencies: Foundational principles and core features*. https://www.bis.org/publ/othp33.pdf

Bank for International Settlements. (2024). *Central bank digital currencies: Legal aspects of retail CBDCs*. https://www.bis.org/publ/othp88_legal.pdf

Barontini, C., & Holden, H. (2019). *Proceeding with caution: A survey on central bank digital currency* [BIS papers]. Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap101.htm

Bindseil, U., Cipollone, P., & Schaaf, J. (2024a) *Digital euro: Debunking banks' fears about losing deposits*. The ECB blog. https://www.ecb.europa.eu/press/blog/date/2024/html/ecb.blog20240219~ccb1e8320e.en.html

Bindseil, U., Marrazzo, M., & Sauer, S. (2024b). *The impact of central bank digital currency on central bank profitability, risk-taking and capital* [Occasional paper series no. 360]. European Central Bank. https://doi.org/10.2866/1376869

Bossu, W., Itatani, M., Margulis, C., Rossi, A., Weenink, H., & Yoshinaga, A. (2020). *Legal aspects of central bank digital currency: Central bank and monetary law considerations*. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020254-printpdf.ashx

Caccia, E., Tapking, J., & Vlassopoulos, T. (2024). *Central bank digital currency and monetary policy implementation* [Occasional paper series no. 345]. European Central Bank. https://doi.org/10.2866/710472

Česká národní banka. (2022). *Digitální peníze centrálních bank*. https://www.cnb.cz/export/sites/cnb/cs/platebni-styk/.galleries/digitalni-penize-centralnich-bank-cbdc/download/digitalni-penize-centralnich-bank-CBDC.pdf

European Central Bank. (2020). *Report on a digital euro*. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf

European Central Bank. (2023). *A stocktake on the digital euro*. https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs231018.en.pdf

Guo, S., Kreitem, J., & Moser, T. (2024). DLT options for CBDC 1. *Journal of Central Banking Theory and Practice*, *13*(1), 57–88. https://doi.org/10.2478/jcbtp-2024–0004

Hrabčák, L., & Štrkolec, M. (2024). EU regulation of the crypto-assets market. *Białostockie Studia Prawnicze*, *29*(1), 27–45. https://doi.org/10.15290/bsp.2024.29.01.02

Infante, S., Kim, K., Orlik, A., Silva, A. F., & Tetlow, R. (2024). Retail CBDC: Implications for banking and financial stability. *Annual Review of Financial Economics*, *16*(1), 207–232. https://doi.org/10.1146/annurev-financial-082123–105958

Jozipović, Š., Perkušić, M., & Mladinić, N. (2024). A comparative review of the legal status of national cryptocurrencies and CBDCs: A legal tender or just another means of payment. *Pravni Vjesnik*, *40*(1), 77–96. https://doi.org/10.25234/pv/27044

Kohajda, M., & Moravec, J. (2021). Legal issues of stablecoins. *Daně a finance*, *28*(1–4), 93–98.

Lau, Y. M. et al. (2018). *Cross-border interbank payments and settlements: Emerging opportunities for digital transformation*. https://ink.library.smu.edu.sg/sis_research/7562

Mancini-Griffoli, T., Martinez Peria, M. S., Agur, I., Ari, A., Kiff, J., Popescu, A., & Rochon, C. (2018). *Casting light on central bank digital currency*. International Monetary Fund. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233

Morales-Resendiz, R., Ponce, J., Picardo, P., Velasco, A., Chen, B., Sanz, L., Guiborg, G., Segendorff, B., Vasquez, J. L., Arroyo, J., Aguirre, I., Haynes, N., Panton, N., Griffiths, M., Pieterz, C., & Hodge, A. (2021). Implementing a retail CBDC: Lessons learned and key insights. *Latin American Journal of Central Banking*, *2*(1). https://doi.org/10.1016/j.latcb.2021.100022

Murphy, K., Tao, S., Zhou, S. Y., Tsuda, N., Zhang, N., Budau, V., Solomon, F., Kao, K., Vucinic, M., & Miggiani, K. (2024). *Central bank digital currency data use and privacy protection* [Fintech notes 2024/004]. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/FTN063/2024/English/FTNEA2024004.ashx

Náñez Alonso, S. L., Echarte Fernández, M. Á., Sanz Bas, D., & Kaczmarek, J. (2020). Reasons fostering or discouraging the implementation of central bank-backed digital currency: A review. *Economies*, *8*(2). https://doi.org/10.3390/economies8020041

Nieborak, T. (2024). Central bank digital currency as a new form of money. *Białostockie Studia Prawnicze*, *29*(1), 189–203. https://doi.org/10.15290/bsp.2024.29.01.12

Pocher, N., & Veneris, A. (2021). *Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme*. SSRN. https://ssrn.com/abstract=3759144

Sasongko, D. T., & Yazid, S. (2020). Integrated DLT and non-DLT system design for central bank digital currency. In *Proceedings of the 5th International Conference on Sustainable Information Engineering and Technology* (pp. 171–176). https://doi.org/10.1145/3427423.3427447

Schueffel, P. (2023). CBDCs: Pros and cons. A comprehensive list and discussion of the advantages and disadvantages of central bank digital currency. *Journal of Digital Assets*, *1*(2), 49–56. https://doi.org/10.23164/journal.230808.000004

Vodrážka, M., Bízek, T., & Vojta, M. (2022). *Are there relevant reasons to introduce a retail CBDC in the Czech Republic from the perspective of the payment system?* [BIS papers no. 123]. Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap123_g.pdf

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.10

Received: 29.12.2024
Accepted: 3.07.2025

Luljeta Plakolli-Kasumi
University of Prishtina, Kosovo
luljeta.plakolli@uni-pr.edu
ORCID ID: https://orcid.org/0000-0002-5806-3683

AI in the Banking Sector: Lessons from the Schufa Case

Abstract: The advent of Artificial Intelligence (AI) has opened many opportunities and, equally, has brought many challenges. This is also true for the banking sector, as the Schufa case attests. The purpose of this paper is to examine the CJEU's decision in the Schufa case regarding AI use within the banking sector and its legal implications. This case questions recent practices concerning credit scoring and demands more robust protection of individual rights and a more accountable use of AI in the financial sector. The ongoing dependence of banks on automated decision-making to assess the creditworthiness of their clients raises important questions about transparency and fairness regarding the outcomes of such assessments. The paper offers an analysis of the GDPR, namely Article 22(1), and the criteria for automated decision-making clarified in the Schufa case, particularly in situations that fall outside the scope of the GDPR.

Keywords: AI in banking, automated decision-making, data protection, individual rights, legal implications

Introduction

Today, bank services are just a click away (Gavrila, 2024, p. 1415), thanks to the digital transformation that has come with the advent of the internet (Kozak & Golnik, 2020, pp. 285–286). Artificial intelligence (AI) has further transformed how banks operate and interact with their clients, enabling banks to optimise back-office processes, reduce costs, and increase productivity (Srivastava, 2024). One such process is credit scoring, 'a statistical method used to predict the probability that a loan applicant, existing borrower, or counterparty will default or become delinquent' (World Bank, 2019, p. 2). In other words, through credit scoring, banks assess the creditworthiness of their clients before deciding whether to disburse a loan. Not only that: as

© 2025 Luljeta Plakolli-Kasumi published by Sciendo.
This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

discussed by Hurley and Adebayo (2016, p. 154), credit reports are also reviewed by employers and landlords, thus significantly affecting individuals.

Banks used to evaluate a client's creditworthiness based on credit bureau registries, which contained traditional and structured data such as employment and borrowing history, loan repayments, account balance, and such like (Bertrand & Klein, 2021, p. 3). However, in the era of big data, credit registries have started to rely more on unstructured data (Nan Jiang & Novik, 2021), such as mobile phones, social networks (Óskarsdóttir et al., 2019, pp. 27–28), behavioural loan tracking, location-based information, and mobile app data (Jiang et al., 2021), among others. AI has reconceived credit scoring by leveraging algorithms to analyse a wide range of data sources and predict the 'future financial behaviour' of clients (Cariaga, 2024).

In addition to assessing creditworthiness, AI-powered credit scoring is also used to detect fraudulent activities (Zagha, 2024). AI enables automated decision-making, whereby a third party, usually a private agency, uses AI-powered algorithms to assess the creditworthiness of an individual who applies for a loan, and lenders rely on this credit scoring to decide whether to grant the loan or not (Ettorre, 2023). Despite its advantages and the contention that it provides for more accurate predictions (Vidal & Menayovski, 2019), research suggests that it has also made credit scoring less transparent and more biased and unexplainable (Heaven, 2021). Because the AI used to make this assessment is trained upon existing data, which can be biased, it can only exacerbate existing divides (Vidal & Barbon, 2019, p. 6).

In the face of these advances, the Schufa case substantiates the ongoing tensions between technological advancements and safeguards for individual human rights and freedoms. While automated credit scoring reduces time and allows for more tailored financial services, it may discriminate against certain groups. The large amounts of data gathered from different structured and unstructured sources and fed into these algorithms may lead to an unfair playing field for consumers who want to access financial instruments. The so-called 'black box' feature of these algorithms makes the model unexplainable, difficult to understand, and less transparent for consumers. Hence the decision in the Schufa case helps us understand these complexities and paves the way for a more balanced approach between the utilisation of AI in banking services and more robust safeguards for individual human rights and freedoms.

1. AI uses in the banking sector: Algorithmic assessment of creditworthiness

A literature review attests to banks' growing reliance on automated decision-making processes. Credit ratings, predictions of bank failure, and the detection of cyberthreats are some of the many other instances where AI is used in the banking industry (Farishy, 2023, pp. 1726–1729). AI also accelerates anti-money launder-

ing operations (Jain, 2024) and, furthermore, allows for more personalised banking experiences and tailored financial advice (Narang et al., 2024, p. 131) through natural language processing for customer service automation and AI-powered chatbots (Kolleshi & Golemi, 2024, p. 77; Tabaku et al., 2025, p. 4178–4179). The use of AI in banking services has become a necessity rather than discretionary (Fares et al., 2022), giving rise to Banking 4.0, which integrates state-of-the-art technology in the daily operations of banks (Polireddi, 2024, p. 1).

Credit scoring, another expansion of AI in the banking industry, has changed how banks assess their clients' soundness; it largely departs from traditional methods involving subjectivity and bias in the assessment process (De Moor et al., 2018; Hughes, 2019). While automated credit scoring has reduced human intervention, hence subjectivity, it is not immune to biases, since the data used to train algorithms can also contain historical, selection, and measurement biases (Boyer, 2024). Moreover, these algorithms are unexplainable; therefore automated decisions based on algorithmic data lack the justification a human decision would provide. If individuals cannot understand how and why certain decisions affecting them are made by algorithms, challenging those decisions becomes difficult and issues of fairness and transparency emerge. Consumers should be able to challenge automated decisions, especially those that greatly affect their lives, such as loan decisions. A statement of reasons is instrumental in challenging a decision (Ettorre, 2022), and automated decisions contain no such reasoning.

2. 'Automated' decision-making under the General Data Protection Regulation

The General Data Protection Regulation (GDPR) provides safeguards against the effects of automated decisions (Silveira, 2023). Article 22(1) provides that 'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Article 22(1) has sparked many debates about its nature, namely whether it provides for an active or a passive right of the data subject. Some authors view it as a provision conferring the active right that should be invoked by the subject (Tosoni, 2021), while others view it as a general prohibition, namely an inherent right (Pery & Simon, 2024). National courts of the EU Member States have also interpreted Article 22 as a 'general prohibition' (Kuner et al., 2021, p. 96).

Another ambiguity concerning Article 22(1) revolves around the 'solely automated' criteria. As boundaries between human and automated decision-making are often blurred (Council of Europe, 2016, p. 4), courts have been called upon to interpret whether 'semi-automated decision-making' falls within the wording of Article 22(1). Several national courts have interpreted this provision narrowly, thus

excluding from its application decisions that involve human judgement in the process (Kuner et al., 2021, p. 98). Courts have so far upheld that meaningful human involvement in automated decision-making ensures the lawfulness of the processing (Judgment of the Amsterdam Court of Appeal, 2023). 'Meaningful' is the key word, implying that human intervention must be active and undertaken by someone with 'authority, competence, capacity, diligence or independence' (AEPD, 2024). These criteria must be assessed on a case-by-case basis. Evidence for and explanation of this active and meaningful intervention must be presented to data subjects, as ruled by the Amsterdam Court of Appeal in the Uber case (Judgment of the Amsterdam Court of Appeal, 2021). This approach ensures the transparency, explainability, and supervision of algorithms, which are the main principles enshrined in the GDPR, aswell as key quality requirements for AI systems (Balasubramaniam et al., 2023, p. 2).

Another key requirement of Article 22(1) of the GDPR concerning automated decision-making is that such decisions must produce legal effects or significantly affect the data subject. The increasingly widespread use of automated decision-making algorithms has raised many concerns about the legal and societal impact of such decisions. There have been many devastating cases where people have been deprived of their fundamental human rights because of algorithmic bias. As emotionless and mechanical decision-makers (Woodruff et al., 2020, p. 5), these algorithms are opaque (Stefanski & Żywolewska, 2024, pp. 54–55, 58) and may yield biased and discriminatory outcomes, which are difficult to understand and challenge (Vaassen, 2022, pp. 2–3). Algorithms are important in determining various critical decisions, including selecting candidates for employment, prioritising patients for medical treatment, and approving loans, rental agreements, or college admissions (Ananya, 2023). The childcare benefits scandal in the Netherlands is the most demonstrative example of how algorithms can significantly and negatively impact the lives of many. The Dutch tax authority relied on self-learning algorithms to detect cases of incorrect and fraudulent childcare allowances. The algorithm was based on racial profiling and consequently led to many low-income families being falsely accused of fraud and their lives being ruined (Amnesty International, 2021). The case of Amazon is another example of a biased algorithm that excluded women from certain technical jobs (Dastin, 2018); the algorithm disproportionately weighted features such as gender (Rejmaniak, 2021, p. 32). Such decisions further aggravate gender inequalities, thus significantly affecting women entering the job market.

If all three of the abovementioned requirements are cumulatively met, the data subject has the right to request from the controller meaningful information about the logic involved in such decision-making, according to Article 15(1)(h) of the GDPR, unless exceptions provided in Article 22(2) apply. According to Article 22(2), paragraph (1) does not apply if 1) the decision is necessary for purposes of the contract between the data subject and a data controller, 2) proper safeguards are guaranteed

by the law to which the controller is subject, and 3) the decision is based on the data subject's explicit consent.

The recent judgment of the CJEU in the Schufa case has sparked a heated debate among academics and the banking industry. The ruling provides a broader interpretation of what constitutes automated decision-making given the significant effect that automated credit scoring may have on bank clients applying for loans.

3. The Schufa case

The Schufa case concerns an automated credit scoring that was provided by Schufa, a German private agency, to a bank regarding a client who was applying for a loan. An algorithm was used to determine the client's creditworthiness, which provided a low score (probability value) and ultimately led to the bank's refusal of the loan request. The client asked Schufa to disclose the data used for this scoring and erase allegedly incorrect data (Judgment of the CJEU, 2023, paras 14–15). Schufa denied the request, citing trade secrecy, and explained that it had a contractual arrangement with the bank, which provided that the bank receives automated credit scoring by Schufa, and that the final decision concerning loan disbursement lies with the bank (para. 16). As a second step, the client addressed the German Data Protection Authority (DPA) in Hesse with a request to be granted access to information and erasure (para. 17). The DPA rejected the request based on a lack of evidence regarding Schufa's non-compliance with the legal data protection requirements (para. 18). The client appealed the decision of the DPA before the Administrative Court in Wiesbaden, Germany (para. 19). The latter stayed the proceedings and made a request for a preliminary ruling from the CJEU on the interpretation of Article 22(1) of the GDPR and whether it applies to the activities of private credit-rating agencies such as Schufa (para. 27).

The central dilemma of the referring court was how to ensure legal protection in situations when contractual arrangements, such as those between Schufa and the bank, make it challenging to provide access to the additional information to which the data subject is entitled under Article 15(1)(h) of the GDPR. Schufa's disclaimer in the contract that the ultimate decision lies with the lender and should not be solely based on automated credit scoring leaves the data subject in limbo. On the one hand, it limits the liability of a private credit-scoring agency such as Schufa to provide further information because it is not the party which is adopting the automated decision-making (para. 23). On the other hand, while the bank is adopting the automated decision-making, it has no information on the data used for the credit scoring (para. 23).

Before clarifying this dilemma, the CJEU applied all three cumulative criteria of Article 22(1) of the GDPR to determine whether automated credit scoring falls within its realm. It held that concerning the first requirement of a 'decision', this concept is quite broad and encompasses 'the result of calculating a person's creditworthiness in

the form of probability value concerning that person's ability to meet payment commitments in the future' (para. 46). Concerning the second criterion, namely that the decision must be based solely on automated decision-making, it has been already established that according to the narrow interpretation of Article 22(1), decision-making that involves a meaningful human intervention is out of the scope of the GDPR. According to the CJEU ruling, although 'automated', the final decision concerning the loan disbursement might still be human, especially in banks that apply so-called 'multi-stage profiling' (Ettorre, 2023), which involves both human and automated decisions (Binns & Veale, 2021, p. 321). However, for this to happen, the bank must play a 'decisive role' in granting loans (Opinion of Advocate General, 2023, paras. 46–47). In the Schufa case, the indications were that the bank's decision was greatly 'predetermined' by the automated scoring (Opinion of Advocate General, 2023, para. 47); therefore, the automated score formed the 'decision' (para. 47). Schufa argued that it only provided preparatory data on which the lender's decision could be based, an argument which was rejected by the Court (Clark & Grentzenberg, 2023). As regards the third criterion, the CJEU ruled that credit scoring amounts to profiling, leading to decisions producing legal effects or significantly affecting individuals, namely a refusal to grant the loan applied for (Judgment of the CJEU, 2023, paras 48, 61, 62). With all three cumulative criteria met, the CJEU ruled that individuals are entitled to request and receive meaningful information regarding the logic behind automated scoring. This information is to be provided by agencies like Schufa because, according to the CJEU, the automated score formed the decision and the bank just endorsed it (paras 61–62).

While the CJEU ruling in the Schufa case strengthens data protection and enhances transparency concerning the logic behind automated decisions and the inner workings of the algorithms involved, many fear growing challenges in the financial sector and beyond (Abrams & Goldstein, 2023). Cani and Mazelliu (2025, pp. 518–523) demonstrate that robust governance frameworks such as transparency, accountability, and rigorous oversight in automated processes are required to safeguard individuals' rights, a lesson no less applicable to AI applications in banking.

From the perspective of data subjects, with the increasing use of AI in banking services and the automatisation of decisions in many other private and public sectors, the landmark ruling in Schufa ensures that opaque algorithms do not discriminate against individuals. It also extends the obligation to comply with Article 22(1) of the GDPR to credit reference agencies, and not only lenders, in situations when automated scoring is decisive and significantly affects individuals (Boardman & Lölfing, 2023). This case also confirms the very nature of Article 22(1) of the GDPR as a general prohibition, 'the infringement of which does not need to be invoked individually by a person' (Rebelo & Pacheco de Andrade, 2024, p. 5).

Because banks use AI for many other processes, such as cyberthreat detection, anti-money laundering operations, and other personalised banking services, many fear that the Schufa ruling may lead to varying outcomes (Centre for Information

Policy Leadership, 2024). The Schufa ruling also has implications for other industries and sectors (Goldstein, 2023). In light of the CJEU's decision, other automated processes can also be considered automated decision-making if the criteria explained in Schufa are met.

4. Future implications

As Rebelo & Pacheco de Andrade (2024, p. 7) rightly point out, the Schufa ruling does not fully resolve the complexities of GDPR compliance in automated credit scoring. Rather, it helps us understand them and ensures a more balanced approach between using AI in banking services and ensuring proper safeguards for individual human rights and freedoms. The formula set by this landmark ruling seems straightforward: organisations and financial institutions that want to stay clear of any data protection violations must ensure meaningful human involvement in the decision-making process, especially regarding decisions that produce legal effects or significantly impact individuals. However, as organisations and institutions strive for increased efficiency, improved accuracy, and cost reduction, their over-reliance on and investment in automated processes will continue, and they must keep abreast of their legal obligations, especially regarding transparency and accountability. The Schufa ruling requires credit-scoring agencies to provide individuals with meaningful information about the logic, significance, and envisaged consequences of automated credit-scoring processes. This ensures that individuals understand and can challenge decisions significantly impacting their financial prospects. According to the logic of the Schufa ruling, this obligation cannot be delegated using any contractual provision between credit-scoring agencies and lenders, and such provisions will be unenforceable. In this case, credit-scoring agencies and lenders will be jointly accountable to individuals and must demonstrate compliance with the law and binding precedents such as the Schufa ruling.

Credit-rating agencies cannot use trade secrecy as a legitimate reason to deny a request for disclosure of the scoring methodology (Shao, 2024). This entails that both banks and credit-scoring agencies, as third parties, must adapt their contractual arrangements to comply with the GDPR and reassess and adapt the AI systems used for automated credit scoring, which should now provide for human oversight. Such contractual arrangements must provide for the clear responsibilities of each party vis-à-vis data subjects, as well as clear procedures for compliance.

Conclusions

The Schufa case attests to the growing tensions between technological developments and the need to protect individual rights. The CJEU's ruling clarifies the application of Article 22(1) of the GDPR, emphasising transparency and accountability in

automated decision-making processes. While automated systems offer efficiency and accuracy, they bring challenges, including potential biases and a lack of transparency. Meaningful human involvement in decision-making is crucial to mitigate these issues, especially when decisions have significant implications and impacts on individuals. The Schufa ruling not only reinforces GDPR-based rights but also solidifies broader ethical requirements by mandating a constant fairness assessment and insisting upon transparency by revealing individuals' right to understand the rationale behind the results of scoring. This is in line with general AI ethics guidelines that emphasise the necessity of maintaining human oversight in autonomous systems and giving individuals the capacity to comprehend and dispute decisions that impact them.

Financial institutions and credit-scoring agencies must ensure compliance with data protection regulations to prevent discrimination and uphold individual rights. As AI continues to evolve, ongoing caution and adaptation of legal frameworks will be necessary to balance innovation with ethical considerations and ensure that it does not undermine fundamental human rights.

Applied prospectively, the Schufa ruling raises many avenues for further research. A particular area of focus is how to successfully implement explainability in AI systems in the financial sector and, in so doing, ensuring that automated decisions are transparent as well as intelligible to affected parties. Equally importantly, it is imperative to study methodologies for incorporating meaningful human oversight within AI-driven decision-making systems to provide accountability and forestall over-reliance on automated systems. Examining the far-reaching consequences of the Schufa decision on other industries that employ automated decision-making can provide insight into its impact on data protection and individual rights across various fields. In addition, examining the interaction between the GDPR and new AI legislation, such as the EU AI Act, can determine how legal frameworks can be aligned to efficiently regulate AI technologies while protecting individuals' rights. By exploring these avenues, future research can play a role in the evolution of sound legal and ethical frameworks that promote trustworthy AI implementation in the financial industry and other sectors.

REFERENCES

Abrams, M., & Goldstein, L. A. (2023). *CJEU case in SCHUFA has far reaching implications beyond credit scoring: Policy analysis*. The Information Accountability Foundation. https://www.information-accountability.org/_files/ugd/ffea53_5c4ae2a7dc1a49248fcc331accf50721.pdf.

Agencia Española Protección Datos (AEPD). (2024, 4 March). *Evaluating human intervention in automated decisions*. https://shorturl.at/Mgi6l

Amnesty International. (2021, 25 October). *Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms*. https://shorturl.at/RnZ7M

Ananya. (2023, 7 September). Algorithms are making important decisions: What could possibly go wrong? *Scientific American*. https://www.scientificamerican.com/article/algorithms-are-making-important-decisions-what-could-possibly-go-wrong/

Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkanen, K., & Kujala, S. (2023). Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, *159*, 1–15.

Bertrand, J., & Klein, P. O. (2021). Creditor information registries and relationship lending. *International Review of Law and Economics*, *65*, 1–43.

Binns, R., & Veale, M. (2021). Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR. *International Data Privacy Law*, *11*(4), 319–332.

Boardman, R., & Lölfing, N. (2023, December 19). *Key takeaways from the CJEU's recent automated decision-making rulings: Opinion*. IAPP. https://shorturl.at/rGQhY

Boyer, J. (2024). *The future of credit: AI or human judgment?* EmildAI. https://shorturl.at/2TeSi

Çani, E. M., & Mazelliu, A. (2025). Navigating the algorithmic shift and the legal implications of artificial intelligence in Albania's public administration. *Italian Journal of Public Law*, *17*(2), 496–527.

Cariaga, V. (2024, 25 April). *Artificial intelligence based credit scoring: How AI could set your credit score*. Yahoo Finance. https://shorturl.at/BJpts

Centre for Information Policy Leadership. (2024). *Decoding responsibility in the era of automated decisions: Understanding the implications of the CJEU's SCHUFA judgment*. Hunton Andrews Kurth.

Clark, J., & Grentzenberg, V. (2023, December 13). *EU: Significant new CJEU decision on automated decision-making*. DLA Piper. https://shorturl.at/XLpCo

Council of Europe. (2016). *Study the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. ,4. https://rm.coe.int/study-on-algorithmes-final-version/1680770cbc

Dastin, J. (2018). *Insight – Amazon scraps secret AI recruiting tool that showed bias against women*. Reuters. https://shorturl.at/xKxJI

De Moor, L., Luitel, P., Sercu, P., & Vanpee, R. (2018). Subjectivity in sovereign credit ratings. *Journal of Banking and Finance*, *88*, 366–392.

Ettorre, F. P. (2022, 14 February). *The right to contest automated decisions*. The Digital Constitutionalist. https://digi-con.org/the-right-to-contest-automated-decisions/

Ettorre, F. P. (2023, 17 March). *Is credit scoring an automated decision? The opinion of the AG Pikamäe in the case C-634/21*. The Digital Constitutionalist. https://goto.now/NCrGd

European Union. (2016, 27 April). Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (Text with EEA relevance).*OJ L 119, 4.5.2016, p. 1–88.*

Fares, O. H., Butt, I., & Lee, S. H. M. (2022). Utilisation of artificial intelligence in the banking sector: A systemic literature review. *Journal of Financial Services Marketing*, *28*, 835–852.

Farishy, R. (2023). The use of artificial intelligence in banking industry. *International Journal of Social Service and Research*, *3*(7), 1724–1731.

Gavrila, A. R. (2024). Digitalization in banking: Navigating the effects of automated decision-making on customer experience. *Proceedings of the International Conference on Business Excellence*, *18*(1), 1413–1424.

Heaven, W. D. (2021, 17 June). Bias is not the only problem with credit scores – and no, AI cannot help. *MIT Technology Review*. https://goto.now/NK5H1

Hughes, T. (2019, May 17). *Human versus machine: The pros and cons of AI in credit*. Global Association of Risk Professionals. https://shorturl.at/Or4LJ

Hurley, M., & Adebayo, J. (2016). Credit scoring in the era of big data. *Yale Journal of Law and Technology*, *18*, 148–216.

Jain, P. (2024). Research paper on the impact of artificial intelligence on the banking sector. *Amity University Noida – Amity Law School*. https://ssrn.com/abstract=4907776

Jiang, J., Liao, L., Lu, X., Wang Z., & Xiang, H. (2021). Deciphering big data in consumer credit evaluation. *Journal of Empirical Finance*, *62*, 28–45.

Judgment of the CJEU of 7 December 2023 on the case of *OQ v. Land Hessen, intervener Schufa Holding, A. G.*, C634/21, ECLI:EU:C:2023:957.

Judgment of the Court of Amsterdam of 4 April 2023 on the case of *The Netherlands v UBER B. V. ??*, C/13/692003/HA RK 20–302.

Judgment of the Court of Amsterdam of 24 February 2021 on the case of *XXX*, Rb. Amsterdam, C/13/696010/HA ZA 21–81.

Kolleshi, M., & Golemi, E. (2024). Impact of artificial intelligence on the Albanian banking system. *Interdisciplinary Journal of Research and Development*, *11*(2), 75–82.

Kozak, S., & Golnik, B. (2020). Migration of the banking sector to digital banking in Poland. *Economic and Regional Studies*, *13*(3), 284–294.

Kuner C., Bygrave, L. A., & Docksey, C. (Eds.). (2021). *The EU General Data Protection Regulation: A commentary*. Oxford University Press.

Nan Nijang, C., & Novik, N. (2021, 10 August). *Leveraging big data and machine learning in credit reporting*. World Bank Blogs. https://goto.now/gsUfo

Narang, A., Vashisht, P., & Bajaj, B. (2024). Artificial intelligence in banking and finance. *International Journal of Innovative Research in Computer Science and Technology*, *12*(2), 130–134.

Opinion of Advocate General Pikamae of 16 March 2023 on the case of *OQ v. Land Hessen, intervener Schufa Holding, A. G.*, C634/21, ECLI:EU:C:2023:957.

Óskarsdóttir, M., Bravob, C., Sarrautee, C., Vanthienenc, J., & Baesensc, B. (2019). The value of big data for credit scoring: Enhancing financial inclusion using mobile phone data and social network analytics. *Applied Soft Computing*, *74*, 26–39.

Pery, A., & Simon, M. (2024, January). *International data privacy compliance, professional perspective – GDPR curbs use of AI via Article 22 decision*. Bloomberg Law. https://shorturl.at/b1658

Polireddi, N. S. A. (2024). An effective role of artificial intelligence and machine learning in the banking sector. *Measurement: Sensors*, *33*, 1–9.

Rebelo, D. M., & Pacheco de Andrade, F. (2024). *Schufa's case C-634/21 on ADM: The 'lender' quest for GDPR-friendly scoring has not been settled yet!* JusGov Research Paper Series, no. 2024–2023.

Rejmaniak, R. (2021). Bias in artificial intelligence systems. *Bialystok Legal Studies*, *26*(3), 25–42.

Shao, C. (2024, 27 August). *Schufa II case: Further insights on automated credit scoring*. Information Governance Services. https://shorturl.at/JK8aO

Silveira, A. (2023, April 10). Finally, the ECJ is interpreting Article 22 GDPR (on individual decisions based solely on automated processing, including profiling). *Unio EU Law Journal*. https://shorturl.at/xvjUj

Srivastava, S. (2024, 26 September). *AI in banking – how artificial intelligence is used in banks*. Appinventiv. https://appinventiv.com/blog/ai-in-banking/

Stefanski, K., & Zywolewska, K. (2024). Lack of transparency in algorithmic management of workers and trade unions' right to information: European and Polish perspectives. *Bialystok Law Studies*, *29*(2), 53–63.

Tabaku, E., Duci, E., Kapciu, R., & Kosova, A. M. (2025). Exploring the impact of artificial intelligence in banking: A case study on the integration of virtual assistants in customer service. *International Research Journal of Modernisation in Engineering Technology and Science*, *7*(1), 4177–4183. https://www.doi.org/10.56726/IRJMETS66700

Tosoni, L. (2021). The right to object to automated individual decisions: Resolving the ambiguity of Article 22(1) of the General Data Protection Regulation. *International Data Privacy Law*, *11*(2), 145–162.

Vaassen, B. (2022). AI, opacity, and personal autonomy. *Philosophy and Technology*, *35*(88), 1–20.

Vidal, M. F., & Barbon, F. (2019). *Credit scoring in financial inclusion: How to use advanced analytics to build credit-scoring models that increase access. Technical guide*. Consultative Group to Assist the Poor (CGAP)/World Bank.

Vidal, M. F., & Menajovsky, J. (2019, 5 September). *Algorithm bias in credit scoring: What's inside the black box?* CGAP. https://goto.now/oPTBu

Woodruff, A., Anderson, Y. A., Armstrong, K. J., Gkiza, M., Jennings, J., Moessner, C., Viégas, F., Wattenberg, M., Webb, L., Wrede, F., & Kelley, P. G. (2020). 'A cold, technical decision-maker': Can AI provide explainability, negotiability, and humanity? *ArXiv Abs*, 2012.00874, 1–23.

World Bank. (2019). *Credit scoring approaches guidelines.* The World Bank Group.

Zagha, N. S. (2024, 25 February). *Artificial intelligence real use cases for credit scoring in banks and fintech firms*. LinkedIn. https://goto.now/oMpOG

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.11

Received: 24.03.2025
Accepted: 29.04.2025

Karol Karski
University of Warsaw, Poland
k.karski@wpia.uw.edu.pl
ORCID ID: https://orcid.org/0000-0003-0757-6283

Paweł Mielniczek
Get Compliant Sp. z o.o., Poland
pawel.mielniczek@gclawyers.eu
ORCID ID: https://orcid.org/0000-0003-3465-6326

Generative AI in International Trade Law: Navigating Opportunities and Challenges

Abstract: The subject of this article is an analysis of the impact of generative AI (GenAI) on international trade law, from the perspective of both the threats and the opportunities of integrating GenAI into international trade. It addresses topics including intellectual property law, international trade law principles, information security, trade negotiations, contracts, competition, liability and AI ethics. The authors employ a holistic approach, examining numerous applications of GenAI in international trade. They conclude with how the international legal framework for GenAI may help people navigate challenges and seize opportunities to benefit international trade.

Keywords: generative artificial intelligence, international trade law, intellectual property law, AI regulations, AI standards

Introduction

Trade law has, historically, adapted to technological breakthroughs, dating back to steam power, then electricity and finally digital evolution. Each time, the context in which the law functioned determined the legal norms. For example, the rise of the steam-powered railway industry in the 19th century prompted legal acts such as the USA Interstate Commerce Act of 1887 (Congress of the United States of America,

© 2025 Karol Karski, Paweł Mielniczek published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

1887) to safeguard public interests from abuses of private companies' dominant position (Dempsey, 2012). Now, the AI age is not only prompting discussions on how to regulate the possibilities of this growing technology before it becomes too dangerous, but also on how lawyers and other stakeholders in international trade can and should use it (Anwansedo et al., 2024; Bar, 2024).

Generative AI (GenAI), understood as AI able to generate new content like text, images, audio and video, already supports various legal and non-legal processes, from drafting contracts, through managing documents, to optimizing supply chains and decision-making. Even before the ChatGPT era, the ideas about the regulation of AI systems were focused around principles such as transparency, explainability, accountability, safety, privacy and security (Bar, 2025, pp. 25–108; Peng et al., 2021, p. 21). With the popularization of GenAI systems, values like fairness, inclusiveness, the promotion of human values or even human control of technology have started to reflect the needs that might be neglected in the case of uncontrolled development of such systems.

Existing frameworks, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (WTO, 2017b), accepted almost worldwide, have been analysed as to whether and to what extent they apply to AI-generated content (ThankGod, 2023, p. 8). Laws and international agreements prepared in the AI age, such as the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, often already take it into account (Babikov et al., 2024; Council of Europe, 2024a). It should be remembered, however, that this Convention has not yet entered into force (Council of Europe, 2024b).

The needs for regulation come from different stakeholders. Developed countries, for example, tend to standardize cross-border practices, with one of the most illustrative examples being the GDPR and other EU acts that require following EU standards even outside the Union, including when sharing data outside the European Economic Area. Focus on data protection and information security indicates specific needs or preoccupations, such as cyberthreats and the need for uniform protection against them. On the other hand, freedom of expression and information needs a system of checks and balances, with the risks both to society and to individuals, such as misinformation, hallucinations (AI providing incorrect, wrongly generated information) and deepfakes (which not only allow someone to be harassed, but provide more opportunities for cybercriminals, including identity theft and phishing attempts).

In this paper, we provide suggestions about how to strike a fair balance between the risks and the opportunities posed and brought by GenAI to international trade. There are numerous potential risks and mistakes in either underregulating, overregulating or wrongly regulating the use of GenAI and its outcomes. While many see the integration of AI into global trade as an opportunity to enhance efficiency, manage costs and streamline the supply chain (Igbinenikaro & Adewusi, 2024a), others point out an intrinsic ambiguity when law that does not directly address AI is interpreted (Igbinenikaro & Adewusi, 2024b, pp. 492–493). While many states and inter-

national organizations, including the European Union, try to regulate specific aspects of AI, including data flows, data privacy and classification of GenAI outputs (Thank-God, 2023, p. 10), according to a World Economic Forum White Paper (Ahmed et al., 2024, p. 3), too many uncoordinated efforts 'have led to fragmented and divergent requirements that are likely to create cross-border trade frictions and undermine governmental objectives, creating barriers to the use' of GenAI.

1. Generative AI-related principles

The coming of the AI age is the right time to re-examine the foundational principles of international trade law – not to revolutionize them, but to make sure their content and application remains both up to date and future-proof. For instance, the transparency principle enshrined in Article III of the General Agreement on Trade in Services (GATS) (WTO, 2017a), requiring Member States to publish 'all relevant measures of general application which pertain to or affect the operation of this Agreement', while leaving room for the initiative of proactive Member States, might not be enough to serve as a legal requirement to be transparent on the application of GenAI in the context of international trade.

From the perspective of a principle of non-discrimination, we might ask questions about the democratization of access to GenAI tools, which are often seen to have regional restrictions (for example due to AI or privacy law conditions, where higher requirements usually mean less available tools or functions). Other international trade law principles (like fairness, reciprocity, good faith, equity and proportionality) may also be interpreted as applicable, at least partially, to autonomous GenAI systems, the entities providing or distributing them, their users and the content they generate.

If we assume that certain advanced GenAI tools in the hands of one subject of international law might create imbalances or unfair advantage against another, a new question arises as to how law can even address this issue and to what extent it is possible to introduce new legal norms and agreements designed to promote equal chances, or at least reciprocity. The above-mentioned Council of Europe Framework Convention, the Organisation for Economic Co-operation and Development's AI Principles (OECD, 2024), the United Nations Educational, Scientific and Cultural Organization's Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021), as well as the G7 International Guiding Principles on Artificial Intelligence and on a Code of Conduct for AI Developers (European Commission, 2023a, 2023b, 2023c) and the G20 AI Principles (Ministry of Foreign Affairs of Japan, 2019), provide different principles for different actors. To synthesize them, we observe that the fulfilment of these principles would require them to be applicable to states, other subjects of in-

ternational law, AI developers and deployers, and other stakeholders, as well as businesses and other trade actors.[1]

According to the above-cited frameworks, states should promote responsible AI development, including through legislative and policy frameworks. Both the proposed and already agreed principles typically adopt a risk-based approach, requiring the pre-analysis of various AI threats (typically to human rights and the rule of law) and going through mitigation, monitoring and continuous improvement phases as a standard that should be domestically enforced in state parties to such commitments.[2] Governments are also encouraged to promote fair competition and non-discrimination in AI practices, including through entering into international trade agreements as appropriate.

The principle of transparency would require a clear statement of the logic on which the AI system functions. In a broad understanding (especially referring to either high-risk or high-transparency environments, such as the functioning of important state processes), that would also include disclosing the sources of data on which the AI system has been trained, as well as the process of how it takes decisions or develops outputs.[3] What seems to have the most support is the requirement to disclose that given content is AI-generated – not only post factum, but also in the case of tools or functions where it is not clear if AI is involved (e.g. support chats, helplines, etc.). That would allow recipients not only to be aware of AI involvement, but also to ask questions and make their own verifications and checks so as not to be misled by often experimental models.

On one side we have free information flows, and on the other data protection and security requirements. This is particularly visible in the context of international data transfers and the notion of information sovereignty, particularly important to jurisdictions with a high level of privacy regulations. This is another challenge for international law, as data protection laws vary widely across different states, with the EU sometimes being perceived as overregulating, which might thwart innovation (Nizza, in press, pp. 19–20). In addition, the existing guidance already suggests the potential to go deeper and require alignment with human rights and sustainability goals, supporting rather than replacing human decision-making.[4]

GenAI-supported decision-making in the context of international trade law is not limited to aspects of financial fairness, including the prohibition of anti-compet-

1 The principles in their current shape would still be too vague to bring harmonization, similarly to human rights law, as described by Karska (2019, pp. 56–57).

2 On the challenges of enforcing the liability of multinational corporations, see for example the considerations by Karska & Karski (2021, pp. 429–430).

3 On logic disclosure and transparency in the context of employment, see for example Méndez & Kurzynoga (2023, p. 209).

4 On threats to human rights from transnational corporations, see for example Karska (2022, pp. 248–249).

itive practices (e.g. unfair pricing or digital monopolies). Considerations of transparency in the supply chain, for example, would go further here, and where relevant might require ensuring the traceability of goods to enable verifications of ethical sourcing. Similarly, considerations of customs and logistics, even if limited in the context of digital products or services, would also entail questions about addressing potential trade barriers and the fair treatment of all traders or service providers. We thus conclude that following international trade law in good faith would contribute not just to a good level of compliance in GenAI usage in the context of decision-making, but also to the fair development of international trade.

2. Imbalances and unfair advantages and how to address them

As illustrated by the 2025 US tariffs crisis, international trade development is decided by the policies of subjects of international law, which are followed by international law to make them dependent upon a binding and clear framework. The same applies to GenAI, where international trade law, irrespective of its source, might help prevent new challenges and address existing ones, such as imbalances or unfair advantages. In this respect, among the sources of imbalances, the priorities to address would be:

- the technical advantages of some international law subjects. The most AI-advanced economies might be able to invest and gain competitive advantage thanks to the benefits of new technologies to economy and trade, such as process automation and optimization, increases in productivity or quality, and increases in cost efficiency.
- the infrastructural capacity of some international law subjects, such as fast internet access, efficient devices and data centres. These might allow AI-driven economies to advance faster, both spreading AI adoption among its public and facilitating more ambitious and customised implementation projects.
- HR and implementation costs. Highly qualified human resources in developed countries are better prepared to implement GenAI, which, along with bigger investment potential in the case of fully fledged implementation projects or the development of so-called middleware or other non-publicly available GenAI models or agents, becomes limited to those who can afford it – increasing their relative ability to innovate and adapt (Ahmed et al., 2024, p. 9).

All of the above may deepen imbalances with less AI-advanced economies, if they do not adopt similar solutions. It might not be possible to completely fix these challenges just through legal norms, as investing in education, training and widely available GenAI tools would require directed policies and agreements (at any level), where AI access would be treated as a common good and a revolution serving everyone, rather than just a tool for gaining competitive advantage. Since for many, these might be two extremes, balancing them might end up focusing on providing every

subject of international law with a fair, equal framework to compete in – and that might be started with a uniform set of principles about AI usage and development.

International organizations such as the World Trade Organization (WTO) may play a pivotal role in advocating policies that help sustainable and equitable technological advancement among its Member States. The quantifiable results of these affirmative initiatives would cover:

- the establishment of local technology ecosystems, such as incubators and technology parks, to support local innovation and engagement in GenAI.
- the modification of trade policies to safeguard local markets from inequitable competition from AI-advanced nations – at least giving them more time to adapt and develop resilience.
- the promotion of open standards and interoperability aimed at assisting AI-developing countries – including by facilitating access to open technologies and infrastructure.

3. Stakeholder analysis and risk–benefit mapping

Implementing GenAI in a way where threats are minimized and opportunities seized requires the cooperation of stakeholders both from the international community and domestic actors. Intergovernmental organizations, non-governmental organizations, states, technology firms, businesses and even end users all have their role to play in shaping not only how GenAI is designed and implemented, but also how and for what purposes its outputs are used. International organizations like the Asia-Pacific Economic Cooperation point out the need to harmonize regulatory frameworks (Igbinenikaro & Adewusi, 2024a, p. 5). However, an interesting point made by Chander (2021, p. 118) is that 'AI might be designed for different environments, nurtured on data from polities that might behave differently. This is a form of the well-known problem that AI trained on, say, a largely white (and male) population, might perform poorly with respect to other populations.' Thus defining who is the stakeholder is not as obvious as it seems, as anyone not included or not appreciated enough might find some biased examples.

The harmonized standards, whatever their shape, should then address the vulnerabilities and risks to values common to all stakeholders and, foremostly, the public policy objectives.[5] Only from this perspective is a precise enough risk–benefit mapping possible, while still subject to cooperation between multiple interest groups.

5 However, AI regulation or standards would always be limited by the unpredictable nature of international relations, including open or indirect but intentional non-compliance with international legal standards, including in hybrid war and conflict and competition strategies, such as engineered migration. For more on such situations, see for example Kużelewska & Piekutowska (2023).

Ultimately, it is the balancing of regulation with legitimate public policy objectives, such as protecting stakeholders against threats to their rights and freedoms, that has been notified by various countries to the WTO's Technical Barriers to Trade Committee (Fonseca Azevedo, 2024, p. 2).

4. Ethical dimensions and legal dilemmas

Ethical questions about the application of GenAI to international trade not only revolve around biases or discriminatory or dangerous decision-making; more frequently, legal issues will refer to security and intellectual property, including voices about the privileges of technology-owning firms that impede innovation and knowledge distribution (Jones, 2023, p. 6). The World Economic Forum White Paper (Ahmed et al., 2024, p. 3) highlights mistrust due to misinformation as another significant risk.

The legal dilemma arising from the ethical questions is to what extent AI should be regulated to avoid allegations of overregulation bias, including indirectly requiring AI to actually pursue partisan or ideological agendas dressed up as values common to everyone.[6] Ching-Fu Lin (2021, p. 243) states openly that '[a]lgorithms are not objective. Rather, they carry the existing biases and discriminations against minority groups in human society.'[7] This perspective, although not optimistic, might highlight the conclusion that no matter how advanced AI becomes, legal dilemmas will never be answered with one perfect legal framework, but rather with a set of checks and balances, including balances against overregulation itself.[8]

5. GenAI in trade negotiations and contracts

GenAI provides a great amount of value to the conclusion of negotiations and the performance of contract in international trade, such as automated drafting, predictive analytics, translations and even smart contracts, with terms directly embedded in the code (Köksal & Sarel, in press, pp. 101–153). Implementing GenAI further to manage contracts might reduce errors, speed up drafting and highlight potential risks, disputes or inconsistencies to address or negotiate. Even misunderstandings as to the interpretation of contracts may be addressed more efficiently with the help of GenAI.

6 On the challenges of reaching an international consensus on adopting binding instruments, see for example Karska (2021, p. 483).

7 See also Kleinberg et al. (2018).

8 This applies not only to the topic of this article, but in any context where AI might be used to assist with, or even directly apply, law. On the question of who (machine or human) is the judge determining what is lawful and unlawful, see the chapter by Meyer et al. (2020). See also in this context interesting articles by Kowalski (2024) and Kamiński (2024).

At least two viewpoints regarding the function of GenAI in trade talks and contracts exist. First, in phases where contracts are drafted and concluded, GenAI can both automate and enhance quality at every stage (both conceptually and in negotiations), among other things by drafting, managing, monitoring and updating contracts, including adjusting them to the needs and interests of all stakeholders. That might be subject primarily to the GenAI-related principles discussed above.

Another perspective is GenAI-driven trade, where GenAI tools would be present not as a means to manage contracts, but as a subject matter of or context to those contracts. If the use of GenAI might apply or affect the performance of the contract in any way, it might be worth not only incorporating or transposing specific GenAI-related principles, in the form of obligations between parties, but also covering indemnification clauses, liability allocation or even insurance policy requirements to address risks related to GenAI-driven trade (Igbinenikaro & Adewusi, 2024b, p. 497). That being said, regulation and liability allocation should make GenAI-driven trade even more efficient, allowing for its ordered use within the legal relationship.

6. Intellectual property and creative outputs

GenAI is challenging the longstanding intellectual property (IP) principle of human authorship (Gaffar & Albarashdi, 2024, p. 3). The human-centred approach of international IP law, such as the Berne Convention for the Protection of Literary and Artistic Works (WIPO, 1979), may provide the recently popular interpretation that only human-created works are subject to IP rights and protections, with questions arising about the degree of human contribution to the shape of the final work. This applies also to patents, as demonstrated in the case of Thaler, who was denied protection of his inventions, generated by an AI tool, by US and UK copyright offices.[9] Another dimension is the use of IP-protected works to train or otherwise provide GenAI models with input data. As illustrated by Thomson Reuters v. Ross Intelligence, one entity may successfully claim that the use of copyrighted content for that purpose might constitute a copyright infringement, rather than amounting to fair use (United States District Court for the District of Delaware, 2025).

However, irrespective of these standards, international trade will experience even more AI-generated content.[10] Most trade relations do not involve copyright transfers, and even if they do, detecting and proving violations might not always be straightfor-

9 See the judgment of Thaler v. Perlmutter (United States Court of Appeals for the District of Columbia Circuit, 2025).

10 Hence discussion on the protection of such content is inevitable. Perhaps one day, extremely creative and individualized AI might even be recognized as somehow unique, though recognition of the rights of AI subjects, similar to artificially created companies, is unlikely. See Karski & Ziemblicki (2021, p. 512).

ward. While some scholars suggest the updating of the notion of authorship as being a significant challenge for policymakers and judicial systems (Gaffar & Albarashdi, 2024, p. 2), we believe that the minimum standard in any international trade relations is transparency and good faith, meaning that GenAI must not be used as an unfair advantage or a tool to violate the purpose of contracts and laws in a more sophisticated way. Where dispute resolution or human intervention plays a role, the parties to international trade relations might choose to use only those GenAI tools that provide functionalities and evidence sufficient to implement the agreed standards.[11]

7. Market regulation and data flows

Next to the above-mentioned need to balance information security and the data protection requirements of certain jurisdictions with the need for a free flow of information, often necessary to even use some of the GenAI tools available in the market (Khan, 2024, p. 107), the use of GenAI might also be significant to the application of other regulations. For example, controlling innovative tools and huge datasets might bring certain subjects into dominant positions, potentially heading towards monopolization and anti-competitive practices. Differences in regulations and the depth of regional AI standards might further complicate these issues, resulting in a fragmentation of the regulatory landscape, which is detrimental to global trade.

As Mariarosaria Comunale and Andrea Manera (2024, p. 46) found in their review of the academic literature and policy actions on AI in the economic context, the challenges can be summarized in three takeaways: (1) 'AI effects are uncertain', (2) 'policy and research are partly disconnected' (literature focuses on employment and productivity,[12] policies are about ethics, bias and security), with regulators avoiding addressing economic issues, and (3) regulations have a lot of differences and 'face difficult trade-offs'. Foremostly, the right angle, meaning understanding the perspectives, needs and interests of all stakeholders, is a necessary condition to strike a fair balance between competing values, both adopting the right international trade policies and regulating AI usage in a way to benefit everyone, rather than impeding progress or providing unnecessary barriers.

Conclusion

In conclusion, tackling the issues discussed throughout this paper with legal flexibility is essential to navigate the opportunities and challenges of GenAI. Our key takeaways on what needs addressing are:

11 See Gienas (2024).
12 See for example Baran (2024).

– regulatory fragmentation, resulting in overregulation and barriers rather than significantly impacting GenAI use in trade globally (Ahmed et al., 2024, p. 6).[13]
– data privacy and security, including the fact that as of today, most GenAI tool providers do not provide security guarantees, or provide only limited ones (e.g. to business accounts), including not using data input by users for its own purposes without their active consent.
– ethical and bias-related matters, revolving around the principles of fairness, transparency and non-discrimination (all stakeholders may play both positive and negative roles in applying and executing these).
– IP concerns (both the ownership and other legal safeguards of AI-generated content), as well as the protection of human-made copyrighted works against unregulated and nearly undetectable infringements through AI.[14]
– economic disparities, as advanced GenAI can contribute to imbalances and unfair advantages in international trade, with regulators and states reluctant to address the economic perspective.

Regulatory pathways that could help balance the competing interests should be a mix of international cooperation and harmonization efforts (Shaffer, 2021, p. 45), a risk-based approach and specific standards designed to safeguard transparency and accountability, as well as supporting ethical guidelines, certification mechanisms and capacity-building, to not just regulate but provide meaningful impact, and moving GenAI development in a fair and right direction that is beneficial to international trade.

REFERENCES

Ahmed, U., Naas, P., Evenett, S. J., & Kugler, K. (2024). *ChatWTO: An analysis of generative artificial intelligence and international trade* [White paper]. World Economic Forum – Global Future Council on International Trade and Investment.

Anwansedo, F., Gbadebo, A. D., & Akinwande, O. T. (2024). Exploring the role of AI-enhanced online marketplaces in facilitating economic growth: An impact analysis on trade relations between the United States and sub-Saharan Africa. *Revista de Gestão Social e Ambiental*, *18*(6), 1–15. DOI:10.24857/rgsa.v18n6–139

Babikov, O., Fedorenko, I., Omelchenko, O., Lyseiuk, A., & Panova, O. (2024). The observance of human rights and freedoms during the covert obtaining of information in criminal proceedings. *Białostockie Studia Prawnicze*, *29*(4), 197–215. DOI:10.15290/bsp.2024.29.04.12

Bar, A. (2024). Identyfikacja pochodzenia i znakowanie treści syntetycznych a problem ochrony prawnoautorskiej wytworów powstających z wykorzystaniem sztucznej inteligencji. *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, *3*(165), 56–80.

13 See also remarks on soft law limitations by Karska & Karski (2023, p. 544).
14 Including different approaches in IP law, as illustrated in an article focused on ChatGPT considerations in EU law by Markiewicz (2023, p. 166).

Bar, A. (2025). *Obrazy generowane z wykorzystaniem sztucznej inteligencji. Status prawnoautorski*. Wolters Kluwer.

Baran, K. (2024). The right of trade unions to information in the era of the fourth and fifth industrial revolutions. *Białostockie Studia Prawnicze*, *29*(2), 29–38. DOI:10.15290/bsp.2024.29.02.03

Chander, A. (2021). Artificial intelligence and trade. In M. Burri (Ed.), *Big data and global trade law* (pp. 115–127). Cambridge University Press. DOI:10.1017/9781108919234.008

Comunale, M., & Manera, A. (2024). *The economic impacts and the regulation of AI: a review of the academic literature and policy actions* [Working paper no. 24/65]. International Monetary Fund.

Congress of the United States of America. (1887). *Interstate commerce act*. The National Archives and Records Administration. https://www.archives.gov/milestone-documents/interstate-commerce-act

Council of Europe. (2024a). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS no. 225, 17 May 2024. https://www.refworld.org/legal/agreements/coeministers/2024/en/148016

Council of Europe. (2024b). Treaty Office: Chart of Signatures and Ratifications of Treaty 225: Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law: CETS no. 225. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=225

Dempsey, P. S. (2012). The rise and fall of the interstate commerce commission: The tortuous path from regulation to deregulation of America's infrastructure. *Marquette Law Review*, *95*(4), 1151–1189.

European Commission. (2023a, 30 October). Commission welcomes G7 leaders' agreement on guiding principles and a code of conduct on artificial intelligence [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5379

European Commission. (2023b, 30 October). *Hiroshima Process international guiding principles for advanced AI systems* [Policy and legislation]. https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-guiding-principles-advanced-ai-system

European Commission. (2023c, 30 October). *Hiroshima Process international code of conduct for advanced AI systems* [Policy and legislation]. https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems

Fonseca Azevedo, M. da (2024). *Navigating the AI frontier in international trade law* [Working paper series no. 4/2024]. World Trade Institute.

Gaffar, H., & Albarashdi, S. (2024). Copyright protection for AI-generated works: Exploring originality and ownership in a digital landscape. *Asian Journal of International Law*, *15*, 23–46. DOI:10.1017/S2044251323000735

Gienas, K. (2024). Trenowanie AI a prawo autorskie. Zeszyty Naukowe Uniwersytetu Jagiellońskiego. *Prace z Prawa Własności Intelektualnej*, *3*(165), 5–55.

Igbinenikaro, E., & Adewusi, A. O. (2024a). Policy recommendations for integrating artificial intelligence into global trade agreements. *International Journal of Engineering Research Updates*, *6*(1), 1–10. DOI:10.53430/ijeru.2024.6.1.0022

Igbinenikaro, E., & Adewusi, A. O. (2024b). Navigating the legal complexities of artificial intelligence in global trade agreements. *International Journal of Applied Research in Social Sciences*, *6*(4), 488–505. DOI:10.51594/ijarss.v6i4.987

Jones, E. (2023). Digital disruption: Artificial intelligence and international trade policy. *Oxford Review of Economic Policy*, *39*, 70–84. DOI:10.1093/oxrep/grac049

Judgment of the United States Court of Appeals for the District of Columbia Circuit of 18 March 2025 on the case of *Thaler v. Perlmutter*, 687 F. Supp. 3d 140 (D. D. C. 2023). https://media.cadc.uscourts.gov/opinions/docs/2025/03/23–5233.pdf

Judgment of the United States District Court for the District of Delaware of 11 February 2025 on the case of *Thomson Reuters Enterprise Centre GmbH et al. v. Ross Intelligence Inc*, no. 1:20-cv-00613-SB. https://www.ded.uscourts.gov/sites/ded/files/opinions/20–613_5.pdf

Kamiński, M. (2024). Podmiot kompetencji administracyjnej w zautomatyzowanych procesach stosowania prawa na tle problematyki legitymacji prawno-demokratycznej delegowania kompetencji na systemy sztucznej inteligencji i odpowiedzialności prawnej za ich działania lub zaniechania. *Prawo i Więź*, *53*(6), 239–263. DOI:10.36128/PRIW.VI53.1102

Karska, E. (2019). Nowe tendencje w międzynarodowym prawie ochrony praw człowieka jako odpowiedź na zmiany. In A. Tarwacka (Ed.), *Tempora Mutantur Cum Legibus. Księga Jubileuszowa z okazji 20-lecia Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie* (pp. 48–58). Wolters Kluwer.

Karska, E. (2021). Drafting an international legally binding instrument on business and human rights: The next step towards strengthening the protection of human rights. *International Community Law Review*, *23*(5), 466–485. DOI:10.1163/18719732–23050004

Karska, E. (2022). Biznes i prawa człowieka – perspektywa Europy Środkowo-Wschodniej. In E. Cała-Wacinkiewicz, J. Menkes, J. Nowakowska-Małusecka, & W. S. Staszewski (Eds.), *Stosunki sąsiedzkie w świetle prawa międzynarodowego* (pp. 241–253). C. H. Beck.

Karska, E., & Karski, K. (2021). Special issue editorial. Business and human rights: Legal aspects. *International Community Law Review*, *23*(5), 427–432. DOI:10.1163/18719732–23050001

Karska, E., & Karski, K. (2023). Current challenges of international and European human rights law: Introductory remarks. *International Community Law Review*, *25*(6), 539–545. DOI:10.1163/18719732-bja10112

Karski, K., & Ziemblicki, B. (2021). Commercial companies as applicants before the European Court of Human Rights. *International Community Law Review*, *23*(5), 503–525. DOI:10.1163/18719732–23050006

Khan, A. (2024). The intersection of artificial intelligence and international trade laws: Challenges and opportunities. *IIUM Law Journal*, *32*(1), 104–107. DOI:10.31436/iiumlj.v32i1.912

Kleinberg, J., Ludwig, J., Mullainathan, S., & Sunstein, C. R. (2018). Discrimination in the age of algorithms. *Journal of Legal Analysis*, *10*, 113–174. DOI:10.1093/jla/laz001

Köksal, B., & Sarel, R. (in press). The smart contracts trilemma. *University of Illinois Law Review*, 1–64. DOI:10.2139/ssrn.4689013

Kowalski, M. (2024). The impact of artificial intelligence on the future functioning of administrative courts. *Prawo i Więź*, *53*(6), 173–185. DOI:10.36128/PRIW.VI53.988

Kużelewska, E., & Piekutowska, A. (2023). Belarus' violation of international obligations in connection with artificial migration pressure on the Belarus–European Union border. *Białostockie Studia Prawnicze*, *28*(1), 39–55. DOI:10.15290/bsp.2023.28.01.03

Lin, C.-F (2021). Public morals, trade secrets, and the dilemma of regulating automated driving systems. In S.-Y. Peng, C.-F. Lin, & T. Streinz (Eds.), *Artificial intelligence and international economic law* (pp. 237–254). Cambridge University Press. DOI:10.1017/9781108954006.013

Markiewicz, R. (2023). ChatGPT i prawo autorskie Unii Europejskiej. *Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej*, *2*(160), 143–171.

Méndez, M. L., & Kurzynoga, M. (2023). The presumption of the employment relationship of platform workers as an opportunity to eliminate obstacles arising from competition law in the conclusion of a collective agreement: The example of Spain. *Białostockie Studia Prawnicze*, *28*(4), 197–216. DOI:10.15290/bsp.2023.28.04.12

Meyer, T., Marsden, C., & Brown, I. (2020). Regulating internet content with technology: Analysis of policy initiatives relevant to illegal content and disinformation online in the European Union. In G. Terzis, D. Kloza, E. Kużelewska, & D. Trottier (Eds.), *Disinformation and digital media as a challenge for democracy* (pp. 309–326). Intersentia.

Ministry of Foreign Affairs of Japan. (2019). G20 AI principles. https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf

Nizza, U. (in press). What do AIs think about the AI Act? An experimental analysis of the EU approach on artificial intelligence. *European Business Law Review*, *36*(2), 1–20. DOI:10.2139/ssrn.4976521

Organisation for Economic Co-operation and Development (OECD). (2024). *Revised recommendation of the Council on Artificial Intelligence, adopted on 3 May 2024, C/MIN(2024)16/FINAL*. Organisation for Economic Co-operation and Development https://one.oecd.org/document/C/MIN(2024)16/FINAL/en/pdf

Peng, S.-Y., Lin, C.-F., & Streinz, T. (2021). Artificial intelligence and international economic law: A research and policy agenda. In S.-Y. Peng, C.-F. Lin, & T. Streinz (Eds.), *Artificial intelligence and international economic law* (pp. 1–26). Cambridge University Press. DOI:10.1017/9781108954006.002

Shaffer, G. (2021). Trade law in a data-driven economy: The need for modesty and resilience. In S.-Y. Peng, C.-F. Lin, & T. Streinz (Eds.), *Artificial intelligence and international economic law* (pp. 29–53). Cambridge University Press. DOI:10.1017/9781108954006.00

ThankGod, J. C. (2023). Artificial intelligence and international trade law: Navigating legal challenges in the age of automation. *SSRN Electronic Journal*. DOI:10.2139/ssrn.4706943

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021, 23 November). *Recommendation on the ethics of artificial intelligence, adopted on 23 November 2021*. https://unesdoc.unesco.org/ark:/48223/pf0000381137

World Intellectual Property Organization (WIPO). (1979). *Berne Convention for the Protection of Literary and Artistic Works (as amended on 28 September 1979) (authentic text)*, TRT/BERNE/001. https://www.wipo.int/wipolex/en/text/283698

World Trade Organization (WTO). (2017a). *General Agreement on Trade in Services (GATS), Annex 1B*. https://www.wto.org/english/docs_e/legal_e/gats_e.htm

World Trade Organization (WTO). (2017b). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (as amended on 23 January 2017). Annex 1C*. https://www.wto.org/english/docs_e/legal_e/31bis_trips_e.pdf

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.12

Received: 27.10.2024
Accepted: 3.07.2025

Dariusz Szostek
Uniwersytet Śląski w Katowicach, Polska
dariusz.szostek@us.edu.pl
ORCID ID: https://orcid.org/0000-0002-8924-6968

Agnieszka Malarewicz-Jakubów
Uniwersytet w Białymstoku, Polska
malarewicz@uwb.edu.pl
ORCID ID: https://orcid.org/0000-0001-5964-4546

Maddalene Castellani
University of Verona, Italy
castellani@triberticastellani.com
ORCID ID: https://orcid.org/0000-0002-4748-8256

Koncepcja i podstawy prawne dla nowego ujęcia rejestru – „Rejestr 3.0"

The Concept and Legal Basis for a New Approach to Registers: 'Register 3.0'

Abstract: This article introduces the authors' original concept of 'Register 3.0', a modernized model of public registers designed to meet the demands of the evolving European digital economy and the increasing algorithmization of law. In the context of significant regulatory developments in the European Union, particularly the adoption of the eIDAS2 Regulation, the authors emphasize the urgent need to reformulate the architecture and function of public registers. Register 3.0 is envisioned as an interoperable, automated, and highly secure data system, built upon cutting-edge technologies. A central component of this concept is datafication, understood as the real-time and automatic acquisition of data from reference sources without the need for manual processing. The article presents a comparative analysis of three generations of registers: traditional data repositories (Register 1.0), interoperable systems with partial automation (Register 2.0), and advanced registers integrated with algorithmic legal frameworks (Register 3.0), capable of issuing legal decisions and initiating cascading legal consequences autonomously. The authors discuss the possibility of embedding legal rules within algorithmic architecture – a process referred to as 'crypto-law' – where traditional legal norms are encoded directly into secure digital environments, thus enabling fully automated legal and administrative processes. Furthermore, the article explores practical applications of this concept, such as the Unified Business Registry system

© 2025 Dariusz Szostek et al. published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

in Dubai, as proof of the feasibility and effectiveness of Register 3.0 in real-world scenarios. By examining the legal, technological, and institutional prerequisites for implementation, the authors argue that Register 3.0 not only supports the automation of state functions and judicial systems but also serves as a foundation for next-generation legaltech solutions. The study opens the door to further interdisciplinary research on adapting European legal frameworks to accommodate these innovations, positioning Register 3.0 as a cornerstone of future digital governance.

Keywords: Register 3.0, digital economy, blockchain, Distributed Ledger Technology (DLT), smart contracts, datafication, eIDAS2, interoperability, process automation, data security, algorithmization of law
Słowa kluczowe: „rejestr 3.0", gospodarka cyfrowa, blockchain, Distributed Ledger Technology (DLT), smart contracts, danyfikacja, eIDAS2, interoperacyjność, automatyzacja procesów, bezpieczeństwo danych, algorytmizacja prawa

Wprowadzenie

Kadencja Parlamentu Europejskiego 2019–2024 to okres wzmożonych prac i kompleksowej regulacji rynku cyfrowego i tzw. „gospodarki cyfrowej". Pojęcie to nie jest nowe – pojawiło się po raz pierwszy w połowie lat 90, kiedy to utożsamiano je z łączeniem technologii inteligentnych maszyn i ludzi (Boratyńska, 2021). Przez lata uległo ono ewolucji i objęło swoim zakresem nie tylko systemy cyberfizyczne ale także usługi cyfrowe czy wykorzystanie AI[1]. Europejski rynek cyfrowy, ale także „gospodarka cyfrowa", wymaga nowoczesnych regulacji prawnych pozwalających na konkurowanie z USA czy rozwiniętymi rynkami azjatyckimi. Istotnym dokumentem UE w tym zakresie jest przyjęty przez Parlament Europejski i Radę (UE) 2022/2481 decyzją z dnia 14 grudnia 2022 r. program polityki *Droga ku cyfrowej dekadzie do 2030 r.* (tekst mający znaczenie dla EOG)[2]. Jej konsekwencją jest m.in. zmiana „filozofii" działania europejskiego rynku cyfrowego, w tym nowe ujęcie dokumentu (tzw. dokument 3.0). W naszej ocenie, współczesna gospodarka cyfrowa, aby sprostać oczekiwaniom nowoczesnego rynku, wymaga dodatkowo nowego ujęcia i sposobu funkcjonowania rejestrów.

Polityka *Droga ku cyfrowej dekadzie* główny nacisk kładzie na promowanie skoncentrowanego na człowieku i opartego na prawach podstawowych, inkluzywnego, przejrzystego i otwartego środowiska cyfrowego, a także wykorzystanie bezpiecznych i interoperacyjnych technologii oraz usług cyfrowych zgodne z zasadami, prawami i wartościami Unii. Ponadto, na opracowanie kompleksowego i zrównoważonego ekosystemu interoperacyjności infrastruktury cyfrowej, w której kluczowe są obliczenia wielkiej skali, przetwarzanie brzegowe, przetwarzanie w chmurze, obliczenia kwantowe, AI, zarządzanie danymi – w tym zarządzanie da-

1 Kolejne definicje gospodarki cyfrowej wskazują na innowacyjne coraz bardziej zaawansowane technologie wdrażane w poszczególnych branżach gospodarki światowej. Konferencja Narodów Zjednoczonych do Spraw Handlu i Rozwoju UNCDAD w 2017 roku wskazała na wdrażanie systemów cyberfizycznych, obejmujących między innymi robotyzację i automatyzację produkcji, usługi chmurowe, dane z mobilnych źródeł czy sztuczną inteligencję (Boratyńska, 2021).

2 Dz.U. UE.L.2022.323.4

nymi zawartymi w różnych rejestrach – a które w obecnej postaci nie spełniają potrzeb nowoczesnego obrotu.

Mając powyższe na uwadze, należy zadać pytanie badawcze: czy dotychczasowe ujęcie i koncepcja rejestru są wystarczające dla współczesnego obrotu gospodarczego? Czy mamy wystarczające podstawy prawne, aby na gruncie prawa europejskiego wyodrębnić nowy rodzaj rejestru nazwanego przez autorów „rejestrem 3.0”? A jeżeli tak, to w jaki sposób miałby funkcjonować i w jaki sposób dane w nich zapisane powiązać z domniemaniami prawnymi?

1. Rejestry elektroniczne a danatyzacja gospodarki cyfrowej

W literaturze ekonomicznej wskazuje się na trzy podstawowe elementy gospodarki cyfrowej: usieciowienie społeczeństwa, transformację cyfrową oraz gospodarkę opartą na danych. Konsekwencją ostatniego jest wyodrębnienie pojęcia „danyfikacja” (zwana także „datafikacją” z ang. *datafication*), oznaczającego pozyskiwanie danych z różnego rodzaju systemów informatycznych wytwarzanych przez użytkowników internetu zarówno indywidualnych, biznesowych, jak i instytucjonalnych. W literaturze prawniczej już ponad dekadę temu wskazano, iż coraz istotniejszy jest dostęp do informacji (Szpor, 2009), czy też szerzej do danych, w miejsce klasycznego dostępu do dokumentu (Szostek, 2012). Przez wiele lat rejestry służyły jako tradycyjne repozytoria dokumentów, z czasem coraz bardziej jako repozytoria danych, na podstawie których pozyskiwane są informacje. Cechą charakterystyczną dotychczasowych rejestrów było to, iż stanowiły źródło informacji dla człowieka, który na ich podstawie podejmował odpowiednie decyzje.

Obecnie jesteśmy na etapie coraz głębszej algorytmizacji procesów, w tym algorytmizacji prawa, łącznie z algorytmizacją wydawania decyzji czy nawet orzeczeń (Newell & Marabelli, 2015). W środowisku naukowym, jak i w literaturze odbywa się dyskusja co do dopuszczalności, ale także zakresu zautomatyzowania procesu decyzyjnego – tzw. Legaltech 3.0 (Szostek, 2021). Zagadnienie to jest wyjątkowo ciekawe, wymaga jednakże odrębnych, pogłębionych badań, zarówno na gruncie prawa wspólnotowego, jak i krajowego, a co za tym idzie – wykracza poza zakres wąskich ram niniejszego artykułu.

Pytanie, czy tradycyjne rejestry są adekwatne do potrzeb LegalTech 3.0, jest w tym miejscu jak najbardziej zasadne. Gospodarka cyfrowa opiera się o dane, ale przede wszystkim o ich agregację[3] (LeBreton i in., 2022). Jej podstawą jest rozliczalność, ale też ich „czystość” oraz bezpieczeństwo (w znaczeniu niezmienności). Ten ostatni element stał się kluczowym w aspekcie zaufania do danych, systemów oraz algorytmów i przewija się we wszystkich aktach prawnych tworzących europejski rynek cyfrowy,

3 Przez agregację danych na potrzeby niniejszego artykułu przyjmuje się, iż jest to proces zbierania, łączenia i organizowania różnorodnych źródeł informacji w spójną strukturę lub format.

nakładając na przedsiębiorców szereg obowiązków w zakresie bezpieczeństwa zarówno danych, jak i wykorzystywanych algorytmów (Lubasz, 2025). Wystarczy tylko spojrzeć na regulacje rozporządzenia AI Act (Parlament Europejski i Rada, 2024) czy cały pakiet przepisów dotyczących bezpieczeństwa, bezpieczeństwa informacji, cyberbezpieczeństwa, podatności systemów uregulowanych w rozporządzeniu DORA (Parlament Europejski i Rada, 2022), rozporządzeniu MiCA (Parlament Europejski i Rada, 2023) czy dyrektywie NIS 2 (Parlament Europejski i Rada, 2022). Regulacji poddano także dostęp do danych w obrocie B2B oraz B2C i prawo do przenoszenia danych (Data Act) (Parlament Europejski i Rada, 2023).

Jak w tym aspekcie wygląda problematyka rejestrów elektronicznych i czy dotychczasowe regulacje są w tym zakresie wystarczające, aby wysnuć koncepcję „rejestru 3.0"? Badania przedstawione w artykule mają charakter wstępny i odnoszą się nie tyle do konkretnego rodzaju rejestru (jak rejestr handlowy czy księga wieczysta), ile do ogólnej koncepcji interoperacyjnego rejestru opartego o nowoczesne narzędzia informatyczne, w tym także uwzględniające DLT, tokenizację procesów czy wykorzystywanie *smart contract*.

2. Rejestr[4] 1.0, 2.0

W chwili obecnej korzystamy w UE z bardzo wielu rejestrów, zarówno publicznych, jak i prywatnych. Te ostatnie stanowią ciekawy przykład wykorzystania nowoczesnych narzędzi informatycznych coraz częściej opartych o DLT i rejestry

4 Patrz: Oleński (2006) oraz Nyczaj & Ruszkowski (2009). W literaturze wskazuje się, że zgodnie z ustawą o informatyzacji (Dz.U. Nr 64, poz. 565 z 2005 z późn zm) rejestr publiczny to rejestr, ewidencja, wykaz, lista albo inna forma ewidencji, służąca do realizacji zadań publicznych, prowadzona przez podmiot publiczny na podstawie odrębnych przepisów. J. Oleński proponuje podział ze względu na kryterium obiektu rejestrowanego: 1. podmiotów, 2. obiektów materialnych, 3. procesów ekonomicznych, 4. zdarzeń społecznych, ekonomicznych, technicznych, ekologicznych lub innych rejestrownych i ewidencjonowanych jako niezbędne organom administracji publicznej. Wskazał również, że definicja obejmuje rejestry zarówno prowadzone przez podmioty publiczne, jak i niepubliczne (np. samorządy zawodowe). T. Stawecki wskazuje, iż rejestr publiczny to zbiór informacji o osobach, rzeczach, i posiada następujące cechy: 1. utworzony na podstawie przepisów prawa, 2. prowadzony przez organ rejestrowy, 3. przyjęcie, utrwalenie a następnie ujawnienie określonych w nim informacji następuje w drodze decyzji, 4. prowadzenie rejestru i ujawnienie zawartych w nich informacji rodzi skutki prawne dla osoby, której wpis dotyczy, jak i dla organu, 5. jest jawny (Stawecki, 2005). W doktrynie rozróżnia się pojęcia (Oleński, 2006): rejestr, ewidencja i wykaz. W rejestrze zakres informacji i tryb jego funkcjonowania wyznaczają potrzeby identyfikacji i klasyfikacji obiektów rejestrowych, a w ewidencji procedury administracyjne, które ona obsługuje. W przypadku rejestru utworzenie bazy danych to cel główny, a dalsze jej wykorzystanie to kwestia wtórna, a w przypadku ewidencji wytworzony zbiór danych to niejako „produkt uboczny" realizowanej procedury. Kryterium odróżnienia pomiędzy rejestrem a wykazem polega na trybie aktualizacji. Wykaz aktualizuje się z pominięciem procedur administracyjnych. Na potrzeby artykułu, przyjmujemy uproszczenie terminologiczne, nie wgłębiając się we wskazywane w literaturze różnice, aby wykazać istotę nowego ujęcia obiegu informacji w ramach rejestru 3.0.

rozproszone a także wpisy w blockchain. Rejestry pełnią szereg funkcji: stanowiącą, identyfikacyjną, weryfikacyjną, klasyfikacyjną, integracyjną, normalizacyjną, kontrolną oraz informacyjną (Oleński, 2006). W aspekcie rejestrów publicznych często dodatkowo mamy do czynienia z funkcją legalizacyjną, dokonywaną, czy to na podstawie decyzji, czy też postanowienia sądowego, mającą charakter konstytutywny lub deklaratywny. Na potrzeby niniejszego artykułu przyjmujemy, iż rejestr publiczny to przede wszystkim oficjalna, referencyjna baza danych (fizyczna lub w postaci elektronicznej), utworzona przez upoważniony do tego organ, instytucję lub sąd na podstawie i w granicach przepisów prawa. Najczęściej wpis danych do rejestru publicznego wywołuje skutki prawne zarówno dla osoby, której wpis dotyczy, jak i czasami także dla organu lub instytucji i to nie tylko tych, które dokonały wpisu. Konstytutywny wpis do rejestru bardzo często wywołuje skutki prawne dla wielu podmiotów, podobnie jak zmiana tego wpisu, często nie pozostając bez wpływu na zapisy w innych rejestrach. Współczesny obrót wymaga szybkiej, sprawdzonej, zweryfikowanej, autentycznej i referencyjnej (pewnej) informacji, w tym tej zawartej w rejestrach. Autentyczność, integralność, domniemania prawne powiązane z danymi i wpisami do rejestru oraz pewność danych (odnośnie także skutków prawnych) była i jest kluczowa zarówno dla państwa, wymiaru sprawiedliwości, jak i obrotu gospodarczego. Funkcje weryfikacyjna i kontrolna od dawna są wskazywana jako kluczowe dla rejestrów. Funkcja weryfikacyjna polega na tym, że w rejestrach powinny znajdować się aktualne informacje potrzebne do sprawdzenia przez podmioty mające interes prawny, jaki jest status prawny, organizacyjny lub ekonomiczny danej osoby czy podmiotu, i powinny znajdować się tam aktualne informacje. Funkcja kontrolna natomiast polega na tym, iż na podstawie rejestru użytkownik (w tym także podmioty publiczne, sądownictwo) powinien móc zweryfikować jakość informacji, a rejestr powinien dawać rękojmię wiary publicznej, za którą bierze odpowiedzialność państwo (por. Oleński, 2006). W tym zakresie funkcja rejestru się nie zmieniła. Niestety narzędzia pozwalające na zapewnienie wspomnianej autentyczności, integralności, jak i referencyjności, jakie dają nam tradycyjne rejestry, odbiegają od potrzeb współczesnego obrotu. Dane w nich zawarte często nie mają charakteru aktualnego (przykładowo: pomimo wydania aktu zgonu, w wielu rejestrach nie ma informacji o śmierci osoby do momentu zgłoszenia tego faktu albo przez organ, albo przez zainteresowanych). Są także jednym z powodów opieszałości zarówno administracji (Trzcińska, 2023), jak i nieterminowości wymiaru sprawiedliwości[5], w którym wiele czasu absorbuje nawał pracy, często związanej z koniecznością manualnej weryfikacji danych, dokumentów czy też rejestrów, zamiast – przy dobrze skonstruowanym rejestrze czy też systemie re-

5 Na opieszałość wymiaru sprawiedliwości zwraca się uwagę praktycznie od zawsze, wskazując za niesprawiedliwe już samo długie czekanie na wyrok. Przykładem może tu być historyczna publikacja z 1885 (Lerned, 1885) czy praca (Esper, 1970).

jestrów 3.0 – wykorzystywać ją na pracę merytoryczną[6]. Tradycyjne ujęcie – czy też rozumienie – rejestru to: baza danych, z której organ lub sąd pozyskują dane, tworząc dokumenty 1.0 lub odpowiednik elektroniczny dokumentu tzw. dokument 2.0[7], który przesyłany jest w sposób tradycyjny lub elektroniczny, np. skrzynkę do doręczeń. Na potrzeby niniejszego artykułu przyjmujemy, iż jest to rejestr 1.0.

W literaturze wskazuje się na podział rejestrów na pierwotne oraz wtórne, co wiąże się z pojęciem relacji referencyjności[8] informacji. W ramach przyjętego w naszej koncepcji pojęcia „rejestr 2.0" mieści się: interoperacyjność[9] między rejestrami czy też systemami informatycznymi, w których rejestr jest umiejscowiony, gdzie dane z rejestrów pierwotnych pozyskiwane są, czy też wykorzystywane, w rejestrach wtórnych. Decyzje, orzeczenia, mające charakter konstytutywny, czy też inne czynności z reguły w dalszym ciągu wydawane są przez ludzi, po uprzedniej kontroli danych. Nowocześniejsza i szybsza jest wymiana danych czy też informacji. Ale w ramach „rejestru 2.0" orzecznikiem, jak także weryfikującym dane, pozostaje człowiek. Dane pozyskiwane są zarówno automatycznie (w ramach interoperacyjności), jak i ze źródeł tradycyjnych, w tym także poprzez wprowadzenie danych przez człowieka.

3. Rejestr 3.0 jako element algorytmizacji prawa

Prawo w kodach algorytmicznych to już nie tylko teoretyczna koncepcja naukowców (Wood, 2018; Wright & De Filippi, 2015) – to realne wdrożenia. Jesteśmy świadkami faktycznej realizacji koncepcji Lawrence Lessiga powiązania prawa z kodem algorytmicznym (1999, s. 3 i nast.). To już nie pojedyncze głosy, ale coraz szerszy nurt

6 Przykładem jest chociażby sytuacja, gdy sędzia w Polsce dla pozyskania danych z systemu PESEL musi albo wydać zarządzenie i pozyskać tradycyjny dokument pobrany przez sekretariat sądu, często po kilku dniach od wydania zarządzenia, albo przeszukiwać samodzielnie bazę, nie podejmując w tym czasie innej pracy merytorycznej.

7 Dokument 2.0 najczęściej zapisywany jest w formacie PDF, może być opatrzony kwalifikowanym podpisem elektronicznym, kwalifikowaną pieczęcią elektroniczną lub zapisany w blockchain jako plik. Może, ale nie musi, być powiązany z domniemaniami prawnymi. Może mieć charakter dokumentu urzędowego albo prywatnego. Nie jest jednakże aktywny; stanowi zamkniętą całość.

8 Odpowiednikiem tego pojęcia jest zwrot „odnośnik" lub wzorzec. A pojęcia, takie jak rejestr referencyjny lub baza referencyjna, należy traktować jako odpowiednik pojęcia rejestr pierwotny, baza pierwotna. Por. (Nyczaj & Ruszkowski, 2009).

9 W Polsce kwestię wymiany danych między rejestrami oraz ich interoperacyjność reguluje w chwili obecnej rozporządzenie Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U z 22 maja 2024 r., poz. 773). Definicja opisowa interoperacyjności zawarta jest w § 4 rozporządzenia. Podstawową zasadą wymiany danych w ramach interoperacyjności określonej w przepisach jest zapewnienie autentyczności danych, integralność, rozliczalność, bezpieczeństwo, w tym analityka podatności, dostępność, niezaprzeczalność, poufność a także wykorzystywanie atrybutów.

(Hassan & De Filippi, 2017), który z powodzeniem został odzwierciedlony w umowach prywatnych poprzez realizację w *smart contracts* i zapis w DLT czy blockchain[10].

W swojej publikacji G. Wood zauważył, iż rozwój kryptografii powoduje materializowanie się koncepcji kodu jako prawa (2018). Nazywa je kryptoprawem, gdzie reguły prawne (wybrane) znane z prawa tradycyjnego umiejscowione zostają w silnie bezpiecznej przestrzeni cyfrowej opartej o kryptografię (stąd wyprowadzone zostało pojęcie „kryptoprawo”). W raporcie *Legislation as code for New Zealand* (Barraclough, Fraser & Barnes, 2021) podjęto szerzej tę problematykę, wskazując zarówno na wady, jak i zalety implementacji prawa w algorytmy. Zwrócono przy tym na istotną rolę bezpieczeństwa algorytmów oraz danych wykorzystywanych w takich systemach oraz ryzykach z tym związanych.

„Implementacja prawa w kodzie, czy też architekturze algorytmu, wymaga wspólnej pracy i przygotowania przez prawników i programistów. Prawnicy, a wcześniej ustawodawca poprzez reguły prawne regulują stosunki społeczne, informatycy wprowadzają te reguły w systemy informatyczne. Następuje tu przecięcie nauk ścisłych i prawa, co wymusza zmianę w metodyce funkcjonowania obu grup, ale też zmianę metodyki stosowania wiedzy oraz kontrolowania prawidłowości implementowanych reguł w kody” (Szostek, Prabucki & Wyczik, 2021, s. 13).

Bezpieczeństwo, czy też pewność zapisanych w rejestrach danych, staje się kluczowe. I to zarówno w aspekcie technicznym, jak także prawnym (domniemania). W literaturze (chociażby Tripathi, Ahad & Casaliano, 2023), wskazuje się na atrakcyjność rejestru blockchainowego i tokenów w nim wpisanych, ze względu na nieusuwalność danych i duże bezpieczeństwo technologiczne oraz pewność zapisu (wysoki poziom autentyczności oraz integralności wpisanych danych). Bezpieczeństwo technologiczne jako ważny element rejestrów jest wskazywane jako kluczowe przez środowisko techniczne czy też informatyczne. Prawnicy inaczej postrzegają rejestry. Przede wszystkim jako gwarancję autentyczności, referencyjności danych połączoną z domniemaniami prawnymi – dotyczy to zarówno rejestru 1.0, 2.0, jak także koncepcji „rejestru 3.0”.

Czymże w ocenie autorów jest „rejestr 3.0” i czym różni się od rejestru 2.0 oraz 1.0? Przede wszystkim: 1) poziomem automatyzacji transferu danych między systemami (chociaż ten postulat odnosi się także w naszej koncepcji do „rejestru 2.0”); 2) „zaszyciem” w algorytmach reguł prawnych (inżynieria prawa), co umożliwia zautomatyzowanie, z pominięciem udziału człowieka, wydawania decyzji także mających charakter konstytutywny (a co odróżnia „rejestr 2.0” od „rejestru 3.0”); 3) kaskadowość rejestru, tzn. wpis do rejestru na podstawie automatycznie wydanej decyzji może stanowić podstawę do dalszej zautomatyzowanej decyzji, a ta do dalszej; 4) możliwość na każdym etapie kontroli przez człowieka; 5) rozliczalność. Inaczej ujmując, „rejestr 3.0” to rejestr umożliwiający podejmowanie decyzji także o charak-

10 Szersze omawianie problematyki blockchain czy DLT wychodzi poza zakres niniejszej pracy

terze konstytutywnym, w tym też wpisów do rejestru w ramach LegalTech 3.0. Przy czym nie przesądzamy o technologii, jaka do takiego procesu może być wykorzystywana, chociaż w chwili obecnej optymalną wydaję się technologia blockchain, DLT oraz tokenizacja procesów. Możliwe jest także zastosowanie AI, ale niekoniecznie.

Istotą dla realizowanej koncepcji rejestru 3.0 jest koncepcja danatyzacji dokumentu (tzw. dokument. 3.0), który nie jest powiązany z nośnikiem jak papier czy zamknięty kryptografią jak dokument 2.0, ale jest interaktywnym dokumentem, pozyskującym dane z referencyjnych rejestrów w czasie rzeczywistym, stanowiących podstawę do zautomatyzowanej decyzji. A wymiana danych między rejestrami następuje w sposób automatyczny, referencyjny, bezpieczny na dużym poziomie cyberbezpieczeństwa, w czasie rzeczywistym, z możliwością weryfikacji danych historycznych, bez udziału lub (w zależności od ustalonego procesu) z udziałem czynnika ludzkiego (tzw. wyroczni) akceptującego zmiany lub wpis.

Jako przykład, dla zrozumienia istoty koncepcji „rejestru 3.0", wskazujemy możliwość wykorzystania kryptoprawa w stokenizowanym akcie zgonu, który z Rejestru Stanu Cywilnego, w miejsce tradycyjnego aktu zgonu (jako dokumentu 1.0, który jest przedkładany w wielu organach, instytucjach, sądach), funkcjonowałby np. w technologii rozproszonego rejestru[11] i *smart contracts*[12] (od lat wykorzystywanych w obrocie cywilnym), który m*ógłby* „z automatu" wywoływać na przykład: umorzenie karnych postępowań, uniemożliwiać wpis zmarłej osoby do rejestrów, regulować kwestię wypłaty emerytury czy renty (podejmując decyzję o braku przelewu), uniemożliwi*ć* realizację recepty, wypłaty środków z konta bankowego i wiele, wiele innych czynności. W niektórych miejscach wywoływałby skutek informacyjny (jak np. w księgach wieczystych – odnotowanie faktu zgonu), czy w postępowaniach cywilnych, gdzie sędzia w czasie rzeczywistym miałby informację o śmierci strony, a co za tym idzie – np. wejściu do postępowania następców prawnych. I to wszystko działoby się automatycznie, bez potrzeby przedkładania jakichkolwiek dokumentów.

Rozwiązania oparte o automatyzm decyzji realnie działają w innych systemach prawnych. Nie miejsce w niniejszym artykule na opis takich rozwiązań na świecie (por. wcześniejsze projekty: Ebbers, Jansen & van Deursen, 2016), warto jednakże przykładowo wskazać na chociażby *Rejest Unifield Business Registy* w Dubaju (UBR) wdrożony przez DED (*Dubai Economic Department*) i ciągle rozwijany[13], którego

11 To tylko przykład technologii. Regulacje w zakresie rejestru 3.0 i budowy nowej infrastruktury rejestrów powinny być neutralne technologicznie.

12 Które, wbrew nazwie, mogą i są wykorzystywane także dla innych czynności niż wykonanie umów.

13 W ramach projektu zdefiniowano grupy użytkowników: tzw. wydawcy danych, czyli podmioty dokonujące referencyjnego wpisu do rejestru, oraz subskrybenci danych mogący być zarówno podmiotami rządowymi, organami wymiaru sprawiedliwości, jak i podmiotami prywatnymi. Nic nie stoi na przeszkodzie, aby pierwotni subskrybenci byli wydawcami w innych konfiguracjach. System jest ciągle rozwijany i obejmuje już ok. 2 tysięcy usług. Por. (Khan, Shael, Majdalawieh,

głównym założeniem jest traktowanie rejestru jako bazy referencyjnych danych, wykorzystywany do usług dla organów administracji, wymiaru sprawiedliwości, obywateli, osób prawnych itd. Oparty jest o blockchainową technologię, zapewniając bezpieczeństwo i transparentność danych, ale także współpracę i wymianę danych pomiędzy różnymi podmiotami a także automatyzację decyzji.

4. Rozporządzenie eIDAS2 – podstawą prawną dla koncepcji „rejestru 3.0”?

Współczesne rejestry publiczne stanowią istotne źródło danych[14]. O wartości rejestru stanowi nie tylko jakość danych, ale także szybkość dokonywanych zmian w odniesieniu do rzeczywistości, na podstawie których agregowane są informacje[15], a w konsekwencji czego – możliwość wykorzystywania ich poprzez Big Data[16] w różnych analizach, w tym predykcyjnych, ale także do wydawania decyzji. Do tej pory Big Data głównie wykorzystywana była przez podmioty prywatne. Coraz częściej możliwości, jakie daje, są doceniane przez rządy i organizacje międzynarodowe. Stąd wprowadzana interoperacyjność między rejestrami (rejestr 2.0), a także koncepcja „rejestru 3.0”, dla którego prawne podstawy znajdujemy w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (eIDAS2)[17].

Interoperacyjność oraz cyfryzacja w ramach rejestru 2.0 skupiona jest głównie na wsparciu administracji czy też organów sądownictwa oraz „wystawieniem” usług cyfrowych dla społeczeństwa lub przedsiębiorców w ramach danego rejestru. Interoperacyjność takich usług funkcjonuje w ograniczonym zakresie i co najwyżej na

Nizamuddin & Nicho, 2022) Por. także National blockchain Blueprint for Qatar 2022, https://www.qcb.gov.qa/Documents/SuperVision/QCB%20-%20DLT%20Guideline.pdf

14 Na potrzeby artykułu przyjmuje się definicję „danych” zaproponowaną przez Jamesa O. Hicksa: „reprezentacja faktów, pojęć lub instrukcji w sformalizowany sposób umożliwiający ich komunikowanie, interpretowanie lub przetwarzanie przez ludzi lub w sposób zautomatyzowany” (por. Hicks, 1984).

15 Na potrzeby niniejszego artykułu przez informacje rozumie się „wiedzę dotyczącą obiektów, takich jak fakty, zdarzenia, rzeczy, procesy lub idee, w tym koncepcje, która w pewnym kontekście ma znaczenie”. Definicja wyprowadzona ze standardu na potrzeby technologii informatycznych ISO/IEC 2382:2015.

16 Pojęcie to dotyczy zbioru danych, które ze względu na swoją złożoność lub wielkość nie są możliwe do zarządzania i analizy w zwykły sposób lub byłoby to znacznie utrudnione bądź niewydajne. Por. norma ISO 20546:2019. Cechami wskazującymi na Big Data jest: duża objętość danych, duże tempo generowania i przetwarzania danych, duża różnorodność danych, wiarygodność danych i wartość informacyjna.

17 Dz.U. EU L257/73 z 28 sierpnia 2014 r. Krytycznie na ten temat: Quinn & Connolly (2021).

poziomie lokalnym (krajowym). A podejmowanie decyzji dokonywane jest z reguły przez człowieka.

Unia Europejska, nie tylko w ramach polityki *Europa Cyfrowa 2030*, ale także w ramach legislacji zmienia ten stan rzeczy, skupiając się na usłudze i obywatelu UE, a nie na rejestrze jako takim. Podwaliną dla „rejestru 3.0" może stać się, zgodnie z rozporządzeniem eIDAS2, jednolite w skali całej UE narzędzie (*EU Wallet*) pozwalające na uwierzytelnianie w czasie rzeczywistym danych (stanowiących atrybuty), a także tożsamość osób fizycznych, jak i podmiotów prawnych. A zmiana danych (atrybutów) w jednym miejscu automatycznie będzie odnotowywana, czy też zauważalna, przez wszystkie strony ufające[18] w ramach usług zaufanych.

Od 24 grudnia 2026 r. państwa członkowskie zobowiązane są do udostępnienia obywatelom UE (ale co istotne także innym podmiotom, np. takim jak osoby prawne) europejskiego portfela tożsamości[19] (dalej EU Wallet), w ramach którego państwa członkowskie mają obowiązek umieszczania elektronicznych poświadczeń atrybutów[20] wydanych przez podmiot sektora publicznego odpowiedzialnego za źródło autentyczne lub w jego imieniu lub przez podmiot sektora publicznego, który jest wyznaczony przez państwo członkowskie do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródło autentyczne. Inaczej ujmując, państwa są zobowiązane udostępniać w czasie rzeczywistym dane jako atrybuty z repozytoriów lub systemów, za prowadzenie których odpowiedzialny jest podmiot sektora publicznego i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem UE lub prawem krajowym w tym z praktykami administracyjnymi[21]. Mogą więc stanowić w ramach „rejestru 3.0" podstawę do wydawania zautomatyzowanej decyzji. Wskazano przy tym minimalny zakres atrybutów: 1) adres,

18 Zgodnie z art. 3 pkt. 6 znowelizowanego rozporządzenia eIDAS „strona ufająca" oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej, europejskich portfelach tożsamości cyfrowej lub innym środku identyfikacji elektronicznej lub na usłudze zaufania.

19 Europejski portfel tożsamości cyfrowej oznacza środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom, ufając im oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęcie elektronicznych – art. 3 pkt. 42 eIDAS.

20 „Elektroniczne poświadczenie atrybutów" oświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów. „Atrybut" oznacza cechę charakterystyczną, właściwą dość, prawo lub zezwolenie osoby fizycznej lub prawnej lub przedmiotu. A „walidacja" oznacza proces weryfikacji i potwierdzania, że dane w postaci elektronicznej są ważne zgodnie z niniejszym rozporządzeniem (art. 3 eIDAS).

21 Zgodnie z art. 3 pkt. 47 „źródło autentyczne" oznacza repozytorium lub system, za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, który zawiera i udostępnia atrybuty dotyczące osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczny zgodnie z prawem Unii lub prawem krajowym, w tym z praktykami administracyjnymi.

2) wiek, 3) płeć, 4) stan cywilny, 5) skład rodziny, 6) narodowość lub obywatelstwo, 7) wykształcenie, tytuły i licencje, 8) kwalifikacje zawodowe, tytuły i licencje, 9) pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych, 10) publicznoprawne zezwolenia i licencje, oraz w odniesieniu do osób prawnych 11) dane finansowe i dane dotyczące przedsiębiorstwa[22].

Elektroniczne poświadczenie atrybutów powinno zawierać informacje na temat statusu ważności poświadczenia lub miejsce usług, w którym można dowiedzieć się o ważności poświadczenia[23], oraz zestaw danych jednoznacznie reprezentujących źródło autentyczne (art. 45f eIDAS), a w przypadku jego unieważnienia traci ważność od momentu unieważnienia i nie można przywrócić jego statusu. Dodatkowo, podmioty sektora publicznego wydające poświadczenie atrybutów mają obowiązek zapewnienia interfejsu z europejskimi portfelami tożsamości cyfrowej, co powoduje, iż atrybuty przez nie wydawane muszą być dostępne w każdym EU Wallet wydanym w EU, także przez inne państwa niż państwo podmiotu sektora publicznego wydającego atrybut. Dodatkowo, na podstawie art. 45g eIDAS dostawcy elektronicznych poświadczeń atrybutów muszą zapewnić użytkownikom europejskiego portfela tożsamości możliwość żądania otrzymywania, przechowywania elektronicznego poświadczenia atrybutów, a także zarządzania nim, niezależnie od państwa członkowskiego, w którym zapewniony jest europejski portfel tożsamości[24].

Rozporządzenie eIDAS2 wprowadza ponadto nowe narzędzia: 1) „kwalifikowany rejestr elektroniczny", któremu nie można odmówić skutku prawnego ani dopuszczalności w postępowaniu sądowym wyłącznie z tego powodu, iż ma postać elektroniczną. A wpis danych zawartych do kwalifikowanego rejestru elektronicznego korzysta z domniemania ich niepowtarzalnego i dokładnego, sekwencyjnego uporządkowania oraz ich integralności (art. 45l oraz 2) „kwalifikowaną usługę archiwizacji", za sprawą czego dane przechowywane przy użyciu tej usługi korzystają z domniemania ich integralności i pochodzenia przez cały okres przechowywania (art. 45 i). Narzędzia te mogą stanowić istotny element powiązania wpisu do „rejestru 3.0", nawet funkcjonującego jako rejestr rozproszony, z domniemaniami prawnymi.

Rozporządzenie eIDAS2 stanowi okazję do zbudowania nowej jakości usług dla obywateli UE, ale także podstawę do utworzenia „rejestrów 3.0". Bez wątpienia eIDAS2 wpłynie na zwiększenie automatyzacji transferu danych. Daje też kontrolę nad danymi przez człowieka, a także możliwość rozliczalności. To od państw zależeć będzie ewentualne „zaszycie" w algorytmach reguł prawnych, a co za tym idzie – wprowadzenia kaskadowości rejestru, w konsekwencji czego - „rejestru 3.0". I niekoniecznie musi to być algorytm AI – przynajmniej na wstępnym etapie. Konieczność przebudowy systemów informatycznych, w zgodności z narzędziami eIDAS2, stanowi okazję do tego

22 Por. załącznik VI do rozporządzenia eIDAS

23 Por. pkt. „i" załącznika VII do rozporządzenia eIDAS.

24 Nie miejsce w niniejszym artykule na szersze omówienie eIDAS, ze względu na zakres tematu.

typu działań. Wymaga jednakże zmiany mentalnej i określenia dalekosiężnych celów w cyfryzacji państwa, w tym zwiększenia automatyzacji w podejmowaniu decyzji, przy ciągłej (ale ewentualnej, a nie koniecznej) kontroli przez człowieka.

Można tego też nie robić i pozostać na poziomie „rejestru 2.0", gdzie decyzja zawsze podejmowana będzie przez człowieka, na podstawie danych wpisanych do rejestru. Ale czy to usprawni administrację? Wiele osób obawia się automatyzacji wydawania decyzji, w tym utraty kontroli przez człowieka. Oczywiście zawsze istnieje ryzyko wadliwości systemów informatycznych i błędów w wydawaniu decyzji. Ale czy nie mamy do czynienia z błędami ludzi przy ich wydawaniu? Stąd w naszej koncepcji „rejestru 3.0" możliwość kontroli wpisywanych danych przez człowieka także *ex post* tak, jak mamy z tym do czynienia w przypadku dokonywania wpisu w dniu dzisiejszym przez człowieka. Dobrym wzorem jest tutaj wskazany przykład rejestru *Unifield Business Registy* w Dubaju

Podsumowanie

W niniejszym artykule stanowiącym zaledwie początek poważniejszych badań problemu postawiono kilka pytań badawczych: „czy dotychczasowe ujęcie i koncepcja rejestru są wystarczające dla współczesnego obrotu gospodarczego?", „czy mamy wystarczające podstawy prawne, aby na gruncie prawa europejskiego wyodrębnić nowy rodzaj rejestru nazwanego przez autorów „rejestrem 3.0"?", „a jeżeli tak, to w jaki sposób miałby funkcjonować, i w jaki sposób dane w nich zapisane powiązać z domniemaniami prawnymi?".

W naszej koncepcji „rejestr 3.0" stanowi połączenie pewności i przejrzystości danych wpisanych w rejestrze, optymalnie w czasie rzeczywistym w odniesieniu do odnotowywanego faktu; rozliczalność tychże danych, a ponadto wysoki poziom automatyzacji transferu danych między systemami. Wiąże się także z „zaszyciem" reguł prawnych w algorytmach, umożliwiających zautomatyzowanie, z pominięciem udziału człowieka, wydawania decyzji; kaskadowością rejestru; a wreszcie z możliwością kontroli przez człowieka na każdym etapie i wysokim poziom cyberbezpieczeństwa. Nie jest to tylko koncepcja teoretyczna. Rozwiązanie oparte na koncepcji „rejestru 3.0" wdrożone i rozwijane jest w podawanym przykładzie rejestru w Dubaju. Koncepcja jest więc nie tylko możliwa do wdrożenia, ale rzeczywiście działa.

W Europie, ale także i na poziomach krajowych, wymaga to nowego przemyślenia, a w konsekwencji przebudowania rejestrów, do czego mamy właśnie okazję w związku z wejściem w życie rozporządzenia eIDAS 2, będącego istotnym i bardzo ważnym uzupełnieniem oraz łącznikiem pakietu unijnych przepisów dotyczących gospodarki cyfrowej, cyberbezpieczeństwa, tożsamości cyfrowej, ale także przepisów krajowych dotyczących rejestrów, systemów stanowiących źródło autentyczne. W Unii Europejskiej jest wytyczną dla zmian w zakresie myślenia, ale także podej-

ścia do rejestrów i innych źródeł autentycznych atrybutów. Umożliwia pełną cyfryzację, ale – co najważniejsze – automatyzację procesów w organach administracji, sądownictwa, ale także biznesu. Nie tylko umożliwia, ale stanowi istotny pretekst[25] do przebudowania rejestrów i innych źródeł autentycznych (ewidencji, wykazów itd.) i stworzenia systemu, który odpowiadałby założeniom wskazanym w niniejszym artykule dla „rejestru 3.0” umożliwiającego nie tylko w czasie rzeczywistym potwierdzanie atrybutów, ale także wykorzystanie przez administrację narzędzi np. AI opartych na prawdziwych i rzeczywistych, zweryfikowanych i autentycznych źródłach. Problematyka wymaga dalszych badań i rozwinięcia.

Na pytanie badawcze: „czy mamy wystarczające podstawy prawne, aby na gruncie prawa europejskiego wyodrębnić nowy rodzaj rejestru nazwanego przez autorów <rejestrem 3.0>?” nie można odpowiedzieć jednoznacznie. Z jednej strony mamy pakiet przepisów unijnych wręcz wymuszających zmiany. Z drugiej strony konieczne są przepisy wykonawcze oraz istotne zmiany w przepisach krajowych i nowe koncepcje dla funkcjonowania rejestrów, z czym jeszcze jakiś czas musimy poczekać. Konieczna jest także zmiana procesów, jak dokonano tego w przytaczanym przykładzie Dubaju. Proces zmian został jednakże zapoczątkowany, a kierunek zmian w UE – wyraźnie zarysowany.

BIBLIOGRAFIA

Boratyńska K., Cieślik E., Kacperska E., Łukasiewicz K. & Milewska A. (2021). *Gospodarka cyfrowa we współczesnym świecie – kraje V4,* Wydawnictwo SGGW.

Ebbers W. E, Jansen M. G. M. & van Deursen A. J. A. M (2016). Impact of the digital divide on e-government: Expanding from channel choice to channel usage, *Government Information Quarterly 33*(4), 685–692.

Esper, T. L. (1970). Tardines of Attorneys as Contempt of Court. *Cleveland State Law Review,* (19). https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=2793&context=clevstlrev

Hicks J. O. (1984). *Management Information System: A User Prespective.* West Publishing Company, 1984, ss. 645.

Hassan, S. & De Filippi, P. (2017). The Expansion of Algorithmic Governance: From Code is Law to Law is Code. https://journals.openedition.org/factsreports/4518#tocfrom1n3

Khan, S., Shael, M., Majdalawieh, M., Nizamuddin, N. & Nicho, M. (2022). Blockchain form Goverments. The Case of the Dubai Goverment. *Sustainability, 14*(11), https://www.mdpi.com/2071–1050/14/11/6576

Lerned W. L. (1885). The tardiness of Justice. *The North American Review*, *140*(343), 498–508. https://www.jstor.org/stable/25118493?seq=5

25 Por. koncepcje wykorzystania AI na źródłach autentycznych: https://www.linkedin.com/pulse/understanding-role-public-records-governance-chris-chiancone-tuwic. Pobrano 6 października 2024 r.

LeBreton James M., Moeller Amanda N., & Wittmer Jenell L. S. (2022). Data Aggregation in Multilevel Research: Best Practice Recommendations and Tools for Moving Forward. *Journal of Business and Psychology, 38*(4). https://www.researchgate.net/publication/365719487_Data_Aggregation_in_Multilevel_Research_Best_Practice_Recommendations_and_Tools_for_Moving_Forward

Lessig, L. (1999). *Code and Law of Cyberspace*, Basic Books.

Lubasz, D. (2025). *RODO dla AI. Zgodność z zasadami godnej zaufania sztucznej inteligencji w modelu data protection by design*, Wolters Kluwer.

Newell, S. & Marabelli, M. (2015). Strategic opportunities (and challenges) of algorithmic decision-making: A call for acttion on the long-term societas effects of „datification". *Journal of Strategic Information System, 2.* https://www.sciencedirect.com/science/article/abs/pii/S0963868715000025?via%3Dihub

Nyczaj, K. & Ruszkowski, J. (2009). Definicje, klasyfikacje oraz modele integracji rejestrów publicznych, *Wiadomości Statystyczne, 12*. https://bazekon.uek.krakow.pl/gospodarka/163932632

Oleński, J. (2006). *Infrastruktura informacyjna państwa w globalnej gospodarce,* Wydawnictwo UW. https://historiainformatyki.pl/infrastruktura-informacyjna-panstwa-w-globalnej-gospodarce-wydawnictwo-uw-warszawa-2006

Quinn, J., & Connolly, B. (2021). Distributed ledger technology and property registers: displacement or status quo. *Law, Innovation and Technology*, *13*(2), 377–397.

Parlament Europejski i Rada. (2024). Rozporządzenie Parlamentu Europejskiego i Rady 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji.

Parlament Europejski i Rada. (2022). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności sektora finansowego Dz.U L33/1.

Parlament Europejski i Rada. (2023). Rozporządzenie Parlamentu Europejskiego i Rady 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów Dz.U L 150/40.

Parlament Europejski i Rada. (2022). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE Dz.U L 333/80.

Parlament Europejski i Rada. (2023). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020 Dz.U L 23.12.2023

Szpor, G. (2009). Prawne problemy wykorzystania nowych technologii w administracji publicznej i wymiarze sprawiedliwości, Warszawa.

Stawecki, T. (2005). *Rejestry publiczne. Funkcje instytucji*, Wydawnictwo Prawnicze LexisNexis.

Szostek, D., Prabucki, R. & Wyczik, J. (2021). [w:] D. Szostek (red.), *LegalTech*, C.H. Beck

Szostek, D. (2012). *Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej*, C.H. Beck.

Szostek, D. (2021). *LegalTech*, C.H. Beck.

Tapscott, D. (1995). *The Digital Economy. Rethinking Promise and Peril in the Age Networked Inteligence*. McGraw-Hill.

Tripathi, G., Ahad, M. A. & Casaliano, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challanges, *Decision Analytics Journal*, (9). https://www.sciencedirect.com/science/article/pii/S2772662223001844?via%3Dihub

Trzcińska, D. (2023). Problematyka głównych przyczyn bezczynności i przewlekłości w prowadzeniu spraw administracyjnych z zakresu ochrony środowiska. *Gdańskie Studia Prawnicze*, *4*(61), 38–51.

Wood, G. (2018). Ethenrnum: A secure decentralised generalised transaktion ledger. https://www.win.tue.nl/~mholende/seminar/references/ethereum_yellowpaper.pdf

Wright, A. & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *Social Science Research Network, 34*, 41–52.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.13
Received: 2.10.2024
Accepted: 15.04.2025

Mariusz Maciejewski
Akademia Leona Koźmińskiego, Polska
maciejewski@kozminski.edu.pl
ORCID ID: https://orcid.org/0000-0002-6183-6325

Administracja publiczna rynku finansowego wobec innowacji. Centrum innowacji (*innovation hub*), piaskownica regulacyjna (*regulatory sanbox*) i inne specjalne instytucje regulacyjne innowacji

The Public Administration of the Financial Market towards Innovation: Innovation Hubs, Regulatory Sandboxes and Other Special Regulatory Institutions of Innovation

Abstract: The digitalization of products and services on the financial market creates new challenges for public authorities administering this area. The Polish Financial Supervision Authority (PFSA) has been legally obliged to take care of the security of the market and at the same time support the innovation of it. Currently, innovation is strongly related to digitalization. This means that the PFSA has had to find legal and organizational solutions to fulfil these obligations. This article presents an argument indicating the contradiction between security and innovation. It then discusses solutions that allow the maximization of both security and innovation in the financial market. These solutions were developed in the administrations of highly developed financial markets and have already been transferred or can be transferred to the practice of the PFSA. On the basis of the British solutions, the article gives the examples of and discusses the most important solutions, collectively referred to as special regulatory institutions for innovation, i.e. innovation hubs, regulatory and digital sandboxes and innovation pathways.

Keywords: innovation hubs, regulatory sandboxes, virtual sandboxes, financial market regulation, financial market supervision
Słowa kluczowe: centrum innowacji, piaskownica regulacyjna, piaskownica wirtualna, nadzór nad rynkiem finansowym

© 2025 Mariusz Maciejewski published by Sciendo. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.

Wprowadzenie

Rynek finansowy jest obszarem szczegółowej regulacji ze względu na jego ogromne znaczenie dla systemu gospodarczego oraz społecznego. Z powodu tego znaczenia prawodawca ustanowił organ władzy publicznej administrujący tym obszarem, a w art. 2 Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym wskazał temu organowi następujące cele do realizacji – zapewnienie dla tego rynku: prawidłowego funkcjonowania, stabilności, bezpieczeństwa, przejrzystości, zaufania do rynku finansowego, ochrony interesów uczestników rynku finansowego, również poprzez rzetelną informację dotyczącą funkcjonowania rynku.

Jak z powyższego wyliczenia widać, priorytetem prawodawcy jest zapewnienie szeroko rozumianego bezpieczeństwa rynku, ponieważ, upraszczając, można powiedzieć, że pozostałe cele zostaną zrealizowane tylko na bezpiecznym rynku. Powyższym celom odpowiadają liczne regulacje prawne, krajowe oraz unijne, dotyczące tradycyjnych oraz nowych sektorów rynku finansowego – bankowego, kapitałowego, ubezpieczeniowego, funduszy emerytalnych, kryptoaktywów[1]. Regulacje te zawierają wiele instytucji prawnych służących bezpieczeństwu rynku, ponieważ jego zapewnienie wymaga podjęcia środków eliminujących zagrożenia. Można powiedzieć, że im więcej regulacji eliminujących ryzyka (np. im wyższe są kapitałowe bariery wejścia, liczniejsze wymogi dotyczących zachowań danego podmiotu w toku prowadzenia działalności itd.), tym mniejsze ryzyko dla tego podmiotu, rynku i klientów dany podmiot generuje. Omawianie ich wykracza poza założenia niniejszego artykułu, wydaje się jednak, że teza o znacznym obciążeniu regulacyjnym profesjonalnych podmiotów rynku finansowego raczej nie będzie kwestionowana[2].

Jest również niezaprzeczalnym faktem, że aktualnie wszystkie, w tym tradycyjne, historycznie ugruntowane, sektory rynku finansowego stają wobec nowych trendów rozwoju cywilizacji, wśród których jednym z kluczowych jest informatyzacja / cyfryzacja produktów, ich dystrybucji oraz procesów z tym związanych. Wymagania rynku oraz inne uwarunkowania nie pozwalają profesjonalnym podmiotom rynku finansowego na pozostawanie biernym obserwatorem, ale wymagają od nich proaktywnego włączenia się w zachodzące zmiany czy też nawet przyjęcia roli lidera zmian ze względu na posiadane zasoby oraz możliwości działania. Niezależnie od aktywności podmiotów historycznie uczestniczących w rynku finansowym, część tej działalności prowadzona jest przez nowe podmioty typu start-up. Wyodrębnia się je w grupę podmiotów tworzących innowacje technologiczne w sektorze finansowym, określane dalej jako podmioty FinTech.

1 Warto odnotować, że w odniesieniu do kryptoaktywów dopiero MiCA wyklarowała sytuację prawną, wprowadzając *expressis verbis* nadzór publiczny nad tym rynkiem (zob. Hrabčák & Štrkolec, 2024).

2 Np. szerzej w odniesieniu do sektora bankowego (zob. Koleśnik, 2017); ogólnie też (Fal, 2022).

Można zasadnie twierdzić, że cel KNF w postaci bezpieczeństwa rynku jest w pewnym zakresie sprzeczny z ideami rozwoju, postępu oraz innowacyjności na rynku finansowym. Całkowite bezpieczeństwo wymaga bowiem całkowitego wyeliminowania ryzyk dla nadzorowanego obszaru. Tymczasem każda innowacyjność czy nawet niewielka zmiana z natury rzeczy zawiera w sobie mniejszy lub większy stopień ryzyka wystąpienia negatywnych skutków. I choć tym ryzykiem można zarządzać – czasami ograniczyć je nawet do dość niskiego poziomu – to wydaje się, że nigdy nie można go zupełnie wyeliminować. Stąd powyższa teza o sprzeczności wydaje się uzasadniona. Tymczasem hipoteza badawcza niniejszego opracowania głosi, że istnieją takie metody administracyjnoprawnego ułożenia relacji bezpieczeństwa i rozwoju, które pozwalają zmaksymalizować poziomy zarówno bezpieczeństwa, jak i rozwoju, mimo ich powierzchownej sprzeczności.

Obszerne uregulowanie dla celów bezpieczeństwa oznacza duże obciążenia po stronie podmiotów nadzorowanych. I o ile duże podmioty o ugruntowanej pozycji oraz nowe podmioty wyposażone w duże zasoby kapitałowe mogą sobie pozwolić na zapewnienie zgodności z regulacjami (także z nowymi, jak np. dotyczącymi ESG czy zrównoważonego rozwoju, Fedorowicz & Zalcewicz, 2024, s. 47 i nast.; Jurkowska-Zajdler & Schweigl, 2024, s. 205), o tyle może być to problematyczne lub nawet niemożliwe dla podmiotów nowych z niewielkimi zasobami kapitałowymi. Ogranicza to wejście do systemu dla tych podmiotów, a przez to ogranicza równocześnie innowacyjność rynku finansowego przez blokowanie wejścia nowych uczestników. Poza tym, działania innowacyjne w rozległym środowisku prawnym często będą rodziły wątpliwości co do tego, czy nie naruszają istniejących wymagań regulacyjnych, zwłaszcza w sytuacji, gdy organ publiczny administrujący rynkiem finansowym jest zobowiązany do zapewnienia bezpieczeństwa rynku. Jest to zatem kolejny istotny czynnik ograniczający innowacyjność. Uwagi te aktualne są również w odniesieniu do działań innowacyjnych, które mogą być także podejmowane przez podmioty już uczestniczące w tym rynku.

Mimo tej naturalnej sprzeczności bezpieczeństwa i innowacyjności, w art. 4 ust. 1 pkt 3a ustawy o nadzorze nad rynkiem finansowym, prawodawca nałożył na KNF także zadanie (a więc nie cel) w postaci podejmowania działań mających na celu wspieranie rozwoju innowacyjności rynku finansowego. Zresztą, pośrednio obowiązek wspierania innowacyjności rynku finansowego (przy uwzględnieniu bezpieczeństwa) można także wywodzić interpretacyjnie z celu, jakim jest prawidłowe funkcjonowanie rynku finansowego wyrażone w art. 2 ustawy o nadzorze nad rynkiem finansowym. Ta opozycja (pozorna, co zostanie dalej wykazane) dotyczy również zagranicznych organów administrujących, można więc stwierdzić, że organy administracji rynku finansowego różnych krajów stają wobec problemu: bezpieczeństwo czy rozwój o rozsądnym tempie[3]. Albowiem rozwój jest równoznaczny z

3 Szerzej na ten temat np. (Faykiss, Papp, Sajtos & Toros, 2018, 43–67).

innowacjami, ze zmianami. Zmianą może być np. wejście z nową instytucją prawną w istniejące i znane środowisko albo wejście z już istniejącą i znaną instytucją prawną do nowego środowiska. Konieczność ustalenia właściwej granicy pomiędzy bezpieczeństwem a innowacyjnością i rozwojem rynku finansowego skłoniła organy nadzoru do poszukiwania rozwiązań, które pozwolą określić tę granicę tak, aby jednocześnie osiągnąć oba cele w postaci bezpieczeństwa oraz rozwoju rynku. Takie rozwiązania zostały wypracowane w organach regulacyjnych państw anglosaskich. Niniejszy artykuł przedstawia rozwiązania wprowadzone przez brytyjski Financial Conduct Authority (FCA). Warto zwrócić uwagę na praktykę tego organu ze względu na jego zaawansowanie w badanym obszarze, co wynika, obok niewątpliwych zasobów, wiedzy i kompetencji, także z wagi rynku finansowego tego kraju dla gospodarki i społeczności światowej. Są one warte odnotowania i omówienia w literaturze, ponieważ wiodące organy nadzoru nad rynkiem finansowym posiadają znaczącą wiedzę oraz zasoby zaangażowane w rozwój metod administrowania powierzonym im obszarem, a jednocześnie są niejako zmuszone nadążać za dynamicznym rozwojem profesjonalnych podmiotów rynku finansowego. Z tego powodu też bywają prekursorami rozwiązań, które następnie są przenoszone do kompetencji organów administracji innych krajów, czego przykładem może być nadzór na podstawie ryzyka stworzony w amerykańskim nadzorze rynku bankowego, przenoszony następnie do organów administracji innych sektorów rynku finansowego, a następnie do kompetencji organów administracji innych obszarów (Brunner, Hinz & Rocha, 2008, s. 6 i nast.; Nadolska, 2011, s. 51 i nast.). Innym przykładem może być wprowadzenie omówionej niżej instytucji piaskownicy regulacyjnej do prawa farmaceutycznego (Simons & Simons, 2023), do tzw. Artificial Intelligence Act[4], do prawa energetycznego (Fal, 2022, s. 41–42; Będkowski-Kozioł, 2022, s. 19 i nast.) oraz do oficjalnych, ogólnych dokumentów UE[5], w tym do Europejskiej Agendy Innowacji (*European Innovation Agenda*)[6]. Niezależnie od prac organów administracji, równocześnie prowadzone są prace akademickie nad rozwiązaniami mającymi odpowiedzieć na aktualne

4 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji); Dziennik Urzędowy Unii Europejskiej 2024/1689; w tym zakresie zob. Wyderka, 2023, s. 4 i nast.

5 Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, 16.11.202 r.; zob też. Regulatory sandboxes and experimentation clauses as tools for better regulation: Council adopts conclusions; www.pubaffairsbruxelles.eu/ ; https://www.pubaffairsbruxelles.eu/eu-institution-news/regulatory-sandboxes-and-experimentation-clauses-as-tools-for-better-regulation-council-adopts-conclusions/ (dostęp 10.09.2024 r.).

6 Agenda deklaruje poprawę warunków w celu umożliwienia innowatorom testowania nowych pomysłów w ramach piaskownic regulacyjnych, informacja prasowa Komisji Europejskiej, Com-

wyzwania (np. Zetzsche, Buckley, Barberis & Arner, 2017, s. 31 i nast.; Brown & Piroska, 2021, s. 19 i nast.).

1. Odpowiedź na wyzwania – specjalne instytucje regulacyjne innowacji (SIRI)

Odpowiedzią organów administracji rynku finansowego na trend rozwojowy w postaci cyfryzacji produktów, usług i procesów i wynikających stąd nowych możliwości rozwoju jest grupa rozwiązań, które można określić jako specjalne instytucje regulacyjne innowacji (SIRI). Na potrzeby rozważań w zakresie polskiego prawa administracyjnego specjalne instytucje regulacyjne innowacji (SIRI) należy rozumieć jako normy prawne dotyczące bezpośrednio działalności innowacyjnej, które stanowią *lex specialis* w stosunku do regulacji ogólnych i są ustanawiane w celu ułatwienia działalności innowacyjnej. Instytucje te mogą wprowadzać, bezpośrednio lub pośrednio, zwolnienia od obowiązków regulacyjnych ciążących na podmiotach administrowanych, szczególne uprawnienia dla tych podmiotów lub mogą tworzyć specjalne „świadczenia" administracyjne ułatwiające działalność innowacyjną. Specjalne instytucje regulacyjne innowacji mogą być regulowane przepisami każdej rangi i każdego poziomu, zaczynając od dyrektyw i rozporządzeń UE po regulaminy ustanawiane przez organy administracji zarządzające SIRI. W zakresie SIRI mieszczą się m.in. instytucje organizacyjno-prawne określane jako *innovation hub* (dalej tłumaczone jako centrum innowacji), *regulatory sandbox* (piaskownica regulacyjna[7]), *digital sandbox* (piaskownica cyfrowa), *innovation pathways* (ścieżki innowacyjne), *regulatory pilot regime* (dalej tłumaczone jako regulacyjny system pilotażowy) i inne. Część z tych instytucji istnieje już w regulacjach prawnych rynku finansowego w Polsce i szerzej na świecie. Można sądzić, że będą się one rozwijać i zmieniać w miarę zdobywania doświadczeń, a także w miarę postępu badań naukowych oraz praktyki organów administracji. Należy zaznaczyć w tym miejscu, że na ten moment w literaturze i praktyce terminologia przedmiotu jest zróżnicowana. Tak np. centra innowacji definiuje się czasami jako instytucję organizacyjno-prawną pozwalającą podmiotom FinTech kontaktować się z organem nadzoru w celu zadawania pytań, wyjaśniania wątpliwości i uzyskiwania niewiążących wskazówek (Parenti, 2020, s. 9). Tą ścieżką podąża praktyka KNF. Tymczasem nazewnictwo i praktyka FCA jest już inna. Niniejsze opracowanie proponuje uogólnione ujęcie tematu, bazujące na podejściu brytyjskim, bez wnikania w kwe-

mission presents new European Innovation Agenda to spearhead the new innovation wave, 5 lipca 2022; https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4273 (dostęp 10.09.2024 r.).

7 W literaturze pojawiła się też nazwa „regulacyjne środowisko testowe" zaproponowana przez K. Marchewkę-Bartkowiak (2019, s. 61–75).

stie bardzo szczegółowe, dzięki czemu ustalenia mogą pozostać aktualne mimo postępujących zmian.

2. Centrum innowacji (*innovation hub*) – najogólniejsze ramy

W celu stworzenia warunków dla rozwoju innowacji w środowisku silnie regulowanym organy administracji przyjmują pewną politykę publiczną w tym obszarze[8]. Najbardziej ogólną ramą dla prowadzenia polityki publicznej najczęściej jest instytucja organizacyjno-prawna, określana jako centrum innowacji (*innovation hub*). Można przyjąć, że jest to administracyjny inkubator innowacji, w ramach którego funkcjonują szczegółowe instytucje organizacyjno-prawne, stanowiące konkretne, wyraźnie zdefiniowane *sui generis* „usługi"[9] dla podmiotów administrowanych prowadzących działalność innowacyjną. I tak np. w obrębie centrum innowacji brytyjskiego FCA funkcjonują następujące instytucje szczegółowe (www.knf.gov.pl): piaskownica regulacyjna, piaskownica cyfrowa, ścieżka innowacyjna. Nie jest to jednak powszechnie przyjmowane rozwiązanie. I tak polska Komisja Nadzoru Finansowego uruchomiła centrum innowacji jako program w rozumieniu zarządzania publicznego. W jego ramach UKNF prowadzi dialog z podmiotami sektora m.in. FinTech, udzielając im stosownych wyjaśnień na zadane zapytania i wspierając tym samym rozwój nowoczesnych technologii na rynku finansowym przy zachowaniu bezpieczeństwa i odpowiedniej ochrony klientów (www.knf.gov.pl). Z kolei organizowana przez KNF piaskownica wirtualna jest w tym przypadku instytucją równoległą. Elementem spajającym w przypadku KNF wydaje się być element organizacyjny, wyodrębniony w strukturze organizacyjnej urzędu Departament Innowacji Finansowych FinTech (DFT). Wydaje się, że ujęcie brytyjskie lepiej odpowiada potrzebom zarządzania, jednak na tym etapie rozwoju polskiego sektora FinTech kwestia ta ma znaczenie drugorzędne. Niemniej jednak artykuł będzie opierał się w dalszym ciągu na systematyce i pojęciach brytyjskich jako wzorcowych.

Należy w tym miejscu podnieść, że, jak się wydaje, anglosaskie systemy prawne dają organom administracji dość dużą elastyczność w prowadzeniu polityki publicznej wobec podmiotów administrowanych w porównaniu z innymi systemami prawnymi[10], do których można zaliczyć także system polskiego prawa administra-

8 Z racji, że – co już wspomniano – podejście to rozwija się najbardziej w krajach anglosaskich, stąd terminologia tam używana jest terminologią zarządzania publicznego. Nie jest ona do końca spójna z pojęciami polskiego prawa administracyjnego. Z tego powodu, w pewnej części opracowania posłużono się terminologią zarządzania publicznego, częściowo zaś pojęciami polskiej nauki prawa administracyjnego, gdyż pełne przyjęcie języka zarządzania publicznego mogłoby uczynić tekst mniej zrozumiałym czy wręcz błędnym w obrębie drugiego paradygmatu.

9 Tego sformułowania używa FCA na stronie internetowej FCA Innovation Hub.

10 Na różnice w zakresie ulg regulacyjnych stosowanych w poszczególnych krajach UE zwraca uwagę R. Parenti (2020, s. 34).

cyjnego. Tytułem przykładu można tylko wskazać, że w Australii organ regulacji rynku finansowego, Australian Securities and Investments Commission (ASIC), może wydawać zwolnienia z obowiązku uzyskania zezwolenia na określoną działalność regulowaną i w praktyce takie zwolnienia wydaje (Bromberg, Godwin & Ramsay, 2017, s. 17). Dlatego też przenoszenie rozwiązań anglosaskich do polskiego systemu prawa administracyjnego może być utrudnione. Rozwiązaniem tego problemu może być jednak wprowadzanie specjalnych instytucji regulacyjnych innowacji rozporządzeniami unijnymi, jak to ma miejsce w przypadku rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/858 z dnia 30 maja 2022 r. w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, a także zmiany rozporządzeń (UE) nr 600/2014 i (UE) nr 909/2014 oraz dyrektywy 2014/65/UE.

W dalszym ciągu opracowania zostaną omówione SIRI według praktyki brytyjskiego FCA, który to organ jest liderem wprowadzania tego rodzaju rozwiązań. Pierwsza piaskownica regulacyjna na świecie została utworzona przez FCA w 2016 r. (Bromberg, Godwin & Ramsay, 2017, s. 5). Była to instytucja rozwijająca wcześniej uruchomione centrum innowacji, inicjatywę cieszącą się sporym zainteresowaniem podmiotów FinTech, o czym świadczy fakt, że w ciągu pierwszych osiemnastu miesięcy funkcjonowania wpłynęło tam ponad pięćset wniosków i zapytań (*requests*) (Bromberg, Godwin & Ramsay 2017, s. 5; McCarthy, 2023). We wrześniu 2024 r. FCA oferował podmiotom FinTech następujące instytucje, które można usystematyzować, zaczynając od najszerszego zakresu: piaskownicę regulacyjną (*regulatory sandbox*), piaskownicę cyfrową (*digital sandbox*) oraz ścieżki innowacyjne (*innovation pathways*).

Wydaje się, że brytyjskie ukształtowanie SIRI odzwierciedla fazy rozwoju przedsiębiorstwa typu start-up, którymi niewątpliwie są podmioty FinTech, oraz związane z tym fazy rozwoju produktu w ujęciu biznesowym. W poszczególnych fazach rozwoju podmioty takie mają odpowiednie potrzeby i „usługi" oferowane przez FCA odpowiadają na te potrzeby w poszczególnych etapach rozwoju[11]. Tutaj kolejność będzie jednak odwrócona – im wcześniejsza faza rozwoju, tym mniejszy zakres ułatwień będzie potrzebny. I tak omówione niżej ścieżki innowacyjne odpowiadają pierwszemu etapowi rozwoju (tzw. *pre-seed*), piaskownica cyfrowa etapowi drugiemu, zalążkowemu (tzw. *seed*), a piaskownica regulacyjna etapowi trzeciemu, wczesnemu (tzw. *early stage*). Kolejny, czwarty etap, etap wzrostu (*growth stage*), powinien już odbywać się w podstawowych warunkach regulacyjnych.

11 Etapy rozwoju start-upu za: (Basel Area Business & Innovation Agency, b.d.); jest to systematyka często stosowana w ekosystemie start-upów.

3. Piaskownica regulacyjna (*regulatory sandbox*) – ograniczone badanie produktu / usługi na rzeczywistym rynku

Instytucją najbardziej zaawansowaną i skupiającą chyba najwięcej uwagi praktyków oraz teoretyków jest *regulatory sandbox* – w dosłownym tłumaczeniu: piaskownica regulacyjna. Na pierwszy rzut oka wydaje się, że dosłowne tłumaczenie tego pojęcia na język polski nie jest najlepszym rozwiązaniem i może nie przyjąć się w siatce pojęciowej polskiego prawa administracyjnego oraz jego doktryny. Jednakże, mimo pewnych zastrzeżeń co do takiego nazewnictwa, można postawić tezę, że warto przy nim pozostać ze względu na fakt, iż zarówno praktyka, jak i dyskusja teoretyczna w tym obszarze odbywa się głównie w krajach anglosaskich i języku angielskim. Dlatego – za sprawą takiego tłumaczenia pojęcia – można będzie zbudować sprawną komunikację i wymianę wiedzy pomiędzy jurysdykcjami oraz uniknąć ewentualnych nieporozumień.

W literaturze anglojęzycznej prezentowane są różne definicje piaskownicy regulacyjnej. L. Bromberg, A. Godwin, I. Ramsay definiują piaskownice regulacyjne jako instytucje organizacyjno-prawne, w ramach których organ administracji przyznaje podmiotom FinTech zwolnienia z wymogów uzyskiwania określonych zezwoleń oraz przyznaje warunkowe zwolnienia z określonych wymogów regulacyjnych (Bromberg, Godwin & Ramsay 2017, s. 1). Dzięki temu podmioty FinTech mogą testować swoje koncepcje biznesowe bez konieczności zapewnienia zgodności z określonymi regulacjami rynku finansowego (Bromberg, Godwin & Ramsay, 2017, s. 34). Kolejnym założeniem jest to, że podmioty FinTech korzystają z piaskownicy regulacyjnej przez określony czas i po wyjściu piaskownicy, jeśli będą chciały kontynuować swoją działalność, będą musiały ostatecznie spełnić wszystkie wymogi regulacyjne na kolejnym etapie swojego rozwoju (Bromberg, Godwin & Ramsay, 2017, s. 34). W trakcie uczestnictwa w piaskownicy regulacyjnej podmioty FinTech mogą oferować swoje produkty czy usługi w ramach zdefiniowanych granic, którymi, obok czasu, mogą być też maksymalna liczba klientów czy maksymalna ekspozycja finansowa (Bromberg, Godwin & Ramsay, 2017, s. 5). Te oraz inne uwarunkowania zasadniczo są określane przez organy regulacyjne w regulaminie piaskownicy regulacyjnej dla wszystkich uczestników. Mogą też być indywidualizowane dla konkretnego uczestnika – podmiotu FinTech (Bromberg, Godwin & Ramsay, 2017, s. 5). Jak wskazują cytowani Autorzy, piaskownice regulacyjne są zarządzane przez pracowników centrów innowacji (*innovation hubs*), będących jednostkami organizacyjnymi regulatorów (nadzorców) rynku finansowego, którzy to pracownicy pomagają podmiotom FinTech w poruszaniu się w wymogach regulacyjnych (Bromberg, Godwin & Ramsay, 2017, s. 1).

Z kolei R. Parenti pisze, że piaskownice regulacyjne są instytucją organizacyjno-prawną udostępniającą bezpośrednie środowisko testowe dla innowacyjnych produktów, usług lub modeli biznesowych, zgodnie ze szczegółowym planem testo-

wania, który zwykle obejmuje pewien stopień ulgowości regulacyjnej w połączeniu z pewnymi zabezpieczeniami (Parenti, 2020, s. 9).

H. J. Allen, za częścią literatury, definiuje piaskownice regulacyjne jako środowisko, w którym podmioty FinTech mogą przeprowadzać ograniczone testy swoich innowacji na realnych klientach przy mniejszej liczbie wymogów regulacyjnych, mniejszym ryzyku sankcji administracyjnych i stałych wskazówkach ze strony organu regulacyjnego (Allen, 2019, s. 580). Jednocześnie Autorka zaznacza, że to właśnie zaangażowanie organu administracji we „współpracę" z podmiotami FinTech w piaskownicy regulacyjnej różni tę instytucję prawną od innych form ulg i wyjątków (Allen, 2019, s. 580).

P. Faykiss, D. Papp, P. Sajtos, A. Toros wskazują, że piaskownica regulacyjna umożliwia podmiotom FinTech, przez określony czas, dokonanie oceny ich produktu finansowego, modelu biznesowego w środowisku testowym z udziałem realnych klientów i kontrolowanym przez organ regulacyjny, przy jednoczesnym zwolnieniu z pewnych obowiązków regulacyjnych (Faykiss, Papp, Sajtos & Toros, 2018, s. 54).

Z kolei T. Madiega, A. L. Van De Pol, obok wyżej wymienionych elementów, trafnie wskazują *expressis verbis* w swojej definicji fakt, że uczestnictwo w piaskownicy regulacyjnej odbywa się pod nadzorem organu regulacyjnego/nadzorczego (Madiega & van de Pol, 2022, s. 2). Podkreślają również, że jest to narzędzie uczenia się, zarówno podmiotów regulowanych, jak i organów regulujących (Madiega & van de Pol, 2022, s. 2; Marchewka-Bartkowiak, 2019, s. 68). Ten ostatni aspekt zasługuje na podkreślenie, ponieważ obserwacja przez organ administracji rozwoju sytuacji produktu lub usługi w piaskownicy regulacyjnej będącej rzeczywistym rynkiem służy w istocie także rozwojowi kompetencji organu administracji, który dzięki tej obserwacji może gromadzić wiedzę i na jej podstawie opracowywać narzędzia nadzorcze dostosowane do nowych zjawisk na rynku finansowym.

W polskiej literaturze *regulatory sandbox* bywa tłumaczone jako regulacyjne środowisko testowe i jest definiowane jako środowisko specjalnie stworzone przez regulatora publicznego w celu przetestowania w odizolowanym otoczeniu (np. grupie klientów) możliwych skutków wdrożenia nowego rozwiązania technologicznego. Głównym celem zorganizowania tego „eksperymentu" jest weryfikacja założeń nowatorskiego rozwiązania, ale także ocena przez regulatora, czy dana koncepcja wpisuje się w obowiązujący zakres regulacji albo czy wymaga innych rozwiązań, aby mogła zostać wdrożona na szeroką skalę (Marchewka-Bartkowiak, 2019, s. 62). Piaskownice regulacyjne to koncepcja stworzenia wydzielonego, bezpiecznego środowiska, w którym można eksperymentować bez ponoszenia prawnych konsekwencji porażki – przydatna wszędzie tam, gdzie nowe przedsięwzięcia napotykają wysokie bariery wejścia związane głównie z koniecznością posiadania licencji (Szpringer, 2018, s. 88).

Jak widać z powyższego zestawienia, prezentowane definicje są raczej podobne, choć kolejni autorzy skupiają uwagę na różnych aspektach sprawy. Warto zebrać

wszystkie istotne elementy i zaproponować pełne ujęcie definicyjne adekwatne do polskich warunków doktrynalnych i prawnych.

Wydaje się zatem, że można stwierdzić, iż piaskownica regulacyjna to instytucja prawno-organizacyjna zarządzana przez organ publiczny administrujący określonym obszarem, umożliwiająca wprowadzenie podmiotowi na rzeczywisty rynek innowacyjnego produktu lub usługi (komponent realizacyjny) w celu zbadania jego funkcjonowania w realnych warunkach, w sposób określony parametrami ustanowionymi przez organ administracji (czasowymi, liczbą klientów, wartością produktów lub usług itd.), pod obserwacją tego organu administracji, z możliwością zwolnienia podmiotu uczestniczącego przez organ administracji z przestrzegania pewnych regulacji oraz umożliwiająca podmiotowi wprowadzającemu stosunkowo łatwy dostęp do informacji pochodzących od organu administracji, dotyczących regulacji prawnych mogących mieć zastosowanie do tego podmiotu, jego produktów lub usług (komponent informacyjny).

Choć większość definicji w literaturze odwołuje się do kategorii „testów" produktów i usług, wydaje się, że istotę piaskownicy regulacyjnej lepiej oddawałoby definiowanie jej przez możliwość zbadania rzeczywistych skutków produktów lub usług oferowanych na rzeczywistym rynku, aczkolwiek w ograniczony sposób. Wprawdzie zakresy pojęć „test" i „badanie" są zbliżone, to jednak w tym przypadku, w kontekście kontaktu z rzeczywistym rynkiem, wydają się być istotnie różne. Można to zauważyć, patrząc z perspektywy rozwoju produktu/usługi. Testy produktu czy usługi odbywają się od momentu powstania pierwszego prototypu, zakładają różny stopień dopuszczalnych skutków negatywnych oraz różny poziom wyciąganych wniosków, a ponadto nie zawsze będą się odbywać „na rzeczywistych użytkownikach". Tymczasem w piaskownicy regulacyjnej produkty/usługi są testowane już na końcowym etapie ich rozwoju i dojrzałości, a ich wyniki są z dużą uwagą obserwowane i analizowane oraz wykorzystywane w dalszej fazie rozwoju produktu/usługi. Do tego – odbywa się to z udziałem rzeczywistych odbiorców. Istnieją zatem znaczące cechy szczególne, które bardziej odpowiadają pojęciu „badania" funkcjonowania w realnych warunkach. Drugi argument może być wyprowadzony z perspektywy klienta korzystającego z innowacyjnego produktu/usługi. Prawdopodobnie klienci przekazujący swoje pieniądze podmiotom FinTech nie chcieliby być obiektem testów, natomiast mniej niechętnie odnieśliby się do udziału w badaniu produktu/usługi.

W przypadku piaskownicy regulacyjnej FCA w jej aktualnym kształcie, podmiot FinTech może otrzymać dostęp do zestawu narzędzi w celu testowania proponowanych innowacji oraz dostęp do potrzebnych informacji regulacyjnych. Obejmuje to: ograniczone zezwolenie na działanie w administrowanym obszarze, pomoc w identyfikacji istniejących regulacji oraz poradnictwo dotyczące samego podmiotu oraz proponowanej innowacji/modelu biznesowego, edukację w zakresie określenia potencjalnych skutków regulacyjnych proponowanej innowacji/modelu biznesowego, indywidualne wskazówki dotyczące stosowania regulacji w ww. zakresie, możliwość zniesienia lub

zmodyfikowania trudnych do spełnienia obowiązków na potrzeby testów (bez modyfikacji prawa krajowego lub międzynarodowego), zobowiązanie do niepodejmowania działań sankcyjnych – w przypadkach, gdy nie jest możliwe wydanie indywidualnych wskazówek lub zniesienia obowiązków (www.fca.org.uk). Warto w tym miejscu wskazać, że brytyjskie badania empiryczne potwierdzają, iż w praktyce niektórych organów regulacyjnych, w ramach piaskownicy regulacyjnej, zmienia się sposób administrowania na partnersko-kooperacyjny, w szczególności polegający na szczególnego rodzaju „przyjaznym" doradztwie co do wymagań regulacyjnych. W Wlk. Brytanii ustalono, że taki sposób administrowania powoduje: zwiększenie kompetencji podmiotu FinTech poprzez przyjazny proces uczenia się oraz zmniejszanie barier utrudniających zapewnienie zgodności z regulacjami, zwiększenie zaufania pomiędzy organem i podmiotem FinTech, poprawę reputacji organu administracji oraz zwiększenie chęci podmiotu FinTech do współpracy z organem w przyszłości (Fahy, 2022, s. 162 i nast.). Natomiast Autorka przywołanego badania nie stwierdziła zmian w motywacji podmiotu FinTech do zachowań zgodnych z regulacjami (Fahy, 2022, s. 182).

4. Piaskownica cyfrowa (*digital sandbox*) – symulacja rynkowa na wyizolowanych rzeczywistych danych

Piaskownicę cyfrową można zdefiniować jako informatyczne środowisko zainstalowane w infrastrukturze organu administracji i udostępnione podmiotom FinTech, odpowiednio zabezpieczone, symulujące realny rynek na podstawie rzeczywistych danych (zgodnych z RODO), jednakże będące odizolowane od tego rynku, w celu testowania innowacyjnych produktów lub usług. Najistotniejszym elementem odróżniającym piaskownicę wirtualną od regulacyjnej jest zatem brak dostępu podmiotu FinTech do rzeczywistego rynku i rzeczywistych klientów. Same udostępniane dane zaś są jak najbardziej rzeczywiste, co pozwala zwiększyć realizm prowadzonych testów.

Dodatkowo, obok samego środowiska symulacyjnego, organ administracji może zaoferować podmiotom FinTech także komponent informacyjny. W wariancie minimalnego instrumentu informacyjnego dołączanego do piaskownicy cyfrowej organ administracji może udzielać podmiotowi FinTech informacji na temat obowiązujących go regulacji rynku finansowego. Ponadto możliwe jest doradztwo ekspertów z branży oraz dostęp do społeczności FinTech (komponent społecznościowy), co ułatwia eksperymentowanie i skalowanie w celu sprawdzenia słuszności koncepcji innowacji (www.fca.org.uk).

W tym zakresie FCA oferuje, oprócz zbiorów danych oferowanych poprzez interfejsy programowania aplikacji (Application Programme Interfaces [APIs]), także wbudowane i odpowiednio zabezpieczone środowisko rozwojowe pozwalające na skalowane eksperymenty, platformę współpracy w celu ułatwienia komunikacji w ramach ekosystemu FinTech, przestrzeń prezentacyjną w celu umożliwienia uczestni-

kom prezentowania swoich rozwiązań i budowania sieci biznesowych, umożliwiając jednocześnie zainteresowanym podmiotom, w tym organom administracji obserwowanie testów w czasie ich trwania i uzyskiwanie rozpoznania organu administracji (www.fca.org.uk). W tym przypadku FCA stosuje zatem również „instrument społecznościowy", którego celem jest łączenie podmiotów zainteresowanych rozwojem innowacji FinTech.

5. Ścieżki innowacyjne (*innovation pathways*) – ułatwiony dostęp do informacji regulacyjnej

To, co FCA nazywa ścieżkami innowacyjnymi, jest w istocie prostym instrumentem informacyjnym, który polega na zaoferowaniu podmiotom FinTech szeregu sposobów przekazywania informacji zindywidualizowanych i adekwatnych dla proponowanej innowacji (www.fca.org.uk). Informacje mogą dotyczyć regulacji prawnych, sposobu ich stosowania przez organ oraz polityki publicznej organu administracji w administrowanym obszarze. W przypadku tego instrumentu podmiot FinTech nie ma zatem możliwości weryfikowania proponowanych innowacyjnych produktów na rzeczywistym czy symulowanym rynku. Można jednak sądzić, że ze względu na wysoki poziom skomplikowania regulacji rynku finansowego jego wartość dla podmiotów FinTech może być znacząca. Zastosowanie tego instrumentu zapewne znajdzie zastosowanie przede wszystkim na wczesnym etapie rozwoju innowacji, kiedy testowanie czy badanie rzeczywistego rynku nie jest jeszcze potrzebne.

Warte ponownego podkreślenia jest to, że ten instrument informacyjny różni się od standardowych instrumentów informacyjnych m.in. tym, że dostęp do informacji regulacyjnej jest szczególnie ułatwiony i zindywidualizowany dla konkretnej innowacji konkretnego podmiotu FinTech.

W tym zakresie FCA oferuje (www.fca.org.uk): indywidualne rozmowy, informacje zwrotne oraz nieformalne wskazówki dotyczące zastosowania regulacji do proponowanej innowacji, wyjaśnienia dotyczące warunków uzyskania właściwego zezwolenia w przyszłości, oddelegowanie kompetentnego urzędnika w celu pomocy w uzyskaniu właściwego zezwolenia, jeśli podmiot FinTech złoży taki wniosek.

6. Otwarty katalog SIRI

W związku z dynamicznym rozwojem rynku finansowego oraz rozwojem jego cyfryzacji, katalog specjalnych instytucji regulacyjnych innowacji wydaje się być katalogiem otwartym, a same instytucje szczegółowe podatne na zmiany. Można spodziewać się więc pojawienia się nowych instytucji szczegółowych w tym obszarze, tworzonych od zera albo przenoszonych z innych obszarów życia społecznego. Natomiast od innych instytucji szczegółowych należy odróżnić inną terminologię

stosowaną dla opisanych wyżej rozwiązań prawno-organizacyjnych. Czasami bowiem niektóre instytucje są wprowadzane do systemu prawa pod innymi nazwami. Na przykład system pilotażowy wprowadzony rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/858 z dnia 30 maja 2022 r. w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, a także zmiany rozporządzeń (UE) nr 600/2014 i (UE) nr 909/2014 oraz dyrektywy 2014/65/UE w swojej istocie może być uznany za piaskownicę regulacyjną. Z kolei w niektórych dokumentach UE pojawia się termin klauzule eksperymentalne (Rada Unii Europejskiej, 2020), przez które rozumie się przepisy prawne umożliwiające organom administracji odpowiedzialnym za wdrażanie i egzekwowanie norm prawnych korzystanie z pewnego stopnia elastyczności w indywidualnych przypadkach testowania innowacyjnych technologii, produktów, usług lub podejść (Komisja Europejska, 2020). Jednakże ten sam dokument wskazuje, że klauzule eksperymentalne są często podstawą prawną dla piaskownic regulacyjnych i są już stosowane w prawodawstwie UE oraz w systemach prawnych państw członkowskich (Rada Unii Europejskiej, 2020). Dokonując zatem systematyki czy kwalifikacji nowych instrumentów działania organów administracji, należałoby skupić się na ich istocie opisanej wyżej, a nie na nadawanych im nazwach.

7. Specjalne instytucje regulacyjne innowacji w praktyce KNF

Polska Komisja Nadzoru Finansowego również prowadzi politykę publiczną w obszarze innowacji rynku finansowego. Przede wszystkim należy wskazać, że w strategii KNF na lata 2021–2025 wskazano cele strategiczne prowadzące w trzech kierunkach zmian (główne motywy zmian): skuteczniejsze i efektywniejsze wykorzystanie danych, informacji i wiedzy, bardziej proaktywny nadzór, lepsze zarządzanie organizacją.

Cele te zostały osadzone w 4 powiązanych ze sobą perspektywach (głównych obszarach zmian): rynku finansowego, interesariuszy, procesów wewnętrznych, aktywów (Urząd Komisji Nadzoru Finansowego, 2021, s. 6).

Perspektywa procesów wewnętrznych wskazuje, jakich niezbędnych zmian w swoim działaniu zamierza dokonać UKNF, aby dostarczyć wartości rynkowi finansowemu i interesariuszom. W tej perspektywie KNF deklaruje, że uwzględnia współczesne wyzwania wynikające z innowacji i rozwoju technologii (Urząd Komisji Nadzoru Finansowego, 2021, s. 7). Perspektywa interesariuszy z kolei określa wartości, jakie KNF zamierza dostarczyć wybranym grupom swoich interesariuszy, z uwzględnieniem faktu, że cele różnych interesariuszy mogą być rozbieżne. W tej perspektywie KNF deklaruje stworzenie przestrzeni do rozwoju innowacji i stosowania nowych technologii na rynku finansowym (Urząd Komisji Nadzoru Finansowego 2021, s. 7). Kwestia wykorzystania nowych technologii na rynku finansowym zajmuje zatem istotne miejsce w strategii KNF.

Z analizy ogólnie dostępnych dokumentów wynika, że w ramach jej realizacji, a także w ramach realizacji ustawowego zadania powierzonego KNF, tj. wspierania rozwoju innowacyjności rynku finansowego (art. 4 ust. 1 pkt 3a ustawy o nadzorze nad rynkiem finansowym) (Urząd Komisji Nadzoru Finansowego, 2024, s. 178), KNF oferuje podmiotom FinTech dwie instytucje organizacyjno-prawne: innovation hub oraz virtual sanbox[12]. Natomiast godnym podkreślenia jest fakt, że pojęcie piaskownicy regulacyjnej jako „oferty" KNF dla podmiotów FinTech w sprawozdaniu KNF za 2023 r. nie pojawia się. Oznacza to, że KNF nie prowadzi piaskownicy regulacyjnej sensu *stricto*. Z analizy strony internetowej wynika, że prace nad tym instrumentem były prowadzone, jednakże zostały zakończone w III kwartale 2021 r. z rezultatem w postaci deklaracji, że uzyskane wyniki będą stanowiły jeden z elementów, na podstawie których Urząd podejmie decyzję o możliwym do wdrożenia w krajowym porządku prawnym modelu piaskownicy regulacyjnej (www.knf.gov.pl).

Natomiast jeśli chodzi o Innovation Hub prowadzony przez KNF, jest on określany jako program i jest instrumentem czysto informacyjnym. Zatem byłby to odpowiednik ścieżki innowacyjnej realizowanej przez brytyjski FCA. W jego ramach KNF prowadzi dialog z podmiotami sektora FinTech, SupTech oraz RegTech, udzielając im stosownych wyjaśnień na zadane zapytania (www.knf.gov.pl). W ramach tego programu podmiot pytający może uzyskać: wsparcie ze strony UKNF w identyfikacji właściwych przepisów prawa, regulacji i stanowisk nadzorczych mających zastosowanie do danego podmiotu, modelu biznesowego, oferowanego produktu lub usługi finansowej; informacje o zasadach działania nadzoru, trybie uzyskania zezwolenia na prowadzenie określonego rodzaju działalności oraz dokumentach i wytycznych dostępnych na stronie internetowej KNF; określenie wymogów uzyskania zezwolenia Komisji Nadzoru Finansowego na prowadzenie działalności nadzorowanej, z uwzględnieniem skali i sposobu świadczenia usług przedstawionych w modelu biznesowym prowadzenia określonej działalności nadzorowanej; dodatkowe wsparcie merytoryczne od innych niż KNF instytucji wskazanych na stronie internetowej (https://www.fintech.gov.pl) w zakresie uzyskania informacji na temat rządowych programów wspierających, które są kierowane również do podmiotów z sektora innowacji finansowych.

Jak podaje UKNF w swoim sprawozdaniu za rok 2023, do programu Innovation Hub wpłynęło 13 pytań. Pytania dotyczyły m.in. rynku usług płatniczych, sektora bankowego, zagadnień dotyczących kryptoaktywów, crowdfundingu, InsurTech, robodoradztwa oraz rynku kapitałowego (Urząd Komisji Nadzoru Finansowego, 2024, s. 178). Ponadto w 2023 roku KNF wydała interpretacje w trybie art. 11b ustawy o nadzorze nad rynkiem finansowym dotyczące m.in. rynku kapitałowego, kryptowalut oraz usług płatniczych (Urząd Komisji Nadzoru Finansowego, 2024, s. 178). Przepis art. 11b przyznaje podmiotom wykonującym lub zamierzającym wykonywać działalność nadzorowaną przez KNF możliwość wystąpienia o wydanie interpretacji w ich indywidualnej

12 Tymi terminami posługuje się Komisja Nadzoru Finansowego i jej urząd.

sprawie dotyczącej zakresu i sposobu stosowania przepisów regulujących rynek finansowy, jednakże tylko w przypadku, gdy przedmiotem wniosku są wyłącznie produkty i usługi, które mają na celu rozwój innowacyjności rynku finansowego.

Jeżeli chodzi o piaskownicę wirtualną, to Regulamin udziału w testach w środowisku Piaskownicy Wirtualnej UKNF stanowi, że uczestnik jest uprawniony do zainstalowania w środowisku Piaskownicy Wirtualnej testowanego przez siebie oprogramowania oraz wprowadzenia danych testowych oraz prowadzenia testów funkcjonalnych zainstalowanego przez siebie oprogramowania w ramach funkcjonalności i technologii dostępnych w Piaskownicy Wirtualnej, przy czym zakazany jest szereg aktywności, jak np. prowadzenie testów bezpieczeństwa czy prowadzenie testów wydajnościowych (Urząd Komisji Nadzoru Finansowego, 2020).

W zasobach wirtualnej piaskownicy w pierwszym rzędzie KNF udostępnił środowisko symulujące transakcje bankowe w celu umożliwienia rozwoju innowacji w ramach tzw. otwartej bankowości. Z kolei ze sprawozdania KNF za rok 2023 wynika, że tego roku KNF udostępnił środowisko testowe SandboxDLT, tzw. „piaskownicę blockchainową", która została uruchomiona we współpracy z Krajowym Depozytem Papierów Wartościowych (Urząd Komisji Nadzoru Finansowego, 2024, s. 178). Ponadto, w 2023 r. UKNF uruchomiła programistyczny interfejs aplikacji BOZON API, agregującej dostępne publicznie informacje zamieszczone przez zagraniczne organy nadzoru na temat podmiotów funkcjonujących z wykorzystaniem Internetu, które publikują informacje w języku polskim lub podają dane kontaktowe charakterystyczne dla obszaru Rzeczypospolitej Polskiej (Urząd Komisji Nadzoru Finansowego, 2024, s. 178). Wydaje się zatem, że ta instytucja SIRI ma przed sobą jeszcze dużą przestrzeń do rozwoju.

Niezależnie od powyższego KNF prowadzi również innego rodzaju działania mające na celu wspieranie innowacji na rynku finansowym, jak np. badania opinii uczestników rynku dotyczące FinTech[13], hackatony, upublicznianie informacji na stronie poświęconej FinTech (https://fintech.gov.pl/), działania edukacyjne dla konsumentów FinTech oraz konferencje naukowe.

13 Np. badanie, jakie przeszkody identyfikują uczestnicy rynku w zakresie rozwoju FinTech; UKNF, Zespół Roboczy ds. Rozwoju Innowacji Finansowych (FinTech) – omówienie propozycji zgłoszonych barier, prezentacja, 25.02.2020 r.; uczestnikami zespołu byli zarówno przedstawiciele sektora publicznego, jak i organizacji branżowych oraz podmiotów bezpośrednio uczestniczących w rynku finansowym; https://www.knf.gov.pl/knf/pl/komponenty/img/Prezentacja_Zespol_roboczy_ds_FinTech_propozycje_barier_69013.pdf.

BIBLIOGRAFIA

Allen, H. J. (2019). Regulatory Sandboxes, *The George Washington Law Review*, *87*(3), 579–645.

Basel Area Business & Innovation Agency. *The 6 stages of a startup (and how to master each)*, https://baselarea.swiss/knowledge-hub/6-startup-stages/ (dostęp: 10.09.2024 r.).

Będkowski-Kozioł, M. (2022). Piaskownice regulacyjne w energetyce – kilka uwag w odniesieniu do projektowanych rozwiązań prawnych, *Energetyka rozproszona*, (7), 19–27.

Bromberg, L., Godwin, A. & Ramsay, I. (2017). Fintech sandboxes: Achieving a balance between regulation and innovation, *Journal of Banking and Finance Law and Practice*, *28*(4), 314–336.

Brown, E. & Piroska, D. (2021). Governing Fintech and Fintech as Governance: The Regulatory Sandbox, Riskwashing, and Disruptive Social Classification. *New Political Economy*, *27*(1), 19–32.

Brunner, G., Hinz, R. & Rocha, R. (2008). Risk-Based Supervision of Pension Funds: A Review of International Experience and Preliminary Assessment of the First Outcomes, *The World Bank Policy Research Working Paper*, nr 4491.

Fahy, L. A. (2022). Fostering regulator-innovator collaboration at the frontline: A case study of the UK's regulatory sandbox for fintech, *Law & Policy*, *44*(2), 162–184.

Fal, K. (2022). Instytucja piaskownic regulacyjnych jako instrument wspierający innowacyjność gospodarek, *Przegląd Ustawodawstwa Gospodarczego*, nr 10, 36–45.

Faykiss, P., Papp, D., Sajtos P. & Toros, A. (2018). Regulatory Tools to Encourage FinTech Innovations: The Innovation Hub and Regulatory Sandbox in International Practice, *Financial and Economic Review*, *17*(2), 43–67.

Fedorowicz, M. & Zalcewicz, A. (2024). Challenges Posed to the EU Financial Market by the Implementation of the Concept of Sustainable Financing, *Białostockie Studia Prawnicze*, *29*(1), 47–59.

Hrabčák, L. & Štrkolec, M. (2024). EU Regulation of the Crypto-Assets Market, *Białostockie Studia Prawnicze*, *29*(1), 27–45.

Jurkowska-Zajdler,A. & Schweigl, J. (2024). Towards the Greening of Banking: A Comparison of the Polish and Czech Financial Markets, *Białostockie Studia Prawnicze*, *29*(1), 205–218.

Koleśnik, J. (2017). Piaskownica regulacyjna jako akcelerator innowacyjności w polskim systemie bankowym. *Prace naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Problemy ekonomii, polityki publicznej i finansów publicznych,* nr 475, 90–99.

Komisja Europejska. (2020). European Commission, TOOL #21. Research & Innovation, Better Regulation Toolbox; European Commission; 6783/20 (COM (2020)103).

Madiega, T. & van de Pol, A. L. (2022). Artificial intelligence act and regulatory sandboxes, Parlament Europejski.

Marchewka-Bartkowiak, K. (2019). Regulacyjne środowisko testowe (regulatory sandbox) – doświadczenia i perspektywy, *Studia BAS*, nr 1, 61–75.

McCarthy, J. (2023). From childish things: the evolving sandbox approach in the EU's regulation of financial technology, *Law, Innovation and Technology*, *15*(1), 1–24.

Nadolska A. (2011). Model nadzoru opartego na ocenie ryzyka na przykładzie doświadczeń Financial Services Authority w ramach struktury ARROW, *Monitor Prawa Bankowego*, nr 6, 51–62.

Parenti, R. (2020). Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies Directorate, General for Internal Policies.

Rada Unii Europejskiej. (2020). Council Conclusions on Regulatory sandboxes and Experimentation Clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age, 23.12.2020 (2020/C 447/01).

Parlament Europejski i Rada Europejska. (2024, 13 czerwca). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji); Dziennik Urzędowy Unii Europejskiej 2024/1689.

Sejm Rzeczypospolitej Polskiej. (2009). Ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j. Dz.U. z 2024 r. poz. 135 ze zm.).

Simons & Simons. (2023). Informacja prasowa The EU pharmaceutical package: The regulatory sandbox, 22 maja 2023; www.simmons-simmons.com/en/publications/clhyv2edp000cuvpkmf66sbru/the-eu-pharmaceutical-package-the-regulatory-sandbox.

Szpringer, W. (2018). *Nowe technologie a sektor finansowy. Fintech jako szansa i zagrożenie*, Poltext.

Urząd Komisji Nadzoru Finansowego. (2020). Regulamin udziału w testach w środowisku Piaskownicy Wirtualnej Urzędu Komisji Nadzoru Finansowego.

Urząd Komisji Nadzoru Finansowego. (2021). Strategia Urzędu Komisji Nadzoru Finansowego na lata 2021–2025.

Urząd Komisji Nadzoru Finansowego. (2024). Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w roku 2023.

www.fca.org.uk

www.knf.gov.pl

Wyderka, K. (2023). Piaskownica regulacyjna jako instrument wspierania innowacji w zakresie sztucznej inteligencji, *Prawo Mediów Elektronicznych*, nr 2, 4–13.

Zetzsche, D. A., Buckley, R. P., Barberis, J. & Arner, D.W. (2017). Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation, *Fordham Journal of Corporate & Financial Law*, *23*(1), 31–103.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.14

Received: 31.12.2024
Accepted: 14.04.2025

Krystian Bartnik
University of Warsaw, Poland
bartnik.krystian94@gmail.com
ORCID ID: https://orcid.org/0009-0004-3602-3981

Can a National Financial Supervisor Support the Development of the Fintech Sector? Innovation Hubs as a Tool for Supporting Innovation: The Examples of Poland, Estonia, and Italy

Abstract: This article aims to examine one of the primary tools utilized by national financial supervisors to support innovative projects in the fintech sector. The analysis focuses primarily on the Innovation Hub established by the Polish Financial Supervision Authority (KNF), with additional insights provided from similar initiatives in two other European countries, Estonia (Finantsinspektsioon) and Italy (Bank of Italy). The article is further enriched by examples from other European Economic Area supervisors. The study seeks to address the question of whether national financial supervisors can effectively support innovative projects through instruments such as innovation hubs.

Keywords: innovation hubs, fintech, innovative projects, facilitators, national financial supervisors, KNF, Finantsinspektsioon, Bank of Italy

Introduction

The events of recent years, such as the COVID-19 pandemic and the aggression of the Russian Federation against Ukraine, have profoundly impacted various aspects of our lives. These events have reshaped societies on multiple levels, prompting critical reflection on their consequences. A pertinent question arises: can such 'black swan' events only generate negative outcomes, or might they also have a positive impact?[1] The

1 The term 'black swan' was introduced by Nassim Nicholas Taleb in his book *The black swan: The impact of the highly improbable*, and refers to a rare, unpredictable event that has a profound impact on reality.

© 2025 Krystian Bartnik published by Sciendo. This work is licensed under the Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 License.

answer to this question, as can be expected, depends on the perspective from which the issue is analysed.

In recent years, the concept of the 'global village', introduced by Marshall McLuhan in his 1962 work *The Gutenberg galaxy: The making of typographic man*, has become increasingly relevant. Its principles are materializing in real time, highlighting how interconnected the world has become; it could even be argued that, as an information society, we have transcended this concept. The fast and worldwide spread of new technologies is a clear example of this trend (Jutt, 2023). For example, the COVID-19 pandemic compelled many individuals who had previously relied on traditional payment methods to adopt cashless alternatives (Korzeniowska et al., 2023, p. 76). Clear changes in consumer preferences for cashless payment methods had already become apparent by 2019 (Meler & Polasik, 2022).[2] This acceleration is also evident in the wide array of technological advancements within the banking and financial sectors. Highly efficient mobile applications, customer identification and verification methods utilizing behavioural analytics, intelligent chatbots, and numerous other innovations are gradually becoming integral components of contemporary banking practices (Nowakowski, 2020, p. 23). In recent years, the fintech sector has experienced a growing adoption of disruptive technologies such as Artificial Intelligence (AI), data analytics, the Internet of Things (IoT), and distributed ledger technology (DLT), including blockchain. These innovative advancements have profoundly reshaped the execution of business processes and transactions within the financial services industry (Nguyen Thanh, 2024, p. 2). A significant step in the European Union was the passing of Directive 2015/2366 on Payment Services in the Internal Market by the European Parliament and the Council of the European Union (PSD2), which formally introduced the concept of open banking.[3] This initiative enabled third-party entities to develop applications utilizing data and services made available by financial institutions.[4]

These events have played a crucial role in driving the expansion of fintech initiatives in recent years. According to the 2023 report *How to do fintech in Poland?*, the number of fintech start-ups in Poland grew from 167 in 2018 to 299 in 2022 (Future Finance Poland / FinTech Poland, 2023). Fintech projects operate within the domain of

2 It is worth noting that the initial phase of the pandemic in particular caused a significant surge in demand for cash. In Poland, for instance, the amount of cash in circulation at the end of 2020 was 35% higher compared to February 2020. However, the increased demand for cash during the pandemic is primarily attributed to hoarding motives – namely, the storage of monetary value as a means of managing risk and liquidity (Kaźmierczak et al., 2021, pp. 60–61).

3 Under Polish law, the Directive was implemented through the Act of 10 May 2018 Amending the Payment Services Act and Certain Other Acts.

4 The most essential component of the technological layer of open banking is the application programming interface. In the context of open banking, 'open' refers to public access for developers to systems and solutions owned by specific companies (in this case, financial institutions, primarily banks).

sensitive data, making it imperative to ensure that such initiatives do not threaten the stability or security of participants in the financial market. The implementation of innovative fintech projects is also often challenging due to complex legal frameworks, a frequently ambiguous regulatory status, and additional layers of emerging compliance requirements, such as those arising from environmental, social, and governance (ESG) policies, which are steadily gaining importance and impose new obligations on both market participants and supervisors (Fedorowicz & Zalcewicz, 2024, p. 52). Additionally, the fintech market is largely dominated by big players with substantial financial resources, making it tough for smaller companies to break through. Fintech innovation is frequently driven by start-ups or young enterprises that lack both the financial resources and the extensive experience required to effectively compete in this environment. To find a balance between supporting innovation and ensuring financial market stability, supervisors in various countries are implementing a range of tools designed to support and facilitate the launch of innovative projects. Among the most significant programmes aimed at fostering innovation are regulatory sandboxes and innovation hubs.[5] There is also an increasing use of new solutions, such as virtual sandboxes, TechSprints, or acceleration programmes (ESA, 2023).[6]

In this article, several research methods have been used, including the presentation of various concepts with elements of comparative analysis, followed by a synthesis of the shared characteristics and observed differences in the approaches to implementing the innovation hub concept. The study also applies the dogmatic and the descriptive legal methods, which facilitate the analysis of binding legal provisions and their practical application. Building on these findings, the article offers conclusions and potential recommendations, while also exploring whether financial market supervisors can truly play an effective role in supporting fintech companies in the implementation of innovative solutions. The initial section of the article provides a general overview of the fintech sector, highlighting the factors shaping its current state and various forms of innovation support. It then examines different approaches to establishing innovation hubs by European supervisors, using Poland, Estonia, and Italy as case studies. The primary focus of the analysis is the Innovation Hub created by the Polish Financial Supervision Authority (KNF); the study explores the objectives and underlying principles of the programme, as well as the conditions for participation. The main sources of information for this analysis include the rules of the Innovation Hub programme issued by the KNF, content from its official website, reports from European supervisory institutions – primarily the 2023 joint report by the European Supervisory Authorities (ESA) on

5 As of October 2023, there were 41 innovation hubs, with at least one in all 30 EEA countries, and 14 regulatory sandboxes in 12 EEA countries.

6 ESA refers to the European Supervisory Authorities. The document is a joint report prepared by the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority.

the functioning of innovation facilitators, innovation hubs, and regulatory sandboxes – and supplementary academic literature; due to the contemporary nature of the topic, there is limited academic literature directly addressing the concept of innovation hubs. Subsequently, the article discusses the innovation hubs established by the Estonian supervisor (Finantsinspektsioon) and the Italian supervisor (the Bank of Italy). These two examples are explored using a similar framework, with additional references and comparisons to the solutions implemented by the Polish supervisor. The overarching aim is to investigate how concepts such as the Innovation Hub can be adapted to different jurisdictions and to analyse the varied approaches European supervisors take to achieve the shared goal of supporting innovation.

1. Innovation hubs as a tool for supporting fintech

Before diving into the concept of an innovation hub, it is essential to first explain what fintech means. The concept of fintech originates from the combination of two English words: finance, referring to financial services, and technology, referring to information technology (Gimpel et al., 2017, p. 245). The term fintech has been defined in various ways, depending on the specific aspects being emphasized; essentially, it refers to using new technologies in the financial sector (Nowakowski, 2020, p. 17). The European Commission defines the term as 'technologically driven innovations in financial services that can lead to the creation of new business models, applications, processes, and products, potentially exerting a significant impact on financial markets, institutions, and the way financial services are delivered' (European Commission, 2018).

According to the definition provided in the joint ESA report on innovation facilitators, an innovation hub is understood as 'a dedicated point of contact for firms to raise enquiries with NCAs [National Competent Authorities] on FinTech related issues and to seek non-binding guidance on the conformity of innovative financial products, financial services or business models with licensing or registration requirements or regulatory and supervisory expectations' (ESA, 2023). Innovation hubs provide fintech start-ups with a platform to engage in dialogue with supervisors while benefiting from the expertise of industry specialists, who offer valuable insights into innovation in financial services. These hubs share a core goal: enhancing firms' understanding of regulatory frameworks and supervisory expectations, delivering tailored guidance to align business models with regulatory standards, and identifying areas where the regulatory framework may require adjustments (ESA, 2023). In such a rapidly evolving economy, where regulatory demands are steadily increasing – a good example being the areas of sustainable banking (ESG) or anti-money laundering – concepts such as innovation hubs gain particular relevance, serving as a practical tool for both market participants and regulators (Jurkowska-Zeidler & Schweigl, 2024, p. 210).

As already mentioned, the innovation hubs are, next to the regulatory sandboxes, the facilitators most frequently introduced by supervisors (Butor-Keler & Polasik, 2020, p. 623). Ideally, there is synergy and interdependence between the various innovation-support tools offered. For example, an innovation hub can be treated as the first phase of contact with a supervisor, during which a start-up will be informed about the legal regime and other potential regulatory requirements. After this phase, the start-up, fuelled by new knowledge, can more consciously apply to the regulatory sandbox. The following sections of this article will provide more detailed insights into innovation facilitators in Italy, which serve as a perfect example of the synergy mentioned earlier (ESA, 2023).

2. The Innovation Hub of the Polish Financial Supervision Authority

The Polish Innovation Hub was launched on 5 January 2018, as a response by the Polish financial supervisor (KNF) to the growing need for support and dialogue with entities in the fintech sector.[7] The Polish Financial Supervision Authority (UKNF) introduced the Innovation Hub at a time when several similar programmes were already operating within the EEA, with the first such facilitators emerging as early as 2016.[8] The UKNF has made information more accessible by creating a dedicated section on its website for the fintech sector, along with a comprehensive standalone platform. This platform consolidates all relevant information and updates pertaining to the fintech industry, including details about the Innovation Hub (FinTech Komisja Nadzoru Finansowego, n.d.).

According to §2 of the rules of the Innovation Hub programme, the programme is intended to promote the development of innovation within the financial market by enabling the UKNF to conduct outreach activities targeted at entities qualifying for participation. These initiatives are directed toward entities participating in the programme whose activities involve the design, development, or implementation of innovative technological solutions, products, or services in the areas of the financial market (fintech), financial market supervision (suptech), and regulatory processes (regtech) (Urząd Komisji Nadzoru Finansowego, 2018).[9] Entities qualifying for par-

7 The KNF serves as the public administration body supervising the financial market in Poland. In carrying out its responsibilities, it operates through the Office of the Financial Supervision Authority (UKNF). For the purposes of this article, both terms can be understood collectively as the Polish financial market supervisor, as the distinction between them is not significant to the subject matter touched on here.

8 In 2016, eight innovation hubs were established. In the following years, the numbers were as follows: 2017: 3, 2018: 10, 2019: 11, 2020: 1, 2021: 4, 2022: 2.

9 The term regtech should be understood as 'Regulatory Technology […] a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities', whereas suptech is defined as the use 'of innova-

ticipation in the programme include both those intending to commence operations within segments of the financial market regulated by the KNF, and those already under KNF supervision that aim to implement innovative financial products or services utilizing advanced information technology.

Within the framework of the programme, participating entities may receive support from the UKNF in identifying the applicable legal provisions, regulatory requirements, and supervisory positions relevant to their business model, financial products, or services. Additionally, the programme offers guidance on supervisory principles, the procedures for obtaining authorization to carry out specific activities, and access to relevant documents and guidelines available on the official KNF website.

Examining the rules of the Innovation Hub programme further, we discover that eligibility for participation in the programme requires the applicant to demonstrate that the proposed project possesses an innovative character. Furthermore, the applicant must provide a preliminary analysis of the regulatory and legal framework applicable to the project and substantiate a real need for support due to uncertainties regarding the legal classification of the planned initiative (Urząd Komisji Nadzoru Finansowego, 2018). According to the supervisor's official guidelines, an innovative project is defined as one that differs from existing solutions, products, or services available on the Polish market, can be considered innovative, and is expected to positively impact the development of the financial innovation sector (fintech) or regulatory and supervisory technologies (regtech/suptech) (FinTech Komisja Nadzoru Finansowego, n.d.). However, these guidelines remain open to considerable interpretation due to the use of vague terminology. For instance, the requirement to 'differ from existing solutions' does not specify the degree of differentiation required. Similarly, the criterion that the project 'can be considered innovative' lacks clarity regarding the evaluating group – whether it refers to domain specialists or the general public. Lastly, the notion of 'positive impact' is inherently subjective, as its assessment is likely to vary based on the perspective of the evaluator. The lack of clear guidelines on how this term is understood by the supervisor poses an interpretative challenge.

It is worth mentioning that the aforementioned lack of an official position by the UKNF regarding the interpretation of the innovation criterion outlined in Article 11b(2) of the Financial Market Supervision Act has been identified as a significant barrier to the development of fintech innovation in Poland. To date, the KNF has not issued an official clarification of this concept (FinTech Komisja Nadzoru Finansowego, 2021). It is important to highlight that Article 11b establishes the framework for the institution of an 'interpretation of the KNF in an individual case', which operates under a distinct legal basis compared to the Innovation Hub. This concept of an 'interpretation of the KNF in an individual case' was introduced during the process of implement-

tive technology to support supervision' and to enable supervisory authorities 'to digitise reporting and regulatory processes' (European Commission, 2020, p. 13).

ing the PSD2 Directive into the national legal framework (Schulz, 2024). Within the scope of the Innovation Hub, participants have the option to apply for an individual interpretation issued by the KNF. To initiate this process, applicants must pay a fee of PLN 1,000, submit the necessary identification details, and provide specific questions regarding the interpretation of applicable legal provisions or the procedure for obtaining authorization to engage in a given activity (Sejm of Poland, 2006). In summary, participation in the Innovation Hub programme is free of charge; however, submitting a request for an individual interpretation requires the payment of a fee.

The primary distinction between enquiries made under the Innovation Hub and those submitted as applications for an individual interpretation lies in their legal effect. Responses and guidance provided through the Innovation Hub are advisory in nature and non-binding (Nowakowski, 2020, pp. 21–22). The primary benefit of obtaining an individual interpretation from the UKNF lies in its legal enforceability. Compliance with such an interpretation ensures that the UKNF cannot undertake supervisory actions against the entity, including the imposition of administrative sanctions. However, it should be emphasized that these interpretations are not binding on third parties or applicable to analogous cases (Synowiec, 2021). It is noteworthy that the scope of enquiries directed to the Innovation Hub typically differs from those posed in requests for an individual interpretation. Questions under the Innovation Hub are often broader and less specific, reflecting the exploratory nature of the programme's advisory role. By contrast, individual binding interpretations address more precise legal ambiguities.

3. The Innovation Hub of the Estonian Finantsinspektsioon

Estonia is widely recognized for its advanced digital infrastructure and commitment to innovation in public administration, which also extends to the financial sector. Its proactive regulatory approach has been highlighted as a model for how early-stage supervisory engagement can facilitate innovation while preserving financial stability and legal certainty (The Fintech Times, 2023). The Innovation Hub was established by the Estonian financial supervisor (Finantsinspektsioon) on 17 June 2021, making it a relatively recent initiative. According to a report on its operation, the creation of the Estonian Innovation Hub was directly linked to amendments in the Financial Supervision Authority Act, which assigned the Finantsinspektsioon the responsibility to foster the development of financial technology within the scope of its mandate and strategic objectives (Finantsinspektsioon, 2022b).

The Estonian financial supervisor has allocated a dedicated sub-section on its official website to fintech-related topics, a practice that aligns with the standard approach adopted by other European regulators. However, the Polish supervisor's approach, comparatively, appears more comprehensive, as it has not only created

dedicated subpages but has also developed a separate website specifically devoted to the fintech sector. According to information provided by the Finantsinspektsioon on its website, the following entities are eligible to apply for participation in the Innovation Hub: financial technology (fintech) companies; current or prospective supervised entities planning to integrate innovative solutions into their operations; companies offering support solutions for financial sector services, even if they do not directly provide financial services; and companies developing innovative supervisory technologies (Finantsinspektsioon, 2022a).

The approach adopted by the Estonian financial supervisor demonstrates a notably broad scope, encompassing entities that neither currently provide nor intend to provide financial services directly but instead focus on delivering solutions to support the financial sector. This inclusive framework contrasts with the practices of many European supervisors, who typically allocate such entities to alternative communication channels rather than granting access to an Innovation Hub programme. Similarly, the guidelines of the KNF do not explicitly address the eligibility of entities that exclusively offer tools and support solutions for the financial sector without engaging in the direct provision of financial services. This distinction underscores a more restrictive interpretation of eligibility criteria within the KNF framework, compared to the Finantsinspektsioon's expansive approach.

To participate in the Innovation Hub operated by the Finantsinspektsioon, applicants must satisfy several conditions. First, the proposed product, service, or risk-control solution must possess an innovative character; this may involve the use of innovative technologies or the novel application of existing technologies. Second, the solution must demonstrate added value by showing a potential to benefit customers or society, or by improving the efficiency of financial intermediaries' operational processes, while maintaining or exceeding the existing standards of risk control. Furthermore, the proposed solution must have sector relevance, meaning it should be classified within the financial sector or have significant applicability to companies operating in that sector. An additional requirement is a clear geographical connection, as the initiative must have a direct link to Estonia. Finally, the applicants and their management teams must be trustworthy, maintaining a clean record and upholding the integrity of the financial sector (Finantsinspektsioon, 2022a).

The Estonian model adopts a holistic approach to fostering innovation, involving not only current or prospective providers of financial services but also entities that develop solutions supporting the financial market without directly offering or intending to offer financial services. However, the Estonian approach stipulates that solutions must demonstrate added value for customers or society or enhance the efficiency of operational processes in the financial sector, all while maintaining existing levels of risk control. Furthermore, the requirement for a direct connection to Estonia may restrict the potential pool of participants in the Innovation Hub programme.

Further analysing the provisions, the Estonian criteria, unlike the Polish framework, do not mandate the submission of a legal analysis or justification for support due to regulatory uncertainties. However, the Estonian supervisor's view of innovation includes the idea that a project might not align with the current legal framework, suggesting that a regulatory analysis may be advisable and helpful. In terms of the entity's credibility, while the KNF does not explicitly include this aspect as a core requirement, its regulations (§ 2(3)) exclude entities listed on the Financial Supervision Authority's List of Public Warnings or equivalent foreign supervisory databases (e.g. BOZON) (Urząd Komisji Nadzoru Finansowego, 2018). Such exclusions align with common supervisory practices to safeguard the integrity of innovation initiatives.

What is still worth noting is the broader description of the concept of innovation used by the Estonian supervisor. A product is considered innovative if it meets one or more specific criteria. One possibility is that few or no similar products, services, or risk-control solutions exist, based on publicly available information. Another criterion is that the product is substantially more innovative, or employs a higher degree of innovation compared to existing solutions. Finally, a product can also be considered innovative if the current legal framework does not clearly define the regulations applicable to the given product, service, or solution. Although in this case the concept of innovation is defined somewhat more broadly than by the Polish supervisor, it seems reasonable to assert that this definition remains insufficiently developed. A set of examples would be desirable to provide clearer guidance on how the supervisor interprets this term. Similar to the Polish supervisor, the Finantsinspektsioon emphasizes that interpretations provided under the Innovation Hub programme are not legally binding.

4. The Innovation Hub of the Bank of Italy

The Italian approach to innovation hubs presents a distinctive model. The Bank of Italy, one of the primary supervisors of the Italian financial market, has established two innovation hubs: the Fintech Channel in 2017 and the Milano Hub in 2021.[10] This institutional commitment is part of a broader national effort to accelerate the digital transformation of the banking sector, to which the Bank of Italy has contributed by encouraging innovation and supporting the fintech ecosystem (Arnaudo et al., 2022, p. 5).

The Fintech Channel, one of the earliest innovation hubs in the EEA, serves as a direct and informal communication point with the Bank of Italy. Its primary function is to address queries related to the legal qualification of specific projects or licensing procedures. Four years later, the Milano Hub was introduced to further enhance the dialogue between the supervisor and market participants. Unlike the Fintech Chan-

10 The ESA lists a total of three innovation hubs in Italy; however, the third one pertains exclusively to insurtech. Moreover, it exhibits characteristics that are more similar to a regulatory sandbox, and it is therefore excluded from this study.

nel, the Milano Hub operates through calls for proposals, inviting market participants to submit innovative project ideas on specific topics within banking, finance, or insurance innovation.[11] This layered approach reflects a wider trend in the Italian regulatory environment, which increasingly recognizes the strategic importance of structured innovation support in ensuring financial stability and regulatory responsiveness (Gugliotta, 2021, pp. 23–24).

Both the innovation hubs established by the Bank of Italy are featured on the official website of the institution, each with a dedicated section. The Fintech Channel offers a straightforward and accessible platform for submitting enquiries via an official form. This tool is open to a broad range of stakeholders, including start-ups, companies, and banking or financial intermediaries proposing innovative solutions in financial and payment services. The availability is not restricted to entities currently offering or intending to offer financial services, thereby embracing a diverse audience. In this case the Bank of Italy's approach aligns closely with that of the Estonian supervisory authority. In alignment with practices seen in Poland and Estonia, the Bank of Italy explicitly states that the information provided through the Fintech Channel is non-binding. However, the Italian supervisor extends this principle further, disclaiming responsibility for unanswered enquiries and clarifying that a lack of response should not be interpreted as tacit approval or agreement with the applicant's interpretation or proposal (Bank of Italy, n.d.a).

The Milano Hub operates on a more structured framework, issuing the aforementioned periodic calls for proposals as open invitations to market participants. Applicants must meet both the general requirements outlined in the rules of the Innovation Hub programme and the specific conditions of each call. While the calls are broadly accessible, their thematic focus inherently narrows the pool of eligible participants by targeting specific areas of innovation (Bank of Italy, n.d.b)[12]. For instance, in the third call for proposals, eligibility extends to individuals and organizations across several categories; in the fintech area, it includes individuals and non-bank or non-financial entities proposing innovative projects. In the innovation area, it encompasses banking, financial, and insurance intermediaries. Finally, in the research and development area, the call is open to universities, research institutes, industry associations, and other relevant entities.

The sole requirement for participation is registration in the relevant registry – either the Italian Register of Companies or its equivalent in the applicant's home

11 To better understand how a call for proposals works, it is helpful to refer to the definition of a 'request for proposal': a business document that announces a project, describes it, and solicits bids from qualified contractors to complete it.

12 This was developed based on the official brochure issued by the Bank of Italy, *The innovation facilitators of the Bank of Italy*, which outlines various forms of innovation support provided by the Italian supervisor, including the Milano Hub.

country for foreign entities (Bank of Italy, 2024a). In addition to the general conditions outlined earlier, the thematic focus of each call plays a pivotal role. For example, the third call for proposals centres on the topic of digital payments, aiming to support projects and ideas that advance the most innovative aspects of instant and digital payment systems (Bank of Italy, 2024b). In this case, the Italian supervisor uses several vague expressions, such as 'innovative' or 'the most efficient', which, as observed with the Polish and Estonian supervisors, often lead to interpretative challenges. Generally, the excessive use of imprecise terms (including general clauses) in the formulation of concepts and definitions within legal language can significantly hinder the practical applicability of such regulations (Gizbert-Studnicki, 2020, pp. 27–28). Despite the use of these vague terms, it is noteworthy that the thematic scope of each call for proposals is described in detail, including a list of potential technologies. Additionally, each call for proposals includes a dedicated section within its provisions that outlines the specific evaluation criteria for submitted projects. This regulatory approach appears to be a best practice that other supervisory authorities should consider adopting. Such a framework fosters a sense of fair competition among participants and provides clear guidelines for the evaluation committee, potentially resulting in fewer complaints related to project rejections.[13] Similar to the Estonian supervisor, the Bank of Italy explicitly excludes from the programme projects involving individuals who have been convicted of crimes or who are under investigation.

A remarkable feature of the Milano Hub is the dedicated support provided to qualified projects. Each selected initiative is assigned an overseer responsible for setting meeting schedules and defining the objectives to be achieved. Additionally, the entity benefits from the expertise of a team of Bank of Italy professionals, offering technical guidance in banking, finance, and other specialized sectors. Participants may also request detailed analyses of the regulatory framework and its underlying sources, as interpreted by the Bank of Italy. As can be read in the FAQs of the Milano Hub, such support typically lasts around six months (Bank of Italy, n.d.b). Moreover, representatives of selected projects are invited to participate in seminars and networking events, fostering collaboration with other participants and stakeholders from the banking and financial sectors. Italy's approach to supporting innovation is both thoughtful and comprehensive. Together with the Fintech Channel and the regulatory sandbox, the Milano Hub contributes to a cohesive framework designed to effectively support innovation in the financial sector.

13 For each call for proposals, instructional videos are also prepared, reflecting the Italian supervisor's inclusive approach to the concept of an innovation hub.

Conclusions

Innovation hubs, alongside regulatory sandboxes, are among the most frequently utilized tools for fostering innovation employed by European supervisory authorities. An analysis of various European innovation hubs reveals several common features, or at least a noticeable trend toward implementing the concept of the innovation hub in a particular form. One such feature is the establishment of dedicated contact points for fintech projects or broadly defined innovation-related initiatives. Some regulators set up a single contact point solely for enquiries related to specific projects, while others provide a general contact for all matters concerning innovation. Another common element is the development of FAQs, which are often updated based on the supervisory authority's accumulated experience. In addition to static resources, some authorities introduce chatbots, which serve as simplified and more user-friendly interfaces for accessing FAQ content. Supervisory authorities are also increasingly organizing meetings and sessions, thereby going beyond formal interactions via written forms and offering opportunities for direct engagement. In some programmes, entities approved for support are assigned dedicated project mentors from the supervisory authority to guide them through the entire process. Finally, innovation hubs often provide regulatory and market-entry support. This includes assistance in analysing the regulatory environment and understanding the conditions necessary for entering the market, particularly in highly regulated sectors such as financial services. Such support typically extends to the licensing process and fulfilling the requirements needed to obtain necessary authorizations.

The concept of the innovation hub is relatively new but has reached a certain level of maturity. A classic example of a well-structured and widely emulated model is the Innovation Hub established in 2014 by the Financial Conduct Authority, the financial supervisor in the UK. However, this article does not aim to focus on this well-documented benchmark, but rather to shed light on other European approaches to creating innovation hubs, including those in smaller economies such as Estonia, or culturally and geopolitically distinct economies such as Poland or Italy.

A comparative analysis of the three innovation hubs, supplemented by observations of others, highlights a significant challenge: the ambiguity of the criteria for qualifying entities for innovation hub programmes. This lack of clarity manifests in the use of vague terminology or overly general and concise guidelines. However, such ambiguities only become a problem when the programme itself is sufficiently developed. Unfortunately, many innovation hubs remain limited to a simple form for posing questions to supervisors, or worse, merely an email address for enquiries.

In today's dynamic world, neither regulators nor legislators can fully keep pace with the rapidly evolving landscape, whether in adapting legal frameworks or supervisory practices. Therefore concepts like the innovation hub are invaluable for businesses and regulatory bodies – and perhaps even for legislators in the longer term. Instru-

ments such as innovation hubs serve a dual purpose: they provide crucial support to young entities that require the guidance of more experienced partners and advisors, while simultaneously enabling regulators to familiarize themselves with novel solutions, potentially preparing them to oversee these innovations in the near future. This two-way learning process becomes even more critical in the face of rapidly expanding regulatory frameworks, such as those related to ESG, which impose increasingly complex and far-reaching obligations not only on market participants but also on supervisory authorities. The implementation of such requirements demands not only formal compliance mechanisms but also systemic adaptation within both financial institutions and supervisory structures (Fedorowicz & Zalcewicz, 2024, pp. 54–55). In this regard, innovation hubs can serve as a strategic platform for preparing both sides of the market for such emerging challenges, ensuring that supervision evolves in parallel with innovation.

One could hypothesize that in an ideal world, regulators would stay at least one step ahead of the business sector; this broader perspective would enable them to ensure market stability – in this case, financial market stability. However, practice and observation suggest otherwise, underscoring the critical importance of dialogue between regulators (and legislators) and businesses. Effective regulation in the digital age cannot be achieved in isolation: it requires structured, continuous, and meaningful collaboration between public authorities and the private sector. Such cooperation should go beyond formal procedures and include genuine consultation mechanisms, working groups, and pilot projects that allow for the joint development of pragmatic and innovation-friendly solutions. In this context, it is important to emphasize the significant role of open application programming interfaces (APIs), which can greatly facilitate the work of both supervised entities and supervisors. APIs enable standardized, secure, and efficient data exchange, which is crucial in the increasingly complex financial ecosystem. By automating the flow of information, they reduce reporting burdens, enhance transparency, and allow for real-time oversight, making supervisory activities more dynamic and responsive. Moreover, APIs foster interoperability between various systems and institutions, enabling better integration of new technologies into existing regulatory frameworks. The trend toward an expanded adoption of APIs seems inexorable, especially when considering the escalating volume of data and the increasing complexity of reporting requirements (Nowakowski, 2020, p. 280). In addition, it is worth noting that innovative tools often aim to enhance supervisory tasks, particularly in the realm of suptech projects. These initiatives leverage technology to strengthen the capabilities of supervisory authorities, increasing their efficiency, precision, and ability to identify emerging risks immediately.

Ultimately, society as a whole stands to benefit from supporting innovative projects. While it is acknowledged that technology and innovation are sometimes used against societal interests, their positive impact on contemporary life remains undeniable. Therefore supporting a cooperative ecosystem – where businesses, regulators,

and lawmakers work together to create conditions conducive to responsible innovation – should be a shared priority.

REFERENCES

Arnaudo, D., Del Prete, S., Demma, C., Manile, M., Orame, A., Pagnini, M., Rossi, C., Rossi, P., & Soggia, G. (2022). *The digital transformation in the Italian banking sector* [Occasional paper no. 682]. Bank of Italy. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4109459

Bank of Italy. (2024a). *Rules to participate in Milano Hub*. https://www.bancaditalia.it/focus/milano-hub/terza-call-for-proposals/Rules_Milano_Hub_3CfP.pdf?language_id=1

Bank of Italy. (2024b). *Third call for proposals – Provisions*. https://www.bancaditalia.it/focus/milano-hub/terza-call-for-proposals/Provisions_Milano_Hub_3CfP.pdf?language_id=1

Bank of Italy. (n.d.a) *Fintech Channel*. Retrieved 14 July 2025, from https://www.bancaditalia.it/focus/fintech/index.html

Bank of Italy. (n.d.b) *Milano Hub*. Retrieved 14 July 2025, from https://www.bancaditalia.it/focus/milano-hub/index.html

Bank of Italy. (n.d.c) *The innovation facilitators of Bank of Italy.* Retrieved 14 July 2025, from https://www.bancaditalia.it/focus/milano-hub/The_innovation_facilitators_of_Bank_of_Italy_ENG.pdf?language_id=1

Butor-Keler, A., & Polasik, M. (2020). The role of regulatory sandboxes in the development of innovations on the financial services market: The case of the United Kingdom. *Economics and Law*, *19*, 621–638.

European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee, and the Committee of the Regions. FinTech action plan: For a more competitive and innovative European financial sector*. https://eur-lex.europa.eu/resource.html?uri=cellar:6793c578–22e6–11e8-ac73–01aa75ed71a1.0001.02/DOC_1&format=PDF

European Commission. (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591

European Supervisory Authorities (ESA) (2023, December 11). *Report. Update on the functioning of innovation facilitators: Innovation hubs and regulatory sandboxes*. https://www.eiopa.europa.eu/publications/joint-esas-report-innovation-facilitators-innovation-hubs-and-regulatory-sandboxes_en

European Parliament and the Council of the European Union. (2015, November 25). Directive 2015/2366 on Payment Services in the Internal Market (O. J. EU L 337, 2015, p. 35, as amended).

Fedorowicz, M., & Zalcewicz, A. (2024). Challenges posed to the EU financial market by the implementation of the concept of sustainable financing. *Bialystok Legal Studies*, *29*(1), 47–59. https://bsp.uwb.edu.pl/article/view/1006/838

Finantsinspektsioon. (2022a, 10 October). *Innovation Hub*. https://www.fi.ee/en/finantsinspektsioon/innovation-hub

Finantsinspektsioon. (2022b). *Finantsinspektsioon Innovation Hub report 2022. Financial supervision in the fintech ecosystem: Observations on the work of the Innovation Hub*. https://www.fi.ee/sites/default/files/2022–09/Innovatsioon_FI_eng_w.pdf

FinTech Komisja Nadzoru Finansowego. (2021, April 28). *Raport z prac Zespołu ds. Rozwoju innowacji finansowych FinTech*. https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_z_prac_Zespolu_ds_rozwoju_innowacji_finansowych_73565.pdf

FinTech Komisja Nadzoru Finansowego. (n.d.). *Homepage / Innovation Hub*. Retrieved 14 July 2025, from https://fintech.gov.pl/innovation-hub

Future Finance Poland / FinTech Poland. (2023). *How to do fintech in Poland? Report 2023*. https://fintech.gov.pl/images/How_to_do_Fintech_2023.pdf

Gimpel, H., Rau, D., & Röglinger, M. (2017). Understanding fintech start-ups: A taxonomy of consumer-oriented service offerings. *Electronic Markets*, *28*, 245–264.

Gizbert-Studnicki, T. (2020). Nieostrość języka prawnego w świetle filozoficznych koncepcji nieostrości. *Studia Iuridica*, *83*, 27–42. https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ceon.element-f3816a27–6717-3c3e-a114–50fa73201a67

Gugliotta, O. R. (2021). The Paris Agreement 5 years later: The challenges of climate finance and multilateral development banks. *Bialystok Legal Studies*, *26*(5), 23–40. https://bsp.uwb.edu.pl/article/view/1156/987

Jurkowska-Zeidler, A., & Schweigl, J. (2024). Towards the greening of banking: A comparison of the Polish and Czech financial markets. *Bialystok Legal Studies*, *29*(1), 205–218. https://bsp.uwb.edu.pl/article/view/1016/848

Jutt, A. (2023, 31 August). *The world is tuning fast into a global village*. https://medium.com/@asgharjuttsst/the-world-is-tuning-fast-into-a-global-village-52b4c3131de8

Kaźmierczak, A., Kotkowski, R., & Maciejewski, R. (2021). Pandemia COVID-19 a popyt na pieniądz gotówkowy i zmiany w zachowaniach płatniczych w Polsce w 2020 r. *Studia i Prace Kolegium Zarządzania i Finansów*, 182(4), 59–76. https://www.researchgate.net/publication/357957942_Pandemia_COVID-19_a_popyt_na_pieniadz_gotowkowy_i_zmiany_w_zachowaniach_platniczych_w_Polsce_w_2020_r

Korzeniowska, A. M., Rutecka-Góra, J., Swacha-Lech, M., & Waliszewski, K. (2023). *Wpływ pandemii COVID-19 na finanse osobiste*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu. https://www.dbc.wroc.pl/dlibra/publication/160295/edition/122054/content

McLuhan, M. (1962). *The Gutenberg galaxy: The making of typographic man*. University of Toronto Press.

Meler, A., & Polasik, M. (2022). *Zwyczaje płatnicze a postrzeganie metod płatności: badanie konsumenckie 2022*. Polska bezgotówkowa & Polasik Research.

Nguyen Thanh, B., Son, H. X., & Vo, D. T. H. (2024). Blockchain: The Economic and Financial Institution for Autonomous AI? *Journal of Risk and Financial Management*, 17(2), 54. https://doi.org/10.3390/jrfm17020054

Nowakowski, M. (2020). *Fintech – technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*. Wolters Kluwer Polska.

Schulz, K. (2024). *Ustawa o nadzorze nad rynkiem finansowym. Komentarz*. Wolters Kluwer Polska.

Sejm of Poland. (2006). Act no. 157 of 21 July 2006 on the Supervision of the Financial Market (consolidated text: Journal of Laws of 2024, item 135).

Synowiec, M. (2021). Indywidualna interpretacja Komisji Nadzoru Finansowego jako środek wykładni przepisów prawa regulujących działalność na rynku finansowym w zakresie innowacyjnym. *Przegląd Prawa Handlowego*, *6*, 38–45.

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable.* Allen Lane.

The Fintech Times. (2023.) *Estonia is the thriving fintech hub of Europe*. https://thefintechtimes.com/estonia-is-the-thriving-fintech-hub-of-europe/

Urząd Komisji Nadzoru Finansowego. (2018). *Regulamin Programu Innovation Hub*. https://www.knf.gov.pl/knf/pl/komponenty/img/Regulamin%20Programu%20Innovation%20Hub.pdf

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 3

DOI: 10.15290/bsp.2025.30.03.15

Received: 10.01.2025
Accepted: 3.07.2025

Piotr Konik
Uniwersytet w Białymstoku, Polska
p.konik@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0001-7766–2887

Umowy o dostarczanie treści cyfrowej lub usługi cyfrowej – uwagi dotyczące charakteru prawnego

Contracts for the Supply of Digital Content or Digital Services: Considerations of Their Legal Nature

Abstract: Chapter 5b of the Consumer Rights Act covers the regulation of contracts for the supply of digital content or a digital service, which is the result of the implementation into the Polish legal order of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on Certain Aspects of Contracts for the Supply of Digital Content and Digital Services. This regulation brings up a number of legal issues, some of which are considered in this study. First and foremost is the question of whether a separate type of contract (in addition to, for example, a sale, exchange or donation contract) has been identified in this way. In view of the conclusion that we are only dealing with a certain class of contracts in this case, the question of what criteria determine inclusion in this category will be analysed, as well as the question of how to distinguish a contract for the supply of digital content from a contract for the supply of digital services. The study also includes a consideration of what type of named or unnamed contracts fall into this category.

Keywords: contracts for the supply of digital content or digital services, digital content, digital services, types of contracts, classes (types) of contracts, named and unnamed contracts
Słowa kluczowe: umowa o dostarczanie treści cyfrowej lub usługi cyfrowej; treści cyfrowe; usługi cyfrowe; typy umów; klasy (rodzaje) umów; umowy nazwane i nienazwane

Wprowadzenie

Nowe technologie w istotny sposób wpływają na obrót prawny, w tym przez rozwój sfery cyfrowej (wirtualnej) oraz specyficznych dóbr stających się przedmiotem świadczeń w stosunkach cywilnoprawnych. Towarzyszy temu wprowadzanie regula-

© 2025 Piotr Konik published by Sciendo. This work is licensed under the Creative Commons Attribution-Non-Commercial-NoDerivatives 4.0 License.

cji prawnych mających za zadanie regulowanie kwestii z tym związanych. Rozdział 5b ustawy o prawach konsumenta (Sejm RP, 2014)[1] obejmuje regulację dotyczącą umów o dostarczanie treści cyfrowej lub usługi cyfrowej, co jest wynikiem implementacji[2] do krajowego (polskiego) porządku prawnego dyrektywy Parlamentu Europejskiego i Rady EU 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Parlament Europejski i Rada EU, 2019)[3]. Rozdział ten obejmuje przepisy dotyczące, przede wszystkim, odpowiedzialności z tytułu niezgodności treści cyfrowej lub usługi cyfrowej z umową (art. 43k–43q u.p.k.), jednak w pierwszej kolejności ustawodawca wyodrębnia kategorię umów, której dotyczy wskazana regulacja. Zabieg ten rodzi kilka doniosłych zagadnień. A mianowicie: Czy dochodzi w ten sposób do wyodrębnienia odrębnego typu umowy? Jeżeli nie, i w rezultacie mamy do czynienia z pewną klasą umów, to co decyduje o zaliczeniu do tej kategorii? Jak odróżnić umowy o dostarczanie treści cyfrowych od umów o dostarczanie usług cyfrowych? Jakie typy umów nazwanych lub nienazwanych mogą się mieścić w tym zbiorze? Zagadnieniom tym zostaną poświęcone rozważania w kolejnych częściach niniejszego opracowania.

Niezależnie od tego istotne jest także dostrzeżenie szerszego tła, a mianowicie, że wyodrębnienie wspomnianej kategorii umów także w oparciu o kryterium podmiotowe (relacja konsument – przedsiębiorca) powoduje automatyczne wyodrębnienie pozostałej sfery stosunków umownych z innymi konfiguracjami podmiotowymi, tj. dwustronnie profesjonalnych czy dwustronnie nieprofesjonalnych oraz związane z nimi pytanie, jak poszczególne kwestie wyglądają w tej sferze. Zagadnienia te wymagają jednak odrębnego opracowania.

1. Umowa o dostarczanie treści cyfrowej lub usługi cyfrowej – czy to odrębny typ umowy?

W pierwszej kolejności należy postawić kwestię, czy wskazana regulacja zawarta w rozdziale 5b ustawy o prawach konsumenta odnosi się do pewnego rodzaju umów wyodrębnianego ze względu na kryterium podmiotowe (umowy z udziałem konsumentów po jednej stronie i przedsiębiorców po drugiej) oraz przedmiotowe (charakter świadczenia i jego przedmiot), czy może jest to regulacja odrębnego typu umowy, w ten sposób (przez wspomnianą regulację) uzyskującego status umowy nazwanej. Ustalenie, że mamy tu do czynienia z odrębnym typem umowy, powodowałoby, że regulacja jego dotycząca byłaby stosowana bez potrzeby poszukiwania i odwoływania się do przepi-

1 Ustawa dalej powoływana jako „u.p.k." bądź „ustawa o prawach konsumenta".

2 Implementacja nastąpiła na mocy ustawy z 4 listopada 2022 r. o zmianie ustawy o prawach konsumenta ustawy – kodeks cywilny orz ustawy – Prawo prywatne międzynarodowe (Sejm RP, 2022), która weszła w życie z dniem 1 stycznia 2023 r.

3 Dyrektywa zwana dalej „Dyrektywą 2019/770".

sów dotyczących innych typów umów, a stosowanie przepisów dotyczących tych innych typów umów byłoby w zasadzie wyłączone, chyba że regulację tę uznalibyśmy za niepełną i wymagającą uzupełnienia przez odwołanie się do przepisów dotyczących innej umowy cechującej się najbliższym podobieństwem. Przyjęcie natomiast, że mamy tu do czynienia z regulacją dotyczącą pewnej klasy (rodzaju) umów wyodrębnionej ze względu na określone cechy, powodowałoby, że otwarta byłaby kwestia kwalifikacji danej umowy dotyczącej danego dobra cyfrowego do określonego typu umowy nazwanej bądź nienazwanej. Wspomniana regulacja służyłaby więc tylko do unormowania określonych kwestii dotyczących pewnego rodzaju umów.

Weryfikacja postawionej kwestii jest doniosła z tego choćby względu, że – jak wskazuje się w doktrynie – sama dyrektywa nie narzuca określonego typu umów o dostarczanie treści cyfrowej lub usługi cyfrowej, pozostawiając tę kwestię ustawodawstwom krajowym (Pecyna, 2021, s. 608)[4]. Nie byłoby więc żadnej przeszkody do tego, żeby polski ustawodawca wprowadził taką regulację. Niezależnie od tego można dodać, że sama stylizacja art. 3 ust. 1 Dyrektywy 2019/770 zdaje się sugerować podążanie w kierunku typologicznego ujęcia.

Przechodząc do istoty zagadnienia, można ogólnie stwierdzić, że kategorię typów umów wyodrębnia się przy uwzględnieniu kryterium treści umowy, a więc biorąc pod uwagę przewidziane w umowie prawa i obowiązki stron oraz ich rozkład i sposób powiązania ze sobą. Uszczegóławiając tę kwestię i uwzględniając spostrzeżenia Z. Radwańskiego na gruncie umów nazwanych, można wskazać, że o wyodrębnieniu typu umowy decyduje sposób ujęcia poszczególnych elementów zobowiązania powstającego z danej umowy, tj. takich elementów, jak podmioty (strony), treść świadczenia, w tym jego przedmiot oraz relacja świadczeń do siebie, jeżeli pojawia się ich więcej w stosunku zobowiązaniowym. W rezultacie jest to pewien wzorzec, w którym wspomniane elementy przybierają swoistą postać, i który spełnia pewną typową funkcję społeczną (Radwański, 1977, s. 210–211)[5]. Przy czym nazwa nadana takiemu wzorcowi jest pomocna, ale nie jest przesądzająca (Radwański, 1977, s. 211–212). Mając to na uwadze, można poczynić następujące spostrzeżenia:

Regulacja rozdziału 5b ustawy o prawach konsumenta dotyczy umów, którym przypisać można typową funkcję, jaką jest zapewnienie obrotu skonkretyzowaną, specyficzną kategorią dóbr, tj. treściami cyfrowymi i usługami cyfrowymi (dalej zbiorczo określanymi także jako „dobra cyfrowe").

Regulacja rozdziału 5b ustawy o prawach konsumenta dotyczy ściśle określonej sfery podmiotowej. Odnosi się ona mianowicie (i wyłącznie) do umów zawieranych przez konsumentów z przedsiębiorcami, na co wskazuje art. 1 u.p.k. Co więcej, cho-

4 Podobnie M. Ostaszewski (2023, s. 117) wskazujący, że na gruncie Dyrektywy 2019/770 mamy do czynienia jedynie z kategorią zbiorczą.

5 Odnośnie typów umów oraz kategorii umów nazwanych i nienazwanych zob. szerzej S. Grzybowski (1976, s. 15–21); A. Brzozowski (2020, s. 500–504).

dzi – jak wynika to choćby z art. 43h–43i u.p.k. – o umowy, w których konsument i przedsiębiorca występują w określonych rolach w stosunku zobowiązaniowym, a mianowicie przedsiębiorca jest stroną zobowiązaną do dostarczenia konsumentowi określonych treści cyfrowych lub usługi cyfrowej. Na podstawie art. 7aa u.p.k. w sposób tożsamy z konsumentem traktowana jest także osoba fizyczna zawierająca umowę bezpośrednio związaną z jej działalnością gospodarczą, gdy z treści tej umowy wynika, że nie ma ona dla tej osoby charakteru zawodowego, wynikającego w szczególności z przedmiotu wykonywanej przez nią działalności gospodarczej, udostępnionego na podstawie przepisów o Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

Treść umowy ma przewidywać obowiązek przedsiębiorcy do określonego świadczenia, które określone zostało przez ustawodawcę jako zachowanie polegające na „dostarczaniu" określonego przedmiotu.

Przedmiot świadczenia jest też ściśle scharakteryzowany jako treść cyfrowa bądź usługa cyfrowa. Przy czym zarówno pojęcie treści cyfrowej, jak i usługi cyfrowej zostało zdefiniowane. Stosownie do art. 2 pkt 5 u.p.k treść cyfrowa to dane wytwarzane i dostarczane w postaci cyfrowej. Natomiast usługa cyfrowa to – zgodnie z art. 2 pkt 5 u.p.k. – usługa pozwalająca konsumentowi na: a) wytwarzanie, przetwarzanie, przechowywanie lub dostęp do danych w postaci cyfrowej; b) wspólne korzystanie z danych w postaci cyfrowej, które zostały przesłane lub wytworzone przez konsumenta lub innych użytkowników tej usługi; c) inne formy interakcji za pomocą danych w postaci cyfrowej.

Kwestia, czy regulacja ta dotyczy całości świadczeń stron i relacji pomiędzy nimi, jest bardziej złożona. W pierwszej kolejności należy dostrzec, że w rozdziale 5b ustawy o prawach konsumenta kwestia ta nie jest wyraźnie uregulowana (Południak-Gierz, 2025, komentarz do art. 43h–43i, Nb 5), odmiennie niż w Dyrektywie 2019/770. W art. 3 ust. 1 Dyrektywy 2019/770 wskazuje się mianowicie, że stosuje się ją do umów, na podstawie których przedsiębiorca dostarcza lub zobowiązuje się dostarczyć konsumentowi treści cyfrowe lub usługę cyfrową, a konsument płaci cenę lub zobowiązuje się do jej zapłaty. Stylizacja tego przepisu jest zaś zbliżona do ujęcia kodeksowego przepisów przedstawiających *essentialia negotii* poszczególnych umów nazwanych, co mogłoby wskazywać, że w Dyrektywie 2019/770 chodzi właśnie o podobne podejście i określenie, że konsument też powinien spełnić na rzecz przedsiębiorcy świadczenie polegające na zapłacie ceny, które to świadczenie ma być odpowiednikiem świadczenia drugiej strony, co wskazywałoby także na wzajemność omawianej kategorii umów. W rezultacie, możliwy byłby wniosek, że nie inaczej powinna być interpretowana regulacja zawarta w ustawie o prawach konsumenta, skoro ma być zgodna z Dyrektywą 2019/770. Wniosek ten nie byłby jednak prawidłowy, na co wyraźnie wskazuje sama Dyrektywa 2019/770, która w motywie 12 *expressis verbis* przesądza, że nie określa ona charakteru prawnego umów o dostarczanie treści cyfrowych lub usługi cyfrowej, pozostawiając prawu krajowemu rozstrzygnięcie kwe-

stii, czy takie umowy stanowią, na przykład, umowę sprzedaży, umowę o świadczenie usługi, umowę najmu lub umowę *sui generis*. Ustawodawca krajowy, nie powielając dokładnie treści art. 3 ust. 1 Dyrektywy 2019/770, tym samym jej nie naruszył, a przy tym przyjął rozwiązanie bardziej klarowne i jednoznaczne, oderwane od uregulowania pełnego rozkładu świadczeń stron. Ściśle rzecz ujmując, regulacja zawarta w ustawie dotyczy tylko jednego, charakterystycznego świadczenia i dobra, które jest jego przedmiotem. Nie mamy tu choćby wzmianki o świadczeniu drugiej strony (a zwłaszcza o cenie, co mogłoby wskazywać na umowę sprzedaży) lub świadczeniach ani też zastrzeżenia, że one nie występują (co mogłoby wskazywać na przykład na umowę nieodpłatną). Niezależnie od tego należy też dostrzec, że samo określenie „dostarczanie", którym posługuje się ustawodawca, zostało ukształtowane zakresowo bardzo szeroko, o czym będzie mowa dalej.

W rezultacie, chociaż ustawodawca dość obszernie reguluje pewną kategorię stosunków zobowiązaniowych, to nie prowadzi to do wyodrębnienia nowego typu umowy określonego jako umowa o dostarczenie treści cyfrowych lub usług cyfrowych[6]. Chodzi więc o pewien rodzaj umów[7] wyodrębnianych z uwagi na kryterium świadczenia i jego przedmiotu oraz kryterium podmiotowe, a nie nowy typ umowy nazwanej[8].

2. Kwalifikowanie umów do kategorii umów o dostarczanie treści cyfrowej lub usługi cyfrowej

Mając na uwadze rozważania zawarte w punkcie poprzedzającym, należy przyjąć, że ustawodawca wyodrębnia pewną klasę (rodzaj) umów po to, żeby odnieść do niej regulację dotyczącą specyficznych aspektów dotyczących wykonywania zobowiązań wynikających z takich umów, zgodności z umową przedmiotu świadczenia występującego w takich zobowiązaniach, a także konsekwencji braku zaistnienia takiej zgodności. Owo wyodrębnienie następuje przy użyciu dwóch kryteriów, a mianowicie kryterium podmiotowego (cała ustawa dotyczy przede wszystkim stosunków zobowiązaniowych pomiędzy konsumentami i przedsiębiorcami), a także kryterium przedmiotowego w postaci specyficznego świadczenia, które opisane zostało jako polegające na dostarczaniu treści cyfrowej lub usługi cyfrowej. Uwagi wymaga to ostatnie kryterium. W odniesieniu do niego można poczynić kilka następujących spostrzeżeń:

6 W doktrynie wskazuje się, że „w normach polskiego prawa cywilnego nie przewidziano umowy nazwanej, która mogłaby pokrywać wszystkie te obowiązki zobowiązaniowe wynikające z umowy o dostarczanie treści cyfrowych lub usługi cyfrowej" – zob. W. Dybka (2025, komentarz do art. 2, Nb 97 i podana tam literatura).

7 Podobnie zakwalifikowano wyodrębnienie umów o dostarczanie treści cyfrowych lub usług cyfrowych na gruncie Dyrektywy 2019/770 – zob. M. Ostaszewski (2023, s. 117); W. Dybka (2025, komentarz do art. 2, Nb 97).

8 Kategorię umów nazwanych i nienazwanych należy odnosić do typów umów, a nie rodzajów.

W ujęciu tradycyjnym i przy uwzględnieniu tradycyjnych przedmiotów, tj. tradycyjnych dóbr, można przyjąć, że dostarczanie typowo odnoszone jest do dóbr materialnych i rozumiane jest jako zachowanie prowadzące do zapewnienia władztwa faktycznego (posiadania) (Górniak & Wanat, 2025, komentarz do art. 43j, Nb 8) nad danym dobrem, które jest przedmiotem świadczenia, czy szerzej – przekazanie kontroli nad przedmiotem świadczenia (Południak-Gierz, 2025, komentarz do art. 43j, Nb 2). Pojęcie to typowo nie odnosi się natomiast do (nie obejmuje zakresem znaczeniowym) usług, które – w języku prawniczym – „są świadczone", a nie dostarczane[9]. W rezultacie zastosowanie tego pojęcia, zarówno do treści cyfrowych, jak i usług cyfrowych, już na pierwszy rzut oka, może wydawać się niewłaściwe. Jednak uwzględniając: cel regulacji, jakim jest unormowanie zagadnień dotyczących wykonywania i odpowiedzialności za nienależyte wykonanie zobowiązań dotyczących specyficznych dóbr w postaci treści cyfrowych i usług cyfrowych; neutralne technologicznie podejście przy kształtowaniu regulacji (z założenia ma ona odnosić się do wszelkich potencjalnych rozwiązań technicznych, tj. wszelkich treści cyfrowych i usług cyfrowych niezależnie od sposobu ich powstawania i udostępniania konsumentowi); trudności językowe w znalezieniu bardziej adekwatnego pojęcia odnoszącego się do specyficznej kategorii dóbr – użycie tego pojęcia można uznać za uzasadnione. Należy wszakże przyjąć, że sfomułowanie „dostarczanie" powinno być w tym przypadku rozumiane w sposób odmienny od dotyczącego dóbr materialnych, uwzględniający specyfikę dóbr cyfrowych i szeroki na tyle, aby objąć nim także świadczenie usług cyfrowych. W rezultacie pojęciu „dostarczanie" będziemy nadawali różne znaczenia w zależności od przedmiotu dostarczania, tj. inne w odniesieniu do dóbr materialnych (zwłaszcza rzeczy), a inne w odniesieniu do szeroko rozumianych dóbr cyfrowych[10]. Przy czym, także w odniesieniu do tych ostatnich sytuacja nie wygląda jednolicie, gdyż dostarczanie treści cyfrowych na nośniku materialnym będzie rozumiane tak, jak przy dostarczaniu rzeczy (co wynika z art. 43i ust. 8 u.p.k.). Tak więc można przyjąć, że nawet na gruncie ustawy o prawach konsumenta pojęcie to nie jest jednolite, w zależności od tego, czy treści cyfrowe dostarczane są na nośniku materialnym, czy nie. W konsekwencji, w zakresie tego pojęcia będą się mieścić różne zachowania.

Trudność z ustaleniem zakresu tego pojęcia spowodowana jest także przez to, że zostało ono użyte w odniesieniu do dwóch – jak się wydaje – różnych kategorii świadczeń, tj. tych, których przedmiotem są treści cyfrowe, i tych obejmujących usługi cyfrowe. W rezultacie zachodzi potrzeba odróżnienia umów o dostarczanie treści cyfrowych od umów o dostarczanie usług cyfrowych, co ma także znaczenie

9 Zwraca się na to uwagę w piśmiennictwie – zob. w odniesieniu do Dyrektywy 2019/770, M. Ostaszewski (2023, s. 113).

10 Sfera cyfrowa wymusza więc nie tylko odrębne potraktowanie wykonywania zobowiązania dotyczącego dóbr cyfrowych czy odpowiedzialności z tytułu nienależytego wykonania zobowiązania, ale także modyfikację w sferze pojęć i ich znaczeń.

na gruncie wykonywania zobowiązań wynikających z takich umów, gdyż rozróżnienia w tym zakresie dokonuje sama ustawa, przewidując odrębną regulację w odniesieniu do obu tych kategorii. Ta regulacja może być pomocna, gdyż wskazanie przez ustawodawcę, kiedy treść cyfrowa albo usługa cyfrowa są dostarczone, pozwala na ustalenie także tego, co ustawodawca uznaje za istotne dla takiego dostarczenia w odniesieniu do danej kategorii świadczenia. I tak, stosownie do art. 43j ust. 2 u.p.k., dostarczenie treści cyfrowej nastąpi już w przypadku udostępnienia konsumentowi lub fizycznemu lub wirtualnemu urządzeniu (które konsument wybrał samodzielnie) treści cyfrowej lub środka pozwalającego na uzyskanie dostępu do treści cyfrowej lub jej pobranie lub gdy konsument lub takie urządzenie uzyskali do niej dostęp. Natomiast, zgodnie z art. 43j ust. 3 u.p.k., z dostarczeniem usługi cyfrowej moglibyśmy mieć do czynienia już wtedy, gdy konsument lub fizyczne lub wirtualne urządzenie (które konsument wybrał samodzielnie w tym celu) uzyskali dostęp do usługi.

W odniesieniu do treści cyfrowych dostarczanie obejmuje dwie kategorie. Po pierwsze, „udostępnienie" ich konsumentowi lub fizycznemu lub wirtualnemu urządzeniu, przy czym obok treści cyfrowej ustawa wyodrębnia środek pozwalający na uzyskanie dostępu do treści cyfrowej lub jej pobranie (np. link, którego aktywacja uruchamia pobieranie pliku) (Południak-Gierz, 2025, komentarz do art. 43j, Nb 14). Po drugie, przepis wyróżnia także „uzyskanie dostępu" do treści cyfrowej. Pomimo podobnego brzmienia obu pojęć należy stwierdzić, że opisują one odmienne sytuacje. Można przyjąć, że „udostępnienie" związane jest z wyodrębnieniem środowiska cyfrowego konsumenta, czy szerzej sfery cyfrowej (przestrzeni internetowej, przestrzeni wirtualnej), do której konsument ma już zapewniony dostęp. Mogą to być urządzenia fizyczne (np. komputer, smartfon) czy wirtualne (np. chmura obliczeniowa). Wprowadzenie treści cyfrowej – bądź środka pozwalającego na uzyskanie dostępu do treści cyfrowej lub jej pobranie – do tej właśnie sfery (np. przez przesłanie treści cyfrowej lub loginu i hasła do portalu dostawcy, gdzie treść ta się znajduje) może pozwalać na przyjęcie, że doszło do dostarczenia w omawianej postaci. Natomiast, gdy dostarczenie treści cyfrowej ma nastąpić poza tą sferą, konieczne będzie uzyskanie dostępu do sfery, w której znajduje się ta treść cyfrowa[11] (np. przez zapewnienie dostępu do portalu dostawcy, gdzie treść ta się znajduje, ale bez pośrednictwa środka pozwalającego na uzyskanie dostępu)[12].

11 K. Górniak & E. Wanat (2025, komentarz do art. 43j, Nb 7) wskazują, że „różnica na poziomie pojęciowym sprowadza się do poziomu aktywności po stronie konsumenta, która jest niezbędna do skorzystania z treści cyfrowej. Poziom ten jest większy, gdy konsument ma tylko możliwość skorzystania z treści cyfrowej (*made available*), a mniejszy, gdy mu ją udostępniono (*made accessible*)".

12 Przy formułowaniu tego przykładu widoczna jest trudność w odróżnianiu (rozdzielaniu) „udostępnienia" i „uzyskania dostępu". W doktrynie trafnie zwraca się uwagę na fakt, że dostęp do treści cyfrowych lub usług cyfrowych może być mniej lub bardziej bezpośredni – tak K. Górniak & E. Wanat (2025, komentarz do art. 43j, Nb 5). Wskazuje się, że niemal bezpośredni dostęp do treści cyfrowej uzyskuje się w przypadku, gdy np. gdy konsument pobiera treść cyfrową na swój komputer.

Wprowadzenie treści cyfrowych do środowiska cyfrowego, czy szerzej sfery cyfrowej (przestrzeni internetowej, przestrzeni wirtualnej) konsumenta, zwłaszcza przez pobranie, może spowodować stan, w którym konsument ma możliwość nie tylko korzystania z tej treści, ale także dokonywania w ramach swojego środowiska cyfrowego faktycznych dyspozycji jej dotyczących i przy uwzględnieniu jej charakteru. Przykładowo może decydować co do przechowywania treści cyfrowych, miejsca przechowania, w tym jego zmiany, bądź o usunięciu treści cyfrowych. Można w uproszczeniu traktować to jako odpowiednik władztwa faktycznego w odniesieniu do rzeczy czy innego dobra materialnego.

Mając na uwadze treść art. 43j ust. 3 u.p.k., można dostrzec, że w przypadku usług cyfrowych chodzi tylko o uzyskanie dostępu. W rezultacie dostrzega się, że usługi cyfrowej nie można pobrać (Ostaszewski, 2023, s. 109) (choć podkreślić trzeba, że nie musi ono wystąpić w odniesieniu do każdego przypadku treści cyfrowej, która też może być dostarczona przez uzyskanie dostępu). W doktrynie wskazuje się także na element władztwa przedsiębiorcy przy usłudze cyfrowej i oderwanie się od niego przy treści cyfrowej (Górniak & Wanat, 2025, komentarz do art. 43h, Nb 8). Spostrzeżenie to jest trafne, choć mamy tu znowuż odwołanie się do znanego pojęcia, typowo odnoszonego do dóbr materialnych, które przy dobrach niematerialnych zapewnia raczej intuicyjne wyobrażenie (przybliżenie) odnośnie tego, co jest przedstawiane. Przy rzeczach, czy szerzej – dobrach materialnych, kwestia przedstawia się prościej, a przynajmniej jest dobrze rozpoznana[13]. Przy analizowanej kategorii świadczeń chodzi o to, że przy usłudze cyfrowej dostawca ma zachowany bezpośredni i ciągły wpływ na dane dobro cyfrowe, które pozostaje w jego sferze oddziaływania, tj. w jego środowisku cyfrowym. Tym samym ma także zapewniony wpływ na to, co jest dostarczane konsumentowi. Taki wpływ nie jest jednak wykluczony także przy treściach cyfrowych, których dostarczanie odbywa się przez uzyskanie dostępu. Przy treściach cyfrowych może więc chodzić nie tylko o dostęp do nich, ale i umożliwienie ich pobrania. W tym ostatnim przypadku dane treści cyfrowe pozostawałyby natomiast w sferze wpływu konsumenta i mógłby on dokonywać w odniesieniu do takich treści cyfrowych określonych dyspozycji w ramach jego środowiska cyfrowego. Natomiast w przypadku uzyskania dostępu – co może wystąpić zarówno w odniesieniu do treści cyfrowych, jak i usług cyfrowych – różnica pomiędzy obu tymi kategoriami świadczeń może się zacierać, a w rezultacie może chodzić o takie samo zachowanie. Rozróżnienie, czy mamy wówczas do czynienia z dostarczaniem treści cyfrowych lub usługi cyfrowej, zależeć będzie od charakteru samego świadczenia. Tu zresztą widać, że może chodzić o te same dobra cyfrowe, co – w zależności od zastosowanego przez przedsiębiorcę rozwiązania – może zostać zakwalifikowane jako dostarczenie treści

13 Dobro takie może być w ogóle we władztwie faktycznym jakiejś osoby i raczej wiadomo, czy znajduje się we władztwie wyłącznym tej czy innej osoby, albo też, czy mamy do czynienia ze współwładztwem.

cyfrowych albo jako dostarczenie usługi cyfrowej. Widoczne jest to choćby przy kategorii określanej mianem „oprogramowanie jako usługa"[14].

W rezultacie, uogólniając, można przyjąć, że „dostarczanie" w odniesieniu do treści cyfrowych bądź usług cyfrowych obejmuje zachowanie przedsiębiorcy, uzależnione od rozwiązania technicznego zastosowanego przez danego przedsiębiorcę i charakteru przedmiotu świadczenia, prowadzące do stworzenia stanu, w którym istnieje już po stronie konsumenta możliwość korzystania z treści cyfrowych lub usługi cyfrowej w sposób zgodny z ich funkcją[15]. Przepisy art. 43j ust. 2 i ust. 3 u.p.k. doprecyzowują, na czym ono może polegać w odniesieniu do danej kategorii świadczenia. Określenie konkretnego sposobu dostarczenia może zostać dokonane przez strony w umowie.

W doktrynie wskazuje się, że dostarczanie treści cyfrowej lub usługi cyfrowej to zachowanie przedsiębiorcy, które nie wymaga współdziałania ze strony konsumenta, a zwłaszcza przyjęcia świadczenia (Górniak & Wanat, 2025, komentarz do art. 43j, Nb 8 i podana tam literatura)[16]. Jest to jednak ujęcie zbyt ogólne. Można powiedzieć, że nie występuje przyjęcie tożsame z tym, jakie występuje przy materialnym przedmiocie świadczenia, a nie brak przyjęcia w ogóle. Natomiast element współdziałania przez konsumenta przy wykonywaniu zobowiązania widoczny jest w zachowaniu polegającym na wyborze (i poinformowaniu o nim drugiej strony) fizycznego lub wirtualnego urządzenia, któremu ma być udostępniona treść cyfrowa lub środek pozwalający na uzyskanie dostępu do tej treści lub jej pobranie[17].

Analizowana klasa umów obejmuje umowy, w których świadczenie dostarczania ma odnosić się wyłącznie do treści cyfrowej lub usługi cyfrowej, w tym także w przypadku, gdy treści cyfrowe występują na nośniku materialnym, tj. przedmiocie materialnym, który służy wyłącznie jako ich nośnik (art. 43h ust. 1 u.p.k.). Nie zaliczają się do tej kategorii umowy dotyczące dostarczenia towaru z elementami cyfrowymi, choć w ich przypadku treści cyfrowe lub usługa cyfrowa są także przedmiotem świadczenia. W rezultacie można też dostrzec szerszą kategorię, tj. umowy ze świadczeniem obejmującym elementy cyfrowe. Regulacja prawna jej dotycząca jest niejednolita. Różni się

14 Na przykład edytor tekstów Word można było mieć zainstalowany na swoim komputerze (treść cyfrowa) albo korzystać z takiego edytora bez konieczności instalacji, a przez dostęp do niego za pośrednictwem Internetu.

15 Podobnie K. Południak-Gierz (2025, komentarz do art. 43j, Nb 2) i podana tam literatura. Podobnie K. Górniak & E. Wanat (2025, komentarz do art. 43j, Nb 4–5) wskazują, że „kluczowym wymaganiem jest uzyskanie przez konsumenta dostępu do treści lub usługi cyfrowej", a także, że „dostęp ten powinien być rozumiany jako faktyczna możliwość korzystania z treści lub usługi cyfrowej w sposób zgodny z ich funkcją".

16 Kwestia ta zależna jest jednak od postrzegania przyjęcia świadczenia i wymaga odrębnego zbadania – zob. szerzej P. Konik (2024, s. 24–28).

17 Podobnie zauważają K. Górniak & E. Wanat (2025, komentarz do art. 43j, Nb 8), choć wskazują na zwłokę wierzyciela.

ona w zależności od tego, czy świadczenie obejmuje samą treść cyfrową, czy usługę cyfrową (stosuje się przepisy rozdziału 5b ustawy o prawach konsumenta), treść cyfrową na nośniku materialnym (stosuje się przepisy rozdziału 5b ustawy o prawach konsumenta, ale z wyłączeniem art. 43j ust. 1–7), czy towar z elementami cyfrowymi (stosuje się przepisy rozdziału 5a ustawy o prawach konsumenta). Ponadto przepisów rozdziału 5b ustawy o prawach konsumenta nie stosuje się także w odniesieniu do kategorii wyraźnie wskazanych w art. 43j u.p.k.[18]

3. Typy umów w ramach kategorii umów o dostarczanie treści cyfrowej lub usługi cyfrowej

Ustalenie, że regulacja zawarta w rozdziale 5b ustawy o prawach konsumenta nie przewiduje odrębnego typu umowy o dostarczenie treści cyfrowej lub usługi cyfrowej, a także, że odnosi się ona do wyodrębnionej klasy (rodzaju) umów, skłania do rozważań dotyczących typów umów, jakie mogłyby zostać zaliczone do tej klasy, a w szczególności do odpowiedzi na pytanie, czy należą do tej kategorii jakieś umowy nazwane. Przypomnieć trzeba, że sama Dyrektywa 2019/770 w motywie 12 *expressis verbis* wskazuje, że nie przesądza ona charakteru prawnego umów o dostarczanie treści cyfrowych lub usługi cyfrowej, pozostawiając rozstrzygnięcie tej kwestii prawu krajowemu. Przy czym wskazanie na umowę sprzedaży, umowę o świadczenie usługi, umowę najmu lub umowę *sui generis* ma charakter jedynie przykładowy. W szczególności nie stanowi to podstawy do wniosku, że w grę wchodzą na pewno wskazane umowy, a także wniosku, że inne typy umów nie mogą być w tym zakresie brane pod uwagę. W doktrynie kwestia ta była dostrzeżona i dyskutowana na wiele lat przed wejściem w życie zmiany ustawy o prawach konsumenta będącej wynikiem implementacji Dyrektywy 2019/770. Rozważania te odnosiły się w dużej mierze do uregulowań zawartych w samej Dyrektywie 2019/770 bądź jej projekcie, przy czym punktem odniesienia – co zupełnie zrozumiałe – były znane i wyróżniane do tej pory typy i rodzaje umów[19]. Poglądy te były

18 Niezależnie od tego, stosownie do art. 3 pkt 10 u.p.k., przepisów ustawy nie stosuje się do umów zawieranych poza lokalem przedsiębiorstwa, jeżeli konsument jest zobowiązany do zapłaty kwoty nieprzekraczającej pięćdziesięciu złotych, z wyjątkiem art. 7a.

19 J. Pisuliński (2013, s. 802) wskazuje, że mogą to być umowy przenoszące prawa do określonych treści cyfrowych, umowy licencyjne, umowa o świadczenie usług czy jakaś inna umowa nazwana. E. Macierzyńska-Franaszczyk (2017, s. 296) wskazuje natomiast, że umowa taka może być kwalifikowana jako umowa sprzedaży, najmu, leasingu, umowa o dzieło, o świadczenie usług czy też umowa *sui generis* niezaliczana do żadnego z wymienionych typów. Zob. też M. Ostaszewski (2023, s. 117), który odwołując się do dotychczasowych poglądów formułowanych w doktrynie, wskazuje, że są w dużej mierze aktualne na gruncie Dyrektywy.

raczej formułowane ogólnie i tylko co do niektórych kategorii odnoszone były pogłębione rozważania[20].

Aktualnie obowiązująca ustawa o prawach konsumenta, wprawdzie nie wprowadza odrębnego typu bądź typów umów nazwanych dotyczących treści cyfrowych lub usług cyfrowych, a – jak wcześniej wskazano – normuje jedynie klasę (kategorię) umów wyróżnianych przede wszystkim z uwagi na kryterium charakteru świadczenia odnoszącego do tych treści cyfrowych lub usług cyfrowych, to jednak wywiera ona istotny wpływ na analizowaną kwestię. W przypadku stwierdzenia, że w tej sferze mamy do czynienia z umowami nienazwanymi, powoduje ona mianowicie zmniejszenie potrzeby (i znaczenia) poszukiwania w konkretnym przypadku regulacji dotyczącej określonej umowy nazwanej. Podkreślić trzeba, że takie poszukiwanie miałoby znaczenie wobec uprzedniego stwierdzenia braku regulacji jakiejś istotnej kwestii związanej z konstrukcją bądź wykonywaniem zobowiązania wynikającego z danej umowy nienazwanej. Umowa nienazwana wprawdzie nie ma regulacji ustawowej dotyczącej tylko jej, jednak zastosowanie do niej znajdują przepisy ogólne o czynnościach prawnych (umowach), a także – jeżeli istnieją – te, które dotyczą jakiegoś rodzaju (klasy) umów, do którego zaliczyć można daną umowę nienazwaną. Poszukiwanie regulacji dotyczącej uregulowanego typu jakiejś umowy wchodzi więc zwykle w grę, gdy zachodzi potrzeba rozstrzygnięcia kwestii nieuregulowanej w przepisach znajdujących zastosowanie do danej umowy nienazwanej. Przy czym, podkreślenia wymaga, że przy umowie nienazwanej problem dotyczy zwykle (i przede wszystkim) świadczenia charakterystycznego, w tym dotyczącego charakterystycznego dobra (niepieniężnego). W analizowanym przypadku, wobec uregulowania, przynajmniej ogólnego, kwestii dotyczącej wykonywania zobowiązania z umowy o dostarczanie treści cyfrowych lub usług cyfrowych czy prawidłowości takiego świadczenia, problem kwalifikacyjny (kwalifikacji typologicznej) traci, przynajmniej częściowo, na znaczeniu i zostaje ograniczony do przypadków, których nie da się rozstrzygnąć na gruncie przepisów dotyczących wszystkich umów bądź określonego ich rodzaju, w tym tych zawartych w rozdziale 5b ustawy o prawach konsumenta[21].

Dalsze, bardziej szczegółowe rozważania można ująć w poniższych punktach, zastrzegając, że będą one miały często charakter zaznaczenia (wskazania) problemów niż ich rozwiązania (co możliwe byłoby dopiero na gruncie konkretnych przypadków):

20 Można jednak odnotować także wypowiedzi bardziej szczegółowe odnoszące się skonkretyzowanych zagadnień – zob. na przykład te powołane przez M. Ostaszewskiego (2023, s. 117).

21 Na szereg kwestii nieuregulowanych w tym rozdziale zwraca się uwagę w doktrynie – zob. W. Dybka (2025, komentarz do art. 2, Nb 98).

Jak już wskazano, nie można wyodrębnić jednego, odrębnego typu umowy o dostarczenie treści cyfrowej lub usługi cyfrowej[22], a w grę potencjalnie może wchodzić co najmniej kilka takich typów o różnym charakterze prawnym[23].

Przy badaniu, czy w ramach kategorii umów o dostarczanie treści cyfrowych lub usług cyfrowych można wyodrębnić umowy, które dają się zakwalifikować do jakiegoś typu umowy nazwanej, konieczna jest analiza regulacji (zwłaszcza kodeksowej) dotyczącej poszczególnych typów umów, w tym sposobu ujęcia poszczególnych typów, a zwłaszcza świadczeń stron i ewentualnie ich przedmiotów. Pomocne w tej kwestii będą wcześniejsze ustalenia dotyczące tego, na czym polega dostarczanie treści cyfrowej oraz dostarczanie usługi cyfrowej.

Można dostrzec, że większość wyodrębnionych w kodeksie cywilnym typów umów nazwanych dotyczy dóbr materialnych, a zwłaszcza rzeczy. Tylko niektóre mają na tyle ogólnie określony przedmiot świadczenia, że mógłby on swoim zakresem objąć szeroko rozumiane dobra cyfrowe. Wskazać można tu umowę o dzieło, a także umowę darowizny. Przy czym znaczenie tego pierwszego typu umowy byłoby ograniczone do przypadków, gdy dobra cyfrowe miałyby zostać – w ramach tej umowy – dopiero wytworzone[24] i mieć cechy dzieła[25] (np. stworzenie programu komputerowego, stworzenie strony internetowej[26]). Wydaje się zaś, że największą część obrotu stanowią dobra już istniejące (gotowe) i raczej o charakterze standardowym, a obrót nimi ma charakter masowy. W odniesieniu do umowy darowizny wskazać zaś trzeba jej niewielki udział w obrocie, a także wyłączenie stosowania przepisów rozdziału 5b do tego typu umów przewidziane w art. 43i pkt 2 u.p.k. W rezultacie uzasadniony jest wniosek, że umowy o dostarczanie treści cyfrowych lub usług cyfrowych to, w zasadzie, umowy nienazwane. Mogą to być, przy tym, kształtujące się dopiero typy umów bądź już ukształtowane empiryczne typy umów. Mogą one odpowiadać typom umów nazwanych (być do nich podobne), choć odnosić się do odmiennego dobra niż rzecz bądź inne dobro, do którego stosuje się przepisy dotyczące danego typu umowy (np. dobra inne niż rzecz wskazane w art. 555 k.c. dotyczącym

22 W. Dybka (2025, komentarz do art. 2, Nb 97) – zob. uwagi dotyczące rozważanego – na etapie prac nad projektem ustawy o prawach konsumenta – rozwiązania polegającego na odpowiednim stosowaniu do umów o dostarczanie treści cyfrowych lub usług cyfrowych przepisów o umowie sprzedaży. Zob. też B. Więzowska-Czepiel (2024, komentarz do art. 43h, Nb 6).

23 Trafne i aktualne są poglądy formułowane w tej kwestii jeszcze na gruncie poprzedniego stanu prawnego – zob. choćby J. Pisuliński (2013, s. 802); E. Macierzyńska-Franaszczyk (2017, s. 296); M. Ostaszewski (2023, s. 117).

24 Odnośnie wątpliwości, czy umowa o dostarczanie treści cyfrowych lub usług cyfrowych (a więc i ustawa o prawach konsumenta) obejmuje umowy dotyczące wytwarzania treści cyfrowych – zob. K. Południak-Gierz (2025, komentarz do art. 43h-43i, Nb 15).

25 Zob. szerzej co do cech dzieła i wątpliwości w tym zakresie A. Brzozowski (2018, s. 419–429, Nb 10–18).

26 Przykład ten wskazywany jest w doktrynie, choć z wątpliwościami – zob. W. Dybka (2025, komentarz do art. 2, Nb 98).

sprzedaży[27]). W praktyce, jedynie w uproszczeniu odwołujemy się wtedy do nazwy jakiejś umowy nazwanej.

Biorąc pod uwagę ogólnie ujęty rezultat, jaki powstaje w wyniku wykonania konkretnego zobowiązania wynikającego z umowy o dostarczanie treści cyfrowych lub usług cyfrowych, można wyodrębniać pewne dalsze klasy umów, a w ich ramach – ich typy. Można mianowicie wskazać – nawiązując do tradycyjnie dokonywanych podziałów (zob. np. Macierzyńska-Franaszczyk (2017, s. 296) – kategorie umów: prowadzących do rozporządzenia treściami cyfrowymi; prowadzących do zapewnienia używania (korzystania) treści cyfrowych; prowadzących do uzyskania usługi (Górniak & Wanat, 2025, komentarz do art. 43h, Nb 9).

Z uwagi na charakter dobra, jakim są treści cyfrowe, dokładne rozdzielenie, z którą kategorią umów wskazanych w punkcie poprzedzającym – tj. umowa prowadząca do rozporządzenia treściami cyfrowymi czy umowa prowadząca do zapewnienia używania treści cyfrowych – mamy do czynienia w konkretnym przypadku, nie wydaje się *in abstracto* możliwe i do sformułowania nadają się jedynie kryteria ukierunkowujące bardziej szczegółowe analizy. W doktrynie wskazuje się jako istotne kryterium trwałości udostępnienia treści cyfrowych, w tym zwłaszcza w aspekcie czasowym. Podobieństwo do umowy sprzedaży występuje zaś wtedy, gdy „umowa przewiduje trwałe i ostateczne przeniesienie treści cyfrowych wraz z takim samym przeniesieniem prawa do korzystania z danych treści" (Ostaszewski, 2023, s. 118)[28]. Uzupełniając te spostrzeżenia, można podnieść, że rozpatrywany powinien być całościowy rezultat, jaki powstaje w wyniku wykonania danej umowy – ma on być zbliżony do tego, jaki zapewniają umowy prowadzące do rozporządzenia rzeczą. Ważne są więc nie tylko definitywność (trwałość czasowa) nabycia i zakres nabytych uprawnień, zwłaszcza co do korzystania z treści cyfrowych, ale także element władztwa nad tymi treściami (w swoim środowisku cyfrowym nabywcy) i możliwość dysponowania nimi, co zwykle będzie miało miejsce, w przypadku dostarczenia treści cyfrowych konsumentowi bądź fizycznemu lub wirtualnemu urządzeniu przez niego wskazanego, a zwłaszcza pobrania takiej treści[29]. Przy czym, dla ustalenia typu umowy konieczne jest jeszcze uwzględnienie innych cech świadczenia przedsiębiorcy (np. czy jest jednorazowe, sekwencyjne czy ciągłe[30]), występowania i charakteru świadczenia drugiej strony i ewentualnego powiązania pomiędzy świadczeniami obu stron (w szczególności co do wzajemności). W zależności od tych ustaleń można rozpa-

27 W. Dybka (2025, komentarz do art. 2, Nb 98) jako otwartą do dalszej analizy uważa kwestię kwalifikowania umowy dotyczącej treści cyfrowych jako sprzedaży praw, o której mowa w art. 555 k.c.

28 K. Górniak & E. Wanat (2025, komentarz do art. 43h, Nb 9) wskazują natomiast na „definitywny dostęp (nieograniczony w czasie) do treści cyfrowej".

29 Co do tej kwestii – podobnie W. Dybka (2025, komentarz do art. 2, Nb 98).

30 W tej kwestii, na gruncie Dyrektywy 2019/770 – zob. szerzej M. Ostaszewski (2023, s. 114–116). Co do rodzaju świadczeń przedsiębiorcy – zob. też W. Dybka (2025, komentarz do art. 2, Nb 98).

trywać podobieństwo do sprzedaży, zamiany, darowizny bądź umowy podobnej (np. dostarczenie treści cyfrowych w zamian za usługę lub dane osobowe).

W przypadku, gdy wskazany w punkcie poprzedzającym rezultat nie występuje, a zwłaszcza, gdy brak wspomnianej definitywności (w tym trwałości czasowej) nabycia treści cyfrowych[31], nie występuje element władztwa nad treściami cyfrowymi bądź zakres korzystania jest ograniczony, zachodziłoby podobieństwo do umów dotyczących korzystania z cudzych rzeczy. W zależności od występowania świadczenia drugiej strony, jego charakteru oraz ewentualnego związku pomiędzy świadczeniami obu stron (w szczególności wzajemności) mogłoby być to podobieństwo do umowy najmu, leasingu bądź użyczenia. Jeżeli zaś zachodziłaby możliwość pobierania pożytków przynoszonych przez treść cyfrową, w grę wchodziłoby także podobieństwo do umowy dzierżawy.

Ustalenie, na czym polega rezultat uzyskany przez wykonanie zobowiązania wynikającego z danej umowy o dostarczanie treści cyfrowej, pozwoli na znalezienie konkretnej umowy nazwanej najbardziej podobnej do rozpatrywanej umowy nienazwanej, a następnie rozpatrzenie zastosowania jej regulacji *per analogiam* do określonej kwestii nieuregulowanej przy danej umowie nienazwanej (Dybka, 2025, komentarz do art. 2, Nb 98).

Przy kwalifikowaniu umów do kategorii umów o dostarczenie usługi cyfrowej w pierwszej kolejności pojawia się problem związany z niejednoznacznością samego pojęcia usługi. Ponadto zachodzi dodatkowa trudność z odróżnieniem jej od korzystania z treści cyfrowych[32], tym bardziej, że dostarczanie usługi cyfrowej, jak i dostarczanie treści cyfrowych może przybrać postać uzyskania dostępu do nich. Jednak przebrnięcie przez ten problem i zakwalifikowanie, że mamy jednak do czynienia z usługą cyfrową, związane jest z pewnym ułatwieniem, gdyż w takiej sytuacji art. 750 k.c. rozstrzyga, jakie przepisy należy stosować do takiej umowy. Wskazuje on, że do umów o świadczenie usług, które nie są uregulowane innymi przepisami, stosuje się odpowiednio przepisy o zleceniu. Przy czym, podobnie jak w przypadku nienazwanych umów pośrednictwa, co do których zachodzi wątpliwość, czy nie bardziej odpowiednie dla nich są przepisy dotyczące umowy agencyjnej, także w odniesieniu do usług cyfrowych można rozważać, czy nie są bardziej adekwatne dla nich inne przepisy (np. w odniesieniu do usługi przechowywania treści cyfrowych w chmurze obliczeniowej przepisy dotyczące umowy przechowania[33]).

31 K. Górniak, E. Wanat (2025, komentarz do art. 43h, Nb 9) wskazują na tymczasowy dostęp do treści cyfrowych.

32 Co do tego problemu kwalifikacyjnego – zob. szerzej W. Dybka (2025, komentarz do art. 2, Nb 89–95 i podana tam literatura).

33 Odnośnie wątpliwości dotyczących kwalifikowania umowy o udostępnienie oprogramowania zainstalowanego w chmurze obliczeniowej do przechowywania plików konsumenta – zob. W. Dybka (2025, komentarz do art. 2, Nb 98 i podana tam literatura).

Przy umowach, w których przedmiot świadczenia daje się zakwalifikować jako utwór, zastosowanie znajdą dodatkowo przepisy prawa autorskiego.

Podsumowanie

W ramach podsumowania można sformułować następujące spostrzeżenia:

Analiza regulacji prawnej zawartej w rozdziale 5b ustawy o prawach konsumenta nie daje podstawy do przyjęcia, że umowa o dostarczanie treści cyfrowych lub usług cyfrowych stanowi odrębny typ umowy. Należy przyjąć, że mamy tu do czynienia z wyodrębnioną przez ustawodawcę klasą (rodzajem) umów, do której odnoszona jest szczególna regulacja dotycząca przede wszystkim wykonywania zobowiązań z takich umów, problematyki zgodności (niezgodności) świadczenia z umową oraz konsekwencji prawnych niezgodności.

Klasa ta nie jest jednorodna i w jej ramach można wyodrębnić dwie odrębne kategorie w zależności od tego, czy świadczenie dotyczy treści cyfrowych, czy usługi cyfrowej. Przy czym w obu przypadkach świadczenie zostało opisane tym samym zwrotem, tj. „dostarczanie", co można rozumieć jako zachowanie przedsiębiorcy, uzależnione od rozwiązania technicznego zastosowanego przez danego przedsiębiorcę i charakteru przedmiotu świadczenia, prowadzące do stworzenia stanu, w którym istnieje już po stronie konsumenta możliwość korzystania z treści cyfrowych bądź usługi cyfrowej w sposób zgodny z ich funkcją. Przepisy art. 43j ust. 2 i ust. 3 u.p.k. doprecyzowują, na czym ono może polegać w odniesieniu do danej kategorii świadczenia. Określenie konkretnego sposobu dostarczenia może zostać dokonane przez strony w umowie.

Analizowana klasa umów obejmuje umowy, w których świadczenie dostarczania ma odnosić się wyłącznie do treści cyfrowej lub usługi cyfrowej, w tym także w przypadku, gdy treści cyfrowe występują na nośniku materialnym, tj. przedmiocie materialnym, który służy wyłącznie jako ich nośnik (art. 43h ust. 1 u.p.k.). Nie obejmuje ona umów, których przedmiotem świadczenia są towary z elementami cyfrowymi.

Regulacja zawarta w rozdziale 5b, choć dotyczy tylko pewnej klasy umów, to powoduje zmniejszenie potrzeby (i znaczenia) badania typologii umów, a zwłaszcza poszukiwania w konkretnym przypadku regulacji dotyczącej określonej umowy nazwanej, która mogłaby zostać zastosowana do kwalifikowanej umowy nienazwanej.

Umowy o dostarczanie treści cyfrowych lub usług cyfrowych nie dają się zakwalifikować do jednego typu umowy, w szczególności umowy podobnej do sprzedaży. Poza nielicznymi wyjątkami – w zasadzie będą to umowy nienazwane.

Biorąc pod uwagę ogólnie ujęty rezultat, jaki powstaje w wyniku wykonania konkretnego zobowiązania wynikającego z umowy o dostarczanie treści cyfrowych lub usług cyfrowych, można wyodrębnić kategorię umów: prowadzących do roz-

porządzenia prawem do treści cyfrowych, prowadzących do zapewnienia używania (korzystania) treści cyfrowych oraz prowadzących do uzyskania usługi.

Ustalenie, na czym polega rezultat uzyskany poprzez wykonanie zobowiązania wynikającego z danej umowy o dostarczanie treści cyfrowej, pozwoli na znalezienie konkretnej umowy nazwanej najbardziej podobnej do rozpatrywanej umowy nienazwanej, a następnie rozpatrzenie zastosowania jej regulacji *per analogiam* do określonej kwestii nieuregulowanej przy danej umowie nienazwanej.

W odniesieniu do umów o dostarczenie usług cyfrowych ustalenie regulacji dotyczącej typu umowy nazwanej, która byłaby stosowana do analizowanej umowy, jest prostsze niż w przypadku umów o dostarczanie treści cyfrowych, a to za sprawą art. 750 k.c. odsyłającego do odpowiedniego stosowania przepisów o umowie zlecenia.

BIBLIOGRAFIA

Brzozowski, A. (2020). Umowy nazwane i nienazwane. w: K. Osajda (red.), *System Prawa Prywatnego. Prawo zobowiązań – część ogólna*. t. 5. (ss. 500–504), C.H. Beck.

Brzozowski, A. (2018). Umowa o dzieło. w: J. Rajski (red.), *System Prawa Prywatnego. Prawo zobowiązań – część szczegółowa*. t. 7. (ss. 410–484), C.H. Beck.

Dybka, W. (2025). Komentarz do art. 2 lit. 5–5a. w: M. Pecyna (red.), *Rękojmia konsumencka. Komentarz* (2nd ed.) C.H. Beck (Legalis).

Górniak, K. & Wanat, E. (2024, 2025). Komentarz do art. 43h–art. 43j. w: M. Pecyna (red.), *Rękojmia konsumencka. Komentarz* (wyd. 1 i 2), C.H. Beck (Legalis).

Grzybowski, S. (1976). Stosunki zobowiązaniowe nazwane, nienazwane i mieszane. w: S. Grzybowski (red.), *System prawa cywilnego*. t. III, cz. 2, (ss. 15–21), Ossolineum.

Macierzyńska-Franaszczyk, E. (2017). Umowa o dostarczanie treści cyfrowych według projektu dyrektywy o dostarczanie treści cyfrowych. w: Z. Kuniewicz & D. Sokołowska (red.), *Prawo kontraktów*. (ss. 293–302), Wolters Kluwer Polska.

Konik, P. (2024). *Wierzycielski obowiązek współdziałania przy wykonywaniu zobowiązania i odpowiedzialność za jego naruszenie,* C.H. Beck.

Ostaszewski, M. (2023). Charakter prawny umów o dostarczanie treści lub usługi cyfrowych. *Acta Iuridica Resoviensia*, Nr (1), 106–122.

Parlament Europejski i Rada UE (2019). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz. Urz. UE L 136 z 22.05.2019, str. 1 oraz Dz. Urz. UE L 305 z 26.11.2019, str. 60).

Pecyna, M. (2021). Implementacja dyrektywy o umowach o dostarczanie treści cyfrowych lub usługi cyfrowej – wyzwania dla ustawodawcy krajowego. *Kwartalnik Prawa Prywatnego* 2021, (3), 607–624.

Pisuliński, J. (2013). Stosowanie wspólnych europejskich przepisów o sprzedaży do treści cyfrowych, w: A. Matlak & S. Stanisławska-Kloc (red.), *Spory o własność intelektualną. Księga jubileuszowa*

dedykowana Profesorom Januszowi Barcie i Ryszardowi Markiewiczowi, (ss. 793–317), Wolters Kluwer Polska.

Południak-Gierz, K. (2025). Komentarz do art. 43h – art. 43j, w: P. Machnikowski (red.), *Ustawa o prawach konsumenta*, Legalis.

Radwański, Z. (1977). *Teoria umów*. Państwowe Wydawnictwo Naukowe.

Sejm Rzeczpospolitej Polskiej. (2014). Ustawa z 30 maja 2014 r. o prawach konsumenta (Dz.U. 2014, poz. 827; tj. Dz.U. 2024, poz. 1796).

Sejm Rzeczpospolitej Polskiej. (2022). Ustawa z 4 listopada 2022 r. o zmianie ustawy o prawach konsumenta, ustawy – kodeks cywilny orz ustawy – Prawo prywatne międzynarodowe (Dz.U. 2022, poz. 2337).

Więzowska-Czepiel, B. (2024). Komentarz do art. 43h–art. 43j, w: B. Kaczmarek-Templin, P. Stec & D. Szostak (red.), *Ustawa o prawach konsumenta. Kodeks cywilny (wyciąg). Komentarz*, C.H. Beck (Legalis).