Ius et Securitas 2/2024 | ISSN 3071-799X

Paweł Pelc
Law Firm of Attorney-at-Law Pawel Pelc in Warsaw
ORCID: 0000-0002-5007-568X
pawel.pelc@gmail.com

Soft Law in Cybersecurity Regulations Addressed to Polish Financial Institutions

Abstract

According to Polish Constitution there are strict limitations related to establishing the law, however in practice it is commonly accepted that the existing law (in this contexts known as 'hard law') is supplemented by soft law established also by entities not entitled to create law. One of such institutions is Polish Financial Supervisory Authority, which has issued various document named recommendations, guidelines or communications, based or on specific legal authorisation or only on the general duties established by law addressed to the supervised entities (either generally or on sectoral basis). Some of such soft law acts were related to the operational risk management including also cybersecurity issues. This hasn't change after the PFSA became a body responsible for cybersecurity for the banking and financial infrastructure sector as well. European Union Law was supplemented by guidelines of European Supervisory Authorities. After Digital Operational Resilience Act (DORA) and related Regulatory Technical Standards (RTS) are in force, at least of the existing soft law would be replaced by such 'hard law', but this is unlikely that the soft law, in the area of the cybersecurity of the financial institutions, is not in use anymore.

The aim of the article is to analyse soft law, which is included in the regulations on cybersecurity, and concerns Polish financial institutions. The basic research method is a legal-dogmatic method, through which issues of cybersecurity of financial institutions are analysed.

Keywords: cybersecurity, soft law, financial institutions, DORA, RTS.

Introduction

Activity of financial institutions is based on trust of customers[1] and other counter partners, while at the same time being increasingly dependent on digitalization[2]. This makes them especially vulnerable on cyberattacks, as due to strong connections between financial institutions and financial markets there is a risk of uncontrolled withdrawals of deposits or resignation from other financial relations in case of successful cyberattack against such entities. A good example of this occurred during the financial crisis of 2007/2008, when lack of trustworthy information about real situation of banks drastically affected interbank operations[3] and required the intervention of central banks to support liquidity in the marked.

Moreover banks and other financial institutions are especially attractive to state sponsored operations, treated as part of hybrid war as well as state sponsored criminal activity in addition to operations of criminals not connected with state operations[4].Good example of such vulnerabilities was Russian aggression against Ukraine, which, especially in the phase of hybrid war, included cyberattacks against Ukrainian critical infrastructure, including banks – just before the full scale invasion of Russian troops in kinetic phase[5].

Supervision and oversight over financial institutions

Due to their role in the economy and interactions with customers banks and other financial institutions are usually subject to supervision of financial supervision authorities. There is no single model of supervision over finan-

[1] More P. Pelc, *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, No. 2, p. 152.

[2] P. Pelc, *Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych*, „Cybersecurity and Law" 2021, No. 2, p. 130.

[3] *Polska wobec światowego kryzysu gospodarczego*, Warszawa 2009, p. 29.

[4] P. Milik, G. Pilarski, *Cyberattacks and bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, "Cybersecurity and Law" 2023, No. 1, p. 108-126.

[5] P. Pelc, *Lekcje dla Polski jako członka NATO ze sposobu prowadzenia działań w cyberprzestrzeni w trakcie rosyjskiej agresji przeciwko Ukrainie*, [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. 25 lat członkostwa w NATO*, Chałubińska-Jentkiewicz, K. Gawkowski, Z. Nowak, Ł. Piątkowski, K. Wąsik [eds.], Gliwice 2024, p. 229.

cial institutions. There are specialised supervisory authorities responsible only for supervision over part of financial market, similar to Superintendency of Pension Funds (responsible for pension funds and occupational pension plans supervision), Polish Office of Insurance Supervision (responsible for insurance oversight – but without licensing powers), Banking Supervisory Commission (banks) or Securities (and Exchange) Commission (capital market), that used to function in Poland. Another model is partial integration comparable to Polish Insurance and Pension Funds Supervisory Commission (responsible for supervision over insurance and pension markets). There is also a possibility of full integration, like in Poland since 2006 where the Polish Financial Supervisory Commission is responsible for supervision over various types of financial institutions (at the beginning: insurance, pension funds and capital markets, since 2008 – also bank, since 2012 – credit unions and in various moment also another institutions). In some countries the supervision was delegated to central banks (either only over banks or including another financial institutions). Another solution implemented in other countries was the so called 'Twin Peaks' model, in which there are separate supervisory authorities responsible for stability of the institution and for customers relations. Often there is balance between strong state supervision and regulation on one side and self regulation on another. In addition to traditional supervision aimed at individual financial institutions, additional macro supervisory bodies were created on the European Union and member states level – not directed at separate financial institutions but a the market in its entirety.

Financial market is also known to be fast developing and adapting to innovations. Often such innovations may lead to problems or even financial crisis, like in the year 2007/2008, caused by some derivatives related to subprime debt (so called "subprime crisis"). It leads to a need for an adequate time frame of reaction of the supervisory authorities to the market development and changes there.

Financial institutions in the cybersecurity system

Financial institutions are also treated as part of critical infrastructure and at least some of their services are threated as key services. It leads to treatment of at least some of the financial institutions as parts of cybersecurity

systems, which creates additional duties for such institutions. Due to that Polish Financial Supervisory Authority is one of the authorities responsible for cybersecurity of specific sectors – in this case – banking and financial market infrastructure sector[6].

European Union decided in 2022 to regulate cybersecurity framework for financial institutions in DORA (Digital Operational Resilience Act)[7]. As DORA has form of regulation it is directly valid in all member states without need of implementation to the member states legal systems. Earlier EU has regulated issues related to cybersecurity in financial institutions in various forms, or in a form of directives which required the implementation to the member states' legal systems. In case of payment services it was even delegated to guidelines of European Banking Authority[8] Part of the EU regulatory framework are also Regulatory Technical Standards.

In Poland regulations related to cybersecurity of financial institutions were not fully regulated on the level of law and ordonnances, however some rudimentary issues were covered by the laws related to national cybersecurity system, as mentioned earlier (the implementation of NIS directive[9] as well).

Constitutional regulations related to law creation in Poland

Polish Constitutions strictly limits sources of law and entities which can issue law. Based on the art. 87 of the Constitution[10] the sources of universally binding law of the Republic of Poland are: Constitution, laws, ratified

[6] J. Kostrubiec, *Komentarz do art. 41*, [in:] *Ustawa o krajowym systemie cyberbpieczeństwa. Komentarz*. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec [eds.], Warszawa 2022, p. 208.

[7] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC). No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Official Journal of the European Union L 333/1).

[8] P. Widawski, *Zarządzanie ryzykami operacyjnymi i ryzykami dla bezpieczeństwa w wytycznych Europejskiego Urzędu Nadzoru Bankowego i rekomendacji Komisji Nadzoru Finansowego*, [in:] *Cyberbezpieczeństwo, Zarys wykładu*, C. Banasiński [ed.], Warszawa 2023, p. 402.

[9] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union, L 194/1).

[10] Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws, 1997 no. 78, pos. 483 with amendments).

international agreements and ordinances. Additionally there is local law and, regulated in art. 93 of the Constitution, internally binging acts (Resolutions of the Council of Ministers and orders of the Prime Minister and ministers are internal in nature and apply only to organizational units subordinate to the body issuing these acts) – this rule was interpreted rather broadly and in practice extended beyond Resolutions of the Council of Ministers and orders of the Prime Minister and ministers, however for such acts subordination to the body issuing such act is crucial. In line with art. 92 of the Constitution ordinances are issued by the bodies designated in the Constitution, on the basis of a specific authorization contained in the law and for the purpose of its implementation. The authorization should specify the authority competent to issue the regulation and the scope of matters delegated to regulate, as well as guidelines for the content of the act. Ordinances can by issued by the President (art. 142 sec. 1 of the Constitution), Council of Ministers (art. 146 sec. 4 point 2 of the Constitution), Prime Minister (art. 148 point 3 of the Constitution), ministers (art. 149 sec. 2 first sentence of the Constitution) and National Broadcasting Council (art. 213 sec. 2 of the Constitution). The body authorized to issue a regulation may not delegate its powers to another body (art. 92 sec. 2 of the Constitution).

It leads to the situation that supervisory authorities in the financial market cannot issue ordinances. Such authorities cannot issue internally binding acts as financial institutions are not subordinated to them. There is a clear difference between the role of supervisory authority and the central bank. According to Constitutional Court 'The central bank's leading role as a bank of banks means that, despite the independence and formal independence of commercial banks, in terms of monetary policy they are subject to dependence, allowing it to be defined as functional subordination"[11]. There in no such, even functional, subordination between financial institutions and supervisory authority. In such regulatory arrangements supervisory authorities cannot issue neither commonly binding legal acts nor internally binding acts. If there is a need to issue commonly binding acts related to issues not fully regulated in the laws, there is a requirement of clear delegation to issue an ordinance by a body entitled to this – in case of financial institutions typically it is or Minister of Finance or Prime Minister of Council of Ministers.

[11] Judgment of the Constitutional Court of June 28, 2000. K 25/99 (OTK 200/5/141).

Soft law in the supervisory activity in Poland

Therefore, in relation to the regulatory activities of supervisory authorities in Poland, the construction of the so-called 'soft law' was adopted in the doctrine, thus, regulations that are not sources of law in the constitutional sense, nor generally applicable law nor internal law. It takes the form of recommendations, guidelines or rules. However, they should not be of a legislative nature, but only constitute an interpretation of the applicable standards by the supervisory authority.

For example M. Olszak points out that the recommendations of the supervisory authority have been present on the Polish market since 1996, when the then banking supervisory authority began issuing them. A. Jakubiak (who used to be the Chairman of the Polish Financial Supervisory Authority (PFSA) has believed that recommendations are good practices of behaviour of supervised institutions, which allow to limit and mitigate risk from the point of view of stable management of financial institutions. In addition Z. Ofiarski, discussing the views of the doctrine in this regard, has indicated that regulations having the character of 'soft law' are a complementary to the norms of generally applicable law and fill the areas, which the legislator did not regulate in detail. The supervisory authority has no legal basis to enforce its compliance with the soft law it creates from supervised entities[12]. In 2014 during parliamentary works on insurance regulations issue of the soft law issued by PFSA was also subject of interpretation of the Ministry of Finance which considers that recommendations may constitute interpretations of generally applicable regulations, and not impose additional obligations, the

[12] More on the topic: Z. Ofiarski, *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego*, [in:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, A. Jurkowska-Ziedler, M. Olszak [eds.], Warszawa 2016, p. 139; T. Czech, *Miejsce uchwał Komisji Nadzoru Finansowego w systemie źródeł prawa polskiego*, „Monitor Prawa Bankowego" 2013, No. 7-8, p. 74-75; M. Olszak, *Wydawanie przez Komisję Nadzoru Finansowego wytycznych dotyczących sektora ubezpieczeniowego jako przykład zintegrowanego podejścia do wykonywania nadzoru nad rynkiem finansowym*, [in:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, A. Jurkowska-Ziedler, M. Olszak [eds.], Warszawa 2016, p. 161; A. Jakubiak, *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich*, [in:] *Polityka i praktyka regulacji rynków finansowych*, W. Rogowski [ed.], Kraków-Warszawa 2015, p. 24; A. Nadolska, *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021; M. Żak, *Soft law jako instrument koordynacji regulacyjnej good governance*, „Przegląd Legislacyjny" 2019, No. 1, p. 9-33.

observance of which is subject to supervision and may entail negative consequences for the supervised entity[13].

In practice, the supervisory authority issues its recommendations, guidelines and principles either on the basis of a specific legal delegation authorizing it to create soft law acts or without such a basis. Soft law is addressed either to entities operating in more than one segment of the financial market, or to entities operating in more than one segment of the market, or to all supervised entities (like Principles of Corporate Governance for Supervised institutions[14]).

Cybersecurrity and soft law

Regardless, there is a specific legal authorisation in the law related to specific type of the financial institutions, part of the financial market or there is no such specific authorization, PFSA has issued on the December 2014 Guidelines for the management of information technology areas and the security of the information and communication environment for various types of financial institutions[15]. Those guidelines were issued not based on the specific authorisation in the relevant 'sectoral regulations', but based on general clause in the law on supervision of the financial market[16]. PFSA has issued the Guidelines in regards to objectives of supervision over the financial market, specified in art. 2 of the Law on supervision of the financial market such as: ensuring proper functioning of the market, its stability, security and trust in the market, as well as safeguarding interests of its participants

[13] P. Pelc, *Rekomendacje KNF, czyli kwadratura koła*, „Gazeta Ubezpieczeniowa" 2014, No. 25, p. 7.

[14] PFSA, *Zasady ładu korporacyjnego dla instytucji nadzorowanych*, Warszawa 2014.

[15] PFSA, *Guidelines on the Management of Information Technology and ICT Environment Security for General Pension Companies*, Warszawa 2014, *Guidelines on the Management of Information Technology and ICT Environment Security for Insurance and Reinsurance Undertakings,* Warszawa 2014; *Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w towarzystwach funduszy inwestycyjnych*, Warszawa 2014; *Guidelines on the Management of Information Technology and ICT Environment Security in capital market infrastructure entities,* Warszawa 2014, *Guidelines on the Management of Information Technology and ICT Environment Security at Investment Firms*, Warszawa 2014.

[16] The law on 21 July 2006 on supervision over the financial market (Journal of Laws from 2024 pos. 135).

and the task of the Polish Financial Supervision Authority specified in art. 4 item 1 clause 2 of the Law, consists of activities contributing to proper functioning of the financial market.

In case of sectors with clear authorisation to issue 'soft law' PFSA has issued for banks in 2013 Recommendation D on the Management of Information Technology and ICT Environment Security at Banks[17] and similar recommendation for credit unions in 2016[18].

Additionally for institutions supplying the payment services PFSA has issued in 2015 Recommendation concerning the security of payment transactions on the Internet through banks, national payment institutions, national electronic money institutions and credit unions[19].

Those regulations and guidelines issued between 2013 and 2016 were supplemented by Communication from the UKNF on information processing by supervised entities using public or hybrid cloud computing services issued in January 2020[20] addressed to the whole supervised sectors of the financial market.

PFSA in the national cybersecurity system and soft law

Regulations and guidelines related to cybersecurity of financial institutions issued between 2013 and 2016 were developed before PFSA was included in the national cybersecurity system model. However since 2018 the PFSA – as the only authority other than constitutional minister – has be-

[17] PFSA, *Recommendation D on the Management of Information Technology and ICT Environment Security at Banks*, Warszawa 2013.

[18] *Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych*, Warszawa 2016.

[19] PFSA, *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo – kredytowe*, Warszawa 2015.

[20] *Communication from the UKNF on information processing by supervised entities using public or hybrid cloud computing services*, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_UKNF_Chmura_Obliczeniowa_EN_69242.pdf, [accessed: 27.11.2024]. See also: P. Pelc, *„Komunikat chmurowy" Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, No. 2, p. 183-197; K. Dygasiewicz, P. Zapadka, *Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej w czasie gospodarki COVID lub postCOVID w świetle komunikaty Komisji Nadzoru Finansowego,* „Cybersecurity and Law" 2020, No. 1, p. 103-112.

came an authority responsible for cybersecurity of the banking and financial market infrastructure sector[21] in line with art. 41 point 4 of the law on 5 July 2028 of the National Cybersecurity System[22]. According to the law on National Cybersecurity System the authority with purview over cybersecurity is authorised by this law to issue 'soft law' – in the form of recommendations on actions aimed at strengthening cybersecurity, including sectoral guidelines on incident notifications (In cooperation with relevant CSIRTs and sectoral cybersecurity teams)[23]. This rule is in line with motive 47 and art. 14 sec. 7 of the NIS directive.

However it seems that for PFSA its supervisory tools based on regulations related to supervisory functions are more useful compared to the powers as authority competent for cybersecurity in the National Cybersecurity System. The Communication from the UKNF on information processing by supervised entities using public or hybrid cloud computing services issued after the law on National Cybersecurity System was in force, was not issued in line with the procedure regulated in the that law and was presented as a tool to supplement and specify certain recommendations and guidelines issued earlier by PFSA between 2013 and 2016. It also replaced earlier communication from PFSA on this matter issued in 2017[24].

Even though the recommendations, guidelines or communications issued by PFSA– based on the specific clause of the relevant sectoral law or only on general supervisory powers of the PFSA – cannot create the binding rules and are treated by the Ministry of Finance only as interpretation of the existing legal regulations, in practice are very detailed and clearly create new rules and norms which are not present in the legal regulations[25]. Theoretically the

[21] P. Pelc, *The Polish Financial Supervision Authority in the national cybersecurity system*, „Cybersecurity and Law" 2023, No. 1, p. 74, 76.

[22] Journal of Laws from 2024, pos. 1077.

[23] Art. 42 point 5 of the law on National Cybersecurity System.

[24] *Communication from the UKNF of 23 October 2017 on the use of cloud computing services by the supervised entities*, https://www.knf.gov.pl/knf/en/komponenty/img/Cloud_computing_Stanowisko_UKNF_ENG_61423.pdf, [accessed: 20.11.2024]

[25] The PFSA uses wording like: 'Issuance of the Guidelines is necessary due to a significant technological development and systematic increase in importance of IT technology for general pension companies (hereinafter referred to as companies) and managed by pension companies funds, including voluntary pension funds and due to new threats in this domain. The purpose of these Guidelines is to notify companies of expectations of the KNF regarding prudent and stable information technology and ICT environment security management, in

supervised entities shall 'comply or explain' in case of non compliance, but in practice the supervisory authority can enforce implementation of the 'soft law' during inspection process through the individual recommendations in case that the financial institution is not complying. It means that in practice it is very difficult to treat soft law only as interpretations of the existing legal norms, also in the area of cybersecurity and especially, the National Cybersecurity System.

It is important to see increasing role of the soft law not only on national but also on EU's level. Important part of the financial regulation now is soft law as regulatory function is treated as important part of supervisory activity and is distinguish also from creation legally binging norms during legislative process on both – national and EU grounds[26]. Regardless its non-binding character, the soft law created by the European Supervisory Authorities (which do not produce any binding legal effects) can be subject to the jurisdiction of the European Court of Justice[27].

---

particular regarding management of the risk associated with these areas. (...) The KNF expects that decisions concerning the scope and manner of implementation of the solutions specified in these Guidelines are preceded by an in-depth analysis and supported by an appropriate line of reasoning (...) The KNF expects that appropriate actions aimed at implementation of these Guidelines are executed by the companies not later than by 31 December 2016. The Guidelines should be applied in accordance with the "comply or explain" principle. If the companies withdraw from application of the Guidelines, the KNF expects that these companies explain the reasons for failing to apply the Guidelines in their business activity. Information on the application of these Guidelines should be provided in a form that companies fill out as part of their own assessment of compliance with the Guidelines and that is one of the ways of verification by the KNF whether and in what manner Guidelines have been implemented by the companies. These Guidelines also include legal obligations, performance of which is required of company under the applicable law.' (*Guidelines on the Management of Information Technology and ICT Environment Security for General Pension Companies*, p. 4-5), 'The Supervisor underlines that the requirements described in this communication should be applied by the supervised entities before they start processing information in a cloud computing environment." (*Communication from the UKNF on information processing by supervised entities using public or hybrid cloud computing services,* p. 7)

[26] A. Nadolska, *O „fałszywych" wytycznych EBA i prawdziwym celu nadzorczego soft law w sprawie nadzoru nad produktem i zarządzania nim*, „Przegląd Ustawodawstwa Gospodarczego" 2022, No. 6, p. 19-25.

[27] Judgment of the Court (Grand Chamber) of 15 July 202, In Case C911/19 (ECLI:EU:C:2021:599).

DORA and ITC risk

The important to see the changes in the legal regulations related to cybersecurity of financial institutions by issuing DORA. It covers very broad variety of financial institutions[28] and its ITC services providers. According to motive 12 of DORA, its aim is 'to consolidate and upgrade ICT risk requirements as part of the operational risk requirements that have, up to this point, been addressed separately in various European Union legal acts.'[29] In the motive 14 it is stressed that DORA 'helps reduce regulatory complexity, fosters supervisory convergence and increases legal certainty, and also contributes to limiting compliance costs, especially for financial entities operating across borders, and to reducing competitive distortions.'[30] In practice at least some issues regulated by the soft law so far (like EBAs guidelines related to operational risk in payment services) would be now regulated by 'hard law' – DORA. DORA will be also implemented by common regulatory technical standards (RTS) drafted by ESAs through the Joint Committee in consultation with the European Union Agency for Cybersecurity and issued by the European Commission in line with especially art. 15 of DORA.

Regulatory Technical Standards are developed by European supervisory authorities to clarify specific issues not directly regulated at the level of the regulation. Article 290 of the Treaty on the Functioning of the European Union provides that a legislative act may delegate to the Commission the power to adopt non-legislative acts of general application which supplement or amend certain non-essential acts or elements of the legislative act (these are called delegated acts). In accordance with the declaration (number 39) issued in Article 290 of the Treaty on the Functioning of the European Union[31], the develop-

[28] Credit institutions, payment institutions, account information service providers, electronic money institutions, investment firms, crypto-asset service providers, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds, management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirement provision, credit rating agencies, administrators of critical benchmarks, crowdfunding service providers and securitisation repositories (in line with art. 2 sec. 1 letter a-t of DORA).

[29] Motive 12 of DORA.

[30] Motive 14 of DORA.

[31] Official Journal of the European Union C 326/47.

ment of regulatory technical standards requires assistance in the form of technical expertise in a form specific to the field of financial services. Therefore, it is envisaged that draft regulatory technical standards will be developed by the relevant ESAs (paragraph 8, 1, respectively, for the individual ESAs)[32]. In accordance with those regulations, the various ESAs, on the basis of legislative acts, are meant to contribute to the establishment of common high quality regulatory and supervisory standards and practices, in particular, by developing regulatory drafts and implementing technical standards, guidelines, recommendations and other measures, including opinions. This entitlement includes the preparation of drafts of Regulatory Technical Standards. As the prerequisite for their preparation, the relevant legislative act should provide for an appropriate delegation, indicating the appropriate supervisory authority to prepare the project. Article 10-14 of the relevant regulations establishing the various European Supervisory Authorities sets out in detail the procedure for working on Regulatory Technical Standards. The regulations also states that regulatory technical standards are purely technical, cannot resolve strategic or policy issues, and that the scope of their content is determined by the legislative acts that underpin them. The process of their development provides for – in principle - open public consultations and analysis of possible costs and benefits. The power to issue these delegated acts is left to the European Commission, which accepts or rejects the drafts. The European Parliament or the Council may object to the Regulatory Technical Standard adopted by the European Commission.

In practice this will shift at least some part of the cybersecurity regulation from soft law issued on the national level by PFA into 'hard law' issued on the EU level. It means that some rules implemented currently on the 'comply or explain' manner became mandatory based on the new regulatory regime.

[32] Regulation No 1093/2010 of 24 November 2010 on the establishment of the European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (Official Journal of the European Union, L 331/12), Regulation 1094/2010 of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (Official Journal of the European Union, L 331/48), and Regulation 1095/2010 of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision 716/2009/EC and repealing Commission Decision 2009/77/ EC (Official Journal of the European Union, L 331/84).

DORA and RTSs will also create new obligations of the financial institutions in the cybersecurity area.

Conclusions

As the soft law is important tool of the regulating the financial market by the supervisory authorities, it can be also used in relation to operational risks associated to activity of financial institutions, including cybersecurity issues and ICT management. Regardless of the constitutional restrictions related to the tools as entities establishing the law, the soft law issued by the Polish Financial Supervisory Authority is well established in practice and accepted in the doctrine. In such situation, there are no real obstacles to implement the 'hard law' in the area of cybersecurity, however after DORA is in force, the soft law shall be in line with DORA and RTSs.

Based on above presented considerations, further studies related to the soft law role in the cybersecurity regulation related to financial institutions in Poland shall be implemented in the future. It is also important to verify to what extend such soft law is in line with proportionality rule included in EU regulations, including DORA, as soft law can be useful tool to take into consideration size and specific of the activity as well as associated risks related to such activity.

Bibliography

Czech T., *Miejsce uchwał Komisji Nadzoru Finansowego w systemie źródeł prawa polskiego*, „Monitor Prawa Bankowego" 2013, No. 7-8.

Dygasiewicz K., Zapadka P., *Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej w czasie gospodarki COVID lub postCOVID w świetle komunikaty Komisji Nadzoru Finansowego,* „Cybersecurity and Law" 2020, No. 1.

Jakubiak A., *Rekomendacja nadzorcza w kontekście regulacji polskich i europejskich*, [in:] *Polityka i praktyka regulacji rynków finansowych*, W. Rogowski [ed.], Kraków-Warszawa 2015.

Milik P., Pilarski G., *Cyberattacks and bank's liability for unauthorized payment transactions in the online banking system – theory and practice*, "Cybersecurity and Law" 2023, No. 1.

Nadolska A., *O „fałszywych" wytycznych EBA i prawdziwym celu nadzorczego soft law w sprawie nadzoru nad produktem i zarządzania nim*, „Przegląd Ustawodawstwa Gospodarczego" 2022, No. 6.

Nadolska A., *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

Ofiarski Z., *Rola soft law w regulacji rynku finansowego na przykładzie rekomendacji i wytycznych Komisji Nadzoru Finansowego*, [in:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, A. Jurkowska-Ziedler, M. Olszak [eds.], Warszawa 2016.

Olszak M., *Wydawanie przez Komisję Nadzoru Finansowego wytycznych dotyczących sektora ubezpieczeniowego jako przykład zintegrowanego podejścia do wykonywania nadzoru nad rynkiem finansowym*, [in:] *Prawo rynku finansowego. Doktryna, instytucje, praktyka*, A. Jurkowska-Ziedler, M. Olszak [eds.], Warszawa 2016.

Pelc P., *„Komunikat chmurowy" Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, No. 2.

Pelc P., *Lekcje dla Polski jako członka NATO ze sposobu prowadzenia działań w cyberprzestrzeni w trakcie rosyjskiej agresji przeciwko Ukrainie*, [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. 25 lat członkostwa w NATO*, Chałubińska-Jentkiewicz, K. Gawkowski, Z. Nowak, Ł. Piątkowski, K. Wąsik [eds.], Gliwice 2024.

Pelc P., *Rekomendacje KNF, czyli kwadratura koła*, „Gazeta Ubezpieczeniowa" 2014, No. 25.

Pelc P., *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, No. 2.

Pelc P., *The Polish Financial Supervision Authority in the national cybersecurity system*, „Cybersecurity and Law" 2023, No. 1.

Pelc P., *Wybrane regulacje dotyczące cyberbezpieczeństwa instytucji finansowych*, „Cybersecurity and Law" 2021, No. 2.

Ustawa o krajowym systemie cyberbpieczeństwa. Komentarz. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec [eds.], Warszawa 2022.

Widawski P., *Zarządzanie ryzykami operacyjnymi i ryzykami dla bezpieczeństwa w wytycznych Europejskiego Urzędu Nadzoru Bankowego i rekomendacji Komisji Nadzoru Finansowego*, [in:] *Cyberbezpieczeństwo, Zarys wykładu*, C. Banasiński [ed.], Warszawa 2023.

Żak M., *Soft law jako instrument koordynacji regulacyjnej good governance*, „Przegląd Legislacyjny" 2019, No. 1.

* * *

Miękkie prawo w regulacjach dotyczących cyberbezpieczeństwa polskich instytucji finansowych

Streszczenie

Zgodnie z polską Konstytucją istnieją ścisłe ograniczenia związane ze stanowieniem prawa, jednak w praktyce powszechnie przyjmuje się, że obowiązujące prawo (tzw. w tym kontekście „twarde prawo") jest uzupełniane tzw. „miękkim prawem" tworzonym również przez podmioty nieuprawnione do stanowienia „twardego prawa" zgodnie z regulacją konstytucyjną. Jedną z takich instytucji jest Komisja Nadzoru Finansowego, która wydaje różne dokumenty o nazwie rekomendacje, wytyczne lub komunikaty, bądź na podstawie specjalnego zezwolenia ustawowego lub wyłącznie na podstawie ogólnych norm kompetencyjnych ustanowionych przez prawo – skierowane do nadzorowanych podmiotów (lub ogólnie lub do poszczególnych sektorów). Niektóre z takich aktów „miękkiego prawa" były związane z zarządzaniem ryzykiem operacyjnym, w tym także kwestiami cyberbezpieczeństwa nadzorowanych instytucji finansowych. Nie zmieniło się to po tym, jak KNF stała się również organem odpowiedzialnym za cyberbezpieczeństwo w sektorze bankowym i infrastruktury finansowej. Również prawo Unii Europejskiej jest uzupełniane wytycznymi europejskich organów nadzoru. Po wejściu w życie Aktu o cyfrowej odporności operacyjnej (DORA) i powiązanych z nim regulacyjnych standardów technicznych (RTS) przynajmniej w części dotychczasowe regulacji o charakterze „miękkiego prawa" zastąpione powyższymi regulacjami prawnymi, jest jednak mało prawdopodobne, aby „miękkie prawo", również w dziedzinie cyberbezpieczeństwa instytucji finansowych, nie było już stosowane.

Celem artykułu jest dokonanie analizy miękkiego prawa, które jest zawarte w regulacjach dotyczących cyberbezpieczeństwa, a dotyczy polskich instytucji finansowych. Podstawowa metoda badawcza to metoda dogmatyczno-prawna, za pośrednictwem której analizie są poddane kwestie cyberbezpieczeństwa instytucji finansowych.

Słowa kluczowe: cyberbezpieczeństwo, miękkie prawo, instytucje finansowe, DORA, RTS.