The Role of Cybersecurity in the Public Sphere - The European Dimension. Financial Institutions

PAWEŁ PELC

Abstract The subject-matter of the analysis includes the state of the EU legal framework and the proposed amendments in the sphere of the cybersecurity of financial institutions operating in European Union Member States, interests protected by law, and the rationale behind regulatory provisions proposed or adopted by EU legislators, notwithstanding their legal form (strategic documents, directives or regulations).

Keywords: • European Union • cybersecurity • financial institutions • financial market • digital resilience

CORRESPONDENCE ADDRESS: Paweł Pelc, Attorney at law, Ph.D. Student, War Studies University in Warsaw, Academic Centre for Cybersecurity Policy, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warszawa, Poland, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

https://doi.org/10.4335/2022.2.4 ISBN 978-961-7124-11-8 (PDF)
Available online at http://www.lex-localis.press.

This analysis discusses the current and planned EU legal regulations governing the cybersecurity of financial institutions, including the assessment of the premises behind selected regulatory solutions, the role of provisions in respect of the cybersecurity of financial institutions in the context of the objectives and directions of regulations concerning financial institutions in the European Union, adopted in the aftermath of the 2007-2008 financial crisis, including the protection of the public sphere against the consequences of threats which affect financial institutions.

Given the specific nature of cyber threats which are usually of a cross-border nature and are not limited to individual jurisdictions, which results in the internationalisation of both attacks and responses, as well as of their impact (both direct and indirect impact through the "contagion effect"), the European Union is becoming increasingly active in enacting legal regulations in this respect. (The current European Union's initiatives in the sphere of cybersecurity have been discussed by Naydenov and Theacharidou, 2021).

In December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented The EU's Cybersecurity Strategy for the Digital Decade (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2020). In the document, it has been found that cybersecurity constitutes an integral part of security, and is essential for building a resilient, green and digital Europe. The authors also pointed to the increased vulnerability of cyber-attacks in relation to switching to remote work due to the COVID-19 pandemic. The risk of targeting critical infrastructure was also noted. The strategy clearly points to the scale of cyber-attacks on the finance sector.

In June 2021, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published their Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade (European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2021). The authors pointed to the key significance of the fastest possible adoption of proposed legal regulations, including the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148, COM (2020) 823, the Proposal for a Directive on the resilience of critical entities, COM (2020) 829, Proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014, COM (2020) 595, and the Proposal for a directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, COM(2020) 596.

The first of the above documents is the European Commission's Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/1148. It is to replace Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information

systems across the Union (NIS Directive) (OJ EU L 194 of 19.7.2016, p. 1) which is the first piece of EU-wide legislation on cybersecurity and provides legal measures to boost the overall level of cybersecurity in the Union (Krueger, Brauchle, 2021: 16-17). According to the Recitals of this Directive: "Operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructure. It covers all operations including the security, integrity and resilience of network and information systems. The requirements in respect of those systems, which often exceed the requirements provided for under this Directive, are set out in a number of Union legal acts, including: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on OTC derivatives, central counterparties and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. Member States should consider those rules and requirements in their application of lex specialis" (OJ EU, L 194 of 19.7.2016, p. 1, Recital 13). The Directive includes, i.a., credit institutions, trading systems and central counterparties in the group of critical sectors it refers to.

In line with the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive EU 2016/114, the draft Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014, COM (2020) 595, subject to concurrent pending legislative procedure, will be considered to be a sector-specific Union legal act with regard to the financial sector entities, and the provisions of the proposed regulation relating to information and communications technology (ICT) risk management measures, the management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third-party risk should apply instead of those set up under the proposed Directive. Member States should continue to include the financial sector in their cybersecurity strategies and national CSIRTs may cover the financial sector in their activities.

The second draft act mentioned in the Report on implementation of the EU's Cybersecurity strategy is the Proposal for a Directive on the resilience of critical entities. The proposal aims to enhance the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities by increasing the resilience of critical entities providing such services. The European Commission has found that, since the EU financial services acquis establishes comprehensive

requirements on financial entities to manage all risks they face, including operational risks and ensuring business continuity, those entities should be treated as equivalent to critical entities, and the proposed Directive would not involve any additional obligations on the part of financial entities (European Commission, 2020b, Recital 15). The proposal indicates the following EU legal regulations addressed to the financial sector taking into account the issues of cybersecurity: Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ EU L 201, 27.7.2012, p. 1), 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 (OJ EU L 173, 12.6.2014, p. 349), Regulation (EU) No. 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No. 648/2012 (OJ EU L 173, 12.6.2014, p. 84), Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (OJ EU L 176, 27.6.2013, p. 1), and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ EU L 176, 27.6.2013, p. 338).

As regards operational risk management in the sphere of the cybersecurity of a number of financial institutions, particular importance can be assigned to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC (OJ EU 337, 23.12.2015, p. 35) ("PSD 2"). It stipulates that payment service providers are responsible for security measures which need to be proportionate to the security risks concerned. They should also establish a framework to mitigate risks and maintain effective incident management procedures. A vital part of this law is the establishment of a regular reporting mechanism, in order to ensure that payment service providers provide the competent authorities, on a regular basis, with an updated assessment of their security risks and the measures that they have taken in response to those risks. The obligation to report major security incidents without undue delay to the competent authorities was also introduced (OJ EU 337, 23.12.2015, p. 35, Recital 91). It was also found that payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud, while a solid growth of Internet payments and mobile payments should be accompanied by a generalised enhancement of security measures which should be compatible with the level of risk involved in the payment service (OJ EU 337, 23.12.2015, p. 35, Recitals 95 and 96). This was the first EU law addressed to the financial sector which expressly set out cybersecurity requirements (Krueger, Brauchle, 2021: 14).

The third draft act indicated in the Report on implementation of the EU's Cybersecurity Strategy is the Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014 and (EU) No. 909/2014 ("DORA"). The said proposal is part of the digital finance package, which is a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. The digital finance package includes a new Strategy on digital finance for the EU financial sector (European Commission, 2020). The European Commission is of the opinion that it is necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities, with a view to deepening the digital risk management dimension of the Single Rulebook. The starting point for the above decisions was the acknowledgement of the existing high level of interconnectedness across financial entities, financial markets and financial market infrastructures, which may result in a situation where localised cyber incidents could quickly spread from any of the Union financial entities to the entire financial system, unhindered by geographical boundaries (European Commission, 2020d, Recital 3). According to the European Commission, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework, as it would ensure consistency with the cybersecurity strategies already adopted by Member States, and allow financial supervisors to be made aware of the cyber incidents affecting other sectors covered by the NIS Directive (European Commission, 2020d, Recital 16). The European Commission also pointed out that the significant consequences of cyber-attacks are amplified when occurring in the financial sector, an area much more at risk of being the target of malicious propagators pursuing financial gains directly at the source (European Commission, 2020d, Recital 42). In line with the proposed regulation, "digital operational resilience" means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly (through the use of services of ICT third-party providers), the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provisions of financial services and their quality ((European Commission, 2020d, Article 3(1)), while "cyber-attack" means a malicious ICT-related incident by means of an attempt to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset perpetrated by any threat actor (European Commission, 2020d, Article 3(9)). The proposed DORA will have a significant impact on cybersecurity measures taken by numerous financial institutions covered by the scope of this regulation, also through the introduction of a requirement to conduct penetration tests affecting a lot of those entities.

The fourth draft act mentioned in the Report on implementation of the EU's cybersecurity strategy is the Proposal for a directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36,

2014/65/EU, (EU) 2015/2366 and EU/2016/2341. It is part of a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. It complements the DORA proposal and the legal regulations on markets in crypto assets currently being developed. It aligns the directives subject to amendment of the provisions included in the DORA proposal. It has been found that the need to ensure the operational resilience of digital operations in the financial sector against ICT risks has become particularly pressing because of the growth in the market of breakthrough technologies, including those related to crypto assets (distributed ledger or similar technology).

In the Digital Finance Strategy for the EU, the European Commission stated that "the future of finance is digital." Therefore, one of the priorities described in the Strategy is to address new challenges and risks associated with digital transformation. The European Commission believes that technology companies are likely to become an integral part of the financial ecosystem, and, as a consequence, the risks are expected to increase, affecting not only customers of financial institutions, but also broader financial stability issues and competition in financial services markets. Therefore, the prudential supervisory perimeter should capture risks arising from platforms' and technology firms' financial services provisions and from techno-financial conglomerates and groups. According to the European Commission, the EU cannot afford to have the operational resilience and security of its digital financial infrastructure and services called into question. There is also a need to minimise the risk of client funds being stolen or their data being compromised. The objective of the European Commission's activities in this respect is to protect end users of digital finance services, to ensure financial stability, to protect the integrity of the EU finance sector and to provide fair conditions for operation.

The requirement to implement appropriate technical and organisational measures in the scope of personal data processing has been imposed on financial institutions under Articles 32-34 of the GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/ 46/EC (General Data Protection Regulation), (OJ EU L 119, 4.5.2016, p 1).

The aforementioned legal regulations are addressed to private organisations running regulated business activities subject to oversight, either at the EU level or in individual Member States. They result from the recognition of their special functions and their impact going beyond the operations of individual institutions. It is a consequence of recognising the special role of the financial market and the need to protect the customers of finance institutions and to ensure the uninterrupted functioning of institutions operating in this market, and the performance of their tasks.

In the opinion of the European Commission, both the organisation of the financial market and the regulation governing its operations need to ensure security of the participants in

this market. Some of the essential components of the market include the provision of access to that market to licensed entities, the oversight of their operations, and prudential requirements (Kosikowski, 2016: 27-38). Significant changes in this respect were introduced in the European Union after the experience of the financial crisis of 2007-2008 (Kosikowski, 2016: 31-38; Monkiewicz, 2016: 59-73; Kluczewska-Rupka, 2015: 91-105). As a consequence of the growing number of cybersecurity threats, legal regulations concerning cybersecurity and critical infrastructure, including sector-specific regulations in this respect referring to financial institutions or their individual categories, were introduced and further expanded. Provisions in the sphere of cybersecurity were included in Regulation (EU) No. 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No. 648/2012 (OJ EU L. 176, 27.6.2013, p. 1), and Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC, as well as PSD 2 and Regulation of the European Central Bank (EU) No. 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (OJ EU L217, 23.7.2014, p. 16), whereas no such explicit cybersecurity rules were provided in Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ EU L335, 17.12.2009, p. 1), 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, Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, 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 (OJ EU L 257, 28.8.2014, p. 1), and Regulation (EC) No. 1060/2009 of the European Parliament and of the Council of 16 September 2009 on credit rating agencies (OJ EU L 302, 17.11.2009, p.1) (Krueger, Brauchle, 2021: 15). The evolution of the financial market, together with its globalisation and cross-border activities, and the growing scale of the interrelations between individual financial institutions, results in an increased risk of volatility in the case of problems of individual financial institutions, expanding across the entire financial market (Nieborak, 2016: 94-112), which might trigger a shift to the so called "real economy". Consequently, the regulations concerning the financial market are aimed to mitigate the risk of impact of the operations of financial institutions in the public sector, including public finance. A good example of such an approach can be found in the solutions included in the Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms, and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations

(EU) No. 1093/2010 and (EU) No. 648/2012, of the European Parliament and of the Council (OJ EU L 173, 12.6.2014, p. 190), in accordance with which recovery and resolution plans should not assume access to extraordinary public financial support or expose taxpayers to the risk of loss (OJ EU L 173, 12.6.2014, p. 190; Recital 31), and a failing institution should be maintained through the use of resolution tools as a going concern with the use, to the extent possible, of private funds (OJ EU L 173, 12.6.2014, p. 190; Recital 46), while an effective resolution regime should minimise the costs of the resolution of a failing institution borne by taxpayers (OJ EU L 173, 12.6.2014, p. 190; Recital 67). Public interest was taken into account in these legal provisions, as a vital element which allows the application of mechanisms set out in relevant EU legal regulations in respect of financial institutions. "(...) Liquidation under normal insolvency proceedings might jeopardise financial stability, interrupt the provision of critical functions, and affect the protection of depositors. In such a case, it is highly likely that there would be a public interest in placing the institution under resolution and applying resolution tools rather than resorting to normal insolvency proceedings. The objectives of resolution should, therefore, be to ensure the continuity of critical functions, to avoid adverse effects on financial stability, to protect public funds by minimising reliance on extraordinary public financial support to failing institutions, and to protect covered depositors, investors, client funds and client assets." (OJ EU L 173, 12.6.2014, p. 190; Recital 45). Given the above, it should be stated that EU regulations addressed to financial institutions, as a rule private market entities, are aimed to protect a broadly understood public sphere, in order to avoid threats to public funds, financial stability, and only after that the interests of clients of such institutions, although the legal provisions are also far reaching in this respect. The European Commission proposed the extension of consumer protection provided for in Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, (OJ EU L133, 22.5.2008, p. 66) by putting forward the Proposal for a Directive of the European Parliament and of the Council on consumer credits, COM/2021/347 final, i.a., due to the consequences of digital transformation (European Commission, 2021, Recitals 3 and 4). The assurance of the digital resilience of financial institutions, including measures to prevent the contagion effect, are part of the activities (Krueger, Brauchle, 2021: 25-26). Similarly, as in the case of supervision mechanisms, where supervisory authorities shifted from oversight based on the assurance of supervised institutions' compliance with applicable regulations to risk-based supervision, the regulations currently being proposed by the European Commission envisage the financial institutions' transfer from assuring compliance with regulations in the scope of security to management based on the assessment of risk and threats related to their operations. This is owing, i.a., to the perception of cyber threats and cyber risks as a systemic risk affecting the financial sector (European Systemic Risk Board, 2020: 2-3 and 22-39). The European Systemic Risk Board noted the following possibility for a cyber-attack to develop into a threat to the stability of the financial system: "From a macroprudential perspective, the ESRB considers the main shocks to be the destruction, encryption or alteration of data related to value. Such shocks could cause a cyber incident to develop

into a systemic event, impairing the provision of key economic functions, generating significant financial losses and undermining confidence in the financial system" (European Systemic Risk Board, 2020: 3), while such risk was also pointed out by Callies and Baumgarten (Callies, Baumgarten 2020: 1150-1151). The perception of issues related to the cybersecurity of financial institutions and respective legal regulations as a vital part of the security of the public sphere is all the more important considering that the attribution of attack sources is not always clear-cut and that such attacks may be an element of cyber war (for instance as part of the so-called hybrid war), cyber espionage, or cyber terrorism, for which public or parastatal actors may be responsible. Even if an attack is classified as a mere cyber offence, it cannot be ruled out that such cyber criminals are supported or at least tolerated by public actors. Consequently, the public security element is particularly visible in the way the issues related to the cybersecurity of financial institutions are regulated in the European Union. This is also demonstrated in the legal basis for EU cybersecurity laws which are based on the provisions of the Treaty on the Functioning of the European Union referring to freedom, security and justice, the freedom of services, and the smooth operation of payment systems (Callies, Baumgarten, 2020: 1163-1164).

Given the above, it can be stated that the regulations concerning the cybersecurity of financial institutions take into account the specific nature and directions of EU laws addressed to financial institutions, so as to protect the public sphere against threats emerging in relation to the activities pursued by such entities. Therefore, the introduction of separate sector-specific regulations addressed to financial institutions, which are to replace general cybersecurity regulations, should be considered as reasonable. Thanks to this, these solutions may take into account the specific risks which occur in the course of financial institutions' operations, and the EU legislator's preferences in the sphere of protected public interest in relation to such risks.

References:

Callies, C. & Baumgarten, A. (2020) Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective, *German Law Journal*, 21(6), pp. 1149-1179.

Kosikowski, C. (2016) Nowe Prawo rynku finansowego Unii Europejskiej, In: Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warsaw: Wolters Kluwer), pp. 27-38.

Kluczewska-Rupka, A. (2015) Dylematy prawne powołania europejskiej Unii Bankowej, In: Rogowski, W. (ed.) *Polityka i praktyka regulacji rynków finansowych* (Kraków-Warsaw: Oficyna Allerhanda), pp. 91-105.

Krueger, P.S. & Brauchle, J.P. (2021) *The European Union Cybersecurity, and the Financial Sector: A Primer* (Washington DC: Carnegie Endowment for International Peace).

Monkiewicz, J. (2016) Unia Bankowa jako zmiana architektury regulacyjnej i nadzorczej rynku finansowego z perspektywy ekonomicznej, In Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warsaw: Wolters Kluwer), pp. 59-73.

Naydenov, R. & Theocharidou, M. (2021) *EU Cybersecurity initiatives in the finance sector* (Athens: European Union Agency for Cybersecurity).

Nieborak, T. (2016) Unia bankowa – w stronę bezpieczeństwa i stabilności rynku finansowego Unii Europejskiej, In: Jurkowska-Zeidler, A. & Olszak, M. (eds.) *Prawo Rynku Finansowego. Doktryna, instytucje, praktyka* (Warsaw: Wolters Kluwer), pp. 94-112.