Redakcja
Konrad Tarłowski

BEZPIECZEŃSTWO JEDNOSTKI I PAŃSTWA W OBLICZU NOWYCH TECHNOLOGII

ARCHAEGRAPH
Wydawnictwo Naukowe

Bezpieczeństwo jednostki i państwa w obliczu nowych technologii

Redakcja
Konrad Tarłowski

Redakcja
Konrad Tarłowski

BEZPIECZEŃSTWO JEDNOSTKI I PAŃSTWA W OBLICZU NOWYCH TECHNOLOGII

ARCHAEGRAPH
Wydawnictwo Naukowe

Redakcja naukowa
mgr Konrad Tarłowski

Recenzenci
prof. dr hab. inż. Piotr Tadeusz Dela
dr Ryszard Mochocki
dr Paweł Falenta
dr Grzegorz Świecarz

Readakcja techniczna
dr Magorzata Budnik-Minierska
mgr Dawid Kobylański

Korekta, skład i projekt okładki
Karol Łukomiak

ISBN: 978-83-68410-79-2

Wersja elektroniczna dostępna na stronie internetowej wydawcy:
www.archaegraph.pl

ARCHAEGRAPH
Wydawnictwo Naukowe

ŁÓDŹ, MAJ 2026

SPIS TREŚCI

Przedmowa

Dynamiczny rozwój nowych technologii oraz zmieniające się uwarunkowania bezpieczeństwa międzynarodowego sprawiają, że współczesne państwo prawa staje wobec wyzwań o szczególnie złożonym charakterze. Niniejsza monografia podejmuje próbę wielowymiarowej analizy relacji zachodzących między postępem technologicznym, funkcjonowaniem systemów prawnych a ochroną fundamentalnych wartości demokratycznych. Zebrane opracowania tworzą spójną refleksję nad sposobami zapewnienia bezpieczeństwa państwa, ochrony infrastruktury krytycznej oraz poszanowania praw i godności jednostki w realiach postępującej transformacji cyfrowej.

W pierwszej części autorzy pochylają się nad strategicznym znaczeniem edukacji w kontekście współczesnych konfliktów technologicznych oraz dokonują systemowej analizy Krajowego Systemu Cyberbezpieczeństwa w obliczu wdrażania dyrektywy NIS2. Refleksja ta znajduje swoje dopełnienie w analizie bezpieczeństwa cyfrowego pracowników zdalnych, co w dobie narastającej cyfryzacji stało się kluczowym elementem stabilności gospodarczej i ochrony danych.

Druga płaszczyzna rozważań dotyczy fundamentów aksjologicznych i procesowych. Autorzy analizują godność człowieka jako źródło wolności religijnej i ochrony areligijności, przypominając, że technologia musi zawsze pozostawać w służbie humanistycznych wartości. W tym kontekście niezwykle istotny staje się głos dotyczący wykorzystania sztucznej inteligencji w procesie sądowym badanie granic między efektywnością zarządzania sprawami a rzetelnością oceny dowodów cyfrowych.

Ostatni moduł monografii przenosi czytelnika w sferę medycyny estetycznej. Przez pryzmat orzecznictwa sądowego i praktyki organów administracji, autorzy kreślą granice kompetencji między lekarzem a kosmetologiem oraz analizują rozszerzone obowiązki informacyjne. Jest to istotny wkład w dyskusję nad tzw. szarą strefą medycyny, gdzie prawo musi nadążać za dynamicznie rozwijającym się rynkiem usług medycznych i potrzebą ochrony pacjenta.

Niniejsze opracowanie jest efektem pracy badaczy, którzy łączą teoretyczną głębię z uważną obserwacją praktyki stosowania prawa. Mamy nadzieję, że publikacja ta stanie się inspiracją do dalszych badań nad rolą prawa w kształtowaniu zdrowia publicznego, bezpieczeństwa obywateli i jakości życia w złożonej rzeczywistości współczesnej Europy.

dr **Michał Słowak**
Badacz niezależny

EDUCATION AS STRATEGIC INFRASTRUCTURE: CLOSING THE EDUCATION-SECURITY GAP IN TECHNOLOGICAL WARFARE

Abstract: Contemporary security environments are increasingly shaped by rapid technological change, where artificial intelligence, autonomous systems, cyber capabilities, and data integration reshape the nature of conflict. While most global players have responded by increasing defence expenditures and accelerating military modernisation, this article argues that such responses remain incomplete. Existing approaches focus predominantly on material capabilities, while overlooking acritical determinant of long-term strategic capacity: the education system. This article conceptualises education as a form of strategic infrastructure, demonstrating how human capital underpins technological capability, military effectiveness, and strategic autonomy. It identifies a persistent misalignment between education and defence policy, defined as the education security gap which generates structural vulnerabilities and increases long-term technological dependence. Building on this framework, the article examines how contemporary conflicts highlight the operational consequences of this gap and outlines a set of targeted policy pathways for improving alignment between education systems and national security requirements. It concludes that future military advantage will depend not only on the acquisition of advanced technologies, but on the systems that produce and sustain them.

Keywords: Strategic infrastructure, education, security, technological warfare.

Introduction

The character of warfare is undergoing a critical transformation. The shift is clearly observable in recent conflicts, most notably in the war between Russia and Ukraine, as well as in other theatres such as the conflicts in Nagorno-Karabakh and the Middle East. These cases demonstrate the increasing centrality of emerging technologies like AI in shaping battlefield dynamics (King, 2024, p.1; Bendett, 2023,

p.1-10). This growing strategic importance of technological dominance is reflected in political discourse, with Vladimir Putin stating that 'whoever becomes the leader in this sphere will become ruler of the world' (Horowitz, 2018, p. 16). The war in Ukraine has been widely described as the first large-scale "drone war" and even a "data-driven" or "AI-enabled" conflict, where both Russia and Ukraine rely extensively on unmanned systems, cyber operations, and real-time intelligence integration (Bendett, 2023, pp. 1-10). Similarly, the 2020 Nagorno-Karabakh war highlighted the decisive impact of unmanned aerial vehicles, with Azerbaijani drone strikes neutralising Armenian air defence systems and ground forces, demonstrating how drone warfare can alter battlefield outcomes through precision, surveillance, and operational speed (Özkan, 2025, pp. 6–8). The conflicts in the Middle East demonstrated how AI-supported targeting and cyber operations are redefining military effectiveness, as well as moving warfare towards speed, adaptability, and technological integration (King, 2024, p.1). Technological advancements are therefore not merely changing traditional military operations, but rather fundamentally reshaping the conditions under which conflicts are conducted and resolved.

In response to this evolving landscape, most states, predominantly operating within traditional paradigms of warfare, have prioritised military modernisation and increased defence spending in order to maintain or enhance their security posture (Horowitz, 2010, pp.10-30). However, looking at global reality, this response remains incomplete in adequately bridging the gap. Much of the existing policy focus is directed towards increasing present material capabilities, like equipment, platforms, and procurement, while comparatively little attention is given to the underlying systems that enable their effective development, deployment, and adaptation. This article argues that one such system, namely education, remains critically under-integrated into contemporary security and military frameworks. While widely recognised as a driver of economic development, education is rarely conceptualised as a core component of national security. Indeed, it constitutes the foundation through which states may ensure sustainable and independent development of their defence ecosystem. As a result of such misalignment, the relationship between human capital development and military capability remains insufficiently addressed in both policy and academic literature. To address this gap, this article advances three core claims. First, it conceptualises education as a form of strategic infrastructure that underpins the generation and sustainment of technological military capability. Second, it identifies a structural misalignment between education and defence policy, referred to as the education-security gap, which creates long-term vulnerabilities in state capacity. For analytical clarity, the education-security gap is operationalised as the

structural misalignment between national education systems and the competency requirements generated by contemporary security environments. It manifests where education policy, talent development mechanisms, and research ecosystems fail to produce the human capital, technological capacity, and innovation ecosystems necessary for strategic autonomy in domains critical to contemporary warfare, such as artificial intelligence, cybersecurity, advanced engineering, and advanced data systems. Third, it outlines a set of targeted policy pathways and propositions through which this gap can be partially addressed in the short to medium term.

Methodologically, the article adopts a qualitative theoretical-analytical approach combining conceptual analysis with comparative policy illustration. It draws on interdisciplinary literature from security studies, political economy, education policy, and military innovation studies in order to examine the relationship between human capital formation and strategic capacity. The argument is further supported by comparative references to selected state approaches, particularly the United States, China, and Israel, where institutional mechanisms linking education, research, and defence are particularly visible. The purpose is not to provide exhaustive case studies, but to identify recurring strategic patterns that demonstrate how education functions as a determinant of technological military capability.

Education as Strategic Infrastructure

The analysis of national security has traditionally prioritised material capabilities, institutional arrangements, and geopolitical positioning. While these dimensions remain essential, the increasing centrality of technology in warfare necessitates a broader conceptualisation of the foundations of state power. In particular, it requires a reassessment of the role of education systems, which have historically been treated as peripheral to security policy. This paper advances the proposition that education should be understood as a form of strategic infrastructure and an active element of the modern military field. Unlike traditional infrastructure such as transport, energy, or communications, education rarely directly enables the movement of goods or information. Instead, it enables the production and reproduction of human capital, which in turn underpins a state's capacity to generate, operate, and adapt technological systems. In the context of contemporary warfare, where effectiveness increasingly depends on technological sophistication and adaptability, this function becomes strategically decisive.

The relationship between human capital and economic performance is well established in the literature (Becker 1993, p.11). However, its role in shaping

national security outcomes remains under-theorised. Existing scholarship on military effectiveness has emphasised organisational factors, doctrine, and technological diffusion but has paid limited attention to the upstream processes through which the necessary knowledge and competencies are produced and instilled. Recent conflicts reinforce the need for this shift in analytical focus. Rather than concentrating solely on the visible outputs of military power, attention must be directed toward the underlying systems that produce them. Military capability should therefore be understood not as an isolated domain, but as the outcome of a broader ecosystem in which education plays a foundational role. Where education systems fail to produce the competencies required for technological warfare, states risk entering a condition of structural dependency and stagnation, even when investing heavily in military modernisation. This perspective does not suggest that education alone determines security outcomes. Rather, it positions it as a necessary condition for the effective generation, sustainment, and advancement of modern military power.

Policy Misalignment and Its Consequences

Beyond the above-mentioned under-theorization of such relationship, the increasing centrality of technology in warfare is not reflected in practice, where education policy and defence policy continue to operate largely in isolation (Fukuyama 2013, pp.347-355). This disconnect is structural (Mazzucato 2013, pp.20-60). At the policy level, defence strategies remain predominantly focused on the acquisition of material capabilities. Education policy continues to be framed primarily in social and economic terms, with limited reference to its strategic function in supporting national security. As a result, the development of critical competencies, particularly in areas such as artificial intelligence, cybersecurity, data analysis, and advanced engineering remains insufficiently integrated into broader security planning. This misalignment is visible in practice. The war in Ukraine, for example, has highlighted the importance of rapid technological adaptation, including the iterative development of drone systems, real-time data processing, and battlefield-level innovation. The large-scale deployment of low-cost unmanned systems has further demonstrated how drone warfare increasingly rewards speed, adaptability, and continuous technological iteration over conventional assumptions of military superiority (Davis, 2025, p.3). These processes rely heavily on decentralised technical expertise and flexible knowledge systems, rather than solely on pre-existing military structures or number of weapons, planes, tanks, or rockets. Concurrently, many states continue to rely on external suppliers for critical technologies, maintenance,

and upgrades (Mazzucato 2013, pp.20-60). While such arrangements may offer short-term efficiency, they introduce long-term dependencies that constrain strategic autonomy. The inability to independently sustain and evolve technological systems reduces a state's capacity to respond to prolonged or high-intensity conflict, as well as to exercise strategic autonomy in doing so. In this context, reliance on external expertise becomes not merely an economic issue, but a security vulnerability, particularly at a time where multipolarity and the fragmentation of the global order pressure states to become increasingly self-reliant and self-sufficient (Edler, 2024, p.429).

The absence of strong institutional linkages between education systems, research ecosystems, and defence sectors further exacerbates this gap. Universities, academic hubs, and research institutions often operate independently of strategic priorities, while defence establishments lack structured mechanisms for integrating civilian technological expertise. This fragmentation limits the translation of knowledge into operational capability, slows the pace of innovation and does not allow the governments to guide its direction. The consequences of this misalignment are cumulative. States that fail to align education with security requirements risk entering a condition in which military capability is increasingly dependent on external inputs, while internal capacity for adaptation remains limited. Furthermore, it undermines the state's ability to mobilise its wider civilian population to a war economy, rendering responses to conflict delayed and piecemeal. Finally, it ignores the opportunity that education offers the state to shape the long-term development of the defence sector whilst preserving the degree of independence necessary for innovation, particularly as technological sovereignty is increasingly understood as a condition for strategic autonomy itself (Torreblanca, 2025, p.1). In other words, it provides a strategic advantage with actors that are not only external to the state, namely internationally, but also domestically, namely the private sector. Over time, this leads to a divergence between nominal and effective power: states may possess advanced systems, but lack the human capital necessary to fully utilise, maintain, or develop them (Goldin and Katz 2008, pp. 1-25), particularly where such response aims to be immediate and sustainable. In this sense, the "education security gap" should be understood not as a secondary policy issue, but as a structural weakness within contemporary models of state capacity. Addressing this gap requires a fundamental shift in how education is positioned within national security frameworks.

Rapid Policy Pathways

Although addressing the education-security gap, and more broadly any gap within the education ecosystem, requires time and long-term structural reform, the analysis presented in this article suggests that meaningful progress can be achieved through a set of targeted, short to medium term interventions. Crucially, these do not require a comprehensive redesign of education systems, but rather a strategic reorientation of existing institutional capacities toward national security and military objectives.

It is posited that a central priority lies in the deliberate shaping of human capital through targeted talent pipelines in areas critical to technological warfare, including artificial intelligence, cybersecurity, data science, and advanced engineering. Rather than relying on the passive outputs of general education systems, states can adopt a more active approach to talent formation by identifying and supporting individuals with high potential in strategically relevant domains (Kania 2017, pp.5-20). Comparative experience demonstrates the effectiveness of such approaches. In the United States of America, initiatives linked to defence and intelligence institutions have increasingly focused on cultivating specialised AI talent through dedicated funding, scholarships, and structured partnerships with universities, most notably through programmes such as the National Defense Science and Engineering Graduate (NDSEG) Fellowship and broader recommendations implemented following the National Security Commission on Artificial Intelligence. Similarly, China has pursued a more centralised model, embedding talent development within its military-civil fusion strategy, and systematically aligning universities, research institutions, and civilian technology firms with long-term technological and military priorities. Beijing's objective is to create an "integrated national strategic system" in which civilian innovation, particularly in artificial intelligence and emerging technologies, directly supports PLA modernisation and future warfighting capabilities (McFaul et.al. 2025, pp. 4-5). In both cases, the key shift lies in moving from generalised education toward the intentional identification of talent and, consequently, the development of skills and capabilities aligned with national security needs. Comparative evidence indicates that i) targeted scholarship schemes, ii) defence-linked graduate pipelines, and iii) relevant talent identification mechanisms represent rapidly deployable policy tools for states seeking to close the education-security gap in the short to medium term.

At the same time, the effectiveness of such efforts depends on the degree of integration between education systems, research ecosystems, and defence

institutions. Strengthening institutional linkages between these sectors therefore represents a critical pathway for enhancing both innovation and adaptability. In the case of the United States, this integration is operationalised through a network of defence-linked innovation institutions, most notably the Defense Advanced Research Projects Agency (DARPA), as well as newer structures such as the Defense Innovation Unit (DIU), which directly connect universities, academic hubs, start-ups, and private-sector actors with defence procurement and experimentation processes. These mechanisms enable rapid prototyping, testing, and deployment of emerging technologies within military contexts. Similarly, Israel has institutionalised this integration through a tightly coupled system linking elite military units, particularly Unit 8200, with the civilian technology sector, creating a continuous pipeline between military training, higher education, and private innovation (Frenkel 2013, pp.80-99). Former members of these units frequently transition into start-ups and research environments, reinforcing a cycle of knowledge transfer between defence and the broader economy (Senor and Singer 2009, pp.40-80). These cases demonstrate that institutional integration is not simply a matter of coordination but can be operationalised through specific organisational structures, such as defence innovation units, joint research programmes, and military-academic pipelines, that states can replicate in order to accelerate the conversion of knowledge into strategic capability.

Finally, strategic advantage in technological warfare increasingly depends on the capacity to identify a relatively small but strategically decisive cohort of individuals with exceptional technical and analytical potential. As Deming argues, higher-order skills are particularly valuable because they shape not only productivity, but also decision-making, task allocation, and adaptation: functions that become disproportionately important in high-skill technological sectors (Deming, 2024, pp. 3-5). While much policy attention is directed toward training and education systems, the process of early talent identification remains comparatively underdeveloped. Yet, empirical evidence suggests that states capable of systematically recognising high-potential individuals at early stages are better positioned to develop advanced technological capabilities. Israel offers a prominent example, where cognitive and technical aptitude assessments conducted during adolescence, most notably through military pre-screening processes, are used to identify candidates for elite units effectively distinguishing and creating pathways for high-potential individuals before formal training begins (Loewenstein, 2023, pp. 112–118). Similarly, China has institutionalised early identification through specialised secondary schools, national competitions, and selective university tracks that

function as filters for top-performing students in STEM fields, often linked to state priorities in science and technology. In the United States, although less centralised, comparable mechanisms exist through national science competitions, specialised STEM high schools, and selective research programmes concentrated in leading universities and defence-linked talent pipelines. Advanced technical talent is further concentrated through graduate fellowships, federally funded research programmes, and university-to-defence pathways that support national security innovation in areas such as artificial intelligence, cybersecurity, and engineering. As Nice argues, maintaining U.S. military-technological advantage increasingly depends on sustaining these science and engineering pipelines within the broader national security innovation base (Nice, 2024, pp. 2–4). These cases suggest that the ability to systematically identify talent through testing, selection mechanisms, and early differentiation constitutes a distinct and critical component of strategic capacity. In policy terms, this implies that states can significantly enhance their long-term technological capabilities not only by improving education systems broadly, but by implementing structured mechanisms for early talent recognition. Such mechanisms optimise the allocation of resources and opportunities, thus accelerating the benefits in an industry whose increasing significance makes short-term and medium-term wins fundamental.

From a policy perspective, while addressing the education-security gap ultimately requires extensive structural reform, the analysis presented in this section demonstrates that meaningful progress can be achieved through a set of practical, medium to short-term interventions. In particular, the development of targeted talent pipelines, the strengthening of institutional linkages between education, research, and defence, and the implementation of structured mechanisms for early talent identification represent actionable policy tools that can be deployed within existing systems. Unlike broader systemic reforms, which are often constrained by political, institutional, financial, and temporal limitations, these measures enable states to begin aligning human capital development with strategic requirements in the near term. As such, they should be understood not as substitutes for long-term transformation, but as immediate levers through which states can enhance their technological capacity and reduce emerging security vulnerabilities.

Conclusion

The transformation of warfare towards technologically intensive and adaptive forms of conflict does not merely require incremental adjustments in military

capability, but a reconfiguration of how states understand the foundations of security itself. This article has argued that contemporary approaches remain incomplete precisely because they focus on visible outputs, platforms, systems, and procurement, while neglecting the underlying structures that determine their effectiveness. By conceptualising education as a form of strategic infrastructure, the analysis shifts attention from what states possess in the present to what they are capable of sustaining and developing over time. In this sense, military power in technological warfare is less of a function of acquisition than of production capacity, specifically, the ability to continuously generate, adapt, and integrate knowledge into operational systems independently. The persistent misalignment between education and defence policy therefore represents not only a policy gap, but a structural limitation on state capacity.

The implications of this shift are significant. As technological competition intensifies, the distinction between technologically advanced and strategically autonomous states is likely to depend increasingly on the organisation of their human capital systems rather than the scale of their defence spending alone. States that fail to align education with strategic priorities risk entering a condition in which they can access advanced technologies but cannot independently sustain or evolve them, nor doing so in a sufficiently fast and large-scale manner. Importantly, this suggests that the future of deterrence may extend beyond traditional measures of military strength. In an environment defined by rapid innovation and adaptation, the credibility of a state's long-term capability may rest as much on its capacity to produce knowledge as on its ability to deploy force. From this perspective, education is not simply a supporting domain of national security, but one of its primary determinants.

Bibliography

Becker G. S.
1993 *Human Capital: A Theoretical and Empirical Analysis*, Chicago.

Bendett S.
2023 *Drone Warfare in Ukraine: Trends and Implications*, CNA Analysis.

Biddle S.
2004 *Military Power: Explaining Victory and Defeat in Modern Battle*, Princeton.

Davis E. A.
2025 *Drones and the Changing Character of War*, „Parameters", no. 55(4).

Deming D. J.
2024 *Skills and Human Capital in the Labor Market*, National Bureau of Economic Research Working Paper, Cambridge, MA.

Edler J.
2024 *Technology Sovereignty of the EU: Needs, Concepts, Pitfalls and Ways Forward*, European Commission.

Frenkel A.
2013 *The Israeli Defence Industry and the Role of Military R&D*, „Journal of Innovation Economics & Management".

Fukuyama F.
2013 *What Is Governance?*, „Governance", no. 26(3).

Goldin C., Katz L. F.
2008 *The Race between Education and Technology*, Cambridge, MA.

Hanushek E. A., Woessmann L.
2015 *The Knowledge Capital of Nations: Education and the Economics of Growth*, Cambridge, MA.

Horowitz M. C.
2010 *The Diffusion of Military Power: Causes and Consequences for International Politics*, Princeton.

2018 *Artificial Intelligence and International Security*, Center for a New American Security.

Kania E. B.
2017 *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, Center for a New American Security.

King A.
2024 *Digital Targeting: Artificial Intelligence, Data, and Military Targeting*, „Journal of Global Security Studies", no. 9(2).

Loewenstein A.
2023 *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World*, London.

Mazzucato M.
2013 *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*, London.

McFaul C., Bresnick S., Chou D.
2025 *Pulling Back the Curtain on China's Military-Civil Fusion: How the PLA Mobilizes Civilian AI for Strategic Advantage*, Center for Security and Emerging Technology.

Nice A.
2024 *Meeting U.S. Defense Science and Engineering Workforce Needs: The Importance of STEM Talent Pipelines*, National Bureau of Economic Research Working Paper, Cambridge, MA.

Senor D., Singer S.
2009 *Start-Up Nation: The Story of Israel's Economic Miracle*, New York.

Torreblanca J. I.
2025 *Defending EU Democracy and Sovereignty from the New Geopolitics of Technology*, „CEBRI Journal", Year 4, No. 16 (Oct–Dec)

Özkan O. E.
2025 *Unmanned Moral Forces: Drones and Information Warfare*, „Small Wars & Insurgencies".

EDUKACJA JAKO INFRASTRUKTURA STRATEGICZNA: ROLA SYSTEMÓW EDUKACJI W WARUNKACH WOJNY TECHNOLOGICZNEJ

Streszczenie: Współczesne uwarunkowania bezpieczeństwa w coraz większym stopniu kształtowane są przez dynamiczne zmiany technologiczne. Sztuczna inteligencja, systemy autonomiczne, zdolności cybernetyczne oraz zaawansowane przetwarzanie danych w istotny sposób zmieniają charakter konfliktów zbrojnych. Państwa reagują na te zmiany przede wszystkim poprzez zwiększanie wydatków obronnych oraz przyspieszoną modernizację sił zbrojnych. Podejście to koncentruje się jednak głównie na zdolnościach materialnych, pomijając kluczowy czynnik długofalowego potencjału strategicznego, jakim jest system edukacji. Artykuł argumentuje, że edukacja stanowi element infrastruktury strategicznej i powinna być traktowana jako jej równorzędny komponent, na równi z innymi kluczowymi obszarami państwa. Oznacza to, że kapitał ludzki stanowi podstawę zdolności technologicznych państwa, jego efektywności militarnej oraz autonomii strategicznej. Jednocześnie między polityką edukacyjną a obronną utrzymuje się wyraźna niespójność, określana jako luka w edukacji i bezpieczeństwie. Prowadzi ona do powstawania strukturalnych słabości oraz zwiększa długoterminową zależność technologiczną. Na tej podstawie artykuł pokazuje, w jaki sposób współczesne konflikty ujawniają praktyczne konsekwencje tej niespójności. Przedstawia również zestaw działań, które mogą pomóc lepiej powiązać system edukacji z potrzebami bezpieczeństwa państwa. W zakończeniu wskazano, że przyszła przewaga militarna będzie zależeć nie tylko od zdolności pozyskiwania zaawansowanych technologii, lecz także od potencjału ich samodzielnego rozwijania, utrzymania i adaptacji.

Słowa kluczowe: Infrastruktura strategiczna, edukacja, bezpieczeństwo, wojna technologiczna.

mgr **Piotr Wojciech Szczepaniak**

Badacz niezależny
ORCID: 0009-0003-3663-9332

KONDYCJA KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA W POLSCE W KONTEKŚCIE WDRAŻANIA DYREKTYWY NIS2 – ANALIZA SYSTEMOWA

Streszczenie: Artykuł analizuje kondycję krajowego systemu cyberbezpieczeństwa w Polsce w kontekście wdrażania dyrektywy NIS 2, wykorzystując analizę systemową jako główną metodę badawczą. Celem opracowania jest ocena struktury instytucjonalnej systemu, mechanizmów współpracy pomiędzy kluczowymi podmiotami oraz identyfikacja ograniczeń funkcjonalnych wpływających na jego skuteczność. Analiza aktów prawnych, dokumentów strategicznych i raportów instytucjonalnych wskazuje, że system osiągnął względną dojrzałość organizacyjną, jednak pozostaje obciążony deficytami w zakresie spójności funkcjonalnej i koordynacji międzysektorowej. Szczególną luką jest niedostateczna integracja ochrony danych osobowych oraz marginalne uwzględnienie roli indywidualnych użytkowników sieci. Zidentyfikowane ograniczenia mogą utrudniać efektywną adaptację systemu do wymogów dyrektywy NIS 2.

Słowa kluczowe: krajowy system cyberbezpieczeństwa, analiza systemowa, cyberbezpieczeństwo państwa, koordynacja instytucjonalna, dyrektywa NIS 2

Wstęp

Współczesny świat charakteryzuje się rosnącą złożonością systemów społecznych, technologicznych i organizacyjnych, które współdziałają na wielu płaszczyznach. Jednym z kluczowych wyzwań XXI wieku jest zapewnienie bezpieczeństwa w przestrzeni cyfrowej, która stała się podstawowym elementem funkcjonowania państw, gospodarek i społeczeństw. Wobec dynamicznego rozwoju technologii

informacyjno-komunikacyjnych, krajowe systemy cyberbezpieczeństwa stanowią krytyczną infrastrukturę, wymagającą skutecznego zarządzania, koordynacji oraz adaptacji do zmieniających się zagrożeń. Analiza systemowa, jako interdyscyplinarna metoda, oferuje unikalne podejście do badania i doskonalenia złożonych systemów. Umożliwia również zrozumienie struktury, dynamiki oraz interakcji w ramach systemów co jest kluczowe dla samego zrozumienia otaczającego nas świata, jak również ich efektywnego zarządzania czy projektowania (Sienkiewicz 1994, s. 15). Metodyka ta pozwala na holistyczne spojrzenie na problematykę, uwzględniając zarówno aspekty techniczne, organizacyjne, jak i społeczne, co czyni ją szczególnie użyteczną w analizie systemów cyberbezpieczeństwa, które przenikają przez każdy aspekt naszego życia.

Celem badawczym artykułu jest ocena dotychczasowej kondycji krajowego systemu cyberbezpieczeństwa w Polsce z perspektywy analizy systemowej, ze szczególnym uwzględnieniem jego struktury instytucjonalnej, mechanizmów współpracy oraz identyfikacji kluczowych ograniczeń funkcjonalnych w kontekście przygotowań do wdrożenia dyrektywy NIS 2.

W badaniu zastosowano analizę systemową jako interdyscyplinarną metodę badawczą, umożliwiającą holistyczną ocenę złożonych systemów. Analizie poddano strukturę krajowego systemu cyberbezpieczeństwa, role i relacje pomiędzy kluczowymi podmiotami, przepływ informacji oraz mechanizmy reagowania na incydenty. Wykorzystano analizę aktów prawnych, dokumentów strategicznych, raportów instytucjonalnych oraz literatury przedmiotu.

Przeprowadzona analiza wskazuje, że krajowy system cyberbezpieczeństwa w Polsce osiągnął względną dojrzałość instytucjonalną, jednak nadal cechuje się ograniczoną spójnością funkcjonalną oraz fragmentaryzacją działań. Szczególnie widoczna jest luka w zakresie koordynacji międzysektorowej oraz niedostateczne uwzględnienie roli indywidualnych użytkowników sieci jako integralnego elementu systemu. Zidentyfikowane ograniczenia mogą utrudniać skuteczne funkcjonowanie systemu w warunkach zaostrzonych wymogów regulacyjnych wynikających z dyrektywy NIS 2.

Wyniki badania mogą zostać wykorzystane w procesie doskonalenia krajowego systemu cyberbezpieczeństwa, w szczególności przy projektowaniu rozwiązań organizacyjnych i regulacyjnych związanych z wdrożeniem dyrektywy NIS 2. Analiza może stanowić również punkt odniesienia dla decydentów publicznych oraz podmiotów odpowiedzialnych za koordynację działań w obszarze cyberbezpieczeństwa.

Oryginalność badań polega natomiast na zastosowaniu analizy systemowej do oceny kondycji krajowego systemu cyberbezpieczeństwa w Polsce, z naciskiem na relacje pomiędzy jego elementami oraz identyfikację systemowych luk funkcjonalnych. Artykuł wykracza poza opis formalnoprawny, oferując syntetyczną diagnozę zdolności adaptacyjnej systemu w obliczu nadchodzących zmian regulacyjnych.

Model krajowego systemu cyberbezpieczeństwa – ujęcie systemowe

Krajowy system cyberbezpieczeństwa w Polsce stanowi złożoną strukturę instytucjonalno-prawną, której architektura została ukształtowana na gruncie dyrektywy NIS z 2016 roku (Dyrektywa NIS 2016), a obecnie podlega dostosowaniu do wymagań dyrektywy NIS2 przyjętej w 2022 roku (Dyrektywa NIS2 2022). Z perspektywy analizy systemowej, system ten obejmuje wyodrębnione elementy funkcjonalne, zarówno po stronie administracji publicznej, jak i sektora prywatnego, które pozostają ze sobą w relacjach organizacyjnych i operacyjnych. Obejmują one zależności pionowe, związane z nadzorem i przekazywaniem informacji, oraz poziome, polegające na współpracy instytucji i wymianie danych. Całość dopełniają mechanizmy zarządzania oraz sprzężenia zwrotne, umożliwiające dostosowywanie działania systemu do zmieniających się zagrożeń i potrzeb operacyjnych.

Kluczowym aktem normatywnym jest ustawa o krajowym systemie cyberbezpieczeństwa (KSC) z 2018 r., która określa strukturę organizacyjną systemu oraz obowiązki jego uczestników. Na poziomie elementów systemowych, ustawa wyróżnia m.in. operatorów usług kluczowych (OUK) oraz dostawców usług cyfrowych, którzy należą do sektorów o znaczeniu strategicznym. Ich zadaniem jest stosowanie środków technicznych i organizacyjnych adekwatnych do zidentyfikowanego ryzyka, monitorowanie zagrożeń oraz zgłaszanie incydentów poważnych i krytycznych do właściwych organów (Ustawa o KSC 2018). OUK i usługodawcy cyfrowi pełnią zatem funkcję czujników systemowych i punktów wejścia danych operacyjnych do krajowego systemu bezpieczeństwa.

Rolę procesorów informacji i centralnych węzłów reakcji pełnią trzy zespoły CSIRT poziomu krajowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON, zróżnicowane sektorowo. Ich zadania obejmują analizę i obsługę incydentów, komunikację z operatorami, a także współpracę między sobą i z partnerami zagranicznymi, co tworzy sieć relacji poziomych o charakterze informacyjno-operacyjnym (Ustawa o KSC 2018). CSIRT-y działają w strukturze rozproszonej, ale skoordynowanej i pełnią rolę modułów przetwarzających dane zakłóceń w systemie i przekazujących informacje do wyższych poziomów decyzyjnych.

Funkcję zarządzającą pełni Minister Cyfryzacji jako Pełnomocnik Rządu ds. Cyberbezpieczeństwa, który odpowiada za koordynację polityki w całym systemie. W jego strukturze funkcjonuje Pojedynczy Punkt Kontaktowy, będący interfejsem między systemem krajowym a siecią CSIRT-ów i organami współpracy transgranicznej w UE, co stanowi kanał sprzężenia z otoczeniem międzynarodowym (Ustawa o KSC 2018).

System uzupełniają organy właściwe ds. cyberbezpieczeństwa , czyli ministrowie i regulatorzy sektorowi, sprawujący nadzór nad operatorami usług kluczowych w przypisanych obszarach. Ich zadania obejmują kontrolę zgodności z przepisami KSC, co w strukturze systemu odpowiada funkcji mechanizmów nadzorczych i audytowych (Ustawa o KSC 2018).

Całość tworzy rozbudowany system modularny, oparty na wielu współzależnych komponentach, których skuteczność zależy od spójności regulacyjnej, interoperacyjności operacyjnej oraz zdolności adaptacyjnych.

Jednak przy bliższej analizie struktury systemu ujawnia się istotna luka funkcjonalna – brak formalnego i pełnego włączenia ochrony danych osobowych jako komponentu systemowego.

Geneza wyodrębnienia instrumentów ochrony danych osobowych jako odrębnej osi regulacyjnej wynikała z dwóch kluczowych przesłanek systemowych. Po pierwsze, z ograniczonej skuteczności klasycznych mechanizmów ochrony prywatności (cywilnych i karnoprawnych), nieprzystających do realiów przetwarzania danych w erze cyfrowej. Po drugie, z przyjęcia założenia, że środki o charakterze publicznoprawnym (w tym nadzór administracyjny, obowiązki notyfikacyjne, sankcje) stanowią właściwą i proporcjonalną odpowiedź na zagrożenia związane z masowym i zautomatyzowanym przetwarzaniem danych (Safian 2002). Współczesne wyzwania wymagają jednak pójścia o krok dalej, ochrona danych osobowych powinna zostać trwale zintegrowana z systemem cyberbezpieczeństwa jako jego funkcjonalny komponent, a nie jedynie równoległy reżim regulacyjny. Znaczenie systemowe ochrony danych osobowych wywodzącej się z fundamentalnego prawa człowieka do poszanowania życia prywatnego jest niepodważalne. Dane osobowe stanowią nie tylko częsty wektor ataku, lecz także bezpośredni obiekt szkód systemowych w wyniku incydentów cybernetycznych (ENISA 2025).

Cyberbezpieczeństwo i ochrona danych osobowych, choć formalnie uregulowane w odrębnych reżimach prawnych, odpowiednio w ustawie o KSC (Ustawa o KSC 2018) oraz w unijnym Rozporządzeniu 2016/679 (RODO 2016) i krajowej ustawie o ochronie danych osobowych (Ustawa o ochronie danych 2018), w praktyce systemowej przenikają się i pozostają funkcjonalnie współzależne. Z punktu widzenia

analizy systemowej relacja pomiędzy reżimem cyberbezpieczeństwa a ochroną danych osobowych ujawnia istnienie równoległych podsystemów regulacyjnych, pomiędzy którymi brak jest formalnie domkniętych mechanizmów koordynacyjnych.

Zgodnie z art. 33 RODO, administratorzy danych zobowiązani są do zgłoszenia naruszenia do organu nadzorczego (Prezesa UODO) w terminie 72 godzin od jego wykrycia, o ile incydent może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych (RODO 2016). Jednocześnie ustawa o KSC nakłada na te same podmioty obowiązek raportowania incydentu do właściwego zespołu CSIRT (Ustawa o KSC 2018). Powstaje zatem sytuacja podwójnego obowiązku notyfikacyjnego, który wymaga sprawnej koordynacji działań zarówno wewnątrz organizacji (pomiędzy działami IT a inspektorem ochrony danych), jak i na poziomie instytucjonalnym, pomiędzy strukturami cyberbezpieczeństwa a organami ochrony danych.

Mimo tej oczywistej współzależności, Urząd Ochrony Danych Osobowych nie został formalnie włączony w strukturę krajowego systemu cyberbezpieczeństwa i nie pełni roli organu właściwego ani nie uczestniczy w krajowym mechanizmie reagowania na incydenty (Ustawa o KSC 2018). W praktyce jednak współpraca między UODO a zespołami CSIRT okazuje się kluczowa zwłaszcza w przypadku incydentów o charakterze złożonym, obejmujących zarówno naruszenie poufności danych, jak i zakłócenie ciągłości działania systemów. W takich sytuacjach niezbędne jest jednoczesne opanowanie skutków technicznych oraz spełnienie wymogów prawnych, w tym dokonanie stosownych zgłoszeń, podjęcie działań naprawczych i poinformowanie osób, których dane zostały naruszone (RODO 2016; Ustawa o ochronie danych 2018).

Brak sformalizowanych kanałów współpracy, wspólnych procedur lub interoperacyjnych narzędzi wymiany informacji między UODO a CSIRT-ami stanowi realną lukę systemową, ograniczającą zdolność państwa do skoordynowanej i efektywnej reakcji na naruszenia z pogranicza dwóch reżimów. W perspektywie systemowej oznacza to istnienie niedomkniętego obiegu sprzężeń zwrotnych, osłabiającego spójność całego mechanizmu ochrony cyberprzestrzeni i prywatności obywateli.

Powyższe obserwacje potwierdzają, że krajowy system cyberbezpieczeństwa w Polsce charakteryzuje się relatywnie wysokim poziomem instytucjonalizacji i regulacyjnego wykształcenia, jednak nie jest wolny od wewnętrznych niespójności oraz braków integracyjnych, zwłaszcza w obszarach styku z ochroną danych osobowych. Na poziomie strukturalnym system ten prezentuje wysoki stopień dojrzałości, co znajduje odzwierciedlenie w międzynarodowych zestawieniach i analizach porównawczych.

W świetle danych zawartych w Global Cybersecurity Index 2024, opracowywanym przez Międzynarodową Unię Telekomunikacyjną (ITU), Polska została sklasyfikowana w drugiej grupie państw (T2), osiągając łączny wynik 93,54 punktu (ITU 2024). W kategorii „środki organizacyjne", odnoszącej się bezpośrednio do dojrzałości instytucjonalno-strukturalnej systemów cyberbezpieczeństwa, uzyskała 16,66 punktu, co plasuje ją w czołówce państw Unii Europejskiej. Wyższe noty w tej kategorii przypadły jedynie państwom zaliczanym do pierwszej grupy (T1), takim jak Niemcy, Francja czy Szwecja.

Na tle unijnego środowiska regulacyjnego polski system cyberbezpieczeństwa jawi się więc jako zaawansowany organizacyjnie, oparty na ugruntowanych ramach prawnych i instytucjonalnych. Jednocześnie nie pozostaje on wolny od wyzwań związanych z adaptacją do najnowszych standardów europejskich. Dyrektywa NIS2, która weszła w życie 18 października 2024 r., znacząco podnosi poprzeczkę wymagań wobec państw członkowskich, zarówno poprzez rozszerzenie katalogu podmiotów objętych regulacją, jak i przez wzmocnienie mechanizmów nadzoru oraz odpowiedzialności (Dyrektywa NIS2 2022).

Współpraca i mechanizmy reakcji w systemie cyberbezpieczeństwa

Skuteczność krajowego systemu cyberbezpieczeństwa w dużej mierze warunkowana jest jakością współpracy między kluczowymi interesariuszami: instytucjami publicznymi, służbami odpowiedzialnymi za bezpieczeństwo, regulatorami sektorowymi, operatorami infrastruktury krytycznej, a także organami właściwymi dla obszarów powiązanych, takich jak ochrona danych osobowych. Jednym z podstawowych narzędzi służących praktycznej weryfikacji zdolności współdziałania i reagowania na incydenty są ćwiczenia symulacyjne.

W polskich realiach istotną rolę odgrywają między innymi cykliczne ćwiczenia Cyber-EXE Polska, które pełnią funkcję unikalnego forum współpracy międzysektorowej. Inicjatywa ta skupia przedstawicieli administracji publicznej, sektora finansowego, energetycznego, telekomunikacyjnego oraz operatorów usług kluczowych, umożliwiając przećwiczenie rzeczywistych scenariuszy zagrożeń w warunkach kontrolowanych. Ćwiczenia te służą zarówno identyfikacji luk w procedurach współpracy, jak i ocenie funkcjonowania mechanizmów komunikacji operacyjnej pomiędzy komponentami systemu. W efekcie umożliwiają one wytwarzanie oraz weryfikację sprzężeń zwrotnych istotnych dla dalszej adaptacji krajowego systemu cyberbezpieczeństwa. Dzięki temu możliwa staje się diagnoza poziomu gotowości systemu w wymiarze praktycznym, z uwzględnieniem dynamiki reakcji, efektywności

koordynacji oraz odporności instytucjonalnej. Do najczęściej identyfikowanych wyzwań należą m.in. niedoskonałości w zakresie koordynacji między CSIRT-ami sektorowymi a operatorami usług kluczowych, a także brak spójnych protokołów reagowania i wymiany informacji w sytuacjach wielopłaszczyznowych incydentów (Fundacja Bezpieczna Cyberprzestrzeń, 2025).

Obszarem, który nadal wymaga pogłębionej integracji, pozostaje współpraca między podmiotami odpowiedzialnymi za cyberbezpieczeństwo a instytucjami realizującymi zadania w zakresie ochrony danych osobowych. Urząd Ochrony Danych Osobowych, jak wcześniej wskazano, nie został formalnie włączony do struktury krajowego systemu cyberbezpieczeństwa, pomimo odgrywania kluczowej roli w przypadku incydentów naruszających prywatność obywateli oraz integralność danych osobowych.

W ostatnich latach zauważalna jest rosnąca potrzeba zacieśnienia współpracy pomiędzy UODO a zespołami CSIRT oraz innymi elementami systemu KSC. W toku seminarium eksperckiego pt. „Ochrona danych jako element odporności społeczeństwa i państwa", które odbyło się w październiku 2024 r., wielokrotnie podkreślano, że ochrona danych osobowych powinna stanowić integralny komponent bezpieczeństwa państwa. Wskazywano również, że słabym ogniwem systemu bywa często czynnik ludzki, zwłaszcza w kontekście przestrzegania procedur oraz reagowania na naruszenia. Dyskusje eksperckie koncentrowały się m.in. na potrzebie wypracowania efektywnych mechanizmów wymiany informacji między UODO a CSIRT-ami, szczególnie w zakresie incydentów obejmujących naruszenia danych osobowych. Pojawiła się propozycja utworzenia stałych kanałów komunikacji operacyjnej pomiędzy UODO a CSIRT NASK, które umożliwiałyby szybszą reakcję, dwustronne przekazywanie informacji o zagrożeniach oraz zwiększenie skuteczności działań naprawczych. Zwrócono również uwagę na potencjał, jaki tkwi w funkcji Inspektorów Ochrony Danych, zwłaszcza w dużych organizacjach, gdzie mogliby pełnić rolę łączników między sferą cyberbezpieczeństwa a strukturami ochrony prywatności. Uczestnicy zgodzili się, że rozwój współpracy z zespołami CSIRT mógłby znacząco usprawnić obieg wiedzy o podatnościach i incydentach zachodzących na styku cyberbezpieczeństwa i ochrony danych osobowych (UODO 2024).

Również Najwyższa Izba Kontroli zwróciła uwagę na niedostatki w zakresie współpracy międzysektorowej w obszarze cyberbezpieczeństwa. W raporcie opublikowanym w 2022 r. NIK wskazała, że w latach 2019–2021 działania rządu koncentrowały się głównie na ochronie infrastruktury krytycznej, podczas gdy zabrakło kompleksowych inicjatyw nakierowanych na bezpieczeństwo indywidualnych użytkowników Internetu. Obywatele nie zostali objęci systematycznymi progra-

mami edukacyjnymi ani informacyjnymi dotyczącymi zagrożeń w cyberprzestrzeni, co ujawniło istotną słabość systemu na poziomie społecznym (NIK 2022).

Z perspektywy współpracy instytucjonalnej oznacza to, że kanały komunikacji między państwem a społeczeństwem w zakresie cyberbezpieczeństwa nie funkcjonowały w sposób wystarczająco zorganizowany ani efektywny. NIK wskazała m.in. na Ministerstwo Cyfryzacji oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa jako podmioty, które nie podjęły adekwatnych działań informacyjnych ani organizacyjnych, mimo rosnącego zagrożenia ze strony cyberprzestępczości wymierzonej w osoby prywatne. Zwrócono przy tym uwagę, że organy te nie traktowały ochrony obywateli w sieci jako elementu mieszczącego się w zakresie ich bezpośredniej odpowiedzialności (NIK 2022).

Zidentyfikowane przez NIK deficyty wskazują na brak spójnego, międzysektorowego podejścia do bezpieczeństwa społeczeństwa cyfrowego. O ile ochrona infrastruktury państwowej została objęta klarownym nadzorem i priorytetem strategicznym, o tyle obszar ochrony obywateli pozostał rozproszony pomiędzy różne instytucje, takie jak Ministerstwo Cyfryzacji, UODO, Policja czy system oświaty, bez wyraźnego lidera ani skoordynowanego programu działań. Tego rodzaju luka systemowa osłabia zdolność państwa do budowania odporności społecznej na zagrożenia w cyberprzestrzeni, a tym samym wpływa negatywnie na integralność całego systemu bezpieczeństwa cyfrowego (CyberDefence24 2022).

W ostatnich latach podjęto szereg działań zmierzających do poprawy jakości współpracy międzysektorowej. Istotnym krokiem było utworzenie Centralnego Biura Zwalczania Cyberprzestępczości w strukturze Policji, które od stycznia 2022 r. pełni rolę wyspecjalizowanej jednostki odpowiedzialnej za obsługę zgłoszeń dotyczących przestępstw internetowych. Powstanie CBZC wzmocniło zdolności operacyjne organów ścigania i umożliwiło lepszą współpracę z administracją cyberbezpieczeństwa oraz sektorem prywatnym. Biuro skoncentrowało się na pozyskiwaniu specjalistów IT, kampaniach informacyjnych oraz wdrożeniu ujednoliconych procedur przyjmowania zawiadomień o cyberprzestępstwach, co zostało pozytywnie ocenione przez NIK (CyberDefence24 2022).

Również UODO aktywniej uczestniczy w debacie o cyberbezpieczeństwie, sygnalizując potrzebę uwzględnienia perspektywy ochrony danych w politykach publicznych oraz konsultując projekty strategiczne. Wspólne inicjatywy, takie jak kampania informacyjna Ministerstwa Cyfryzacji i NASK dotycząca dezinformacji, wskazują na proces zbliżania się sektorów, które przez lata działały relatywnie niezależnie – od ochrony infrastruktury, przez przeciwdziałanie cyberprzestępczości, po edukację cyfrową (PoradyODO 2025).

Pomimo postępu, nadal występują jednak wyzwania związane z brakiem interoperacyjnych mechanizmów wymiany informacji, np. między CSIRT-ami a Policją czy UODO, a także z niejednoznacznością kompetencji instytucjonalnych. Współpraca międzysektorowa staje się jednak warunkiem koniecznym w obliczu zagrożeń, które nie respektują administracyjnych podziałów kompetencji. Zintegrowane, zespołowe podejście systemowe jest dziś niezbędne dla zapewnienia odporności państwa w cyberprzestrzeni.

Luki i ograniczenia funkcjonowania systemu

Pomimo postępów w budowie krajowego systemu cyberbezpieczeństwa, liczne wyzwania i luki nadal ograniczają jego efektywność. Analiza krytyczna ujawnia trzy główne kategorie problemów: luki legislacyjne, niedostatki kadrowe/organizacyjne oraz ograniczenia technologiczne/infrastrukturalne.

Pierwszym problemem jest niepełne dostosowanie obowiązujących regulacji do zmieniającego się pejzażu zagrożeń. Przykładem jest opóźnienie we wdrożeniu dyrektywy NIS2 (Dyrektywa NIS2 2022), mimo że termin implementacji minął w październiku 2024 r. czy też brak aktualizacji strategii cyberbezpieczeństwa RP od 2019 r (Rada Ministrów, 2019). Kolejną luką jest brak kompleksowej strategii uwzględniającej ochronę indywidualnych użytkowników. Ustawa o KSC koncentruje się na operatorach kluczowych i infrastrukturze, ale nie definiuje jasno odpowiedzialności za bezpieczeństwo „przeciętnego obywatela" w sieci (Ustawa o KSC 2018). W monitorowaniu zagrożeń i w ocenach ryzyka pomijano perspektywę obywateli, przez co działania informacyjne rządu nie były do nich adresowane. Konsekwencją tego jest między innymi niska zgłaszalność incydentów przez poszkodowanych obywateli oraz ich niska wiedza, co robić w razie cyberataku (NIK 2022). Takie zaniedbanie strategiczne jest poważną luką, system okazał się jednostronny, efektywny w ochronie infrastruktury państwowej, ale nieskuteczny w ochronie społeczeństwa jako całości.

Kolejny istotny obszar problemowy dotyczy zasobów ludzkich i organizacyjnych. Sektor cyberbezpieczeństwa zmaga się z chronicznym niedoborem wykwalifikowanych specjalistów, zarówno w administracji publicznej, jak i sektorze prywatnym. W przypadku instytucji państwowych barierą jest ograniczona konkurencyjność wynagrodzeń oraz sformalizowane procedury naboru. Najwyższa Izba Kontroli wskazuje, że trudności te dotyczyły m.in. tworzonego od podstaw Centralnego Biura Zwalczania Cyberprzestępczości, które, aby przyciągnąć kandydatów, musiało oferować dodatkowe świadczenia finansowe. Mimo to tempo rozbudowy formacji pozostaje

niższe od zakładanego (CyberDefence24 2023). Aktualna sytuacja płacowa również nie sprzyja pozyskiwaniu i utrzymywaniu specjalistów, wynagrodzenie funkcjonariuszy zajmujących się zwalczaniem cyberprzestępczości waha się od od ok. 6 500 zł brutto miesięcznie, zależnie od stanowiska i stażu służby. Są to kwoty niewspółmierne do stawek oferowanych w sektorze prywatnym dla osób o porównywalnych kwalifikacjach technicznych i poziomie odpowiedzialności (CBZC 2025), co skutkuje wysoką rotacja personelu i przechodzeniem do sektora prywatnego, oferującego atrakcyjniejsze warunki zatrudnienia.

Kolejnym problemem są ograniczenia technologiczne i infrastrukturalne, choć Polska rozwija zaawansowane systemy umożliwiające automatyczną identyfikację zagrożeń na dużą skalę, takie jak między innymi ARAKIS GOV (CSIRT GOV, b.d.), wciąż istnieją luki w pokryciu wszystkich sektorów i podmiotów nowoczesnymi rozwiązaniami. Najwyższa Izba Kontroli w kwietniu 2025 roku opublikowała wyniki kontroli poświęconej cyberbezpieczeństwu w jednostkach samorządowych. Kontrola objęła przede wszystkim gminy i powiaty – i ujawniła aż 222 nieprawidłowości, z czego tylko 51 zostało usuniętych na etapie postępowania kontrolnego (NIK 2025). Wśród najważniejszych ustaleń kontroli znalazły się między innymi:

- brak systemów monitorowania i planów ciągłości działania: 71 % urzędów nie posiadało planu na wypadek przerwy w funkcjonowaniu systemów teleinformatycznych, co skutkowało brakiem przygotowania na ataki, awarie czy incydenty IT;
- niewystarczające zabezpieczenia podstawowe: wiele jednostek nie wdrożyło prostych, lecz kluczowych mechanizmów – takich jak system zarządzania bezpieczeństwem informacji (SZBI), aktualizacje oprogramowania, przeglądy zabezpieczeń czy szyfrowanie komunikacji, co znacznie osłabiło ich odporność na ataki;
- luki kadrowo-organizacyjne i edukacyjne: urzędy nie przeprowadzały regularnych szkoleń z zakresu cyberbezpieczeństwa, a audyty wykonywano nieskutecznie lub zupełnie pomijano je w wielu przypadkach (NIK 2025).

Infrastruktura państwowa coraz wyraźniej mierzy się także z wyzwaniem skalowalności systemu reagowania na incydenty cyberbezpieczeństwa. Zgodnie z danymi zawartymi w raporcie CERT Polska za 2024 r., skala zagrożeń w cyberprzestrzeni systematycznie rośnie, w 2024 r. zarejestrowano ponad 111 tys. potwierdzonych incydentów cyberbezpieczeństwa, co oznacza wzrost o ok. 23% w ujęciu rok do roku. Jednocześnie do zespołów reagowania trafiały setki tysięcy zgłoszeń, z których każdego dnia analizowano i neutralizowano setki zagrożeń, zapobiegając zakłóceniom

funkcjonowania instytucji publicznych oraz infrastruktury krytycznej państwa (Ministerstwo Cyfryzacji 2025).

Tak wysoka i rosnąca liczba incydentów generuje istotne obciążenie dla dostępnych zasobów operacyjnych i analitycznych, co powoduje konieczność priorytetyzacji obsługi zdarzeń. W praktyce oznacza to, że bez odpowiednio rozwiniętej infrastruktury analitycznej oraz automatyzacji procesów detekcji i reakcji, część incydentów o niższym poziomie krytyczności może pozostać nieobsłużona lub obsłużona z opóźnieniem, co zwiększa ryzyko kumulacji zagrożeń w dłuższym horyzoncie czasowym.

Raport NIK dostarcza również konkretnych danych potwierdzających skalę problemu. Szczególnie alarmujące są ustalenia dotyczące skuteczności organów ścigania: aż 85% cyberataków zgłoszonych przez obywateli pozostało niewyjaśnionych, sprawy umorzono lub zakończono bez wykrycia sprawców, co często wiązało się z realnymi stratami finansowymi i utratą danych. Tylko 2% postępowań zakończyło się identyfikacją i skazaniem sprawcy (NIK 2022). Tak niski wskaźnik skuteczności dowodzi niskiej sprawczości systemu w zakresie walki z cyberprzestępczości, co w połączeniu ze wzrastającą skalą może prowadzić do rosnącego poczucie bezkarności wśród sprawców.

Jednocześnie należy zaznaczyć, że część wcześniej zidentyfikowanych niedoskonałości, zwłaszcza w zakresie braku skutecznych mechanizmów informowania obywateli i ostrzegania społeczeństwa o istotnych zagrożeniach cyberbezpieczeństwa, została częściowo uwzględniona w uchwalonej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (Ministerstwo Cyfryzacji 2026). Nowe przepisy nakładają na podmioty kluczowe i ważne obowiązek informowania użytkowników ich usług o incydentach i zagrożeniach, które mogą mieć wpływ na ciągłość lub jakość świadczeń. Dodatkowo organy właściwe ds. cyberbezpieczeństwa zyskały uprawnienie do wydania decyzji nakazującej publikację ostrzeżeń kierowanych do społeczeństwa, w szczególności w sytuacjach zwiększonego ryzyka lub zagrożeń o charakterze systemowym (Ministerstwo Cyfryzacji 2026)

Choć rozwiązania te nie stanowią jeszcze kompleksowej strategii ochrony „cyfrowego obywatela" i nadal są silnie osadzone w logice ochrony usług oraz infrastruktury, to jednak oznaczają istotne przesunięcie akcentu z wyłącznie infrastrukturalnego podejścia na częściowe uwzględnienie interesu użytkowników końcowych. W tym sensie nowelizacja może być postrzegana jako krok w kierunku modelu cyberbezpieczeństwa, w którym społeczeństwo nie pełni już wyłącznie roli biernego odbiorcy ochrony, lecz staje się aktywnym uczestnikiem działań informacyjnych i prewencyjnych podejmowanych przez państwo.

Społeczeństwo jako element systemu cyberbezpieczeństwa

Świadomość użytkowników i edukacja cyfrowa odgrywają kluczową rolę w kształtowaniu odporności cyberprzestrzeni. Nawet najbardziej zaawansowane regulacje i technologie nie zapewnią skuteczności, jeśli obywatele nie znają podstawowych zasad cyberhigieny. Dlatego edukacja społeczna stanowi jeden z filarów strategii cyberbezpieczeństwa, zarówno w Polsce, jak i w innych krajach UE. Przykładem pozytywnej inicjatywy jest kampania społeczna „Jak nie dać się trollom?", poświęcona walce z dezinformacją (Ministerstwo Cyfryzacji / NASK, 2024). Zjawisko to, zwłaszcza w kontekście wojny w Ukrainie i pandemii COVID-19, stało się istotnym zagrożeniem dla porządku demokratycznego. Polska była i jest celem wrogich kampanii informacyjnych, głównie ze strony Rosji (Służby Specjalne, b.d.). Z badań GLOBSEC (2024) wynika, że 90% Polaków dostrzega to zagrożenie, jednak nadal około 20% społeczeństwa pozostaje podatne na przekazy antyunijne i prorosyjskie (GLOBSEC 2024). Wbrew obawom o tzw. bańki informacyjne, najnowsze badania sugerują, że rzetelna wiedza może ograniczać polaryzację. Eksperyment opublikowany w Nature Communications (2025) wykazał, że osoby konfrontowane z obiektywnymi faktami (także tymi podważającymi ich przekonania) były skłonne do rewizji poglądów, a efekt ten utrzymywał się nawet po miesiącu (Stagnaro & Amsalem 2025). Obok walki z dezinformacją kluczowe znaczenie mają również działania z zakresu codziennej cyberhigieny, w szczególności właściwe zabezpieczanie kont użytkowników. Microsoft potwierdza, że konta chronione mechanizmami wieloskładnikowego uwierzytelniania (MFA) są o ponad 99% mniej podatne na ataki niż te zabezpieczone wyłącznie hasłem. (GS Services, 2025).

Na styku edukacji i praw obywatelskich pojawia się idea „Cyberkarty Praw Człowieka", propozycja systemowego ujęcia praw przysługujących obywatelom w przestrzeni cyfrowej. UE wykonała już pierwszy krok w tym kierunku, przyjmując w 2022 r. Europejską Deklarację Praw i Zasad Cyfrowych, która ma zapewnić, by transformacja cyfrowa przebiegała zgodnie z fundamentalnymi wartościami Unii i z poszanowaniem praw jednostki (Komisja Europejska 2025).

Wnioski i implikacje systemowe

Analizując całościowo kondycję polskiego systemu cyberbezpieczeństwa, można stwierdzić, że znajduje się on w fazie intensywnej przemiany i dostosowywania do nowych realiów zagrożeń oraz regulacji. W kontekście legislacyjnym najważniejszym punktem zwrotnym jest wspomniana nowelizacja ustawy o KSC implementująca

dyrektywę NIS2. Nowe przepisy przewidują przede wszystkim istotne rozszerzenie zakresu podmiotowego systemu cyberbezpieczeństwa poprzez wprowadzenie kategorii podmiotów kluczowych i ważnych, objętych jednolitymi, bardziej rygorystycznymi obowiązkami w zakresie zarządzania ryzykiem, środków organizacyjnych i technicznych oraz raportowania incydentów. Ustawa wzmacnia kompetencje organów właściwych i zespołów CSIRT, rozbudowuje mechanizmy nadzorcze i interwencyjne państwa (w tym wobec dostawców wysokiego ryzyka) oraz porządkuje system reagowania na incydenty o znaczeniu poważnym i krytycznym. Jednocześnie przewidziano okresy przejściowe przed stosowaniem sankcji administracyjnych, co ma umożliwić adresatom norm stopniowe dostosowanie się do podwyższonych standardów cyberodporności (Ministerstwo Cyfryzacji 2026).

Przeprowadzona analiza systemowa prowadzi jednak do wniosku, że dalszy rozwój krajowego systemu cyberbezpieczeństwa w Polsce wymaga nie tylko implementacji dyrektywy NIS2 w wymiarze formalnym, lecz także pogłębionej integracji instytucjonalnej pomiędzy istniejącymi reżimami regulacyjnymi. W szczególności zasadne wydaje się rozważenie włączenia ochrony danych osobowych jako trwałego komponentu funkcjonalnego krajowego systemu cyberbezpieczeństwa.

De lege ferenda należałoby rozważyć formalne wzmocnienie roli Prezesa Urzędu Ochrony Danych Osobowych w strukturze KSC, przynajmniej poprzez ustanowienie ustawowych mechanizmów współpracy i wymiany informacji pomiędzy UODO a zespołami CSIRT poziomu krajowego. Takie rozwiązanie mogłoby przyjąć postać obowiązkowych procedur koordynacyjnych w przypadku incydentów obejmujących jednocześnie naruszenie bezpieczeństwa systemów teleinformatycznych oraz naruszenie ochrony danych osobowych.

Ponadto, analiza ujawnia potrzebę wyraźniejszego normatywnego określenia odpowiedzialności państwa za bezpieczeństwo użytkowników końcowych w cyberprzestrzeni. Obowiązujące regulacje koncentrują się przede wszystkim na ochronie infrastruktury oraz ciągłości usług, podczas gdy ochrona obywateli jako uczestników systemu pozostaje fragmentaryczna i rozproszona kompetencyjnie. W tym kontekście zasadne byłoby rozważenie wprowadzenia spójnych obowiązków informacyjnych i edukacyjnych o charakterze systemowym, przypisanych jednemu podmiotowi koordynującemu.

Wreszcie, z perspektywy funkcjonowania systemu jako całości, istotne znaczenie ma zapewnienie jego zdolności adaptacyjnej, rozumianej jako możliwość szybkiego dostosowywania procedur, struktur organizacyjnych oraz narzędzi prawnych do zmieniającego się krajobrazu zagrożeń. Osiągnięcie tego celu wymaga nie tylko odpowiednich zasobów kadrowych i technologicznych, lecz także elastycznych

ram prawnych umożliwiających skuteczne reagowanie na incydenty o charakterze transsektorowym i transgranicznym. Agencja ENISA regularnie publikuje raporty oceniające stan cyberbezpieczeństwa w UE i nowe trendy. Według raportu ENISA Threat Landscape 2025, obecnie do najpoważniejszych zagrożeń należą: ataki typu ransomware, różne formy szkodliwego oprogramowania, ataków socjotechnicznych, zagrożenia wymierzone w poufność danych, zagrożenia dla dostępności usług, manipulowanie informacjami oraz ataki na łańcuch dostaw oprogramowania i sprzętu (ENISA 2025).

Przyszłe zagrożenia rysują się na horyzoncie już dziś. Jednym z przełomowych czynników jest rozwój sztucznej inteligencji i jej wpływ na bezpieczeństwo. AI może być bronią obosieczną: z jednej strony wspomaga analityków bezpieczeństwa, np. jako narzędzia AI do wykrywania anomalii, a z drugiej strony jest wykorzystywana przez atakujących do nowych, wyrafinowanych form ataku. Kolejnym istotnym problemem związanym z rozwojem sztucznej inteligencji jest ewolucja phishingu z wykorzystaniem generowanych treści typu deepfake. W tym kontekście istotnym instrumentem regulacyjnym jest unijny AI Act (Rozporządzenie (UE) 2024/1689), obowiązujący od 1 sierpnia 2024 r., który wprowadza obowiązek oznaczania treści wygenerowanych przez sztuczną inteligencję, obejmujący teksty, obrazy, nagrania audio i wideo (Rozporządzenie (UE) 2024/1689).

Kolejnym narastającym zagrożeniem są wojny hybrydowe, w których komponent cybernetyczny odgrywa coraz większą rolę. Doświadczenie wojny w Ukrainie pokazało, że cyberataki stały się integralną częścią konfliktu zbrojnego, służą destabilizacji zaplecza, wywiadowi, propagandzie (Kołodziejczyk 2024). Polska, wspierając Ukrainę i będąc na wschodniej flance NATO, stała się celem intensywnych działań w cyberprzestrzeni ze strony rosyjskiej.

Oceniając dzisiaj kondycję systemu, można powiedzieć, że jego fundamenty zostały już zbudowane, mamy prawo, instytucje i rosnącą świadomość zagrożeń. Trzeba jednak pamiętać o podstawowej zasadzie, która mówi, że bezpieczeństwo to nie stan, lecz proces, proces niekończącej się adaptacji do zmieniających się warunków.

BIBLIOGRAFIA

Akty prawne

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 (Dz. U. UE. L. z 2016 r. Nr 194, str. 1).

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) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

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)Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r. poz. 20).

Dokumenty Strategiczne

Rada Ministrów (2019) Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024. Gov.pl. Dostępne na: https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (dostęp: 27.01.2026).

Komisja Europejska (2025) Prawa i zasady cyfrowe. Digital Strategy – Shaping Europe's digital future. Dostępne na: https://digital-strategy.ec.europa.eu/pl/factpages/digital-rights-and-principles (dostęp: 27.01.2026).

Raporty i opracowania instytucjonalne

ENISA (2025) ENISA Threat Landscape (ETL) report 2025.

ITU (2024) Global Cybersecurity Index 2024. International Telecommunication Union. Dostępne na: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (dostęp: 27.01.2026).

Fundacja Bezpieczna Cyberprzestrzeń (2025) Raport z ćwiczeń Cyber-EXE Polska 2024 – CEP24. Dostępne na: https://www.cybsecurity.org/wp-content/uploads/2025/01/Raport-CEP-24__AI-251124-C03B-book.pdf (dostęp: 27.01.2026).

Najwyższa Izba Kontroli (2023) Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości (Informacja o wynikach kontroli, nr ewid. 125/2022/P/21/042/KPB). Warszawa: Najwyższa Izba Kontroli. Dostępne na: https://www.nik.gov.pl/plik/id,27206,vp,30013.pdf (dostęp: 27.01.2026).

Najwyższa Izba Kontroli (2025) Informacja o wynikach kontroli: Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego (Nr ewid. 123/2024/P/24/004/KAP). Warszawa: Najwyższa Izba Kontroli. Dostępne na: https://www.nik.gov.pl/plik/id,30641,vp,33700.pdf (dostęp: 27.01.2026).

GLOBSEC (2024) GLOBSEC Trends 2024: CEE – A Brave New Region? GLOBSEC. Dostępne na: https://www.globsec.org/sites/default/files/202405/GLOBSEC%20Trends%202024.pdf (dostęp: 27.01.2026).

Literatura

Sienkiewicz P.
1994 *Analiza systemowa – podstawy i zastosowania*. Warszawa.

Safian M.
2002 *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informacyjnym*, „Państwo i Prawo, nr 6.

Stagnaro, M.N. & Amsalem, E.
2025 *Factual knowledge can reduce attitude polarization. Nature Communications*, 16, Article 3809.

Kołodziejczyk R.
2024 Zjawisko wojny hybrydowej w konflikcie ukraińsko-rosyjskim. „Rocznik Bezpieczeństwa Morskiego", XIX.

Źródła internetowe

Urząd Ochrony Danych Osobowych (2024) *Ochrona danych osobowych a bezpieczeństwo państwa – wnioski po seminarium UODO i ZUS*. Dostępne na: https://www.uodo.gov.pl/pl/138/3396 (dostęp: 27.01.2026).

CyberDefence24 (2023) Cyberpolicja odpowiada na raport NIK: krytykuje czas, kiedy nas nie było. Dostępne na: https://cyberdefence24.pl/armia-i-sluzby/cyberpolicja-odpowiada-na-raport-nik-krytykuje-czas-kiedy-nas-nie-bylo (dostęp: 27.01.2026).

PoradyODO (2025) Strategia Cyberbezpieczeństwa RP na lata 2025–2029 – uwagi Prezesa UODO. Dostępne na: https://www.poradyodo.pl/cyberbezpieczenstwo/strategia-cyberbezpieczenstwa-rp-na-lata-20252029-uwagi-prezesa-uodo-13009.html (dostęp: 27.01.2026).

Centralne Biuro Zwalczania Cyberprzestępczości (2025) Zarobki – w służbie zwalczania cyberprzestępczości. Policja.pl / cbzc.policja.gov.pl. Dostępne na: https://cbzc.policja.gov.pl/bzc/zostan-policjantem-cbzc/w-sluzbie-zwalczania-cyber/342,Zarobki.html (dostęp: 27.01.2026).

CSIRT GOV (b.d.) System ARAKIS-GOV. Dostępne na: https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html (dostęp: 27.01.2026).

Ministerstwo Cyfryzacji (2025) Krajobraz cyberprzestrzeni: roczne sprawozdanie o cyberbezpieczeństwie. Gov.pl. Dostępne na: https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie (dostęp: 27.01.2026).

Ministerstwo Cyfryzacji (2026) Sejm uchwalił nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa. Gov.pl. Dostępne na: https://www.gov.pl/web/cyfryzacja/sejm-uchwalil-nowelizacje-ustawy-o-krajowym-systemie-cyberbezpieczenstwac(dostęp: 27.01.2026).

Ministerstwo Cyfryzacji / NASK (2024) Jak nie dać się trollom? Rusza kampania o dezinformacji Ministerstwa Cyfryzacji i NASK. Gov.pl. Dostępne na: https://www.gov.pl/web/cyfryzacja/jak-nie-dac-sie-trollom-rusza-kampania-o-dezinformacji-ministerstwa-cyfryzacji-i-nask (dostęp: 27.01.2026).

Służby Specjalne (b.d.) Polska na celowniku dezinformacji. Gov.pl. Dostępne na: https://www.gov.pl/web/sluzby-specjalne/polska-na-celowniku-dezinformacji (dostęp: 27.01.2026).

GS Services (2025) Co to jest uwierzytelnianie wieloskładnikowe (MFA) i dlaczego warto je stosować. Dostępne na: https://gsservices.pl/co-to-jest-uwierzytelnianie-wieloskladnikowe-mfa-i-dlaczego-warto-je-stosowac/ (dostęp: 27.01.2026).

THE CONDITION OF THE NATIONAL CYBERSECURITY SYSTEM IN POLAND IN THE CONTEXT OF IMPLEMENTING THE NIS 2 DIRECTIVE – A SYSTEMS ANALYSIS

Abstract: This article analyzes the condition of the national cybersecurity system in Poland in the context of implementing the NIS 2 Directive, using systems analysis as the primary research method. The aim of the study is to assess the institutional structure of the system, the mechanisms of cooperation between key entities, and to identify functional limitations affecting its effectiveness. Analysis of legal acts, strategic documents, and institutional reports indicates that the system has achieved relative organizational maturity, but remains burdened by deficits in functional coherence and cross-sectoral coordination. A particular gap is the insufficient integration of personal data protection and the marginal consideration of the role of individual network users. The identified limitations may hinder the effective adaptation of the system to the requirements of the NIS 2 Directive.

Keywords: national cybersecurity system, systems analysis, national cybersecurity, institutional coordination, NIS Directive

mgr **Marek Tatarczuk**

Badacz niezależny
ORCID: 0000-0001-8747-3529

GODNOŚĆ CZŁOWIEKA JAKO PODSTAWA TELEOLOGICZNEJ WYKŁADNI WOLNOŚCI RELIGIJNEJ. OCHRONA ARELIGIJNOŚCI W KONSTYTUCJI RP

Streszczenie: artykuł analizuje konstytucyjny model wolności religijnej w Polsce w perspektywie jej aksjologicznych podstaw, ze szczególnym uwzględnieniem godności człowieka jako nadrzędnej wartości konstytucyjnej. Autor wskazuje, że transformacja ustrojowa oraz przyjęcie Konstytucji RP z 1997 r. przyniosły zasadniczą zmianę w pojmowaniu relacji między państwem, religią i jednostką. Wolność religijna – ujęta w art. 53 – przestała być wyłącznie gwarancją instytucjonalną, stając się elementem przyrodzonej godności ludzkiej, z której wywodzą się wszystkie prawa i wolności. Artykuł podkreśla jednak napięcie pomiędzy literalnym brzmieniem przepisów, koncentrującym się na religijności sensu stricto, a ich aksjologiczną i systemową interpretacją, która wskazuje, że wolność religijna obejmuje także wolność od religii i postawy areligijne. Autor argumentuje, że uznanie równorzędności ochrony przekonań religijnych i niereligijnych wynika zarówno z zasady równej godności jednostek, jak i ze współczesnych standardów europejskich dotyczących ochrony wolności myśli, sumienia i wyznania. Artykuł formułuje tezę, że teleologiczna wykładnia art. 53 Konstytucji RP powinna obejmować również areligijność jako wyraz autonomii jednostki i integralny element pluralizmu światopoglądowego w demokratycznym państwie prawnym.

Słowa kluczowe: godność człowieka, wolność religijna, areligijność, Konstytucja RP, wykładnia teleologiczna, pluralizm światopoglądowy

Wstęp

Transformacja ustrojowa roku 1989 przyniosła Polsce nie tylko zmianę systemu politycznego, ale przede wszystkim głęboką reorientację aksjologiczną porządku

prawnego. Punktem zwrotnym okazało się przyjęcie Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku, która na nowo zdefiniowała relacje między jednostką, państwem a sferą wartości transcendentnych. W nowym porządku konstytucyjnym wolność religijna przestała być wyłącznie kwestią gwarancji instytucjonalnych, stając się bezpośrednią emanacją przyrodzonej i niezbywalnej godności człowieka (Wroceński 2016, s. 8). Ujęcie to wpisuje się w szerszą koncepcję ciągłości wartości, na której zbudowana jest III Rzeczpospolita. Jak trafnie ujęła to Alicja Grześkowiak, III RP jest kontynuacją duchowego i aksjologicznego dziedzictwa narodu, a prawo – jako regulator życia społecznego – ma za zadanie chronić fundamentalne wartości, na których opiera się wspólnota państwowa, niezależnie od przejściowego braku suwerennych struktur (Grześkowiak 1999, s. 9-10). To właśnie ten fundament wartości, ugruntowany w godności osoby ludzkiej, stanowi punkt wyjścia dla rozumienia wszystkich wolności i praw.

Jednakże pomiędzy szerokim, ugruntowanym w godności człowieka ujęciem wolności religijnej *sensu largo* a jej szczegółową regulacją w art. 53 Konstytucji RP rysuje się pewne napięcie. Tymczasem współczesne orzecznictwo europejskie, zwłaszcza Europejskiego Trybunału Praw Człowieka (ETPC), od lat potwierdza, że „wolność" w rozumieniu art. 9 Europejskiej Konwencji Praw Człowieka w coraz większym stopniu obejmuje również prawo do niepodzielania żadnej religii, a nawet do krytyki religii. Jak zauważa Javier Martínez-Torrón, przełomowe znaczenie miała tu sprawa *Kokkinakis* z 1993 roku, która zapoczątkowała bogate orzecznictwo strasburskie, odnoszące się nie tylko do klasycznie pojmowanej religijności, ale i do światopoglądów areligijnych (Martínez-Torrón 2011, s. 340-341). Ta ewolucja interpretacyjna na poziomie ponadnarodowym czyni szczególnie pilnym pytanie o to, czy polski model konstytucyjny nadąża za tymi zmianami i czy oferuje adekwatną ochronę osobom o światopoglądzie niereligijnym.

Celem niniejszego artykułu jest odpowiedź na pytanie, czy obowiązujący model konstytucyjny chroni „wolność od religii" na równi z „wolnością do religii" oraz w jakim stopniu aksjologia godności człowieka (art. 30 Konstytucji RP) wpływa na interpretację zakresu przedmiotowego i podmiotowego wolności religijnej wyrażonej w art. 53. Tekst ten stawia tezę, że obowiązujący model konstytucyjny, oparty na godności człowieka jako „zasadzie zasad", nakazuje teleologiczne rozszerzenie wykładni art. 53 ust. 2 na ochronę uzewnętrzniania postaw areligijnych. Postawy te stanowią immanentny element wolności religijnej *sensu largo*, będąc wyrazem autonomii jednostki w sferze światopoglądowej. Niedostateczne wyeksponowanie tego aspektu w doktrynie oraz niekonsekwencja w praktyce orzeczniczej mogą prowadzić do nieuzasadnionego ograniczenia praw jednostki, pozostającego w sprzeczności

z fundamentalnymi zasadami ustrojowymi III RP, w tym z zasadami państwa prawnego i pluralizmu

W części II zrekonstruowany zostanie aksjologiczny fundament wolności religijnej, jakim jest godność człowieka, z uwzględnieniem jej filozoficznych i prawnych konotacji. Część III poświęcona będzie analizie konstytucyjnego modelu wolności religijnej, ze szczególnym uwzględnieniem zakresu przedmiotowego i podmiotowego art. 53, a także relacji z wymiarem instytucjonalnym z art. 25. W części IV, kluczowej dla postawionej tezy, podjęta zostanie próba wykazania, że areligijność zasługuje na ochronę w ramach art. 53. Argumentacja ta zostanie oparta na wykładni systemowej i teleologicznej, przy uwzględnieniu standardów wypracowanych w orzecznictwie ETPC. Analiza ta pozwoli na sformułowanie wniosków *de lege lata* i *de lege ferenda*.

Aksjologiczny fundament wolności religijnej – godność człowieka

Idea, która legła u podstaw całego systemu ochrony praw człowieka w Konstytucji RP, a tym samym również wolności religijnej, jest godność człowieka. Mimo że ustawa zasadnicza nie definiuje tego pojęcia wprost, to właśnie ono stanowi centralną kategorię antropologiczną i prawną, wyznaczającą tożsamość konstytucyjną państwa (Polak, Trzciński 2018, s. 257). Wyrażona w art. 30 Konstytucji zasada godności nie jest jedynie elementem konstytucyjnego decorum, lecz normatywną dyrektywą realnie oddziałującą na rozumienie i stosowanie całego systemu prawa (Polak, Trzciński 2018, s. 273). Piotr Tuleja nazywa ją „zasadą wiodącą", która ma rozstrzygający wpływ na charakter systemu prawa, katalog i treść konstytucyjnych praw człowieka oraz ustrój państwa (Tuleja 2021, art. 30). Podobnie Filip Ciepły podkreśla, że stanowi ona punkt odniesienia dla całego systemu wartości, będąc pierwowzorem wszystkich wartości konstytucyjnych i ostatecznym testem ich znaczenia (Ciepły 2017, s. 141-158). Ferdynand Rymarz dodaje, że wartość godności bardziej niż koncepcja sprawiedliwości nadaje się do urzeczywistnienia postulatów związanych z zaspokojeniem podstawowych potrzeb człowieka (Rymarz 2017, s. 15-22). Godność nie jest odrębną wolnością, przysługuje jej jednak taka sama ochrona jurysdykcyjna, jaką mają konkretne prawa człowieka, w których znajduje swój wyraz (Borski 2014, s. 7-20).

Z perspektywy prowadzonych rozważań kluczowe jest, że godność przynależy każdemu człowiekowi niezależnie od jego światopoglądu, przekonań religijnych czy też ich braku. Lech Garlicki uwypukla, że nie może to oznaczać aksjologicznej indyferentności polskich pojęć konstytucyjnych, bo nieprzypadkowo wstęp do

konstytucji sytuuje ją na tle „chrześcijańskiego dziedzictwa Narodu i ogólnoludzkich wartości". Stąd punktem wyjścia dla rozważań o konstytucyjnym pojęciu godności staje się ujmowanie tego pojęcia w chrześcijańskiej nauce społecznej (Garlicki, Derlatka 2016, uwaga 9 do wstępu). Jednocześnie jednak preambuła wyraźnie adresuje konstytucję zarówno do „wierzących w Boga będącego źródłem prawdy, sprawiedliwości, dobra i piękna, jak i nie podzielających tej wiary, a te uniwersalne wartości wywodzących z innych źródeł". To dualne adresowanie aktu fundacyjnego państwa dowodzi, że u jego podstaw leży założenie o wspólnocie obywateli, którą łączą uniwersalne wartości, niezależnie od ich ostatecznego, religijnego lub areligijnego, uzasadnienia.

W doktrynie podkreśla się, że godność ludzka charakteryzuje się powszechnością, równością, inherentnością i nienaruszalnością (Chojnacki 2022, s. 24-58). Oznacza to, że każdy człowiek, bez względu na wyznawaną religię lub jej brak, ma taką samą godność i nie może być jej pozbawiony. Co więcej, godność ta ma charakter transcendentny wobec innych praw – nie znosi jej nawet czyn budzący największą odrazę (Chrzczonowicz, Kapelańska-Pręgowska 2015, s. 71-102). Jak zauważa Mirosław Granat, godność człowieka jako wartość usytuowana jest ponad prawem i służy każdemu – ma charakter uniwersalny, a nie wybiórczy. Jest też identyczna dla wszystkich ludzi – każdy człowiek ma taką samą godność (Granat 2022, s. 134). Autor ten słusznie czyni przy tym rozróżnienie między godnością ludzką, która jest niezbywalna i nienaruszalna, a godnością osobistą, która może być większa lub mniejsza, a nawet może zostać utracona (Granat 2022, s. 134).

W doktrynie nie jest kwestionowane, że człowiek jako byt psychosomatyczny i społeczny poszukuje wartości. Istnieją wartości zmienne, zależne od sytuacji społeczno-kulturowej, ale są także wartości trwałe, obiektywne i uniwersalne, których istotę wyznacza godność osoby ludzkiej (Mariański 2019, s. 5-6). Z godności wynikają wartości podstawowe i prawa człowieka: równość, solidarność, demokracja, tolerancja, sprawiedliwość społeczna, życie ludzkie, wolny rozwój osobowościowy, a także wolność religijna. Porządek moralny immanentnie związany jest z wzorcami określanymi także przez wiarę, religię i będącą ich następstwem wolność religijną w najpełniejszym tego zwrotu znaczeniu, bo także jako wolność od religii.

Takie rozumowanie nawiązuje do teorii godności ludzkiej Mieczysława Alberta Krąpca, który wiązał występowanie godności z faktem religijnym, oraz Mieczysława Gogacza, który proponował złożone ujęcie godności jako istoty osoby, własności aksjologicznej oraz jej przypadłości (Mazurek 1996, s. 19; Gogacz 1989, s. 195). Ewa Michałkiewicz-Kądziela trafnie odnotowuje, że Krąpiec uważa, iż człowieka określa się poprzez jego stosunek z naturą oraz ze społecznością, a w relacjach tych ujawniają

się takie właściwości, jak zdolność do poznania intelektualnego, miłość, wolność, podmiotowość prawa, zupełność i godność. Gogacz odrzuca natomiast twierdzenie, że godność jest faktem religijnym, gdyż oznaczałoby to, że każdy człowiek nawiązuje relacje z Bogiem, a jest to niemożliwe (Michałkiewicz-Kądziela 2020). To filozoficzne napięcie unaocznia kluczowy dylemat konstytucyjny: jak pogodzić uniwersalny charakter godności, mający służyć wszystkim obywatelom, z jej kulturowym i historycznym zakorzenieniem w tradycji chrześcijańskiej.

Związek między godnością a wolnością religijną jest przy tym nierozerwalny. Jacek Jan Pawłowicz trafnie konstatuje, że „godność i wolność są powiązane ze sobą jak naczynia połączone, a ich wspólnym mianownikiem jest człowiek i jego dobro" (Pawłowicz 2012, s. 76). Oznacza to, że wszelkie ograniczenia wolności religijnej muszą być uzasadnione w świetle godności, a sama wolność religijna jest praktycznym urzeczywistnieniem tej godności w sferze duchowej i światopoglądowej jednostki. W okresie przejściowym pomiędzy PRL a III RP, ale przed przyjęciem obowiązującej ustawy zasadniczej, kluczowym aktem prawnym była ustawa z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania (Dz. U. z 2023 r., poz. 265), której przyjęcie określane było nawet jako „pierwszy krok na drodze kształtowania się wolności religijnej" (Rejs 2019, s. 139). Ustawa ta w art. 1 gwarantowała każdemu obywatelowi wolność sumienia i wyznania, ale ograniczała ją jedynie do obywateli polskich, co stanowiło istotne zawężenie w porównaniu z późniejszym ujęciem konstytucyjnym, które prawo to przyznaje „każdemu".

Konstytucyjny model wolności religijnej (art. 53)

Materię wolności religijnej polski ustrojodawca umieścił w kilku przepisach Konstytucji, stosując metodę dyspersji, na co zwrócił uwagę Trybunał Konstytucyjny w wyroku z 2 grudnia 2009 r. (U 10/07). Trybunał wyjaśnił, że materia konstytucyjna dotycząca wolności sumienia i wyznania składa się z dwu części: instytucjonalnej, dotyczącej relacji między państwem a kościołami i innymi związkami wyznaniowymi, regulowanej przede wszystkim w art. 25 Konstytucji, oraz części odnoszącej się do indywidualnych gwarancji wolności sumienia i wyznania, wynikających zwłaszcza z art. 53 Konstytucji. Trybunał podkreślił, że interpretacja treści normatywnych art. 25 ust. 1 i 2 winna być dokonywana w ścisłym związku z art. 53 ust. 1 i 2 Konstytucji (wyrok TK z 2.12.2009 r., U 10/07).

Podstawowe znaczenie ma art. 53, traktujący o „wolności sumienia i religii". Przepis ten w ust. 1 stanowi, że każdemu zapewnia się wolność sumienia i religii, zaś w ust. 2 precyzuje, iż wolność religii obejmuje wolność wyznawania lub

przyjmowania religii według własnego wyboru oraz uzewnętrzniania jej indywidualnie lub z innymi, publicznie lub prywatnie, przez uprawianie kultu, modlitwę, uczestniczenie w obrzędach, praktykowanie i nauczanie. Wolność religii obejmuje także posiadanie świątyń i innych miejsc kultu w zależności od potrzeb ludzi wierzących oraz prawo osób do korzystania z pomocy religijnej tam, gdzie się znajdują (art. 53 ust. 2 in fine). Lech Garlicki w swoim komentarzu do tych przepisów potwierdza, że wolność religijna została zaliczona do wolności i praw o charakterze osobistym, jej wykorzystywanie bowiem związane jest ściśle z osobowością człowieka, a uznanie i poszanowanie przez państwo i społeczeństwo tych wolności wynika z obowiązku ochrony godności ludzkiej. Zaś godność ta wyraża się m.in. we wrodzonym poszukiwaniu i przeżywaniu przez człowieka pewnych wartości transcendentnych – wobec tego poszukiwanie to musi być uznane, docenione i chronione (Sarnecki 2016, art. 53). Do tego poszukiwania w sposób wyraźny nawiązuje również wstęp do konstytucji, tworząc tym samym jeszcze jedną podstawę konstytucyjną dla uznania wolności zawartych w art. 53.

Powszechnie w zasadzie przyjmuje się podział wolności religijnej na wymiar wewnętrzny (zewnętrznie nienaruszalny) i zewnętrzny (podlegający ograniczeniom). Aneta Maria Abramowicz wyjaśnia, że wymiar zewnętrzny obejmuje różnorakie akty bezpośrednio i trwale związane z wyznawaną religią, w tym uprawianie kultu, nauczanie czy czynności rytualne. W przeciwieństwie do wymiaru wewnętrznego, wolność uzewnętrzniania religii może być ograniczana, jednak jedynie w sytuacjach taksatywnie wymienionych w ustawie (Abramowicz 2007, s. 331-332). Zofia Józefa Zdybicka, klasyfikując prościej, wyjaśnia, że wolność w aspekcie wewnętrznym pozwala człowiekowi na podejmowanie aktu wyboru danej religii i objawia się w sumieniu, w którym człowiek odkrywa prawdę o dobru. Wolność religii w aspekcie zewnętrznym obejmuje wolność do manifestowania swoich przekonań religijnych i wolność od przymusu zewnętrznego w tej dziedzinie (Zdybicka 2006, s. 360).

Ograniczenia wolności uzewnętrzniania religii określa art. 53 ust. 5, który dopuszcza limitację jedynie w drodze ustawy i tylko wtedy, gdy jest to konieczne do ochrony bezpieczeństwa państwa, porządku publicznego, zdrowia, moralności lub wolności i praw innych osób. Dokonując porównania art. 53 ust. 5 z ogólną konstytucyjną klauzulą limitacyjną zawartą w art. 31 ust. 3, zauważymy różnicę tylko taką, że wolność uzewnętrzniania religii nie może być ograniczana ze względu na potrzebę ochrony środowiska. Jak wskazuje Florczak-Wątor, przynależność do określonego wyznania i przyjęte w związku z tym przez daną osobę przekonania moralne mogą mieć wpływ na sposób realizacji powszechnego obowiązku służby wojskowej (w drodze tzw. służby zastępczej), o ile zostanie wykazane, że system wartości i przekonań

związany z daną religią wyklucza możliwość odbywania służby wojskowej bez narażania osoby na zasadniczy konflikt wewnętrzny (Florczak-Wątor 2021, art. 53).

Istotne jest przy tym, co podkreśla Sarnecki, że wolność ta przysługuje „każdemu", a nie tylko obywatelom, co stanowi istotne rozszerzenie w porównaniu z ustawą o gwarancjach wolności sumienia i wyznania z 1989 roku (Sarnecki 2016, art. 53). Jednocześnie Konstytucja posługuje się niekonsekwentną terminologią – w art. 48 ust. 1 mówi o „wolności sumienia i wyznania", w art. 53 ust. 1 i 4 o „wolności sumienia i religii", zaś w art. 53 ust. 7 o „światopoglądzie, przekonaniach religijnych lub wyznaniu". Tę niekonsekwencję można jednak uznać za walor, gdyż semantyczna pojemność tych pojęć pozwala na szerokie ujmowanie wolności religijnej.

Co więcej, konstytucja nie definiuje pojęcia religii. Wojciech Białogłowski i Przemysław Wasylik, w powołaniu na Clarka (Clark 1968, s. 86-87) i Fromma (Fromm 2000, s. 207-208), trafnie przyznają, że religia jest amorficzną koncepcją, a słowa „religia" nie używa się w sensie systemu, który musiałby zawierać pojęcie Boga lub bóstwa, lecz oznacza za jego pomocą „wszelki, właściwy pewnej grupie ludzi system myślowy i etyczny, który dostarcza jednostkom ramy orientacyjnej oraz przedmiotu, w który mogą wierzyć" (Białogłowski, Wasylik 2023, s. 36). Konstytucja nie definiuje pojęcia religii oraz nie daje podstaw do rozstrzygnięć, czy dany zespół poglądów i praktyk jest czy nie jest religią. Istotne znaczenie w tej mierze mają ustalenia pozakonstytucyjne, a nawet pozaprawne – filozoficzne, teologiczne, etnograficzne, kulturowe i religioznawcze.

Trybunał Konstytucyjny w wyroku z 8 czerwca 2011 r. (K 3/09) wyjaśnił, że art. 25 Konstytucji wskazuje na wolność religijną w wymiarze instytucjonalnym i formułuje w szczególności: zasadę równouprawnienia kościołów i związków wyznaniowych; zasadę bezstronności władz publicznych w sprawach przekonań religijnych, światopoglądowych i filozoficznych; zasadę swobody wyrażania przekonań religijnych, światopoglądowych i filozoficznych w życiu publicznym; zasadę poszanowania autonomii i wzajemnej niezależności państwa oraz kościołów i związków wyznaniowych; zasadę współdziałania państwa oraz kościołów i związków wyznaniowych dla dobra człowieka i dobra wspólnego; zasadę regulacji stosunków między państwem a kościołami i związkami wyznaniowymi w drodze dwustronnej (wyrok TK z 8.06.2011 r., K 3/09). Wolność religijna w wymiarze kolektywnym realizowana jest poprzez kościoły i związki wyznaniowe, których status prawny uregulowany jest w aktach indywidualnych (wraz z Kościołem katolickim 15 podmiotów) bądź są wpisane do rejestru kościołów i innych związków wyznaniowych, prowadzonego przez Ministra Spraw Wewnętrznych i Administracji. Jak wynika z danych Ministerstwa Spraw Wewnętrznych i Administracji, na dzień 17 lutego 2026 r. do działu

A rejestru wpisano 176 podmiotów, z kolei w dziale B figuruje 5 organizacji międzykościelnych (https://www.gov.pl/web/mswia/rejestr-kosciolow-i-innych-zwiazkow-wyznaniowych). Przywołane liczby ukazują skalę zjawiska i dowodzą, że w Polsce istnieje ponad 180 podmiotów korzystających z kolektywnej wolności religijnej. Jak zauważono na stronie Centrum Obywatelskiego Prawa Człowieka, zarówno odrębna ustawa, jak i wpis do rejestru dają kościołom i innym związkom wyznaniowym przymiot osobowości prawnej, a które z tego tytułu mają podmiotowość w zakresie praw majątkowych (https://copch.pl/baza-wiedzy/koscioly-i-inne-zwiazki-wyznaniowe-jako-podmioty-wolnosci-religijnej-zagadnienia-ogolne). Jednakże nadmierne akcentowanie wymiaru instytucjonalnego może prowadzić do swoistej teologizacji prawa, w której ochrona przysługuje przede wszystkim zinstytucjonalizowanym formom religijności, kosztem indywidualnych postaw światopoglądowych.

Dylemat areligijności – „wolność od religii" w świetle konstytucji

Literalne brzmienie art. 53 ust. 2 Konstytucji, mówiące o „wyznawaniu lub przyjmowaniu religii", zdaje się pomijać sytuację osób, które nie wyznają żadnej religii i nie chcą jej przyjmować. Bogusław Banaszak wprost stwierdza, że gwarancje wolności religijnej nie obejmują swoim zakresem uzewnętrzniania indywidualnie lub z innymi przekonań ateistycznych, odrzucających wiarę w istnienie sił nadprzyrodzonych i negujących potrzebę istnienia religii (Banaszak 2012, s. 325). Również Anna Korzeniewska-Lasota, oceniając katalog wolności światopoglądowych jako wystarczający i odpowiadający standardom międzynarodowym, zastrzega, że tak określony zakres wolności wyznania nie obejmuje światopoglądu niereligijnego (Korzeniewska-Lasota 2011, s. 214-215).

Taka wykładnia prowadzi do paradoksalnych konsekwencji, które unaoczniają jej wewnętrzną sprzeczność z aksjologią Konstytucji. Jeśli bowiem uznać, że ochrona konstytucyjna przysługuje wyłącznie w sferze religijności *sensu stricto*, to osoba dokonująca konwersji z jednego wyznania na drugie korzysta z pełni gwarancji, podczas gdy ta sama osoba, po dokonaniu apostazji i świadomym wyborze ateizmu, ochronę tę traci. Tymczasem to właśnie możliwość wyboru religii, jej zmiany, a także jej porzucenia stanowi istotę wolności religijnej. Pozbawienie ochrony osoby, która z tej wolności skorzystała, wybierając światopogląd areligijny, czyni tę wolność iluzoryczną. Jeszcze bardziej jaskrawy jest przykład pastafarianizmu – ruchu, który stanowi „przekonanie podobne do religii", gdzie ironicznie „wierzy się, że nie ma Boga", a jego nauki pełnią funkcję analogiczną do religijnego systemu wartości. Głoszenie tych nauk, zgodnie z wykładnią literalną, pozostawałoby poza zakresem

konstytucyjnych gwarancji, mimo że ich zwolennicy powołują się na argumenty natury światopoglądowej. Prowadzi to do sytuacji, w której ochrona przysługuje nie tyle ze względu na naturę wyznawanych przekonań, ile ze względu na ich zgodność z tradycyjnie rozumianą kategorią „religii". Konsekwencją jest hierarchizacja światopoglądów, niedająca się pogodzić z zasadą równej godności wszystkich ludzi, a tym samym – z aksjologicznym fundamentem całego porządku konstytucyjnego.

Wykładnia zawężająca, ograniczająca ochronę wyłącznie do religii w sensie ścisłym, pozostaje jednak w sprzeczności z aksjologicznym fundamentem Konstytucji. Argument aksjologiczny odwołujący się do godności człowieka wskazuje, że godność przysługuje każdej jednostce niezależnie od jej światopoglądu. Ograniczenie ochrony konstytucyjnej wyłącznie do sfery religijnej tworzyłoby niedającą się pogodzić z zasadą równości hierarchię światopoglądów, w której wyznawcy religii byliby uprzywilejowani względem ateistów czy agnostyków. Tymczasem godność nie jest wartością stopniowalną – nie może być jej „więcej" dla wierzących i „mniej" dla niewierzących.

Argument teleologiczny odwołujący się do celu normy wskazuje, że celem art. 53 jest ochrona autonomii jednostki w sprawach światopoglądowych. Wybór areligijności jest takim samym aktem autonomii jak wybór religii. Jak słusznie zauważa Zdybicka, wolność religijna w aspekcie negatywnym chroni człowieka przed jakimkolwiek naciskiem ze strony państwa oraz innych ludzi (Zdybicka 2006, s. 360). Prawo do bycia wolnym od religii stanowi zatem korelat prawa do wyznawania religii.

Argument systemowy odwołuje się do preambuły Konstytucji, która wyraźnie wskazuje na wspólnotę obywateli „wierzących w Boga" oraz „nie podzielających tej wiary, a te uniwersalne wartości wywodzących z innych źródeł". System prawa nie może więc tworzyć podziału na obywateli pierwszej i drugiej kategorii w zależności od ich stosunku do religii. Jak trafnie ujął to Sławomir Drelich, III RP uzyskała formę liberalnej demokracji, a katalog podstawowych wartości sformułowanych w konstytucji został celowo ukształtowany jako wąski i wyważony, by spotkać się z możliwie powszechną akceptacją (Drelich 2019, s. 80-81). W duchu liberalnym, jaki towarzyszył transformacji ustrojowej Polski i jaki w Konstytucji RP z 1997 r. istotnie aksjologicznie wybrzmiał – wolność *per se* jest także „od".

Argument z godnościowej interpretacji prawa odwołuje się do faktu, że Konstytucja nie definiuje pojęcia religii i nie daje podstaw do rozstrzygnięć, czy dany zespół poglądów jest religią. Istotne znaczenie mają tu ustalenia filozoficzne i kulturowe (Białogłowski, Wasylik 2023, s. 36). Jeśli zatem uznamy, że systemem światopoglądowym mogą być również poglądy areligijne, które pełnią w życiu jednostki funkcję analogiczną do religii (dostarczając ramy orientacyjnej i systemu wartości), to brak ich ochrony w ramach art. 53 byłby nieuzasadniony. Co więcej, taka wykładnia

jest nie do pogodzenia z założeniami, które legły u podstaw europejskiego systemu ochrony praw człowieka, wywodzącego wolność myśli, sumienia i religii z prawnonaturalnej koncepcji przyrodzonych i niezbywalnych praw jednostki (Kociubiński 2011, s. 114).

Problem zakresu podmiotowego i przedmiotowego wolności sumienia i religii jest przedmiotem pogłębionych analiz w doktrynie prawa, zarówno polskiej, jak i międzynarodowej. Jak zauważa Jakub Kociubiński, analizując orzecznictwo strasburskie, dla ochrony przewidzianej w art. 9 Europejskiej Konwencji Praw Człowieka kluczowe jest nie tyle samo pojęcie Boga czy religii w sensie ścisłym, co fakt posiadania określonych przekonań, które kształtują tożsamość jednostki (Kociubiński 2011, s. 128). Prowadzi to do wniosku, że system ochrony musi być na tyle pojemny, by obejmować zarówno osoby wierzące, jak i te, które świadomie wybrały światopogląd areligijny.

Na szczególną uwagę zasługuje orzecznictwo Europejskiego Trybunału Praw Człowieka, które w sposób jednoznaczny potwierdza, że areligijność korzysta z ochrony na równi z religią. W przełomowym wyroku w sprawie *Kokkinakis p. Grecji* z 25 maja 1993 r. (skarga nr 14307/88) Trybunał uznał, że wolność myśli, sumienia i wyznania stanowi jeden z fundamentów społeczeństwa demokratycznego, która to wolność dotyczy nie tylko wierzących, ale również ateistów, agnostyków, sceptyków i osób obojętnych (wyrok ETPC z 25.05.1993 r., *Kokkinakis p. Grecji*, § 31; potwierdza to Kociubiński 2011, s. 119). To stanowisko zostało ugruntowane w wielu późniejszych orzeczeniach.

W sprawie *Buscarini i inni p. San Marino* z 18 lutego 1999 r. (skarga nr 24645/94) Trybunał uznał, że wymaganie od osób obejmujących funkcje publiczne złożenia przysięgi na Ewangelię stanowi naruszenie art. 9, gdyż zmusza jednostkę do uzewnętrznienia przekonań religijnych, których może nie podzielać (wyrok ETPC z 18.02.1999 r., *Buscarini i inni p. San Marino*, § 34). Dla potwierdzenia tej linii orzeczniczej kluczowe znaczenie ma wyrok w sprawie *Sinan Işık p. Turcji* z 2 lutego 2010 r. (skarga nr 21924/05), w którym Trybunał wprost stwierdził, że ochrona art. 9 obejmuje zarówno prawo do posiadania przekonań religijnych, jak i prawo do ich nieposiadania (wyrok ETPC z 2.02.2010 r., *Sinan Işık p. Turcji*, § 38-41). W konsekwencji, jak podsumowuje Kociubiński, "również jako religię w rozumieniu wolności gwarantowanej w art. 9 należy rozumieć brak identyfikacji z jakimkolwiek wyznaniem (ateizm, agnostycyzm)" (Kociubiński 2011, s. 117).

Sprawa *Lautsi p. Włochom* z 18 marca 2011 r. (skarga nr 30814/06), choć dotyczyła symboli religijnych, również wpisuje się w ten kontekst. Wielka Izba ETPC podkreśliła w niej obowiązek państwa do zachowania neutralności światopoglądowej w edukacji publicznej, co oznacza, że eksponowanie symboli religijnych może

wpływać na osoby o innych przekonaniach i wymaga wyważenia (wyrok ETPC z 18.03.2011 r., *Lautsi i inni p. Włochom*, § 60). Wszystkie te orzeczenia łączy wspólna oś: ochrona autonomii jednostki w sferze światopoglądowej, której integralną częścią jest zarówno wolność wyznawania religii, jak i wolność od niej.

Powyższe argumenty zdają się sumarycznie prowadzić do wniosku, że konieczne jest odrzucenie wyłącznie literalnej wykładni art. 53 ust. 2 na rzecz wykładni systemowej i teleologicznej, uwzględniającej aksjologiczny fundament konstytucji w postaci godności człowieka oraz standardy międzynarodowe. Wykładnia systemowa w związku z art. 30 i preambułą prowadzi do wniosku, że pojęcie „wolności religii" należy interpretować szeroko, jako obejmujące całokształt spraw związanych ze światopoglądem jednostki – zarówno w aspekcie pozytywnym (wybór i praktykowanie religii), jak i negatywnym (wolność od religii). Wykładnia teleologiczna nakazuje zaś odczytywać cel art. 53 jako ochronę autonomii jednostki w sferze jej najgłębszych przekonań, niezależnie od ich treści.

W tym ujęciu uzewnętrznianie poglądów areligijnych mieściłoby się w pojęciu „nauczania" (art. 53 ust. 2) – jeśli nauczanie może dotyczyć zasad wiary, to dlaczego nie miałoby dotyczyć zasad niewiary? Podobnie „uczestniczenie w obrzędach" w przypadku areligijności może przybrać formę uczestniczenia w wydarzeniach o charakterze świeckim, które pełnią analogiczną funkcję integracyjną i światopoglądową (np. humanistyczne ceremonie zaślubin czy pogrzebów). Jak wskazuje Complak, rozważania o możności ograniczenia wolności religii w warunkach służby wojskowej z jednoczesnym prawem do zwolnienia się z odbywania obowiązkowej służby wojskowej ze względu na przekonania religijne lub wyznawane zasady moralne, prowadzą do konieczności zastanowienia się nad wartością badanej swobody religijnej i obowiązującym stanem prawnym (Complak 2014, art. 53). Taka wykładnia nie prowadzi do „rozdęcia" pojęcia religii, lecz do uznania, że w demokratycznym państwie prawnym ochrona konstytucyjna nie może być uzależniona od tego, czy dane przekonania mieszczą się w tradycyjnie rozumianej kategorii „religii". Skoro bowiem – jak wskazuje Garlicki – potrzeby jednostki w zakresie poszukiwania wartości transcendentnych są zakotwiczone w jej godności, to również potrzeba odrzucenia tych wartości jest takim samym przejawem autonomii i zasługuje na ochronę (Garlicki 2016, art. 30). Rozwiązaniem *de lege ferenda* mogłoby być wyraźne rozszerzenie formuły art. 53 o ochronę światopoglądów niereligijnych, jednak już obecnie – w drodze wykładni prokonstytucyjnej – możliwe jest uznanie, że „wolność religii" implicite obejmuje również wolność od niej.

Zakończenie

Przeprowadzona analiza prowadzi do wniosku, że konstytucyjny model wolności religijnej w Polsce, choć oparty na solidnym fundamencie aksjologicznym w postaci godności człowieka, wykazuje pewną niekonsekwencję w zakresie ochrony areligijności. Literalne brzmienie art. 53 ust. 2, odnoszące się wyłącznie do „wyznawania lub przyjmowania religii", zdaje się pomijać osoby o światopoglądzie niereligijnym, tworząc tym samym nieuzasadnione zróżnicowanie sytuacji prawnej jednostek.

Postawiona we wstępie teza o konieczności teleologicznego rozszerzenia wykładni art. 53 ust. 2 na ochronę postaw areligijnych znajduje potwierdzenie w analizie aksjologicznych podstaw Konstytucji. Godność człowieka – jako źródło wszelkich wolności i praw – nie dopuszcza różnicowania ochrony prawnej w zależności od treści światopoglądu. Skoro godność przysługuje każdemu człowiekowi niezależnie od jego przekonań, to również wolność religijna, będąca jej emanacją, powinna być rozumiana jako obejmująca zarówno aspekt pozytywny (wybór i praktykowanie religii), jak i negatywny (wolność od religii). Argumenty natury aksjologicznej, teleologicznej i systemowej przemawiają za odrzuceniem wykładni zawężającej na rzecz interpretacji uwzględniającej pluralizm światopoglądowy, który jest immanentną cechą demokratycznego państwa prawnego. Jak trafnie wskazuje się w doktrynie, system wartości zbudowano z pomocą kategorii „Boga", ponieważ wiara jest wartością zasługującą na konstytucyjną ochronę, ale jednocześnie preambuła wyraźnie adresuje konstytucję również do tych, którzy tej wiary nie podzielają (Drelich 2019, s. 80-81).

Orzecznictwo Europejskiego Trybunału Praw Człowieka jednoznacznie potwierdza, że art. 9 Konwencji chroni zarówno osoby wierzące, jak i niewierzące, a państwa mają obowiązek zachowania neutralności światopoglądowej. Wskazać wypada na wyraźną tendencję do włączania areligijności w zakres konstytucyjnych gwarancji wolności sumienia i wyznania.

Konsekwencje praktyczne przyjętej wykładni są doniosłe. Oznacza ona bowiem, że uzewnętrznianie poglądów areligijnych – czy to w formie publicznej debaty, uczestnictwa w świeckich ceremoniach, czy też nauczania światopoglądu ateistycznego – podlega takiej samej ochronie jak uzewnętrznianie religii. Ograniczenia tej wolności możliwe są wyłącznie w granicach wyznaczonych przez art. 53 ust. 5, na zasadach tożsamych dla wszystkich światopoglądów. Przyszłe badania nad tym zagadnieniem powinny skoncentrować się na praktycznych implikacjach proponowanej wykładni, w szczególności w kontekście granic uzewnętrzniania areligijności w sferze publicznej oraz potencjalnych kolizji z wolnością religijną w wymiarze pozytywnym.

Istotne byłoby również zbadanie, na ile orzecznictwo sądów powszechnych i Trybunału Konstytucyjnego gotowe jest na przyjęcie zaprezentowanego tu szerokiego rozumienia wolności religijnej.

BIBLIOGRAFIA

Akty prawne

Ustawa z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania (Dz. U. z 2023 r., poz. 265).

Ustawa Zasadnicza dla Republiki Federalnej Niemiec z dnia 23 maja 1949 r., tłum. na jęz. polski, opublikowana przez Niemiecki Bundestag, [online] https://www.btg-bestellservice.de/pdf/80205000.pdf – dostęp 23.02.2026.

Karta Podstawowych Praw i Wolności, w: Konstytucja Republiki Czeskiej, tłum. na jęz. polski M. Kruk-Jarosz, opublikowana przez Bibliotekę Sejmową, [online] https://biblioteka.sejm.gov.pl/wp-content/uploads/2015/07/Czechy_pol_010811.pdf – dostęp 23.02.2026.

Orzecznictwo

Trybunał Konstytucyjny: Wyrok z 2 grudnia 2009 r., sygn. U 10/07, OTK-A 2009, nr 11, poz. 163. Wyrok z 8 czerwca 2011 r., sygn. K 3/09, OTK-A 2011, nr 5, poz. 39.

Europejski Trybunał Praw Człowieka: Wyrok z 25 maja 1993 r., Kokkinakis p. Grecji, skarga nr 14307/88. Wyrok z 18 lutego 1999 r., Buscarini i inni p. San Marino, skarga nr 24645/94. Wyrok z 2 lutego 2010 r., Sinan Işık p. Turcji, skarga nr 21924/05. Wyrok z 18 marca 2011 r., Lautsi i inni p. Włochom, skarga nr 30814/06.

Literatura

Abramowicz A.M.
2007 *Przedmiotowy zakres wolności religijnej*, „Studia z prawa wyznaniowego", nr 10.

Banaszak B.
2012 *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa.

Białogłowski W., Wasylik P.
2022 *O konieczności dekryminalizacji wybranych substancji psychoaktywnych (analiza prawnoporównawcza w ujęciu kontynentalnym i anglosaskim)*, „Opinie i Analizy Instytutu De Republica", Seria PRAWO, nr 30.

Borski M.
2014 *Godność człowieka jako wartość uniwersalna*, „Przegląd Prawa Publicznego", nr 3.

Chojnacki T.
2022 *Godność dłużnika. Idea godności człowieka a ograniczenia egzekucji sądowej*, „Przegląd Prawa Egzekucyjnego", nr 11.

Chrzczonowicz P., Kapelańska-Pręgowska J.
2015 *Handel organami z perspektywy prawa międzynarodowego oraz polskiego prawa karnego*, „Przegląd Sejmowy", nr 6.

Ciepły F.
2017 *Konstytucyjne podstawy rozstrzygania sporów odnoszących się do człowieka jako sprawcy czynu karnoprawnie relewantnego*, „CzPKiNP", nr 2.

Clark W.H.
1968 *Religious Aspects of Psychedelic Drugs*, „California Law Review", vol. 56.

Complak K.
2014 *[komentarz do art. 53]*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. M. Haczkowska, Warszawa.

Drelich S.
2019 *Podstawy aksjologii politycznej III RP na podstawie konstytucji z 2 kwietnia 1997 roku*, „Logos i etos", t. 50, nr 2.

Florczak-Wątor M.
2021 *[komentarz do art. 53]*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* wyd. II, red. P. Tuleja, LEX/el.

Fromm E.
2000 *Mieć czy być?*, przekł. J. Karłowski, Poznań.

Garlicki L.
2016 *[komentarz do art. 30]*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz.* Tom II, wyd. II, red. M. Zubik, Warszawa.

Garlicki L., Derlatka M.
2016 *[komentarz do wstępu]*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* red. L. Garlicki, M. Zubik, t. I, Warszawa.

Gogacz M.
1989 *Filozoficzna identyfikacja godności osoby*, „Studia Philosophiae Christianae", nr 25/1.

Granat M.
2022 *The meaning of human dignity in constitutional law*, [w:] *Rządy prawa jako wartość uniwersalna: księga jubileuszowa Profesora Krzysztofa Wójtowicza*, red. A. Kozłowski, Wrocław.

Grześkowiak A.
1999 *Wystąpienie otwierające konferencję*, [w:] *Przywrócenie ciągłości prawnej między III Rzecząpospolitą Polską i II Rzecząpospolitą Polską – implikacje i konsekwencje. Materiały z konferencji zorganizowanej przez Komisję Ustawodawczą Senatu,* red. M. Lipińska, E. Przychodaj, J. Pietrzak, Warszawa.

Kociubiński J.
2011 *Zakaz dyskryminacji ze względu na wyznanie w orzecznictwie Europejskiego Trybunału Praw Człowieka*, „Acta Erazmiana".

Korzeniewska-Lasota A.
2011 *Zakres wolności sumienia i wyznania*, „Studia warmińskie", nr 48.

Mariański J.
2019 *Godność ludzka jako wartość i sposoby jej uzasadniania w opinii młodzieży*, „Zeszyty Naukowe KUL", nr 4 (248).

Martínez-Torrón J.
2011 *Universal Rights in a World of Diversity – The Case of Religious Freedom*, [w:] *Freedom of Religion in the European Convention on Human Rights*, [b.m.w.].

Mazurek F.J.
1996 *Pojęcie godności człowieka. Historia i miejsce w projektach Konstytucji III Rzeczpospolitej*, „Roczniki Nauk Prawnych", t. VI.

Michałkiewicz-Kądziela E.
2020 *Prawo do tożsamości człowieka w prawie polskim i międzynarodowym*, Warszawa.

Pawłowicz J.J.
2012 *Godność człowieka fundamentem jego wolności*, „Українська полоністика", nr 9.

Polak P., Trzciński J.
2018 *Konstytucyjna zasada godności człowieka w świetle orzecznictwa Trybunału Konstytucyjnego*, „Gdańskie Studia Prawnicze", t. XL.

Rejs P.
2019 *Wolność sumienia i wyznania w orzecznictwie Trybunału Konstytucyjnego*, Warszawa.

Rymarz F.
2017 *Idea powołania adwokackiego i misji adwokatury (Głos w dyskusji na 100-lecie samorządu adwokackiego)*, „Palestra", nr 12.

Sarnecki P.
2016 *[komentarz do art. 53]*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz.* Tom II, wyd. II, red. L. Garlicki, M. Zubik, Warszawa.

Tuleja P.
2021 *[komentarz do art. 30]*, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz,* wyd. II, red. P. Tuleja, LEX/el.

Wroceński J.
2016 *Godność osoby ludzkiej podstawą prawa do wolności religijnej*, „Prawo kanoniczne", nr 3.

Zdybicka Z.J.
2006 *Człowiek i religia*, Lublin.

Źródła internetowe

Human Rights Without Frontiers 2024 *Belarus: Lukashenko attacks religious organizations, broadens grounds for their banning*, [online] https://hrwf.eu/belarus-lukashenko-attacks-religious-organizations-broadens-grounds-for-their-banning/(dostęp 23.02.2026).

SOVA Center 2025 *SOVA's address and recommendations at the OSCE Warsaw Human Dimension Conference - 2025*, [online] https://www.sova-center.ru/en/religion/conference-papers/2025/10/d47120/ (dostęp 23.02.2026).

https://copch.pl/baza-wiedzy/koscioly-i-inne-zwiazki-wyznaniowe-jako-podmioty-wolnosci-religijnej-zagadnienia-ogolne (dostęp 15.05.2023).

https://www.gov.pl/web/mswia/rejestr-kosciolow-i-innych-zwiazkow-wyznaniowych (dostęp 21.01.2021).

HUMAN DIGNITY AS THE BASIS FOR A TELEOLOGICAL INTERPRETATION OF RELIGIOUS FREEDOM. PROTECTION OF IRELIGIOUSNESS IN THE CONSTITUTION OF THE REPUBLIC OF POLAND

Summary: The article analyzes the constitutional model of religious freedom in Poland from the perspective of its axiological foundations, with particular emphasis on human dignity as the supreme constitutional value. The author points out that the political transformation and the adoption of the Constitution of the Republic of Poland in 1997 brought about a fundamental change in the understanding of the relationship between the state, religion, and the individual. Religious freedom – enshrined in Article 53 – ceased to be merely an institutional guarantee and became an element of inherent human dignity, from which all rights and freedoms are derived. However, the article highlights the tension between the literal wording of the provisions, which focuses on religiosity in the strict sense, and their axiological and systemic interpretation, indicating that religious freedom also includes freedom from religion and non-religious attitudes. The author argues that recognizing the equal protection of religious and non-religious beliefs stems both from the principle of equal dignity of individuals and from contemporary European standards concerning the protection of freedom of thought, conscience, and religion. The article formulates the thesis that a teleological interpretation of Article 53 of the Constitution of the Republic of Poland should also encompass non-religiosity as an expression of individual autonomy and an integral element of ideological pluralism in a democratic state ruled by law.

Keywords: human dignity, religious freedom, non-religiosity, Constitution of the Republic of Poland, teleological interpretation, ideological pluralism.

mgr **Wiktoria Świderska**

Uniwersytet Jana Kochanowskiego w Kielcach
Instytut Nauk o Bezpieczeństwie
ORCID: 0009-0000-4148-090X

BEZPIECZEŃSTWO CYFROWE PRACOWNIKÓW ZDALNYCH W DOBIE PRZYŚPIESZONEJ CYFRYZACJI

Streszczenie: Artykuł analizuje wyzwania bezpieczeństwa cyfrowego wynikające z upowszechnienia pracy zdalnej. Autorka wskazuje na ewolucję zagrożeń, w tym zmianę strategii hakerów z destrukcji na skrytą infiltrację. Omówiono techniczne środki ochrony (VPN, chmura, MFA), aspekty behawioralne, gdzie człowiek pozostaje najsłabszym ogniwem (phishing, socjotechnika), oraz ramy prawne, w tym obowiązki pracodawcy wynikające z RODO i Kodeksu pracy. Konkluzja podkreśla konieczność zintegrowanego podejścia łączącego technologię, edukację pracowników i procedury prawne. Wskazano również na znaczenie budowania świadomości cyberbezpieczeństwa wśród pracowników oraz rozwijania odpowiednich kompetencji cyfrowych. Autorka zwraca uwagę na potrzebę wdrażania spójnych polityk bezpieczeństwa i regularnych szkoleń z zakresu ochrony danych. Podkreślono także rolę stałego monitorowania systemów informatycznych i aktualizowania zabezpieczeń. Zwrócono uwagę, że skuteczna ochrona danych wymaga współpracy działów IT, kadry zarządzającej oraz samych pracowników. W rezultacie organizacje powinny traktować cyberbezpieczeństwo jako proces ciągły, wymagający stałego dostosowywania do nowych zagrożeń.

Słowa kluczowe: bezpieczeństwo cyfrowe, ochrona danych osobowych, RODO, cyberzagrożenia, phishing.

Wstęp

Ostatnie lata przyniosły wyraźne przyspieszenie procesów cyfryzacji, które w istotny sposób wpłynęły na funkcjonowanie przedsiębiorstw, instytucji publicznych oraz całego rynku pracy. Rozwój technologii informacyjno-komunikacyjnych,

upowszechnienie chmury obliczeniowej, a także narzędzi wspierających współpracę zespołową i systemów zdalnego dostępu do zasobów organizacji sprawiły, że wykonywanie obowiązków zawodowych coraz częściej odbywa się poza tradycyjną siedzibą pracodawcy (Bąk, 2009 s. 96). Zjawisko to zostało dodatkowo wzmocnione przez globalne kryzysy, w szczególności pandemię COVID-19, która zmusiła wiele organizacji do szybkiego przejścia na model pracy zdalnej lub hybrydowej (Sobczak, 2021, s. 148-149). Przyspieszona cyfryzacja firm i instytucji niesie ze sobą liczne korzyści. Należą do nich m.in. zwiększenie efektywności operacyjnej, większa elastyczność pracy, obniżenie kosztów oraz dostęp do szerszej puli talentów. Jednocześnie zjawisko to rodzi również nowe wyzwania, zwłaszcza w obszarze bezpieczeństwa cyfrowego. Yuval Noah Harari w książce 21 lekcji na XXI wiek z 2018 roku przekonuje, że rosnąca potęga technologii może stać się zagrożeniem. Jego zdaniem rozwój sztucznej inteligencji i nowoczesnych narzędzi cyfrowych niesie ryzyko osłabienia demokracji oraz otwarcia drogi do systemu totalnej, cyfrowej kontroli (Śledziewska, Włoch, 2020, s. 9-10).

Dane, które wcześniej były przetwarzane głównie w kontrolowanym środowisku infrastruktury firmowej, obecnie krążą pomiędzy wieloma urządzeniami, sieciami jak i lokalizacjami (Gembalska-Kwiecień, 2015, s. 46). Pracownicy zdalni w większości przypadków korzystają oczywiście z domowych sieci internetowych, prywatnych komputerów czy urządzeń też mobilnych, co znacząco poszerza powierzchnię potencjalnych ataków cybernetycznych (TTMS, 2026) [dostęp 13.02.2026]. Wzrost znaczenia pracy zdalnej i hybrydowej powoduje, że kwestie bezpieczeństwa informacji oraz ochrony danych osobowych stają się jednym z kluczowych obszarów zarządzania ryzykiem w organizacjach. Cyberzagrożenia, takie jak phishing, złośliwe oprogramowania, nieautoryzowany dostęp do systemów czy wycieki danych, ewoluują i stają się coraz bardziej zaawansowane wraz z rozwojem technologii. Przyczynia się do tego brak odpowiedniej świadomości pracowników, niewystarczające procedury czy niedostosowane narzędzia techniczne, które mogą prowadzić do poważnych incydentów naruszających poufność, integralność i dostępność danych (Delkomtech, 2026) [dostęp 13.01.2026]

Najnowszy raport przygotowany przez Picus Security wskazuje, że cyberprzestępcy zmieniają swoje metody działania i coraz rzadziej dążą do natychmiastowego zakłócania pracy systemów. Z ustaleń wynika, że zamiast szyfrować dane czy wywoływać widoczne ataki, koncentrują się na skrytości, długotrwałym utrzymaniu dostępu oraz pozostawaniu niewykrytymi w środowiskach firmowych. Współzałożyciel firmy i wiceprezes Picus Labs, Süleyman Özarslan, przekazał serwisowi eSecurity-Planet, że branża obserwuje strategiczną zmianę polegającą na odejściu od szybkich,

destrukcyjnych operacji na rzecz cichej i długotrwałej infiltracji. Dane z raportu pokazują spadek przypadków szyfrowania ransomware o 38%, przy jednoczesnym wzroście technik nastawionych na unikanie wykrycia i utrzymywanie ukrytego dostępu, które stanowią obecnie około 80% najczęściej stosowanych metod. Współczesny napastnik nie forsuje już zabezpieczeń siłą, lecz uzyskuje dostęp tak, jakby był uprawnionym użytkownikiem (Underhill, 2026) [dostęp 13.02.2026]

Należy zaznaczyć, iż cyfryzacja wpływa również bezpośrednio na obowiązki prawne pracodawców. Organizacje, które przetwarzają dane osobowe, w szczególności dane pracowników, klientów czy kontrahentów, są zobowiązane do zapewnienia zgodności z obowiązującymi regulacjami prawnymi (Unterschütz, 2021, LEX/el). Należą do nich oczywiście przepisy o ochronie danych osobowych. Praca zdalna nie zwalnia pracodawcy z odpowiedzialności za bezpieczeństwo danych; obecnie wręcz wymaga wdrożenia wielu dodatkowych środków organizacyjnych, jak i technicznych, adekwatnych do zmienionych warunków przetwarzania informacji. Niedopełnienie tych obowiązków może skutkować odpowiedzialnością administracyjną, cywilną, a w niektórych przypadkach także karną. Naruszenia ochrony danych mogą prowadzić do dotkliwych konsekwencji finansowych, takich jak kary administracyjne, koszty usuwania skutków incydentów, a także roszczenia odszkodowawcze (Marciniak, 2023, LEX/el). Równie istotne są konsekwencje wizerunkowe, które mogą trwale obniżyć zaufanie klientów, partnerów biznesowych oraz opinii publicznej do danej organizacji. W gospodarce opartej na informacji reputacja w obszarze bezpieczeństwa danych staje się jednym z kluczowych elementów budowania przewagi konkurencyjnej. Praca zdalna wiąże się także ze zwiększonym ryzykiem nieuprawnionego ujawnienia danych osobowych oraz poufnych informacji firmowych. Brak fizycznej kontroli nad środowiskiem pracy, korzystanie z niezabezpieczonych sieci Wi-Fi, a także używanie tych samych urządzeń do celów służbowych i prywatnych sprzyjają sytuacjom, w których dochodzi do nieumyślnych naruszeń bezpieczeństwa informacji (Delkomtech, 2026) [dostęp 13.01.2026]. Z tego względu ochrona danych w modelu pracy zdalnej wymaga nie tylko odpowiednich narzędzi technicznych, ale także kształtowania właściwych postaw i nawyków wśród pracowników.

Celem niniejszego artykułu jest analiza wyzwań związanych z bezpieczeństwem cyfrowym pracowników zdalnych funkcjonujących w warunkach przyspieszonej cyfryzacji. W szczególności podjęta zostanie próba identyfikacji najczęstszych zagrożeń, z jakimi mierzą się organizacje stosujące model pracy zdalnej lub hybrydowej. Artykuł ma również na celu omówienie kluczowych aspektów prawnych związanych z ochroną danych oraz odpowiedzialnością pracodawców za zapewnienie bezpieczeństwa informacji w środowisku pracy zdalnej. Jednocześnie zwrócono uwagę na

znaczenie czynnika ludzkiego, w tym poziomu świadomości pracowników, kultury bezpieczeństwa informacji oraz roli szkoleń i procedur wewnętrznych. Odrębną część rozważań stanowią zagadnienia prawne dotyczące ochrony danych osobowych oraz odpowiedzialności przedsiębiorstw. Analiza obejmuje obowiązki pracodawców wynikające z przepisów prawa, w tym konieczność wdrażania odpowiednich środków organizacyjnych i technicznych, dokumentowania procesów przetwarzania danych oraz reagowania na incydenty naruszenia bezpieczeństwa. Podjęcie tej problematyki wydaje się szczególnie istotne w kontekście dalszego rozwoju cyfrowych form organizacji pracy, jak również potrzeby lepszego zrozumienia zagrożeń i obowiązków związanych z bezpieczeństwem cyfrowym. Stanowi to bowiem niezbędny warunek zapewnienia stabilnego i bezpiecznego funkcjonowania firm oraz instytucji w erze cyfrowej.

Praca zdalna a bezpieczeństwo cyfrowe

Rozpowszechnienie pracy zdalnej w znaczący sposób wpłynęło na sposób zarządzania bezpieczeństwem informacji w organizacjach. W modelu tradycyjnym większość procesów realizowana była w ściśle kontrolowanym środowisku infrastruktury firmowej, chronionej zarówno pod względem fizycznym, jak i systemowym przez wyspecjalizowane działy IT (Kindervag, 2010) [dostęp 22.01.2026]. Przeniesienie obowiązków służbowych do domów pracowników doprowadziło do rozproszenia środowiska przetwarzania danych, co w istotny sposób podniosło poziom ryzyka cybernetycznego.

Jednym z podstawowych zagrożeń wynikających z pracy w domu jest korzystanie z domowych sieci Wi-Fi, które często nie spełniają standardów bezpieczeństwa stosowanych w sieciach korporacyjnych. Niewłaściwie skonfigurowane routery, słabe hasła, brak szyfrowania lub nieaktualne oprogramowanie sprzętowe mogą umożliwić osobom trzecim przechwycenie transmisji danych lub uzyskanie nieautoryzowanego dostępu do urządzeń pracownika (FS-ISAC, 2020) [dostęp 22.01.2026]. Dodatkowym problemem jest współdzielenie sieci z innymi domownikami, których aktywność w Internecie może pośrednio wpływać na bezpieczeństwo danych służbowych. Istotnym ryzykiem pozostaje także korzystanie z tych samych urządzeń do celów zawodowych i prywatnych. W wielu przypadkach pracownicy używają własnego sprzętu, który nie jest objęty polityką bezpieczeństwa firmy. Instalowanie niezweryfikowanego oprogramowania, wykorzystywanie prywatnych nośników danych oraz brak podstawowych zabezpieczeń zwiększają prawdopodobieństwo infekcji złośliwym oprogramowaniem lub nieumyślnego ujawnienia informacji poufnych

(SailPoint, 2025) [dostęp 23.01.2026]. Granica między sferą prywatną a zawodową ulega zatarciu, co utrudnia skuteczną kontrolę nad przetwarzaniem danych.

Skala zagrożeń znajduje odzwierciedlenie w statystykach incydentów cyberbezpieczeństwa. Raporty międzynarodowych organizacji zajmujących się bezpieczeństwem informacji, takich jak agencje Unii Europejskiej czy uznane firmy badawcze, wskazują na wyraźny wzrost liczby ataków wymierzonych w pracowników zdalnych. Szczególnie często odnotowywane są kampanie phishingowe, ataki typu ransomware oraz próby przejęcia danych uwierzytelniających. Według danych za 2024 rok odnotowano 60-procentowy wzrost liczby zgłoszeń dotyczących naruszeń bezpieczeństwa systemów teleinformatycznych oraz 23-procentowy wzrost faktycznie potwierdzonych incydentów w porównaniu z rokiem 2023. Pełnomocnik Rządu ds. Cyberbezpieczeństwa po raz drugi w historii zaprezentował raport podsumowujący działania państwa w obszarze ochrony cyberprzestrzeni w 2024 r. Niniejsze opracowanie ukazuje zarówno skalę i charakter współczesnych zagrożeń, jak i aktywność instytucjonalną podmiotów odpowiedzialnych za bezpieczeństwo cyfrowe, a także formułuje rekomendacje strategiczne na kolejne lata. W odpowiedzi na rosnącą dynamikę zagrożeń ministerstwo właściwe do spraw cyfryzacji prowadzi prace nad uruchomieniem portalu cyber.gov.pl, wspiera jednostki samorządu terytorialnego w procesach migracji do środowisk chmurowych oraz inicjuje zmiany legislacyjne dotyczące krajowego systemu cyberbezpieczeństwa (Ministerstwo Cyfryzacji, Departament Cyberbezpieczeństwa 2025).

Praca zdalna stała się atrakcyjnym celem dla cyberprzestępców ze względu na mniejszą kontrolę nad środowiskiem pracy oraz większe obciążenie psychiczne pracowników, sprzyjające popełnianiu błędów (Zając, 2021) [dostęp 23.01.2026]. Naruszenia bezpieczeństwa informacji mają bezpośredni wpływ na zobowiązania prawne firmy. Ujawnienie danych osobowych lub poufnych informacji handlowych może skutkować koniecznością zgłoszenia incydentu do właściwego organu nadzorczego, powiadomienia osób, których dane dotyczą, a także poniesienia odpowiedzialności finansowej. Pracodawca, jako administrator danych, ponosi odpowiedzialność za zapewnienie odpowiedniego poziomu ochrony niezależnie od tego, czy praca wykonywana jest w siedzibie firmy, czy w trybie zdalnym (Rozporządzenie (UE) 2016/679, art. 33). Brak odpowiednich środków zabezpieczających może zostać uznany za naruszenie obowiązków wynikających z przepisów prawa.

Techniczne aspekty ochrony

Podstawowym elementem technicznej ochrony pracy zdalnej jest zapewnienie bezpiecznego połączenia między urządzeniem pracownika a zasobami firmowymi. W tym celu powszechnie stosuje się wirtualne sieci prywatne, które umożliwiają szyfrowanie transmisji danych oraz ograniczenie dostępu do systemów wyłącznie dla uprawnionych użytkowników (Rozporządzenie Prezesa Rady Ministrów 2015, s. 232). Usługa VPN tworzy bezpieczny tunel komunikacyjny, chroniąc dane przed podsłuchem i modyfikacją, nawet podczas korzystania z publicznych lub niezaufanych sieci (Microsoft, 2025) [dostęp 23.01.2026].

Szyfrowanie połączeń stanowi jeden z fundamentów bezpieczeństwa informacji w środowisku pracy zdalnej. Mechanizmy kryptograficzne zapewniają poufność i integralność danych, które są przesyłane pomiędzy użytkownikiem a serwerami organizacji. Odpowiednio skonfigurowane protokoły szyfrowania minimalizują ryzyko przechwycenia informacji przez osoby trzecie, jednak ich skuteczność zależy od prawidłowego wdrożenia oraz regularnej aktualizacji (International Organization for Standardization 2022, ISO/IEC 27002). Równie istotnym obszarem są zabezpieczenia urządzeń końcowych, z których korzystają pracownicy. Oprogramowanie antywirusowe, zapory sieciowe oraz systemy wykrywania zagrożeń pozwalają na identyfikację i neutralizację złośliwego oprogramowania. Regularne aktualizacje systemów operacyjnych i aplikacji eliminują znane luki bezpieczeństwa, które mogłyby zostać wykorzystane przez cyberprzestępców. Zaniedbania w tym zakresie stanowią jedną z najczęstszych przyczyn skutecznych ataków (Robinette, 2023) [dostęp 23.01.2026]. Coraz większe znaczenie w pracy zdalnej odgrywa chmura obliczeniowa, umożliwiająca dostęp do danych i aplikacji z dowolnego miejsca. Rozwiązania chmurowe oferują wysoki poziom dostępności i skalowalności, jednak wiążą się również z określonymi ryzykami (Komisja Europejska 2012, COM(2012) 529). Niewłaściwe zarządzanie uprawnieniami, brak segmentacji danych oraz stosowanie słabych mechanizmów uwierzytelniania mogą prowadzić do nieautoryzowanego dostępu do zasobów firmowych oraz naruszenia poufności, integralności i dostępności informacji. Szczególnym zagrożeniem w środowisku chmurowym jest błędna konfiguracja usług, która może skutkować przypadkowym publicznym udostępnieniem danych lub nadaniem zbyt szerokich uprawnień użytkownikom i aplikacjom. Tego rodzaju incydenty często nie wynikają z luk technologicznych samej chmury, lecz z niewystarczającej kontroli procesów po stronie organizacji korzystającej z usług zewnętrznych dostawców (Cloud Security Alliance 2019, Top threats to cloud computing: Egregious eleven).

Istotnym wyzwaniem jest również kwestia odpowiedzialności za bezpieczeństwo danych w modelu chmurowym. Dostawcy usług chmurowych zapewniają zabezpieczenia infrastruktury fizycznej oraz podstawowych warstw systemowych, natomiast odpowiedzialność za właściwą konfigurację usług, zarządzanie dostępem i ochronę danych spoczywa na kliencie. Brak świadomości tego podziału odpowiedzialności może prowadzić do fałszywego poczucia bezpieczeństwa oraz zaniedbań w obszarze zarządzania ryzykiem (National Institute of Standards and Technology 2012, SP 800-146).

W kontekście pracy zdalnej szczególnego znaczenia nabiera kontrola dostępu do zasobów chmurowych. Stosowanie zasady minimalnych uprawnień oraz regularna weryfikacja kont użytkowników pozwalają ograniczyć ryzyko nadużyć i nieautoryzowanego dostępu. Dodatkowym zabezpieczeniem jest wieloskładnikowe uwierzytelnianie, które znacząco utrudnia przejęcie konta nawet w przypadku ujawnienia hasła. Rozwiązania te są szczególnie istotne w sytuacji, gdy pracownicy logują się do systemów z różnych lokalizacji i urządzeń. Nie bez znaczenia pozostaje również kwestia przechowywania i lokalizacji danych w chmurze. Przetwarzanie informacji poza fizyczną infrastrukturą organizacji wymaga uwzględnienia wymogów prawnych dotyczących ochrony danych, w szczególności w zakresie transferu danych do państw trzecich (National Institute of Standards and Technology 2020, SP 800-53 Rev. 5). Organizacje powinny wdrożyć jasno określone polityki dotyczące klasyfikacji danych, zasad ich przechowywania oraz tworzenia kopii zapasowych, aby zapewnić ciągłość działania oraz możliwość szybkiego odtworzenia informacji w przypadku wystąpienia incydentu.

Właściwie zaprojektowane i wdrożone rozwiązania chmurowe mogą skutecznie wspierać bezpieczną pracę zdalną, pod warunkiem że są one elementem spójnej strategii bezpieczeństwa informacji. Integracja zabezpieczeń technicznych z procedurami organizacyjnymi oraz regularne monitorowanie środowiska chmurowego pozwalają minimalizować ryzyka i jednocześnie korzystać z korzyści, jakie niesie ze sobą elastyczny dostęp do danych i aplikacji firmowych.

Zagrożenia behawioralne

Zagrożenia behawioralne stanowią jeden z kluczowych obszarów ryzyka w kontekście bezpieczeństwa cyfrowego pracowników zdalnych. Nawet najlepiej zaprojektowane zabezpieczenia techniczne mogą okazać się nieskuteczne, jeżeli użytkownik końcowy zostanie zmanipulowany do wykonania określonego działania. Cyberprzestępcy coraz częściej koncentrują się na wykorzystywaniu czynnika ludzkiego, uznawanego za najsłabsze ogniwo systemu bezpieczeństwa informacji.

Jednym z najczęściej występujących zagrożeń behawioralnych jest phishing, będący formą ataku socjotechnicznego polegającego na podszywaniu się pod zaufane podmioty w celu wyłudzenia poufnych informacji lub nakłonienia ofiary do określonego działania. Ataki phishingowe przybierają różne formy, w tym fałszywe wiadomości e-mail, SMS-y oraz komunikaty przesyłane za pośrednictwem firmowych komunikatorów. Ich treść często odwołuje się do sytuacji wymagających pilnej reakcji, takich jak rzekome problemy z kontem, konieczność natychmiastowego wykonania przelewu lub aktualizacji danych logowania (Hadnagy, 2018, s. 229). W warunkach pracy zdalnej, gdzie komunikacja odbywa się głównie w formie elektronicznej, a bezpośredni kontakt z przełożonymi jest ograniczony, skuteczność tego typu ataków znacząco wzrasta. Socjotechnika wykorzystuje mechanizmy psychologiczne, takie jak autorytet, strach, presja czasu czy chęć pomocy, aby skłonić pracownika do naruszenia zasad bezpieczeństwa (Goćkowski, 1968, s. 84). Przykładem może być podszywanie się pod pracownika działu IT lub przełożonego oraz prośba o przekazanie danych uwierzytelniających. W środowisku pracy zdalnej, gdzie weryfikacja tożsamości rozmówcy jest utrudniona, ryzyko powodzenia takich działań jest szczególnie wysokie.

Ograniczanie zagrożeń behawioralnych wymaga systematycznego budowania świadomości pracowników w zakresie bezpieczeństwa informacji. Szkolenia z cyberbezpieczeństwa powinny obejmować nie tylko podstawowe zasady ochrony danych, lecz także praktyczne przykłady ataków oraz sposoby ich rozpoznawania. Regularne przypominanie zasad bezpiecznego korzystania z poczty elektronicznej, haseł oraz urządzeń mobilnych pozwala utrwalać właściwe nawyki i zwiększa czujność pracowników. Istotne jest również dostosowanie treści szkoleń do aktualnych zagrożeń oraz specyfiki pracy zdalnej. Procedury bezpieczeństwa stanowią uzupełnienie działań edukacyjnych i pełnią istotną funkcję organizacyjną. Jasno określone zasady dotyczące postępowania z danymi, korzystania z narzędzi informatycznych oraz zgłaszania podejrzanych zdarzeń pomagają ograniczyć ryzyko przypadkowych naruszeń. Pracownik, który wie, jak powinien reagować w sytuacji potencjalnego zagrożenia, jest mniej podatny na manipulację i szybciej informuje odpowiednie osoby o incydencie.

Szczególną rolę w zarządzaniu zagrożeniami behawioralnymi odgrywa polityka bezpieczeństwa informacji obowiązująca w firmie. Dokument ten powinien precyzyjnie określać obowiązki pracowników, zakres odpowiedzialności oraz procedury reagowania na incydenty bezpieczeństwa (Socium, b.d.) [dostęp 26.01.2026]. Skuteczna polityka bezpieczeństwa uwzględnia zarówno aspekty techniczne, jak i organizacyjne, tworząc spójne ramy działania w sytuacjach kryzysowych. Procedury reagowania na incydenty powinny obejmować sposób identyfikacji zagrożenia, kanały

zgłaszania naruszeń, działania naprawcze oraz analizę przyczyn zdarzenia w celu zapobiegania podobnym sytuacjom w przyszłości (Nflo, b.d.) [dostęp 26.01.2026].

W kontekście pracy zdalnej znaczenie zagrożeń behawioralnych dodatkowo rośnie. Rozproszone środowisko pracy, ograniczony bezpośredni nadzór oraz intensywna komunikacja elektroniczna sprzyjają skuteczności działań socjotechnicznych.

Aspekty prawne

Dynamiczny rozwój pracy zdalnej wymusił na organizacjach konieczność dostosowania praktyk przetwarzania danych do obowiązujących regulacji prawnych, w szczególności przepisów dotyczących ochrony danych osobowych oraz prawa pracy. Praca wykonywana poza siedzibą pracodawcy nie zmienia faktu, że pracodawca jako administrator danych ponosi odpowiedzialność za zgodność procesów przetwarzania z przepisami prawa oraz za zapewnienie odpowiedniego poziomu bezpieczeństwa informacji (RODO, 2024).

Ochrona danych osobowych, uregulowana w przepisach RODO, nakłada na pracodawcę szereg obowiązków związanych z przetwarzaniem danych pracowników, klientów oraz kontrahentów. Do podstawowych obowiązków należy zapewnienie, aby dane były przetwarzane zgodnie z zasadami legalności, rzetelności i przejrzystości, a także aby były adekwatne, ograniczone do niezbędnego minimum oraz odpowiednio zabezpieczone (Dz.U. UE L 119, s. 1 ze zm.). W kontekście pracy zdalnej oznacza to konieczność wdrożenia rozwiązań organizacyjnych i technicznych, które umożliwią bezpieczne przetwarzanie danych poza kontrolowanym środowiskiem biurowym. Szczególne znaczenie mają zasady minimalizacji danych oraz kontroli dostępu. Pracownicy zdalni powinni mieć dostęp wyłącznie do informacji niezbędnych do wykonywania powierzonych im obowiązków. Ograniczenie zakresu przetwarzanych danych zmniejsza ryzyko naruszeń oraz potencjalne skutki ewentualnych incydentów. Równie istotne jest stosowanie mechanizmów uwierzytelniania i autoryzacji, które umożliwiają jednoznaczną identyfikację użytkownika oraz monitorowanie dostępu do systemów informatycznych (UODO, 2025) [dostęp 30.01.2026].

Naruszenia ochrony danych osobowych mogą prowadzić do poważnych konsekwencji prawnych. W przypadku stwierdzenia nieprawidłowości organ nadzorczy może nałożyć na administratora danych kary finansowe, których wysokość zależy od charakteru i skali naruszenia. Oprócz sankcji administracyjnych pracodawca może ponosić odpowiedzialność cywilną wobec osób, których dane zostały naruszone, w tym obowiązek naprawienia szkody majątkowej lub niemajątkowej (Dz.U. UE L 119, s. 1 ze zm.). Skutki te dodatkowo potęgują straty wizerunkowe i utratę zaufania do organizacji.

Istotnym obszarem regulacji jest również prawo pracy, które określa obowiązki pracowników wykonujących pracę zdalną. Pracownik zobowiązany jest do przestrzegania zasad bezpieczeństwa i higieny pracy oraz wewnętrznych regulacji dotyczących ochrony informacji. Obejmuje to między innymi obowiązek korzystania z narzędzi i systemów zgodnie z ich przeznaczeniem, ochronę haseł dostępowych oraz nieudostępnianie danych osobom trzecim. Naruszenie tych obowiązków może skutkować odpowiedzialnością porządkową, a w skrajnych przypadkach także odpowiedzialnością materialną lub rozwiązaniem stosunku pracy (Dz. U. 1974 nr 24 poz. 141, z późn. zm.). W kontekście pracy zdalnej pojawia się także zagadnienie monitorowania pracowników. Pracodawca ma prawo kontrolować sposób wykonywania pracy oraz korzystania z narzędzi służbowych, jednak działania te muszą pozostawać w zgodzie z przepisami o ochronie danych osobowych oraz z poszanowaniem prywatności pracownika (Dz. U. 1974 nr 24 poz. 141, z późn. zm.). Monitorowanie powinno być proporcjonalne, jasno określone w regulacjach wewnętrznych oraz poprzedzone poinformowaniem pracowników o jego zakresie i celu. Niedopuszczalne jest stosowanie nadmiernych form kontroli, które mogłyby naruszać prawa i wolności pracowników (Dz.U. UE L 119, s. 1 ze zm.).

Istotnym instrumentem prawnym regulującym zasady pracy zdalnej są umowy oraz polityki wewnętrzne obowiązujące w organizacji. Regulaminy pracy zdalnej określają zasady organizacji pracy, odpowiedzialność stron oraz wymagania dotyczące bezpieczeństwa informacji. Polityki bezpieczeństwa IT precyzują natomiast standardy korzystania z systemów informatycznych, urządzeń służbowych oraz procedury reagowania na incydenty (UODO, 2025) [dostęp 30.01.2026]. Ważnym elementem tych dokumentów są również klauzule dotyczące poufności, które zobowiązują pracowników do ochrony informacji zarówno w trakcie trwania stosunku pracy, jak i po jego zakończeniu. Przewidziane w nich sankcje za naruszenia pełnią funkcję prewencyjną i wzmacniają kulturę bezpieczeństwa w organizacji (Dz. U. 1974 nr 24 poz. 141, z późn. zm.).

Przykłady naruszeń bezpieczeństwa

Analiza rzeczywistych incydentów bezpieczeństwa w organizacjach korzystających z pracy zdalnej wskazuje, że do naruszeń dochodzi zarówno na skutek zaawansowanych ataków cybernetycznych, jak i prostych błędów ludzkich. Częstym scenariuszem są ataki phishingowe, w wyniku których pracownicy nieświadomie przekazują dane logowania do systemów firmowych (Chen, 2026) [dostęp 30.01.2026]. Uzyskany w ten sposób dostęp umożliwia cyberprzestępcom kradzież danych, instalację

złośliwego oprogramowania lub dalszą eskalację ataku w infrastrukturze organizacji. Innym przykładem naruszeń są wycieki danych spowodowane niewłaściwą konfiguracją narzędzi chmurowych lub korzystaniem z niezabezpieczonych urządzeń prywatnych. Praca zdalna sprzyja sytuacjom, w których dokumenty zawierające dane osobowe lub informacje poufne są przechowywane lokalnie bez odpowiednich zabezpieczeń lub przesyłane za pośrednictwem nieautoryzowanych kanałów komunikacji (Datastackhub, 2025) [dostęp 30.01.2026]. W takich przypadkach nawet brak działania osób trzecich może prowadzić do naruszenia przepisów o ochronie danych.

Konsekwencje prawne naruszeń bezpieczeństwa danych mają charakter wielowymiarowy. Organizacje dotknięte incydentami muszą liczyć się z karami administracyjnymi nakładanymi przez organy nadzorcze, a także z postępowaniami sądowymi inicjowanymi przez osoby poszkodowane. W praktyce wiele spraw dotyczy niewystarczających środków technicznych i organizacyjnych, braku szkoleń pracowników lub niedostosowania procedur do specyfiki pracy zdalnej. Analiza tych przypadków pokazuje, że odpowiedzialność pracodawcy często wynika nie tyle z samego faktu wystąpienia incydentu, ile z braku należytej staranności w zapobieganiu zagrożeniom (Enisa, 2022) [dostęp 30.01.2026].

Wnioski płynące z analizy naruszeń bezpieczeństwa wskazują na konieczność stosowania najlepszych praktyk zarówno w obszarze technicznym, jak i prawnym. Do kluczowych działań należy zaliczyć regularne szkolenia pracowników, aktualizację polityk bezpieczeństwa, stosowanie zasady minimalnych uprawnień oraz systematyczne audyty procesów przetwarzania danych. Z perspektywy prawnej istotne jest również dokumentowanie działań podejmowanych w celu zapewnienia bezpieczeństwa, co może stanowić istotny element obrony w przypadku kontroli lub postępowania sądowego. Praca zdalna, mimo licznych korzyści, wymaga od organizacji świadomego i kompleksowego podejścia do bezpieczeństwa cyfrowego (Dz.U. UE L 119, s. 1 ze zm.).

Zakończenie

Dynamiczny rozwój pracy zdalnej, będący jednym z kluczowych efektów przyspieszonej cyfryzacji, w trwały sposób zmienił funkcjonowanie współczesnych organizacji. Przeprowadzona analiza wskazuje, że bezpieczeństwo cyfrowe pracowników zdalnych nie może być ujmowane wyłącznie w kategoriach technicznych, lecz wymaga podejścia kompleksowego, uwzględniającego również czynniki behawioralne oraz ramy prawne. Dopiero integracja tych trzech perspektyw pozwala

na skuteczne ograniczanie ryzyka związanego z przetwarzaniem danych poza tradycyjnym środowiskiem biurowym.

Praca zdalna znacząco zwiększa powierzchnię potencjalnych zagrożeń, zarówno poprzez korzystanie z rozproszonych środowisk informatycznych, jak i poprzez większe obciążenie odpowiedzialnością samych pracowników. Ryzyka wynikające z używania domowych sieci, prywatnych urządzeń czy narzędzi chmurowych pokazują, że ochrona danych wymaga odpowiednio dobranych zabezpieczeń technicznych, jednak nawet najbardziej zaawansowane technologie nie zapewnią pełnej ochrony, jeżeli pracownicy nie będą świadomi zagrożeń oraz zasad bezpiecznego postępowania z informacją. Szczególnie istotnym wnioskiem jest fakt, że naruszenia bezpieczeństwa informacji w środowisku pracy zdalnej mają konsekwencje wykraczające poza sferę techniczną i wiążą się z realnymi skutkami prawnymi, w tym odpowiedzialnością administracyjną i cywilną pracodawców (Dz.U. UE L 119, s. 1 ze zm.). Przepisy dotyczące ochrony danych osobowych oraz prawa pracy jednoznacznie wskazują, że odpowiedzialność za bezpieczeństwo danych spoczywa na organizacji, niezależnie od miejsca wykonywania pracy. Brak odpowiednich procedur, szkoleń czy polityk bezpieczeństwa może zostać uznany za naruszenie obowiązku należytej staranności.

W świetle powyższych ustaleń kluczowe znaczenie mają rekomendacje praktyczne, które mogą realnie podnieść poziom bezpieczeństwa pracy zdalnej. Do podstawowych działań należy zaliczyć stosowanie bezpiecznych mechanizmów zdalnego dostępu, takich jak wirtualne sieci prywatne, szyfrowanie połączeń oraz wieloskładnikowe uwierzytelnianie. Regularne aktualizacje systemów operacyjnych i oprogramowania, a także zabezpieczenia urządzeń końcowych, stanowią fundament ochrony przed powszechnymi zagrożeniami cybernetycznymi. Równie istotne jest inwestowanie w rozwój kompetencji pracowników. Szkolenia z zakresu cyberbezpieczeństwa oraz podnoszenie świadomości zagrożeń pozwalają ograniczyć ryzyko ataków socjotechnicznych i błędów ludzkich. Pracownik świadomy zagrożeń staje się aktywnym uczestnikiem systemu bezpieczeństwa, a nie jedynie jego potencjalnym słabym punktem. Działania edukacyjne powinny być uzupełnione przez jasne i zrozumiałe regulaminy pracy zdalnej oraz polityki bezpieczeństwa IT, zgodne z obowiązującymi przepisami prawa.

Z perspektywy przyszłości bezpieczeństwa cyfrowego coraz większe znaczenie będą odgrywać rozwiązania oparte na sztucznej inteligencji i automatyzacji. Systemy te umożliwiają szybsze wykrywanie anomalii, analizę zachowań użytkowników oraz reagowanie na incydenty w czasie rzeczywistym (Gartner, 2025) [dostęp 11.02.2026]. W środowisku pracy hybrydowej i zdalnej, charakteryzującym się dużą dynamiką oraz zmiennością, takie podejście może znacząco zwiększyć skuteczność ochrony

danych. Jednocześnie istotnym kierunkiem rozwoju pozostają regularne audyty bezpieczeństwa oraz audyty zgodności z przepisami prawa. Umożliwiają one identyfikację słabych punktów w systemach technicznych i procedurach organizacyjnych, a także bieżące dostosowywanie działań do zmieniających się wymagań prawnych i technologicznych. Audyty te nabierają szczególnego znaczenia w środowiskach hybrydowych, w których granice pomiędzy infrastrukturą firmową a zewnętrzną stają się coraz mniej wyraźne (Microsoft, b.d.) [dostęp 11.02.2026].

Podsumowując, kluczowym elementem skutecznego zarządzania bezpieczeństwem pracy zdalnej jest pogłębiona współpraca pomiędzy działami IT a działami prawnymi w organizacjach. Integracja kompetencji technicznych i prawniczych umożliwia opracowanie spójnych oraz efektywnych rozwiązań, które nie tylko zapewniają ochronę danych, lecz także gwarantują zgodność z obowiązującymi regulacjami prawnymi. W warunkach dalszej cyfryzacji oraz rosnącej popularności pracy zdalnej podejście to przestaje mieć charakter jedynie dobrej praktyki organizacyjnej, a staje się koniecznym warunkiem zapewnienia bezpiecznego i stabilnego funkcjonowania współczesnych organizacji.

BIBLIOGRAFIA

Akty prawne i dokumenty

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Wykorzystanie potencjału chmury obliczeniowej w Europie (COM (2012) 529 final), Komisja Europejska.

Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2024 rok, Ministerstwo Cyfryzacji, Warszawa 2025.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) (Dz.U. UE L 119, s. 1 ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 9 listopada 2015 r. zmieniające rozporządzenie w sprawie określenia wzorów formularzy sprawozdawczych, objaśnień co do sposobu ich wypełniania oraz wzorów kwestionariuszy i ankiet statystycznych stosowanych w badaniach statystycznych ustalonych w programie badań statystycznych statystyki publicznej na rok 2015 (Dz. U. 2015, poz. 2044).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy. (Dz. U. 1974 nr 24 poz. 141, z późn. zm.).

Normy i raporty

Cloud Security Alliance, *Top threats to cloud computing: Egregious eleven*, 2019.

International Organization for Standardization, *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*, 2022.

National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, 2020.

National Institute of Standards and Technology, *Cloud Computing Synopsis and Recommendations*, Special Publication 800-146, 2012.

Literatura

Bąk E.
2009 *Nietypowe formy zatrudnienia na rynku pracy*, Warszawa.

Gembalska-Kwiecień A.
2015 *Prawidłowa organizacja środowiska pracy jako jeden z elementów poprawy bezpieczeństwa pracy*, „Zeszyty Naukowe Politechniki Śląskiej – seria: Organizacja i Zarządzanie".

Goćkowski J.
1968 *Kultura, socjotechnika i style oddziaływania na grupy i jednostki*, [w:] *Socjotechnika*, red. A. Podgórecki, Warszawa.

Hadnagy C.
2018 *Social Engineering: The Science of Human Hacking* (2nd ed.), Wiley.

Marciniak J.
2023 *Praca zdalna i hybrydowa. Aspekty organizacyjne i prawne*, LEX/el, Warszawa.

Sobczak A.
2021 *Praca zdalna w warunkach pandemii COVID-19. Problemy efektywności i nierówności społecznych*, „Wychowanie w Rodzinie", t. XXIV (1/2021).

Śledziewska K., Włoch R.
2020 *Gospodarka cyfrowa. Jak nowe technologie zmieniają świat*, Warszawa.

Unterschütz J.
2021 *Praca zdalna*, [w:] M. Mędrala, *Praca zdalna w polskim systemie prawnym*, LEX/el, Warszawa.

Źródła internetowe

Chen D.
2026 *Remote And Hybrid Work In The Cyber Security Industry Statistics*, https://zipdo.co/remote-and-hybrid-work-in-the-cyber-security-industry-statistics/ (dostęp: 27.04.2026).

Datastackhub
2025 *Data Loss Statistics for 2025–2026*, https://www.datastackhub.com/insights/data-loss-statistics/ (dostęp: 27.04.2026).

Delkomtech
2026 *Bezpieczeństwo informacji w firmie,* https://www.delkomtech.pl/bezpieczenstwo-informacji/ (dostęp: 27.04.2026).

Delkomtech
2026 *Cyberzagrożenia w firmie – co naprawdę grozi Twoim danym i systemom?*, https://www.delkomtech.pl/aktualnosci/cyberzagrozenia-w-firmie (dostęp: 27.04.2026).

Enisa
2022 *Remote Identity Proofing - Attacks & Countermeasures,* https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures (dostęp: 27.04.2026).

FS-ISAC
2020 *Work From Home Security Tips for Individuals*, https://www.fsisac.com/hubfs/Resources/WFHSecurityTipsIndividuals.pdf (dostęp: 27.04.2026).

Gartner
2025 *Identifies the Top 6 Use Cases for Generative AI in Legal Departments*, https://www.gartner.com/en/newsroom/press-releases/2025-02-19-gartner-identifies-the-top-6-use-cases-for-generative-ai-in-legal-departments (dostęp: 27.04.2026).

Kindervag, J.
2010 *Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research, 5 November.* https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (dostęp: 27.04.2026).

Microsoft
2025 *What is a VPN? How VPNs work and why you should use one*, https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-is-vpn (dostęp: 27.04.2026).

Microsoft
b.d. *Hybrid it security auditing*, https://www.microsoft.com/security/blog/hybrid-it-security-auditing (dostęp: 27.04.2026).

Nflo
b.d. *Incident Response*, https://nflo.pl/slownik/incident-response/ (dostęp: 27.04.2026).

PBSG
b.d. *Cybersecurity Audit – Why is it worth conducting an audit for compliance with the KSC Act?,* https://www.pbsg.pl/en/cybersecurity-audit-why-is-it-worth-conducting-an-audit-for-compliance-with-the-ksc-act/ (dostęp: 27.04.2026)

Robinette, D.
2023 *What are the Advantages of Intrusion Detection Systems?*, https://www.stamus-networks.com/blog/what-are-the-advantages-of-intrusion-detectionsystems (dostęp: 27.04.2026).

SailPoint
2025 *Bring your own device (BYOD) policies: Security and compliance*, https://www.sailpoint.com/identity-library/byod (dostęp: 27.04.2026).

Socium
b.d. *Polityka bezpieczeństwa informacji (PBI) - definicja, cele, struktura. Jak opracować PBI?*, https://www.socium.pl/polityka-bezpieczenstwa-informacji.html (dostęp: 27.04.2026).

TTMS
2026 *Bezpieczeństwo danych w zdalnym modelu współpracy – ryzyka dostępu i nadużyć*, https://ttms.com/pl/bezpieczenstwo-danych-w-zdalnym-modelu-wspolpracy (dostęp: 27.04.2026).

Underhill, K.
2026 *Picus Red Report 2026 Shows Attackers Favor Stealth Over Disruption* https://www.esecurityplanet.com/threats/picus-red-report-2026-shows-attackers-favorstealthover-disruption (dostęp: 27.04.2026).

Zając, K.
2021 *Praca zdalna zwiększa ryzyko cyberataków*, https://cyberdefence24.pl/bezpieczenstwo-informacyjne/praca-zdalna-zwieksza-ryzyko-cyberatakow (dostęp: 27.04.2026).

DIGITAL SECURITY OF REMOTE WORKERS IN THE ERA OF ACCELERATED DIGITALIZATION

Abstract: The article analyzes the challenges of digital security resulting from the widespread adoption of remote work. The author points to the evolution of cyber threats, including a shift in hackers' strategies from direct destruction to covert infiltration. The study discusses technical protection measures (VPN, cloud solutions, and multi-factor authentication), as well as behavioral aspects, emphasizing that humans remain the weakest link in security systems (phishing, social engineering). It also examines the legal framework, including employer obligations arising from the GDPR and the Polish Labour Code. The conclusion highlights the necessity of an integrated approach that combines technology, employee education, and legal procedures. The importance of building cybersecurity awareness among employees and developing appropriate digital competencies is also emphasized. The author draws attention to the need to implement coherent security policies and conduct regular training in data protection. Furthermore, the role of continuous monitoring of IT systems and regular security updates is underlined. It is noted that effective data protection requires cooperation between IT departments, management, and employees themselves. As a result, organizations should treat cybersecurity as a continuous process that requires constant adaptation to emerging threats.

Keywords: digital security, personal data protection, GDPR, cyber threats, phishing.

Karol Grabowski
Badacz niezależny

PRAWNE I ORGANIZACYJNE RAMY STOSOWANIA SZTUCZNEJ INTELIGENCJI W OCENIE WARTOŚCI DOWODOWEJ MATERIAŁÓW CYFROWYCH – MIĘDZY RZETELNOŚCIĄ PROCESU A EFEKTYWNOŚCIĄ ZARZĄDZANIA SPRAWAMI SĄDOWYMI

Streszczenie: Unowocześnianie funkcjonowania systemu sprawiedliwości i egzekwowania prawa przez sądy polega obecnie na włączaniu potencjału narzędzi sztucznej inteligencji na wszystkich etapach przygotowywania materiału dowodowego. Ma to miejsce zwłaszcza w sytuacjach, gdy konieczna jest analiza dużych ilości materiałów w wielu postaciach. Wiarygodność dowodów jest warunkowana czynnikami, do których należy transparentność, wyjasnialność, równość w dostępie do nich przez strony postępowania. Algorytmy muszą odpowiadać bieżącym potrzebom wymiaru sprawiedliwości w drodze „głębokiego uczenia" maszynowego. AI jest przydatna również w samym procedowaniu spraw. Stosowanie sztucznej inteligencji musi wynikać z obowiązującego prawa w przedmiotowym zakresie.

Słowa kluczowe: sztuczna inteligencja, algorytmy AI, wymiar sprawiedliwości, transparentność i wyjasnialność, obowiązujące prawo, procedury sądowe.

Wstęp

Artykuł koncentruje się na wykorzystywaniu algorytmów AI jako narzędzi wspomagających i usprawniających funkcjonowanie systemu prawa w obecnym stanie uregulowań systemowych. Umożliwia to osiąganie wieloaspektowych korzyści w postaci opracowania materiałów dowodowych i pracy samych sądów jako urzędów.

Narzędzia te znajdują coraz szersze zastosowanie. Dotychczasowy stan prawno-organizacyjny dotyczący stosowania AI w głównej mierze opiera się na utrwalonych zasadach funkcjonowania systemu sądowego i zasadach zdroworozsądkowych. Ważność wymiaru sprawiedliwości dla jednostek i podmiotów zbiorowych wymaga ujęcia zagadnienia w jednolite ramy prawa i dostosowywania go do zgodności z realiami w trybie ciągłym. Obowiązujący akt prawny o sztucznej inteligencji ustala zasady jednolitego rynku i przepisy korzystania z wiarygodnej sztucznej inteligencji na terenie państw UE. Myślą przewodnią dokumentu jest promowanie innowacji i wdrażania AI oraz przeciwdziałanie możliwym zagrożeniom dla zdrowia, bezpieczeństwa i praw podstawowych obywateli, ochrona demokracji i praworządności. Ustalenie zasad zawartych w AI Act poprzedziła analiza ryzyka dla podmiotów stosujących sztuczną inteligencję wobec jej konkretnych zastosowań (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) (Tekst mający znaczenie dla EOG), Document 32024R1689). Szczególnie dotyczy to systemu sprawiedliwości w całej rozciągłości i różnorodności kwestii, które na wszystkich etapach postępowania sądowego i procesowego mogą się pojawiać.

Wykorzystywanie algorytmów w systemie prawa miało już miejsce w projekcie Predictice we Francji w przewidywaniu decyzji w postępowaniach sądowych, w Estonii gdzie technologię AI stosowano w rozpatrywaniu spraw wypadków drogowych, a także w analizie akt Europejskiego Trybunału Praw Człowieka. Użycie systemu sztucznej inteligencji na poszczególnych etapach postępowania powinno uwzględniać jej zalety, ale jeszcze w większym stopniu ograniczenia wynikające z faktu, iż jest to system uczący się i korzystający z wiedzy, która została do jego zasobu wprowadzona. Tym samym może być ona błędna i nieobiektywna, a rzeczywistość cyfrowa nieodpowiadająca prawdziwej. Prawna, organizacyjna, etyczna niejednoznaczność, ograniczona transparentność algorytmów i wyjaśnialność podejmowanych przez AI decyzji, konieczność zapewniania ochrony praw stron i człowieka w postępowaniu, gwarancji praw procesowych, ogranicza możliwość zastosowania algorytmów AI w systemie prawa do wykonywania czynności analitycznych, pomocniczych, np. w ocenie wartości dowodowej materiałów cyfrowych, analizie nagrań wideo, głosowych, materiałów z komunikatorów, kamer przemysłowych, samochodowych. Przywołane przykłady wskazują na skuteczność sztucznej inteligencji wraz

z jednoczesnymi zagrożeniami dotyczącymi nieprawidłowej interpretacji reguł prawa, a tym samym konieczność ludzkiego nadzoru i interwencji w przypadku uzasadnionych wątpliwości.

Koncepcja i rozwój sztucznej inteligencji w systemie egzekwowania prawa

Od 2016 r. na skutek postępów rozwoju programów komputerowych przydatność AI jest rozpatrywana w kontekście zadań, które może wykonywać na różnych etapach egzekwowania prawa. Zdolność samouczenia się algorytmów, umożliwia ich praktyczne, sprawne i skuteczne wykorzystanie w wykonywaniu skomplikowanych czynności analityczno-poznawczych, porównawczych i innych zwłaszcza, gdy wymaga to przeszukiwania znacznych ilości zdygitowalizowanego materiału. Charakterystyka systemów AI skutkuje ich zastosowaniem w analizie dowodów cyfrowych przyczyniając się do wieloaspektowego unowocześniania wymiaru sprawiedliwości, umożliwiając szybką i dokładną ocenę dowodów.

Kierunki rozwoju technologii AI w praktycznym funkcjonowania systemu prawa wymagają antycypowania możliwych kierunków jej zastosowania w wymiarze sprawiedliwości, przewidując jej rozszerzającą się implementację. Trendy i prognozy wskazują na potencjał sztucznej inteligencji w usprawnianiu procesów. W oczywisty sposób wiąże się to również z kodyfikacją roli algorytmów „myślących" w ciągach czynności przewidzianych dla podmiotów prawa- sądów, organów administracji, w gałęziach prawa, postępowaniach cywilnych, karnych, administracyjnych, sądowo-administracyjnych, wyspecjalizowanych postępowaniach prawnych na etapach przewidzianych dla konkretnego rodzaju: przygotowawczego, przygotowywania do rozprawy, jej realizacji, dokumentowania wydania wyroku, postępowania odwoławczego i postępowania wykonawczego (Lex Nawigator, https://www.wolterskluwer.com/pl-pl/solutions/lex/navigator [dostęp: 3.11.2025]).

Wdrażanie i rozszerzanie roli systemów sztucznej inteligencji w wymiarze sprawiedliwości wymaga szczegółowego sprecyzowania zakresu czynności, które mogą analizowane przez algorytmy w sposób go usprawniający, nie naruszający prawa do rzetelnego procesu i nie wchodzący w kolizję z podstawowymi dokumentami: Ustawą z dnia 6 czerwca 1997 r. - Kodeks karny (Dz.U. 2025 poz. 383 ze zm.), Ustawą z dnia 23 kwietnia 1964 r. - Kodeks cywilny (.Dz.U. 2025 poz. 1071 ze zm.), Ustawą z dnia 17 listopada 1964 r. - Kodeks postępowania cywilnego (Dz.U. 2024 poz. 1568 ze zm.), Ustawą z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. 2025 poz. 734 ze zm.) (Płocha 2020, s. 13-14). Niezbędne jest również zapewnianie i utrzymywanie kontroli nad systemami w warunkach przewidywanych zmian. Skuteczne

i bezpieczne wykorzystywanie systemów AI w sądownictwie zależy od adekwatnego podziału kompetencji pomiędzy cyfrowy system i człowieka wyposażonego w specjalistyczną wiedzę i doświadczenie zawodowe. Za konieczne uznaje się analizowanie w trybie ciągłym skutków funkcjonowania systemów sztucznej inteligencji w obowiązującym w danym kraju systemie sądowniczym i zapobieganie umniejszania roli człowieka w decydujących fazach egzekwowania prawa poprzez nadmierne upraszczanie procedur (Kaczmarek-Templin 2022, s. 59-78; Bartoszek 2022, s. 8-29).

Zapewnianie rzetelności procesu oraz skuteczne korzystanie z odwoławczych środków zaskarżenia wiąże się niezaprzeczalnie z koniecznością transparentnego działania algorytmów sztucznej inteligencji i korzystania z nich. Strony procesu, a zwłaszcza pełnomocnicy stron powinni mieć pełną świadomość, iż całkowita przejrzystość działania algorytmów umożliwiła rzetelne dokonanie oceny materiału dowodowego na podstawie, którego zapadły wyroki. Powyższe spowoduje wzrost akceptowalności społecznej wykorzystania AI do wspierania rozstrzygania spraw sądowych, również na skutek skrócenia czasu od chwili wniesienia pozwu do momentu rozstrzygnięcia sprawy. Osiągnięcie postulowanego poziomu publicznego zaufania do procesów przygotowywanych i prowadzonych z użyciem sztucznej inteligencji może być rezultatem zapewniania ciągłości ocen stanu wyjaśnialności działania algorytmów, również z wykorzystaniem wiedzy przedstawicieli zewnętrznych ekspertów i audytorów. Działanie takie pozwala na zwiększenie szans identyfikacji i eliminacji luk oraz potencjalnych błędów w zaprojektowanych procedurach oraz wdrożonej technologii (Kotalczyk 2021, s. 60-66).

Przeniesienie się przestępczości do rzeczywistości cyfrowej i korzystanie z nowoczesnych technologii w celach osiągania korzyści w rozmaitych aspektach funkcjonowania społeczeństw spowodowało, iż przeciwdziałanie im i karanie przestępców wymaga analizowania danych istniejących w świecie wirtualnym. Kluczowym dla wiarygodnego i skutecznego korzystania ze śladów i dowodów cyfrowych w postępowaniu sądowym, z jednoczesnym dochowaniem gwarancji ochrony praw procesowych stron i osób rozstrzygających sprawy sądowe jest wdrażanie odpowiedniego i wszechstronnego systemu weryfikacji danych oraz walidacji dowodów cyfrowych. Opracowane normy techniczne, w tym zaliczające do serii ISO/IEC 17025:2017, dotyczące metod badawczych mają istotne znaczenie w procesie weryfikacji dowodów cyfrowych, ponieważ zapewniają dochowanie postulowanej jakości i kompetencji laboratoriów techniki kryminalistycznej w wykorzystywania dowodów w procesach sądowych. Ścisłe przestrzeganie zasad ekspertyzy technicznej w centrach ekspertyz zapobiega powstaniu przekłamań, występowaniu systemowych błędów i podważania wiarygodności dowodów w procesie sądowym. Rozwój cyberprzestepczosci

oraz możliwość dokumentowania śladów i dowodów z użyciem technik cyfrowych stwarza sytuację, w której zapewnianie jakości we wszystkich rodzajach postępowania z użyciem AI musi obejmować audyt procesu przygotowania i wyboru danych, na których algorytmy będą nieustnie „trenowane" i uczone. Sposoby dokonywania przestępstw typu sextortion, revenge porn, deepfake porn, cybergrooming, których cechą charakterystyczną jest fakt, iż przestępca jest manipulatorem danych cyfrowymi, wzmaga konieczność zapewnienia ustawowej gwarancji autentyczności danych stanowiących dowód. Rosnąca ilość przestępstw tego rodzaju wskazuje na potrzebę dokonania zmian w systemie prawnym dotyczącego rozwoju technologii. System kontroli jakości powinien zawierać w sobie również audyt sposobu przedstawiania oraz analizy uzyskanych wyników algorytmicznych w procesach rozumianych jako całość szczególnie z obszaru prawa gospodarczego, dotyczących kwestii medycznych i innych, w których wymagana jest analizowanie, porównywanie i segregowanie dużej ilości informacji w tym metadanych ogólnych, instytucjonalnych i dziedzinowych. Systematyczne analizowanie skuteczności stosowanych programów sztucznej inteligencji ma istotne znaczenie w procesie wdrożenia systemów je wykorzystujących (Guzik-Makaruk, Zubańska 2023, s. 9-24).

Pewność realizacji prawa procesowego mającego skutkować przeprowadzeniem sprawiedliwego i rzetelnego postępowania sądowego, zakończonego orzekaniem trudnym do podważania zakłada eliminację sytuacji, w których systemy algorytmiczne samodzielnie decydują o rozgraniczeniu strefy, w której system działa automatycznie i bez ingerencji w proces osób uprawnionych do rozstrzygania istoty sprawy. Weryfikowanie z powodu swej interdyscyplinarności powinno obejmować holistyczną współpracę osób biegłych, posiadających kompetencje z zakresu prawa, technologii oraz dziedzin, których dotyczy audytowany obszar. Ponadto systemy powinny być chronione przed nieautoryzowaną ingerencją, naruszeniami systemów bezpieczeństwa algorytmicznego, monitorowane w celu uniemożliwienia zakwestionowania ich wiarygodności, dochowania rzetelności rozstrzygnięć w procedowanych sprawach (Trubalski, Pogłódek 2022). Powszechność stosowania sztucznej inteligencji oraz korzyści z tego wynikającego nie wymagają akceptacji stron, ponieważ bezstronność i brak zaangażowania programów zapewniają korzyści dla wszystkich zantagonizowanych i uczestniczących w procesie stron. Strony powinny jednakże mieć świadomość jej użycia, zwłaszcza gdy osoby bezpośrednio zainteresowane rozstrzygnięciem są ofiarami cyberprzestępstw. Akceptacja ta może być warunkowana odpowiednim jej zarządzaniem przez interesariuszy bezpośrednich lub pośrednich – sędziów. Warunkiem jest również posiadanie przez strony, a zwłaszcza ich pełnomocników, wiedzy dotyczącej przysługujących im praw związanych z systemem AI

oraz informacji o potencjalnych niedoskonałościach i błędach w działaniu algorytmów, które mogą zakłócić działalność systemu. Konsultowanie korzystania z planowanego użycia rozwiązań AI z grupą interesariuszy może zwiększyć poziom akceptacji systemu i uzyskania realnej pewności w zakresie zapewnienia bezpieczeństwa jednostki w aspekcie proceduralnym tak w zakresie jej praw, jak i rozstrzygnięć. Wynika z tego potrzeba edukowania pracowników wymiaru sprawiedliwości na temat ich praw i obowiązków oraz ogółu obywateli w kwestii funkcjonowania systemu AI w polskim systemie wymiaru sprawiedliwości (Czapska, Fiałka 2023, s. 6-26).

Transparentność stosowania technologii AI w praktyce prawa

Stosowanie systemu w wymiarze sprawiedliwości spełnia wymogi przydatności pod warunkiem dochowania transparentności oraz wyjasnialnosci decyzji podejmowanych z jej użyciem, ponieważ tylko w ten sposób gwarantowana jest rzetelność procesowa i zgodność z ochroną praw jednostki. Dochowanie tych wymogów sprzyja zrozumieniu i akceptacji przez użytkowników, uczestników procesów i instrumentariuszy algorytmicznych podstaw, na podstawie których system przygotowuje podstawy podejmowania decyzji. Jednocześnie redukuje to ryzyko naruszania praw procesowych. Kwestie posługiwania się i obsługi systemów wysokiego ryzyka, których to cech AI nabiera w kontekście prawa, reguluje AI Act i ustawa o ochronie danych osobowych (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. ...; Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781 ze zm.).

Transparentność w omawianym kontekście polega na informowaniu podmiotów zainteresowanych i uczestniczących o sposobie pozyskiwania danych stanowiących podstawę podejmowania decyzji oraz potencjalnych zagrożeniach z tego wynikających. Ma na celu zachowanie rzetelności procesowej oraz umożliwienie praktycznego korzystania z praw do odwołań dla stron, które są objęte postępowaniem. Wskazywanie algorytmicznych podstaw działania technologii automatyzacji wzmacnia prawa procesowe oraz ogranicza konsekwencje, które niosą ze sobą powyższe rozwiązania. Niedochowanie zasady transparentności w użyciu sztucznej inteligencji w przygotowywaniu procesów sądowych podważa legitymację procesową oraz zasadność stosowania systemu. Istotę sprawy ilustruje w sposób praktyczny wyrok TSUE C-321/21 dotyczącego prawa strony w procesie karnym do uzyskania informacji o mechanizmach podejmowania decyzji przez system AI, stosowany do tworzenia dowodów oraz prawa do kontroli tych dowodów. Ograniczenie dostępu do materiałów dowodowych przygotowanych przez system sztucznej inteligencji,

a także wszelkie przesłanki mogące wywoływać wątpliwości co do naruszeń praw procesowych lub nieadekwatności przygotowywania procesu decyzyjnego, powinno być uwzględnione w aktualizacji dokumentacji oraz procedur obsługi systemu. Brak transparentności oraz czytelnych rozwiązań systemowych w implementacji technologii sztucznej inteligencji, zwłaszcza w systemach wysokiego ryzyka, skutkuje generowaniem problemów ze zrozumieniem przez strony materiałów dostarczonych przez sztuczną inteligencję, co przełoży się na możliwości skutecznego oskarżania/obrony. Ponadto osłabia to poziom społecznej akceptacji powszechnego stosowania sztucznej inteligencji we wdrażanych systemach (Czapska, Fiałka 2023, s. 6-26). Zagadnienie staje się szczególnie ważne w sprawach dużej wagi lub gdy materiały dowodowe mają złożony charakter. O zróżnicowanym podejściu do kwestii użyteczności AI w kontekście zróżnicowanej transparentności wskazują realia dotyczące m.in. Estonii i Francji, gdzie nie dąży się do stosowania systemów AI w obszarach działalności sądów, jeśli zachodzi wątpliwość pełnego audytowania oraz identyfikowalności danych oraz występuje brak powszechnej akceptacji systemów AI, jeżeli zachodzi ograniczenie transparentności (Kusznieruk, Zemke-Górecka 2023, s. 2-8).

Jednoznaczność stosowania algorytmów dotyczy użycia systemu AI w sposób zapewniający, iż żadna ze stron procesowych nie zrozumie powodów i skutków analizy dowodów w sposób umożliwiający ich dowolną interpretację. Pełna wyjaśnialność zasad funkcjonowania systemu zapewnia brak jakichkolwiek podstaw kwestionowania decyzji podjętych z użyciem AI, a tym samym brak realnych możliwości obrony interesów przez obie strony postępowania. Wymaga to również odpowiedniego przygotowania kadr sądowych, sędziów oraz innych pracowników do umiejętnego czytania, rozumienia i interpretacji raportów przygotowanych poprzez algorytmy sztucznej inteligencji. Specyfika wymiaru sprawiedliwości sprawia, iż implementacja systemów AI wymaga stosowania weryfikowalnych, przejrzystych procedur poprzez opracowywanie odpowiednich reguł rejestrowania relacji algorytmów z elementami materiału dowodowego w celu identyfikowania i lokalizowania występowania potencjalnych obszarów błędów, które mogły pojawić się podczas klasyfikacji danych. Praktyka wskazuje, że implementacja odpowiednich mechanizmów do monitorowania i audytowania systemu AI jest niezbędną częścią zapewniania ochrony praw procesowych i proceduralnych stron w automatycznym systemie AI służącym do analizowania materiałów dowodowych. Doświadczenia systemu prawa w Estonii i Francji wskazują, iż skuteczność AI jest ograniczona, jeśli w fazie wdrożeniowej i użytkowania wytyczne dotyczące audytowania i monitorowania działania wytyczne będą miały postać niepełną lub niewystarczającą (Bartoszek 2022, s. 8-29). Zasady te są szczególnie ważne w kontekście odwołań procesowych oraz ochrony praw stron

procesowych. Doświadczenia Estonii i Szwecji dotyczące systemu AI wskazują, iż powinien on pełnić rolę gwaranta kontroli oraz zwiększać pewność niepodważalności rozstrzygnięć przygotowanych z użyciem AI przez instancje nadrzędne i odwoławcze. Ich implementacja do technologii AI wzmacnia ochronę praw procesowych stron w postępowaniu, zapewnia istnienie pożądanej równowagi oraz prawa stron do kontroli i transparentnej interpretacji decyzji podejmowanych z użyciem AI. System kontrolny może być powszechnie przyjętą metodą zapewnienia przez niezależną od systemu sztucznej inteligencji stronę nadzoru i oceny wydanych werdyktów i rekomendacji w całym obszarze działalności sądowej (Kaczmarek-Templin 2022, s. 59-78).

Transparentność w działaniu i jednoznaczna czytelność decyzji AI szczególne miejsce znajduje w sferze ochrony praw jednostek w sprawach dotyczących danych wrażliwych, takich jak dane osobowe ofiar cyberprzestępczości lub ofiar przemocy domowej. Transparentność mechanizmów przetwarzania materiałów dowodowych za pomocą sztucznej inteligencji jest niezbędna, aby strony postępowania uznały decyzje AI za dopuszczalne, zwłaszcza w kontekście postępującej digitalizacji wymiaru sprawiedliwości. Polski system wymiaru sprawiedliwości w kontekście transparentności i jednoznaczności działania szczególne znaczenie nadaje społecznemu dialogowi dotyczącego możliwości pełnej implementacji systemu AI, konsultacjom w gronie prawników, informatyków i specjalistów innych dziedzin dotyczącym wykorzystywania materiałów opracowanych z jego użyciem w procesach postępowania karnego, wdrażaniu polityk i procedur transparentnego stosowania systemu sztucznej inteligencji w polskich sądach (Wiącek 2024).

Stosowanie materiałów cyfrowych w systemie sprawiedliwości

Użycie danych przyjętych jako dowód w sprawie lub będących analitycznymi opracowaniami materiałów przez systemy sztucznej inteligencji na nośnikach informatycznych uznawanych w systemie prawnym jako dopuszczalne, m.in. płytach CD/DVD, dyskach twardych (HDD/SSD), USB (pendrive), kartach pamięci musi zapewniać ich trwałość, integralność informacji, uniemożliwiać dokonywanie zmian w jakikolwiek sposób. Odpowiada to ustaleniom art. 169–173 k.p.k. Zasada równości stron postępowania nakazuje również zapewnianie dostępu do sprzętu i oprogramowania, co obecnie nie stwarza problemu. Ponadto w kontekście materiałów dowodowych kluczowym problemem jest niekwestionowana integralność i autentyczność. W obowiązującym stanie przepisów odnoszących się do nośników danych zagadnienie to wymaga uzupełniającego uregulowania. Wniosek w tej sprawie

w 2014 r. zgłosił Rzecznik Praw Obywatelskich, zgłaszając potrzebę uznania przez sądy za równorzędne płytom CD/DVD w drodze resortowego rozporządzenia, dowodów- plików cyfrowych: audio, wideo, fotografii dostarczanych urządzeniami usb, mailem, transferem na serwer strony internetowej sądu oraz ustalenie jednolitych zasad weryfikacji autentyczności, integralności, rozliczalności materiałów. Wniosek przez Ministerstwo Sprawiedliwości nie został uznany jako uzasadniony. Sposób przyjęcia i uwierzytelnienia zapisu cyfrowego- materiału dowodowy może zostać niedopuszczony – przez kwestie nośnika, a nie przez to, co w nim faktycznie zawiera. Każdorazowo jest to kwestią uznaniową danego sądu. Nie obowiązuje jedna interpretacja przedstawiania dowodu, a brak standaryzacji powoduje różnorodność orzeczeń i utrudnia wyrokowanie w procesie, co jest sprzeczne z ideą jednorodności sprawiedliwości (Bednorz 2014, s. 125-132). Dowolność i uznaniowość przyjmowania danych cyfrowych na różnych nośnikach oraz uwierzytelnianie materiału potwierdza konieczność wprowadzenia systemowych uregulowań prawnych rangi ustawowej w zakresie dowodów cyfrowych. Brak zdefiniowania procedur w omawianym temacie zakłóca lub uniemożliwia współpracę przy sprawach związanych z dowodami cyfrowymi, zakłócając sprawną komunikację w trakcie procesu / pomiędzy instancjami lub sądami w różnych miejscowościach/, grozi podejmowaniem błędnych decyzji przez dysponowanie informacjami uznanymi za wiarygodne lub nie. Sprawa ta godzi w podstawowe prawa procesowe.

Przyjęty materiał dowodowy musi być bezwarunkowo zabezpieczony przed jego modyfikacją. Ważne jest stworzenie systemu, który uniemożliwi dokonywanie zmian lub pozwoli na błyskawiczne uwierzytelnienie z wykorzystaniem zaawansowanych technologii.

Algorytmy AI znajdują zastosowanie przy sprawach o złożonym charakterze, gdzie analiza danych w tradycyjny sposób znacznie wydłużyła by ich rozpoznanie- gospodarczych, finansowych, marketingowych, medycznych. Użycie systemów analitycznych w rozpoznawaniu spraw dotyczących służby zdrowia wykazało ich wysoką skuteczność w dostrzeganiu złożonych zależności (wzorów), analizowanych danych statystycznych i jakościowych. Wykorzystanie takich rozwiązań technologii predykcyjnych wpływa na skuteczność oddzielenia różnic w materiałach dowodowych, różnicowanie danych dostarczanych na ich podstawie przez strony postępowania. W tym obszarze szczególnie ważne jest monitorowanie oraz walidacja, prowadząca do kontroli nad procesem decyzyjnym przez osoby rozstrzygające. Jest to jednak warunkowane uprzednim uczeniem maszynowym /random forest/ dostarczonym zbiorem danych treningowych pod nadzorem człowieka, walidacją danych ponieważ ich brak grozi wystąpieniem błędnych wyników, przekłamywaniem dowodów,

zapewnieniem prywatności danych i ochrony danych osobowych w praktycznym wykorzystaniu. Prawidłowa walidacja powinna uwzględniać zróżnicowanie prawne w procesie treningu. Rzetelne stosowanie, musi iść w parze z wytycznymi i szkoleniami dla osób rozstrzygających (Kotalczyk 2021,s. 60-66). W analizie dowodów cyfrowych wykorzystywane są systemy, które są w stanie wyciągać wnioski, rozpoznawać wzorce i podejmować w tym zakresie autonomiczne decyzje. Wykorzystywanie AI w dziedzinie prawa, wobec specyfiki dowodów, powinno wiązać się z odpowiednią interpretacją wyników przez ludzi- system nie jest do tego uprawniony. Proces wykorzystywania programów doprowadza do zmiany charakteru ról osób rozstrzygających w kontekście analizy materiału dowodowego, zmian w edukacji w kontekście interwencji w algorytmy, ograniczeń ich efektywności, kompetencji podmiotów orzekających. Wspieranie procesu rozstrzygania spraw przez algorytmy w zakresie predykcji może skutkować pewnym uproszczeniem wielowymiarowego charakteru procesu rozstrzygania i nieuwzględnianie kontekstów precedensowych, pozaprawnych, społecznych, co wyklucza uznawanie przygotowanych danych jako wiążących (Bartoszek 2022, s. 8-29).

Potencjał sztucznej inteligencji tkwi również w usprawnianiu pracy samych sądów podczas procesów i ich pracy jako urzędów. Wprowadzenie i upowszechnienie e-protokołu, cyfryzacja zapisów dźwięku i obrazu znacząco usprawniło proces archiwizacji sesji, poprawiło procedury dostępności zdigitalizowanych akt sądowych dla stron postępowania. Zapis elektroniczny z użyciem sztucznej inteligencji pozwala na odczytywania głosu lub jego transkrypcję, obserwację wizualną uczestników postępowania, zautomatyzowaną analizę tekstu z ekstrakcją kluczowych danych, słów o szczególnym znaczeniu dla sprawy, a także identyfikację emocji i ekspresji uczestników postępowania. Analiza nagrań dźwięku i obrazu zwiększa prawidłowość oceny przekazanych dowodów. Zastosowanie AI do automatycznego zapisu treści wypowiedzi minimalizuje ryzyko błędu podczas zapisywania informacji. Skutkiem ubocznym stosowania zapisu elektronicznego jest prawdopodobieństwo wystąpienia problemów dotyczących bezpieczeństwa, zagrożeń ochrony danych i ich integralności. Całkowite oparcie się na cyfryzacji tych procesów wymaga zdefiniowania standardów przechowywania plików elektronicznych i zagwarantowania autentyczności dostarczanych dowodów. Wykorzystywanie sztucznej inteligencji w obszarach związanych z obsługą dokumentacji elektronicznej oraz logistyką procesową znacznie je upraszcza, jednakże wymaga to dostosowywania przedmiotowych przepisów przez legislatorów i przedstawicieli prawa, polityków w celu doprowadzania ich do logicznej i prawnej zgodności oraz zastosowania do zachodzących procesów w których istotną rolę odgrywać będą systemy AI.

W instytucjach sektora administracji publicznej i sądownictwa algorytmy sztucznej inteligencji są narzędziem zwiększającym ich wydajność i ograniczającym ilość błędów ludzkich, przekładając się na oszczędność finansową. Prawidłowe ich użycie zależy od wykluczenia lub znacznego ograniczenia prawdopodobieństwa wystąpienia multiplikacji błędnej interpretacji przepisów prawnych. To zaś wiąże się z bieżącym nadzorowaniem czy system wyciąga wnioski na podstawie rzetelnych danych, czy nie upraszcza procesów prawnych oraz czy nie powoduje naruszeń praw zainteresowanych stron postępowania rozwoju, doskonaleniem systemów, audytowaniem AI w działach administracji publicznej i sądownictwa. System AI dla sektora publicznego musi być nieustannie monitorowany, co wynika również z samej dynamiki zmian w nim zachodzących. Różnorodność i wieloaspektowość rozpatrywanych spraw w kontekście korzystania w nich z AI, zwiększa nacisk na szczególną odpowiedzialność za bezpieczeństwo danych osobowych, transparentność i niezawodność. Sfera publiczna jako wybitnie wrażliwa, wymaga restrykcyjnego stosowania działań regulacyjnych i audytowych, minimalizujących potencjalne naruszenia prawa ze strony programów opartych na sztucznej inteligencji (Blicharz, Zacharko 2023, s. 348–355).

Wzrost liczby przypadków wykorzystania AI w sferze publicznej, również w sektorach wrażliwych dowodzi, że jest to technologia dojrzała. Dynamika zmian zachodzących w poszczególnych sektorach życia publicznego powoduje, że implementacja i wykorzystywanie sztucznej inteligencji jest ciągłym, ulegającym zmianom i ulepszeniom procesem. Wartość dowodowa materiałów przygotowanych/opracowanych przez AI zależy od zastosowanego uczenia maszynowego, a ponieważ jego zadaniem jest wychwytywanie cech istotnych z perspektywy decyzyjnej zawartych w danych wyjściowych, narzędzie to powinno być albo wszechstronnie przygotowane i uniwersalne albo mieć charakter wyspecjalizowany. Na podstawie przeprowadzonej analizy dokonywana jest ocena faktów odpowiednio z obowiązującymi normami prawa. Efektywność zastosowanych rozwiązań technologii predykcyjnych uzależniona jest od posiadanych przez uczenie maszynowe informacji o cechach rozpoznawczych analizowanego zjawiska, od dostępności danych, materiałów i dokumentów.

Wykorzystywanie sztucznej inteligencji do prognostyki wyroków sądowych powinno stanowić powód do refleksji nad tematem legitymacji tak powstających decyzji oraz nad możliwościami wykorzystywania odwoławczych środków kontroli w związku z ewentualnymi nieprawidłowościami algorytmu. Kluczem do trwałej obecności AI w sądownictwie jest stosowanie kombinacji narzędzi z obszaru prawa publicznego, identyfikowanie problemów występujących przy zarządzaniu cyfrowymi dowodami. Zasadnym wydaje wypracowaniu kryteriów kontroli nad rozstrzygnięciami opartymi

na algorytmach i systemach przetwarzania dowodów w sposób automatyczny, dostosowanych do potrzeb uznawania ich wartości dowodowej. Jednocześnie ma to utrzymywać wymiar sprawiedliwości, jako składnik życia społecznego, oparty na zasadach humanizmu i proces kontrolowany przez osoby uprawnione do rozstrzygania.

AI w praktyce sądowej

Narzędzia sztucznej inteligencji automatyzują i ujednolicają standardy procesowej oceny materiału dowodowego. Redukuje to liczbę błędów, do których może dojść z powodu nadmiernego obciążenia osób, które prowadzą sprawy sądowe, pomaga w podjęciu przez ludzi decyzji w zakresie wartości dowodowej poszczególnych materiałów, co jednakże jest prerogatywą ludzi. Celem wprowadzenia narzędzi AI do systemu egzekwowania prawa jest wyodrębnienie najistotniejszych materiałów dowodowych dla sprawy i automatyczna redukcja liczby dowodów o najmniejszym znaczeniu. Klasyfikacji polega na analizie metadanych, dat i czasu sporządzenia, źródła i typu pliku. Filtracja materiału dowodowego umożliwia składowi orzekającemu sędziemu skupienie się na kluczowych dowodach, jego ocenę, ogranicza utratę czasu. Sztuczna inteligencja ułatwia ujawnienie ukrytych cech, wzorców zależności w obszernych zbiorach danych, podejmowanie adekwatnych decyzji w rozstrzygnięciu skomplikowanych spraw, w których występuje bardzo duża ilość zróżnicowanych danych. W procesach, w których kluczową rolę pełni analiza dokumentów z użyciem języka naturalnego materiał dowodowy stanowią nagrania z mediów społecznościowych lub pliki multimedialne (Kaczmarek-Templin 2022, s. 7; Płocha 2020, s. 13-14).

Znaczenie sztucznej inteligencji w postępowaniu cywilnym rozpoznawczym w trybie procesowym, rośnie od momentu wniesienia pozwu (art. 192 KPC) względem etapu przygotowań do sprawy. Wynika to z powodu dużej liczby pism procesowych składanych w toku procesu zarówno w każdej z instancji. Narzędzie jakim jest system Gaius Lex, umożliwia ograniczanie problemu piętrzenia się pism procesowych w każdej prowadzonej sprawie. Wyposażony w anonimizator, udostępnia ok. 3,5 mln dokumentów prawnych- orzeczeń, interpretacji podatkowych i przepisów. Pozwala na tworzenie własnej bazy dokumentów. Dokonuje automatycznej analizy ryzyk prawnych. Możliwości systemu wspomaganego sztuczną inteligencją pozwalają na zobowiązaniu strony (na podstawie art. 2053 § 1 KPC), do podania w piśmie przygotowawczym wszystkich twierdzeń i dowodów niezbędnych dla rozstrzygnięcia sprawy, pod rygorem utraty prawa do ich powoływania w toku dalszego postępowania. Jego przydatność ułatwia sporządzanie środków

odwoławczych, weryfikację przysługującego zażalenia od konkretnego postanowienia przysługuje zażalenie w świetle obowiązującej wersji kodeksu. Funkcja sztucznej inteligencji ułatwia merytoryczną weryfikację stwierdzeń w uzasadnieniach, również na podstawie orzecznictwa innych sądów, tworzy ich uściślenia i ujednolicenie linii orzeczniczych (https://gaius-lex.pl/ai-procedury-cywilne/ [dostęp: 8.11.2025]). W sprawach z obszaru medycyny wykorzystywany jest wysoko skuteczny system diagnostyczny CheXNet, wytrenowany na obszernym, reprezentatywnym zbiorze danych.

Przydatność algorytmów AI dostrzegalna jest z sprawach dotyczących własności intelektualnej, znaków towarowych, gdy materiał dowodowy ma postać zrzutów ekranów, zapisu strony internetowej, wpisów z urzędowych baz danych. Warunkiem przyjmowania zapisu internetowego jest pewność, że dany zapis pochodzi ze strony internetowej osoby fizycznej/prawnej, będącej jej właścicielem, co ogranicza ryzyko odrzucenia materiału z powodu wątpliwości ich zmiany lub przekłamań chronologii zdarzeń (https://guidelines.euipo.europa.eu/1935543/2117627/wytyczne-dot--znakow-towarowych/3-1-4-4-%C5%9Brodki-dowodowe [dostęp: 8.11.2025]).

Kwestie sporne dotyczące mediów społecznościowych w całym zakresie problematyki: naruszeń dóbr pojedynczych osób, rozstrzygnięć na styku państwo- firmy Bigdata wymagają analizy wielkiej ilości danych cyfrowych, czemu może sprostać algorytm. Znaczną rolę pełnią zapisy w dokumentacji elektronicznej w sprawach o ochronę osób pokrzywdzonych, m.in. „Niebieskich Kart". Archiwizacja danych elektronicznych, przyśpiesza czas wydania decyzji, np. nakazu zbliżania się (Lewoc 2024).

Skuteczność klasyfikacji materiału dowodowego przez systemy sztucznej inteligencji oraz ocena wartości dowodowej materiału cyfrowego jest warunkowana ciągłym rozwojem algorytmów AI i ich dostosowywaniem do wymogów sądownictwa. Ważną kwestią jest zapewnianie kompetencji osób odpowiadających za interpretację i wdrażanie w praktykę analiz dokonanych przez systemy AI, dbanie o transparentność ocen przez algorytmy AI wartości dowodowej.

W kontekście polityki międzynarodowej ważnym aspektem jest wykorzystanie dowodów cyfrowych w konfliktach i wojnach– gromadzenie i wykorzystanie dowodów cyfrowych w sprawach zbrodni wojennych i naruszenia praw człowieka. Wysoka użyteczność narzędzi cyfrowych sprawia, że ściganie i dokumentowanie przestępstw dokonanych przez organy władzy państwa współgra z dostosowaniem i ujednolicaniem regulacji prawnych do zmieniających się realiów.

Narzędzie sztucznej inteligencji e-protokół, w instancjach sądów krajowych ułatwia pracę protokolantów w sądach w ponad 3,5 tys. salach rozpraw, przez co skuteczniejsze jest zorganizowanie akt, łatwiejszy dostęp do nagrania głosu i wideo

dla stron oraz sędziów Dygitalizacja protokołu umożliwia rozbudowę systemów opartych na AI, np. w zakresie przechowywania i udostępniania dowodów cyfrowych. Wiąże się to z gwarantowaniem cyberbezpieczeństwa, zapewniającego integralność i autentyczność dowodów.

Wyzwania i ograniczenia

Podstawową kwestią dotyczącą sztucznej inteligencji jest jej prawne zdefiniowanie i umocowanie, stanowiące podstawę jej stosowania w dziedzinach życia i funkcjonowania społeczeństw, zwłaszcza w obszarach wysoko wrażliwych, do których należy wymiar sprawiedliwości. Dokumentem definiującym „system AI" i tworzącym ramy prawne dla jego bezpiecznego i etycznego stosowania jest przyjęte 13 czerwca 2024 r. przez Parlament Europejski i Radę Rozporządzenie (UE) 2024/1689 w sprawie sztucznej inteligencji –AI Act. Harmonogram wdrażania kluczowych przepisów opiewa na cezury czasowe od 2.02.2025 do 2. 08.2027. Dostosowywanie regulacji prawnych i techniczno-informatycznych powinna postępować wraz z rosnącym ilościowym i rodzajowym zwiększeniem się obszarów używania AI.

W obszarze prawa, rozwój uczenia głębokiego oraz rosnące zasoby danych cyfrowych redefiniują pojęcie sztucznej inteligencji w kontekście prawa, skutkując koniecznością ciągłej analizy norm prawnych i ich dostosowaniem do zmiennej relacji człowiek-maszyna w obszarze przetwarzania informacji i danych. Szczególne uwzględnienie powinny mieć wartości konstytucyjne, w tym rzetelność postępowania. Rozwój w obszarze postępowania dowodowego z dowodów cyfrowych zmusza do podejmowania działań w obszarze transparentności, autonomiczności rozstrzygnięć oraz odpowiedzialności, co wiąże się nieodłącznie z korzystaniem z materiału analitycznego na podstawie, którego następują rozstrzygnięcia procesowe. Styk prawa i systemów AI czyni kluczowymi zagadnienia wyjaśnialności i audytowalności. Decyzje AI muszą być zrozumiałe i akceptowalne, transparentne co zasad ich funkcjonowania, obiektywne i wykluczające podejrzenia działań manipulacyjnych i zakulisowych. Wykorzystywanie niewystarczających i nierzetelnych danych na etapie budowania systemów z zastosowaniem AI może przyczyniać się do powielania uprzedzeń i uproszczeń. Technologia AI wiąże się z potrzebą testowania funkcjonalności algorytmów, kontrolą jakości podejmowanych decyzji oraz zapobieganiem ryzykom społecznym i algorytmicznym. Powinny być ciągle monitorowane.

Podsumowanie

Materiały dowodowe przygotowane przez AI oraz decyzje wydawane na ich podstawie AI muszą być zrozumiałe, aakceptowalne, transparentne co do ich wartości merytorycznej i zasad funkcjonowania, ponieważ zaufanie użytkowników systemu sądowego opiera się na przekonaniu, że algorytmy działają obiektywnie i przejrzyście. Doświadczenia państw-pionierów w dziedzinie korzystania z potencjału AI wskazują na niezaprzeczalne korzyści czasowe, finansowe automatyzowania przygotowania i procedowania spraw. Dynamika zmian zachodzących w życiu społeczeństw, jakościowego i ilościowego rozwoju przestępczości powoduje, iż obecnych możliwości i sposobu algorytmów sztucznej inteligencji nie można uznać za niezmienne i zadowalające. Muszą one być dostosowywane w drodze „uczenia" do zachodzących zmian. Dotyczy to również polityki państwa w obszarze wymiaru sprawiedliwości i programów kształcenia ludzi, odpowiadających krajowym uwarunkowaniom prawnym i technologicznym.

Wgląd w problemy i możliwości wdrożenia sztucznej inteligencji, analiza prawnych, organizacyjnych i technicznych aspektów jej stosowania do oceny wartości dowodowej materiałów cyfrowych w procesie sądowym, potrzeby zapewnienia rzetelności postępowania, skuteczności i efektywności procesu sądowego, wskazuje na istnienie barier organizacyjnych, prawnych i technicznych podczas wprowadzenia sztucznej inteligencji. Potwierdzona została teza, że zapewnianie rzetelności postępowania sądowego z efektywnością i automatyzacją procesu możliwe jest tylko pod warunkiem podziału tych obszarów procesu, w których decyzje mogą być wspomagane przez systemy automatyczne oraz tych, które nie mogą być przez nie w żaden sposób wspierane. Wykazano istnienie znacznego potencjału narzędzi AI w systemie sprawiedliwości, który może być wykorzystany pod warunkiem dostosowywania regulacji prawnych jej dotyczących do jej stanu bieżącego. Celowym jest również wprowadzenie:

- systematyczne testowanie skuteczności systemów AI w procesie oceny wartości dowodowej oraz kontrola nad jego funkcjonowaniem i wykorzystaniem,
- zapewnianie przejrzystości działania i algorytmów sztucznej inteligencji, ich audytowalność i wyjaśnialność,
- weryfikowanie i ocena wiarygodności dowodów cyfrowych z użyciem AI,
- wdrożenie zmian w systemie legislacyjnym, ich adaptowanie do systemów automatyzacji wymiaru sprawiedliwości w procesie sądowym,

- szkolenie kadr (użytkowników, administracji, pracowników, sędziów) w obszarze wykorzystania systemów AI; adekwatna do warunków certyfikacja kadr,
- zmiany w zakresie: metod weryfikacji procesów i audytów w sądach, norm prawnych, certyfikacje, kontrole jakości, audyty oprogramowania i baz danych.

Bibliografia

Akty prawne

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) (Tekst mający znaczenie dla EOG), Document 32024R1689.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2019 poz. 1781 ze zm.).

Literatura

Bartoszek M.
2022 *Zastosowanie sztucznej inteligencji w sądownictwie w świetle zasady skutecznej ochrony sądowej*, [w:] „Folia Iuridica Universitatis Wratislaviensis".

Bednorz A.
2014 *Sztuczna inteligencja i uczenie maszynowe w gerontologii klinicznej*, „Gerontologia Polska".

Blicharz J., Zacharko L.
2023 *Wdrażanie technologii sztucznej inteligencji w administracji publicznej – kilka refleksji*, „Opolskie Studia Administracyjno-Prawne".

Czapska M., Fiałka M.
2023 *Granica między transparentnością wobec podmiotów danych a tajemnicą przedsiębiorstwa w kontekście ochrony danych osobowych ze szczególnym uwzględnieniem AI* [w:] *Projektowanie systemów si zgodnych z RODO,* (r.pr.) J. Groszkowski, Urząd Ochrony Danych Osobowych, Warszawa.

Guzik-Makaruk E. M., Zubańska M.
2023 *Sellected issues of implementation and using in practice new forensic solutions*, „Prawo w Działaniu. Sprawy Karne".

Kaczmarek-Templin B.
2022 *Sztuczna inteligencja (Al) i perspektywy jej wykorzystania w postępowaniu przed sądem cywilnym*, „Studia Prawnicze. Rozprawy i Materiały".

Kotalczyk M.
2021 *Sztuczna inteligencja w służbie polskiego sądu – propozycje rozwiązań*, „IUSTITIA".

Kusznieruk P., Zemke-Górecka A.
2023 *Aspekty i ramy prawne sztucznej inteligencji na gruncie prawa Unii Europejskiej, cz. 2.,* „Europejski Przegląd Prawa i Stosunków Międzynarodowych".

Płocha E. A.
2020 *O pojęciu sztucznej inteligencji i możliwościach jej zastosowania w postępowaniu cywilnym*, „Prawo w Działaniu Sprawy Cywilne".

Trubalski A., Pogłódek A.
2022 *Status ustrojowy prokuratury oraz status prawny prokuratora we współczesnych państwach, t. 1*, Warszawa.

Źródła internetowe

Lex Nawigator, https://www.wolterskluwer.com/pl-pl/solutions/lex/navigator [dostęp: 3.11.2025].

Lewoc M.
2024 *Dokumentacja procedury „Niebieskie Karty" w postępowaniach sądowych*. Studio Profilaktyki Społecznej Adam Rynkiewicz. https://kcpu.gov.pl/wp-content/uploads/2024/12/Dokumentacjaprocedury%E2%80%93Niebieskie%E2%80%93Karty-w--postepowaniach-sadowych-kopia-2.pdf [dostęp: 9.11.2025].

Wiącek M.
2024 II.510.228.2024.MA. Rzecznik Praw Obywatelskich, https://bip.brpo.gov.pl/sites/default/files/2024/05/Do_MS_dowody_nagrania_nosniki_24_05_2024.pdf [dostęp: 6.11.2025].

https://gaius-lex.pl/ai-procedury-cywilne/ [dostęp: 8.11.2025].

https://guidelines.euipo.europa.eu/1935543/2117627/wytyczne-dot--znakow-towarowych/3-1-4-4-%C5%9Brodki-dowodowe [dostęp: 8.11.2025].

LEGAL AND ORGANIZATIONAL FRAMEWORK FOR THE USE OF ARTIFICIAL INTELLIGENCE IN ASSESSING THE EVIDENTIARY VALUE OF DIGITAL MATERIALS – BETWEEN THE FAIRNESS OF THE PROCESS AND THE EFFICIENCY OF COURT CASE MANAGEMENT

Abstract: Modernizing the functioning of the justice system and court enforcement currently involves incorporating the potential of artificial intelligence tools into all stages of evidence preparation. This is particularly true in situations where the analysis of large amounts of evidence in multiple forms is necessary. The credibility of evidence is determined by factors such as transparency, explainability, and equal access to it by the parties to the proceedings. Algorithms must meet the current needs of the justice system through "deep learning." AI is also useful in case handling. The use of artificial intelligence must be consistent with applicable law in the relevant area

Keywords: artificial intelligence, AI algorithms, justice system, transparency and explainability, applicable law, court procedures.

Katarzyna Gurgul

Uniwersytet Wrocławski

ROZSZERZONY OBOWIĄZEK INFORMACYJNY W MEDYCYNIE ESTETYCZNEJ A ODPOWIEDZIALNOŚĆ CYWILNA OSOBY WYKONUJĄCEJ ZABIEG. ANALIZA NA TLE ORZECZNICTWA

Streszczenie: Dynamiczny rozwój rynku medycyny estetycznej i kosmetologii rodzi nowe wyzwania na gruncie prawa medycznego i cywilnego. Artykuł podejmuje problematykę standardu uświadomionej zgody pacjenta w kontekście zabiegów, których celem nie jest ratowanie życia lub zdrowia, lecz poprawa wyglądu zewnętrznego. Celem badawczym pracy jest odpowiedź na pytanie, czy wymogi dotyczące obowiązku informacyjnego powinny być różnicowane w zależności od leczniczego lub wyłącznie estetycznego charakteru interwencji. W oparciu o analizę orzecznictwa Sądu Najwyższego oraz niedawny wyrok Sądu Okręgowego w Poznaniu (sygn. akt XIV C 7/21), Autorka stawia tezę, iż fakultatywny charakter zabiegów estetycznych wymusza rygorystyczne zaostrzenie obowiązku informacyjnego. Wykazano, że przemilczenie ryzyka rzadkich powikłań – nawet przy istnieniu jedynie „cienia podejrzenia" ich wystąpienia – delegalizuje zgodę pacjenta, stanowiąc samodzielną podstawę do zadośćuczynienia za naruszenie praw pacjenta, niezależnie od odpowiedzialności odszkodowawczej za ewentualny błąd w sztuce medycznej.

Słowa kluczowe: medycyna estetyczna, zgoda uświadomiona, obowiązek informacyjny lekarza, błąd medyczny, prawa pacjenta, odpowiedzialność cywilna

Współczesny paradygmat medycyny uległ na przestrzeni ostatnich dekad głębokiemu przeobrażeniu. Medycyna przestała ograniczać się wyłącznie do funkcji terapeutycznej, polegającej na ratowaniu życia, leczeniu chorób i przywracaniu utraconych funkcji organizmu, otwierając się szeroko na interwencje mające na celu korektę defektów urody, przeciwdziałanie procesom starzenia oraz ogólną poprawę

dobrostanu psychofizycznego pacjentów (Safjan 1998, s. 45-47). Dynamiczny rozwój medycyny estetycznej i kosmetologii – w tym w szczególności powszechne wykorzystanie zaawansowanych technologii laserowych – sprawia, że w gabinetach medycznych coraz częściej dochodzi do poważnych, inwazyjnych ingerencji w powłoki skórne. Komercjalizacja tych usług prowadzi do zjawiska swoistej konsumpcjonizacji relacji na linii profesjonalista–pacjent. Oczekujący określonego rezultatu estetycznego pacjent nierzadko traktowany jest przez wykonującego zabieg jak klient usługi rynkowej, co usypia czujność obu stron w zakresie prawno-medycznych rygorów towarzyszących interwencji. Tymczasem z punktu widzenia prawa cywilnego oraz medycznego, fundamentem legalności każdego zabiegu naruszającego integralność cielesną pozostaje instytucja zgody objaśnionej (uświadomionej), uregulowana m.in. w art. 31 ust. 1 i art. 34 ust. 1 ustawy o zawodach lekarza i lekarza dentysty oraz w przepisach ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (Ustawa 1996; Ustawa 2008).

Na tle rosnącej liczby sporów sądowych i roszczeń odszkodowawczych dotyczących powikłań po zabiegach upiększających, krystalizuje się istotny problem badawczy: czy standardy udzielania informacji pacjentowi i odbierania od niego zgody na zabieg powinny być różnicowane w zależności od tego, czy zabieg ma charakter stricte leczniczy (ratujący zdrowie lub życie), czy wyłącznie estetyczny?

W niniejszym artykule podjęto próbę weryfikacji głównej tezy, zgodnie z którą z uwagi na fakultatywny (dobrowolny) charakter zabiegów medycyny estetycznej, wymogi dotyczące uświadomionej zgody pacjenta ulegają rygorystycznemu zaostrzeniu. W odróżnieniu od klasycznych zabiegów medycznych, w których pacjent znajduje się pod presją czasu, bólu lub konieczności ratowania zdrowia (stan wyższej konieczności), w medycynie estetycznej motywacją jest wyłącznie chęć poprawy wyglądu. Zabiegi te mają charakter planowy, co sprawia, że profesjonalista dysponuje odpowiednim czasem na wyczerpujące zrealizowanie obowiązku informacyjnego. W związku z tym, brak rzetelnej informacji o wystąpieniu nawet rzadkich powikłań – zgodnie z ugruntowaną w orzecznictwie Sądu Najwyższego zasadą informowania o najdrobniejszym „cieniu podejrzenia" wystąpienia negatywnych skutków (Wyrok SN 1980; Wyrok SN 2007) – nie tylko delegalizuje samą zgodę, ale stanowi autonomiczną podstawę do zadośćuczynienia za naruszenie praw pacjenta. Naruszenie to istnieje niezależnie od odpowiedzialności deliktowej za ewentualny błąd w sztuce medycznej, co nierzadko umyka uwadze osób wykonujących takie procedury.

Wskazany problem badawczy zostanie poddany dogmatyczno-prawnej analizie ze szczególnym uwzględnieniem dotychczasowej linii orzeczniczej Sądu Najwyższego. Rozważania teoretyczne zostaną osadzone w realiach praktyki sądowej poprzez

obszerne studium przypadku (ang. *case study*), oparte na niedawnym wyroku Sądu Okręgowego w Poznaniu z dnia 29 maja 2025 r. (sygn. akt XIV C 7/21) (Wyrok SO w Poznaniu 2025). Stan faktyczny rozstrzyganej sprawy – w której pacjentka doznała oparzeń i trwałych odbarwień skóry szyi po zabiegu laserowym wykonanym przez lekarza dentystę – w sposób niezwykle precyzyjny obrazuje prawne i finansowe konsekwencje zbiegu odpowiedzialności za brak zgody uświadomionej oraz za niedbalstwo techniczne.

Struktura niniejszego artykułu została podporządkowana logice wywodu naukowego. W pierwszej kolejności zarysowane zostaną prawne ramy zgody uświadomionej i zakresu obowiązku informacyjnego w polskim systemie prawnym. Następnie przeprowadzona zostanie analiza judykatów uzasadniających tezę o zaostrzonym standardzie informacyjnym w medycynie estetycznej. Kolejna część pracy stanowić będzie analizę wspomnianego orzeczenia Sądu Okręgowego w Poznaniu, ze szczególnym uwzględnieniem rozkładu ciężaru dowodu oraz wyceny roszczeń z tytułu naruszenia praw pacjenta. Wnioski końcowe (*de lege lata*) posłużą sformułowaniu postulatów dla praktyki klinicznej i kosmetologicznej, wskazując, iż rzetelnie prowadzona dokumentacja zabiegowa nie jest jedynie wymogiem biurokratycznym, lecz podstawowym wręcz instrumentem ochrony cywilnoprawnej profesjonalisty (Nesterowicz 2019, s. 150).

Prawny standard zgody uświadomionej – pojęcie i podstawa prawna

Każda interwencja medyczna – w tym zabieg z zakresu medycyny estetycznej lub kosmetologii ingerujący w powłoki skórne (np. przy użyciu technologii laserowych) – stanowi z obiektywnego punktu widzenia naruszenie integralności cielesnej człowieka. Aby działanie to nie nosiło znamion czynu bezprawnego (deliktu cywilnego, a w skrajnych przypadkach przestępstwa z art. 192 k.k.), musi zaistnieć okoliczność wyłączająca ową bezprawność, zwana kontratypem. W polskim porządku prawnym fundamentalnym kontratypem legalizującym czynności medyczne jest zgoda pacjenta (Świderska 2007, s. 88). Wyraża ona poszanowanie dla autonomii woli jednostki oraz jej konstytucyjnego prawa do samostanowienia. Niemniej jednak, na gruncie współczesnego prawa medycznego, nie każde oświadczenie woli pacjenta o poddaniu się zabiegowi wywołuje skutek legalizujący.

W doktrynie i orzecznictwie dokonuje się ostrego rozróżnienia pomiędzy tzw. zgodą blankietową (gołą) a zgodą objaśnioną (uświadomioną). Zgoda blankietowa to oświadczenie woli pacjenta, które sprowadza się do samej akceptacji faktu przeprowadzenia zabiegu (np. złożenie podpisu na niewypełnionym szczegółowo

formularzu lub lakoniczne, ustne „zgadzam się"), bez uprzedniego zapoznania go z naturą interwencji i jej możliwymi konsekwencjami. Taka zgoda jest prawnie wadliwa i pozbawiona znaczenia prawnego (Nesterowicz 2019, s. 142 i n.). Rzymska paremia *volenti non fit iniuria* (chcącemu nie dzieje się krzywda) znajduje bowiem zastosowanie wyłącznie wtedy, gdy podmiot wyrażający wolę działa z pełnym rozeznaniem stanu faktycznego. Z tego względu *conditio sine qua non* legalności zabiegu jest uzyskanie zgody uświadomionej. Polega ona na świadomej akceptacji przez pacjenta przewidywanych korzyści oraz potencjalnego ryzyka, stanowiącej zwieńczenie procesu komunikacji z osobą wykonującą zabieg, w ramach którego zrealizowano tzw. obowiązek informacyjny.

Ramy prawne tego obowiązku precyzują przepisy ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (u.z.l.) (Ustawa 1996). Centralne znaczenie ma tu art. 31 ust. 1 u.z.l., który nakłada na lekarza obowiązek udzielania pacjentowi „przystępnej informacji o jego stanie zdrowia, rozpoznaniu, proponowanych oraz możliwych metodach diagnostycznych i leczniczych, dających się przewidzieć następstwach ich zastosowania albo zaniechania, wynikach leczenia oraz rokowaniu" (Zielińska 2022, komentarz do art. 31). Przepis ten należy interpretować ściśle, ze szczególnym uwzględnieniem wymogu „przystępności" informacji. Oznacza to, że komunikat musi być zindywidualizowany, dostosowany do poziomu intelektualnego, percepcji oraz stanu psychicznego danego pacjenta, a jednocześnie wolny od niezrozumiałego, hermetycznego żargonu medycznego.

Obowiązek ten ulega dodatkowej kategoryzacji w przypadku zabiegów operacyjnych oraz metod stwarzających podwyższone ryzyko, do których niewątpliwie zalicza się inwazyjne zabiegi laserowe. Zgodnie z art. 34 ust. 1 u.z.l., do ich wykonania wymagana jest zgoda w formie pisemnej. Z kolei art. 34 ust. 2 u.z.l. wprost determinuje ważność tej formy, stanowiąc, iż „przed wyrażeniem zgody przez pacjenta w sytuacji, o której mowa w ust. 1, lekarz ma obowiązek udzielenia mu informacji zgodnie z art. 31". Dekodując tę normę, należy stwierdzić, że sam podpis na dokumencie nie konwaliduje braków w zakresie ustnego, rzetelnego poinformowania pacjenta o ryzyku. Dokument zgody ma przede wszystkim charakter dowodowy.

Prawny standard uświadomionej zgody nie ogranicza się jednak wyłącznie do obowiązków ustrojowych nałożonych na profesjonalistów medycznych, lecz posiada swoje lustrzane odbicie w sferze praw podmiotowych pacjenta. Systemową gwarancję tego prawa stanowią przepisy art. 16-18 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (u.p.p.) (Ustawa 2008). Przepis art. 16 u.p.p. statuuje ogólne prawo pacjenta do wyrażenia zgody na udzielenie określonych świadczeń zdrowotnych (lub ich odmowy), stanowiące korelat prawa do informacji

(art. 9 u.p.p.). Artykuł 17 u.p.p. dotyczy zgody na zwykłe badanie lub udzielenie innych świadczeń zdrowotnych, dopuszczając formę ustną, a nawet dorozumianą. Natomiast art. 18 u.p.p., analogicznie do przepisów u.z.l., wymaga formy pisemnej dla zabiegów operacyjnych oraz stwarzających podwyższone ryzyko dla pacjenta. Naruszenie tych przepisów skutkuje nie tylko odpowiedzialnością deliktową za ewentualną szkodę na osobie (na zasadach ogólnych Kodeksu cywilnego) (Ustawa 1964), ale kreuje niezależne roszczenie o zadośćuczynienie za samo naruszenie praw pacjenta, o którym mowa w art. 4 ust. 1 u.p.p.

Z perspektywy dogmatyki prawa medycznego oraz ugruntowanego orzecznictwa sądów powszechnych, poprawnie zrealizowany obowiązek informacyjny warunkujący zgodę uświadomioną musi obejmować określony zakres pojęciowy. Pacjent podejmujący decyzję o ingerencji w swoje ciało musi obligatoryjnie wiedzieć:

1. Na czym polega procedura, jakich narzędzi lub preparatów użyje operator, oraz jak będzie przebiegał proces rekonwalescencji.
2. Jakiego rezultatu można się realnie spodziewać i czy istnieją alternatywne, mniej inwazyjne metody osiągnięcia podobnego efektu.
3. Dolegliwości fizjologicznie wpisane w naturę zabiegu, takie jak przejściowy ból, obrzęk, rumień czy uczucie pieczenia, które stanowią naturalną reakcję organizmu i nie są traktowane w kategorii powikłań.
4. Ewentualności wykraczające poza prawidłowy przebieg rekonwalescencji, takie jak trwałe oszpecenie, zakażenie, oparzenia tkankowe, bliznowacenie czy odbarwienia skóry.

Tylko dysponując powyższym, kompletnym zasobem wiedzy, pacjent jest w stanie dokonać właściwego dla siebie bilansu zysków i strat (korzyści terapeutycznych bądź estetycznych w stosunku do ryzyka jatrogennego). Jak słusznie podkreśla się w literaturze przedmiotu, brak rzetelnej informacji w którymkolwiek z tych punktów – a w szczególności przemilczenie ryzyka nietypowych powikłań – sprawia, że oświadczenie woli pacjenta dotknięte jest wadą, a interwencja traci swój legalny charakter (Boratyńska i Konieczniak 2001, s. 234).

Rozszerzony obowiązek informacyjny w medycynie estetycznej

Zakres obowiązku informacyjnego, o którym mowa w art. 31 ust. 1 ustawy o zawodach lekarza i lekarza dentysty, nie ma charakteru absolutnego i jednolitego dla wszystkich dziedzin medycyny. W doktrynie prawa medycznego oraz judykaturze powszechnie przyjmuje się, że granice wymogu uświadamiania pacjenta są

płynne i podlegają gradacji w zależności od teleologii (celu) planowanej interwencji oraz stopnia jej pilności. W klasycznej medycynie naprawczej, ukierunkowanej na ratowanie życia lub zdrowia w stanach nagłych, zakres ten ulega naturalnemu zawężeniu. Z kolei w przypadku zabiegów planowych, a w szczególności tych pozbawionych ścisłych wskazań leczniczych, poprzeczka staranności informacyjnej zostaje zawieszona nieporównywalnie wyżej. Apogeum rygoryzmu w tym zakresie przypada na dziedzinę medycyny estetycznej i kosmetologii inwazyjnej, gdzie wykształciła się koncepcja tzw. rozszerzonego obowiązku informacyjnego (Fiutak 2021).

Fundamentem dla takiego różnicowania standardów jest odmienny rachunek zysków i strat (korzyści do ryzyka jatrogennego), jakiego musi dokonać pacjent. W przypadku interwencji leczniczej, zaniechanie zabiegu zazwyczaj wiąże się z pogorszeniem stanu zdrowia lub śmiercią. Pacjent, niejako zmuszony obiektywnymi okolicznościami, z reguły akceptuje wyższe ryzyko powikłań. Lekarz z kolei, kierując się dobrem pacjenta, koncentruje się na przekazaniu informacji o typowych, dających się przewidzieć i najczęściej występujących następstwach, nie mając obowiązku (a niekiedy wręcz prawa, z uwagi na tzw. przywilej terapeutyczny) epatowania pacjenta kazuistycznymi, skrajnie rzadkimi powikłaniami, które mogłyby go niepotrzebnie i irracjonalnie odwieść od procedury ratującej życie (Nesterowicz 2019, s. 145).

Zupełnie odmiennie kształtuje się sytuacja w przypadku zabiegów o charakterze wyłącznie estetycznym. Pacjent zgłaszający się do gabinetu medycyny estetycznej jest z reguły osobą zdrową w ujęciu somatycznym, a jego jedyną motywacją jest subiektywna chęć poprawy wyglądu zewnętrznego, korekty defektów urody lub odwrócenia procesów starzenia. W takich okolicznościach nie występuje stan wyższej konieczności ani presja czasu. Profesjonalista wykonujący zabieg (lekarz, lekarz dentysta, kosmetolog) ma zatem nieograniczoną możliwość przeprowadzenia wyczerpującego, niespiesznego procesu komunikacyjnego. Co więcej, ewentualne ziszczenie się ryzyka w postaci powikłania (np. bliznowacenia, oparzenia tkankowego, asymetrii twarzy czy trwałych odbarwień) uderza w samo jądro celu zabiegu – zamiast oczekiwanego upiększenia, dochodzi do trwałego oszpecenia. Z tego względu orzecznictwo Sądu Najwyższego ukształtowało niezwykle surowy standard, wymagając, aby zgoda na zabieg kosmetyczny lub estetyczny była oparta na pełnej, niemalże absolutnej wiedzy pacjenta o wszelkich możliwych komplikacjach.

Kierunek ten został wytyczony już w fundamentalnym wyroku Sądu Najwyższego z dnia 5 września 1980 r. (sygn. akt II CR 280/80) (Wyrok SN 1980). Sąd Najwyższy expressis verbis zaprezentował w nim pogląd o konieczności radykalnego zaostrzenia kryteriów zgody na zabieg kosmetyczny w porównaniu do typowej zgody na zabieg leczniczy. W uzasadnieniu wskazano, że brak bezwzględnych

medycznych wskazań do przeprowadzenia interwencji powoduje, iż pacjent musi zostać poinformowany nie tylko o typowych i częstych następstwach, ale również o powikłaniach nietypowych, rzadkich, a nawet sporadycznych. Linia ta była konsekwentnie rozwijana w późniejszych latach.

Kwintesencją rozszerzonego obowiązku informacyjnego w medycynie estetycznej jest wywiedziona z powołanego orzecznictwa doktryna tzw. „cienia podejrzenia". Oznacza ona, że jeżeli na podstawie aktualnej wiedzy medycznej istnieje jakikolwiek, choćby statystycznie znikomy cień podejrzenia wystąpienia negatywnych skutków danego zabiegu, profesjonalista ma bezwzględny obowiązek w pełni i jednoznacznie o tym fakcie pacjenta poinformować (Kubicki 2003, s. 95). Niedopełnienie tego obowiązku – polegające chociażby na poprzestaniu na wskazaniu jedynie łagodnych, przemijających dolegliwości (np. zjawiska pieczenia, czy przejściowego obrzęku po laseroterapii) przy jednoczesnym przemilczeniu ryzyka poparzeń II stopnia i przebarwień – traktowane jest w kategoriach rażącego niedbalstwa informacyjnego.

Konkludując ten fragment rozważań, należy stanowczo stwierdzić, że dobrowolny charakter zabiegów poprawiających urodę de facto wyłącza możliwość powoływania się przez wykonującego zabieg na argument „zwykłego powikłania", jeśli o możliwości jego wystąpienia pacjent nie został wcześniej wyczerpująco pouczony. Przemilczenie ryzyka, którego prawdopodobieństwo oscyluje nawet w granicach ułamka procenta, czyni wyrażoną zgodę prawnie bezskuteczną (pozorną). W konsekwencji interwencja staje się czynem bezprawnym, otwierając drogę do odpowiedzialności odszkodowawczej nie tylko za ewentualny błąd medyczny, ale przede wszystkim kreując autonomiczne roszczenie z tytułu samego faktu naruszenia praw pacjenta do pełnej informacji i świadomego stanowienia o sobie (Wyrok SN 2007b).

Analiza przypadku – ocena standardu informacyjnego i rozkład ciężaru dowodu na tle wyroku Sądu Okręgowego w Poznaniu (sygn. akt XIV C 7/21)

Teoretyczne założenia rozszerzonego obowiązku informacyjnego w medycynie estetycznej znajdują swoje bezpośrednie i rygorystyczne odzwierciedlenie w praktyce orzeczniczej sądów powszechnych. Modelowym przykładem implementacji doktryny „cienia podejrzenia" oraz restrykcyjnego podejścia do oceny ważności zgody pacjenta jest wyrok Sądu Okręgowego w Poznaniu z dnia 29 maja 2025 r. (sygn. akt XIV C 7/21) (Wyrok SO w Poznaniu 2025). Orzeczenie to, ze względu na precyzyjne rozgraniczenie uchybień formalnych od błędów technicznych, dostarcza niezwykle cennego materiału do analizy dogmatyczno-prawnej, w szczególności w aspekcie reżimu dowodowego.

Stan faktyczny rozstrzyganej sprawy ogniskował się wokół zabiegu laserowej redukcji przebarwień posłonecznych skóry twarzy i szyi, wykonanego u powódki przez lekarza dentystę, prowadzącą gabinet medycyny estetycznej. W następstwie procedury, na skutek błędu technicznego polegającego na zbyt mocnym dociśnięciu głowicy lasera i ścieńczeniu warstwy żelu chłodzącego (poniżej 1 mm), powódka doznała oparzeń stopnia IIa oraz trwałych odbarwień skóry szyi. Osią sporu, niezależnie od samego błędu w sztuce, stała się kwestia legalności zabiegu w kontekście dopełnienia obowiązku informacyjnego. Z niespornych ustaleń sądu wynikało, że pacjentka wypełniła ogólny kwestionariusz medyczny, jednakże w dokumentacji zabiegowej zabrakło podpisanego formularza świadomej zgody na zabieg.

Linia obrony strony pozwanej opierała się na dwóch argumentach. Po pierwsze, podnoszono, że pacjentka w natłoku dokumentów najprawdopodobniej omyłkowo pominęła formularz zgody, a samo dobrowolne poddanie się procedurze (przystąpienie do zabiegu) konstytuowało zgodę dorozumianą, a co najmniej ustną. Po drugie, pozwana wskazywała, że uprzedziła powódkę o możliwych skutkach zabiegu, takich jak pieczenie, ból podczas naświetlania oraz obrzęk i zaczerwienienie po jego zakończeniu, traktując te zjawiska jako naturalne następstwa laseroterapii.

Sąd Okręgowy w Poznaniu poddał powyższą argumentację krytyce, obnażając fundamentalne niezrozumienie istoty zgody uświadomionej przez stronę pozwaną. Sąd wprost stwierdził, iż samo ustne wyrażenie zgody na przeprowadzenie zabiegu nie niweluje bezprawności interwencji, jeżeli pacjent nie uzyskał wcześniej szczegółowej wiedzy o możliwych następstwach (Świderska 2007). W ocenie judykatury informacja ograniczająca się do wskazania typowych, przemijających dolegliwości (ból, obrzęk) jest rażąco niewystarczająca. Pozwana przemilczała bowiem ryzyko wystąpienia powikłań nietypowych – oparzeń i trwałych odbarwień skóry. Sąd, odwołując się do specyfiki zabiegów estetycznych, przypomniał, że brak presji czasu oraz dobrowolność poddania się interwencji wymuszają na profesjonaliście obowiązek wyczerpującego poinformowania pacjenta o wszelkich, nawet rzadkich komplikacjach (Fiutak 2021, s. 58). Fakt, że sama lekarka „nie spodziewała się takiego efektu zabiegu", nie zwalniał jej z obowiązku ostrzeżenia o ryzyku, które z punktu widzenia obiektywnej wiedzy medycznej wpisane jest w technologię laserową.

Niezwykle doniosłym elementem omawianego wyroku jest rygorystyczne zastosowanie reguł rozkładu ciężaru dowodu (onus probandi). Zgodnie z fundamentalną zasadą wyrażoną w art. 6 Kodeksu cywilnego (k.c.) (Ustawa 1964), ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne. W procesach medycznych orzecznictwo Sądu Najwyższego jednoznacznie przesądza, że to na podmiocie leczniczym (lekarzu, kosmetologu) spoczywa ciężar udowodnienia,

iż pacjentowi udzielono wyczerpującej, przystępnej informacji, o której mowa w art. 31 ust. 1 u.z.l., oraz że odebrano od niego świadomą zgodę (art. 34 ust. 2 u.z.l.) (Ustawa 1996). Pacjent nie musi dowodzić, że informacji mu nie udzielono (dowodzenie faktu negatywnego tzw. probatio diabolica byłoby zresztą niemożliwe).

W sprawie poznańskiej brak podpisanego formularza wymieniającego expressis verbis ryzyko poparzeń i odbarwień okazał się dla pozwanej lekarki błędem o charakterze fatalnym. Argumentacja o „przypadkowym pominięciu" dokumentu przez powódkę została słusznie zdeprecjonowana przez sąd jako niewiarygodna i nieodnosząca skutku prawnego. To profesjonalista ponosi wyłączne ryzyko braków w dokumentacji medycznej. Dokumentacja ta nie stanowi bowiem jedynie biurokratycznego obciążenia, lecz pełni funkcję podstawowej ochrony dowodowej (Nesterowicz 2019, s. 150). W sytuacji braku pisemnego potwierdzenia zakresu przekazanych informacji, sąd przyjmuje wersję pacjenta, uznając, że wiedza o ryzyku nie została mu przekazana. Tym samym, wobec braku podpisu pod konkretnym, zindywidualizowanym ryzykiem, interwencja pozbawiona jest kontratypu zgody pacjenta, stając się działaniem bezprawnym.

Znamienny w omawianym orzeczeniu jest również sposób wyceny krzywdy (kompensacji) przez Sąd Okręgowy, który doskonale oddaje naturę szkody estetycznej. Ustalając wysokość zadośćuczynienia, Sąd wziął pod uwagę lokalizację powikłań. Zauważono, że powódka doznała oparzeń na szyi, co wprawdzie stanowiło dla niej ogromny dyskomfort i wymusiło zmianę garderoby (noszenie apaszek, golfów), jednakże pozwalało na ukrycie defektu przed otoczeniem. Sąd jednoznacznie zasugerował, że gdyby do identycznego uszkodzenia tkanek doszło na twarzy – obszarze, którego zatuszowanie jest obiektywnie niemożliwe – kwota zadośćuczynienia byłaby wyższa (Wyrok SO w Poznaniu 2025). Argument ten potwierdza, że w sprawach z zakresu medycyny estetycznej kryterium „widoczności oszpecenia" stanowi kluczowy paradygmat miarkowania zadośćuczynienia na podstawie art. 445 § 1 k.c.

Podsumowując analizę przedmiotowego orzeczenia, należy stwierdzić, że stanowi ono ostrzeżenie dla przedstawicieli branży medycyny estetycznej. Pokazuje bowiem, że lakoniczna informacja i braki w dokumentacji mogą zamknąć profesjonaliście drogę do skutecznej obrony w procesie cywilnym, czyniąc go z góry bezbronnym wobec zarzutu naruszenia praw pacjenta, a w konsekwencji warunkując de facto przegranie sporu jeszcze zanim sąd przystąpi do oceny prawidłowości samej techniki zabiegowej.

Zbieg roszczeń kompensacyjnych: Naruszenie praw pacjenta a błąd medyczny (delikt) w świetle praktyki orzeczniczej

Zjawisko wadliwie przeprowadzonego zabiegu medycyny estetycznej, któremu towarzyszy brak uświadomionej zgody pacjenta, generuje na gruncie polskiego prawa cywilnego skomplikowany stan faktyczno-prawny, skutkujący najczęściej kumulacją (zbiegiem) niezależnych reżimów odpowiedzialności. W doktrynie i ugruntowanej judykaturze Sądu Najwyższego wykształcił się bezsporny pogląd o dualizmie roszczeń kompensacyjnych przysługujących poszkodowanemu pacjentowi. Zbieg ten – choć de facto wynika z jednego zdarzenia historycznego (wizyty w gabinecie i poddania się procedurze) – obejmuje roszczenia chroniące zupełnie odmienne dobra prawne i opierające się na odrębnych przesłankach materialnoprawnych. Wyrok Sądu Okręgowego w Poznaniu z dnia 29 maja 2025 r. (sygn. akt XIV C 7/21) stanowi wręcz podręcznikowy przykład takiej kumulacji, obnażając wielopłaszczyznowe ryzyko finansowe ciążące na profesjonalistach z branży estetycznej (Wyrok SO w Poznaniu 2025).

W pierwszej kolejności wyodrębnić należy roszczenie z tytułu zawinionego naruszenia praw pacjenta, zakotwiczone w art. 4 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (u.p.p.) w związku z art. 448 Kodeksu cywilnego (k.c.) (Ustawa 1964; Ustawa 2008). Dobrem prawnie chronionym w tym reżimie nie jest zdrowie sensu stricto, lecz autonomia woli pacjenta, jego godność, prywatność oraz prawo do rzetelnej informacji. Jak wielokrotnie wskazywał Sąd Najwyższy (por. wyroki z dnia 29 maja 2007 r., V CSK 76/07 oraz z dnia 27 kwietnia 2012 r., V CSK 142/11), ochrona na podstawie u.p.p. ma charakter wysoce autonomiczny i uniezależniony od wystąpienia medycznej szkody na osobie (Wyrok SN 2007b; Wyrok SN 2012). Oznacza to, że sam fakt przystąpienia przez lekarza dentystę do inwazyjnego zabiegu laserowego bez odebrania od powódki uświadomionej zgody na piśmie – a więc z zatajeniem ryzyka poparzeń i odbarwień – stanowił czyn bezprawny naruszający jej sferę samostanowienia. W analizowanej sprawie doniosłość tego roszczenia uwidoczniła się już na etapie przedsądowym. Zakład ubezpieczeń (działający z tytułu polisy OC sprawcy) dokonał instytucji tzw. uznania właściwego i dobrowolnie wypłacił powódce kwotę 10 000 zł zadośćuczynienia wyłącznie za naruszenie jej prawa do informacji, słusznie oceniając, iż brak podpisanego formularza czyni obronę w tym zakresie bezprzedmiotową. Sąd Okręgowy w pełni zaaprobował tę wycenę, konkludując, że krzywda polegająca na utracie możliwości świadomego zrezygnowania z ryzykownego zabiegu zasługuje na realną, odczuwalną kompensację,

pełniącą zarazem funkcję dyscyplinująco-represyjną wobec sprawcy (Nesterowicz 2019, s. 148; Wyrok SO w Poznaniu 2025).

Zupełnie odrębną płaszczyznę stanowi klasyczny reżim odpowiedzialności deliktowej (błąd w sztuce medycznej), którego podstawę stanowią przepisy art. 415 k.c. w zw. z art. 444 § 1 i art. 445 § 1 k.c. (Ustawa 1964). W tym przypadku dobrem chronionym jest zdrowie i integralność cielesna powoda. Zaktualizowanie się tej odpowiedzialności wymaga kumulatywnego wykazania przesłanek z art. 415 k.c.: zawinionego i bezprawnego zachowania sprawcy, szkody oraz adekwatnego związku przyczynowego (art. 361 § 1 k.c.).

W sprawie poznańskiej błąd w sztuce medycznej nie miał charakteru uchybienia formalnego, lecz przybrał postać mierzalnego błędu techniczno-wykonawczego (Wyrok SO w Poznaniu 2025). Na podstawie opinii biegłego z zakresu medycyny estetycznej Sąd ustalił, iż operator lasera zbyt mocno docisnął głowicę do skóry powódki. W efekcie doszło do ścieńczenia warstwy żelu chłodzącego poniżej krytycznego progu bezpieczeństwa (1 mm), co zablokowało prawidłowe odprowadzanie energii cieplnej i skutkowało oparzeniami stopnia IIa. Wbrew twierdzeniom pozwanej i jej ubezpieczyciela – którzy próbowali zakwalifikować to zdarzenie jako "normalne powikłanie" poprawnie wykonanego zabiegu – dowód z opinii biegłego bezspornie wykazał, że szkoda wynikała z uchybienia sztuki medycznej.

Niezwykle istotnym elementem oceny zawinienia (winy w ujęciu subiektywnym, tj. niedbalstwa) w analizowanym wyroku stała się kwestia tzw. czynnika ludzkiego, a mianowicie zignorowania bólu powódki. Sąd Okręgowy z całą stanowczością wyartykułował zasadę, iż w zabiegach laserowych ból zgłaszany przez pacjenta przestaje być jedynie subiektywnym dyskomfortem, a staje się obiektywnym czynnikiem ostrzegawczym. Zaniechanie przez pozwaną natychmiastowej reakcji – polegającej na przerwaniu naświetlania, ocenie stanu tkanki i ewentualnej modyfikacji parametrów chłodzenia – oraz zbycie skarg pacjentki zapewnieniem, że odczucia te są "naturalne", wyczerpało znamiona rażącego naruszenia miernika należytej staranności (art. 355 § 2 k.c.) (Ustawa 1964; Wyrok SO wPoznaniu 2025).

Konsekwencją uznania powództwa w reżimie deliktowym było zasądzenie kolejnych kwot, realizujących odmienne funkcje kompensacyjne. Sąd zasądził kwotę 30 000 zł tytułem zadośćuczynienia za doznaną krzywdę fizyczną i psychiczną (cierpienie, wycofanie społeczne, zaburzenia adaptacyjne stwierdzone przez biegłego psychiatrę) oraz kwotę 10 000 zł tytułem odszkodowania majątkowego (zgodnie z zasadą restitutio in integrum), przeznaczonego na pokrycie wyliczonych przez biegłego przyszłych kosztów zabiegów naprawczych w postaci przeszczepu komórek barwnikowych (Wyrok SO w Poznaniu 2025).

Rozłączność obu omówionych reżimów odpowiedzialności obnaża wady powszechnego w branży kosmetologicznej i estetycznej przekonania, iż polisa ubezpieczenia od odpowiedzialności cywilnej (OC) stanowi tarczę chroniącą przed skutkami własnych zaniedbań. Strategia procesowa zakładu ubezpieczeń w analizowanej sprawie ukazuje bezwzględną logikę biznesową: ubezpieczyciel szybko i sprawnie wypłacił środki za brak dokumentacji (chroniąc własne koszty wobec oczywistości naruszenia), pozostawiając jednak osobę wykonującą zabieg w wieloletnim procesie sądowym o błąd techniczny.

Konkludując ten etap rozważań, prawnik procesualista, jak i orzecznik oceniający spory z zakresu medycyny estetycznej, muszą bezwzględnie odróżniać brak zgody uświadomionej od błędu medycznego. Są to dwa niezależne delikty. Brak staranności w sferze informacyjnej delegalizuje interwencję i narusza godność pacjenta, z kolei brak staranności wykonawczej rodzi odpowiedzialność za fizyczne i majątkowe skutki jatrogenne. Skumulowanie obu tych zaniechań prowadzi do zwielokrotnienia ciężaru finansowego spoczywającego na podmiocie leczniczym, czego dowodzi łączna suma obciążeń (należność główna, odsetki ustawowe za wieloletnie opóźnienie oraz koszty sądowe) w sprawie poznańskiej, oscylująca w granicach 80 000 złotych (Wyrok SO w Poznaniu 2025).

Podsumowanie i wnioski *de lege lata*

Przeprowadzona w niniejszym artykule analiza dogmatyczno-prawna oraz studium orzecznictwa – ze szczególnym uwzględnieniem wyroku Sądu Okręgowego w Poznaniu z dnia 29 maja 2025 r. (sygn. akt XIV C 7/21) – w pełni potwierdzają tezę o autonomicznym, wysoce rygorystycznym standardzie obowiązku informacyjnego w medycynie estetycznej i kosmetologii inwazyjnej. Fakultatywny charakter zabiegów poprawiających urodę, brak presji czasu oraz brak medycznych wskazań ratujących życie lub zdrowie sprawiają, że pacjent musi dysponować absolutnie pełnym spektrum wiedzy na temat ryzyka jatrogennego. Ugruntowana w judykaturze doktryna „cienia podejrzenia" bezwzględnie wymaga od profesjonalistów informowania o wszelkich, nawet kazuistycznych i statystycznie marginalnych powikłaniach.

Wnioski płynące z analizy aktualnego stanu prawnego (de lege lata) oraz praktyki orzeczniczej sądów powszechnych zmuszają do zmiany paradygmatu postrzegania obowiązków formalnych przez przedstawicieli branży beauty. W świadomości wielu lekarzy medycyny estetycznej oraz kosmetologów prowadzenie dokumentacji – w tym odbieranie precyzyjnych oświadczeń woli – wciąż jawi się jako uciążliwy, biurokratyczny obowiązek, nierzadko realizowany w sposób fasadowy

(tzw. zgody blankietowe). Tymczasem w świetle reguł dowodowych polskiej procedury cywilnej (art. 6 k.c.), dokumentacja zabiegowa nie jest jedynie biurokracją, lecz stanowi fundamentalne, a niekiedy jedyne narzędzie ochrony prawnej podmiotu wykonującego zabieg.

W sytuacji sporu sądowego to na profesjonaliście spoczywa onus probandi – ciężar wykazania, że pacjent został w sposób przystępny i wyczerpujący poinformowany o konkretnym powikłaniu, które faktycznie u niego wystąpiło (np. o ryzyku oparzeń czy trwałych odbarwień skóry w przypadku laseroterapii). Brak podpisu pacjenta pod zindywidualizowanym ryzykiem pozbawia interwencję niezbędnego kontratypu, jakim jest zgoda uświadomiona. Jak pokazała sprawa poznańska, uchybienie to z góry determinuje przegranie procesu w zakresie naruszenia praw pacjenta (art. 4 ust. 1 u.p.p.), niezależnie od tego, czy w samej warstwie technicznej doszło do błędu medycznego, narażając gabinet, na często dotkliwe w wysokości, straty finansowe i wizerunkowe.

Powyższe konkluzje prowadzą do postulatu de lege lata, skierowanego do środowisk medycznych i kosmetologicznych, dotyczącego systemowej standaryzacji formularzy świadomej zgody. Na obecnym etapie rozwoju rynku medycyny estetycznej posługiwanie się ogólnikowymi kwestionariuszami jest błędem o charakterze systemowym. Formularze powinny podlegać ścisłej kategoryzacji ze względu na specyfikę technologii (np.osobne formularze dla konkretnych procedur laserowych, iniekcji kwasu hialuronowego, czy użycia toksyny botulinowej). Wymaga się, aby dokumenty te expressis verbis wyliczały zarówno typowe, naturalne następstwa zabiegu (ból, rumień, obrzęk), jak i powikłania nietypowe (martwica tkanek, oparzenia, bliznowacenie, ziarniniaki czy ślepota).

Standaryzacja ta – oparta na aktualnej wiedzy medycznej (tzw. EBM – Evidence Based Medicine) i wspierana wytycznymi towarzystw naukowych – pozwoliłaby na ujednolicenie praktyki i znaczące zminimalizowanie ryzyka prawnego. Poprawnie skonstruowana, szczegółowa i podpisana przez pacjenta zgoda zmienia bowiem kwalifikację prawną ewentualnego zdarzenia niepożądanego z „zawinionego naruszenia praw pacjenta" na „akceptowane przez pacjenta ryzyko medyczne".

Reasumując, współczesna medycyna estetyczna to dziedzina obarczona wyjątkowo wysokim ryzykiem cywilnoprawnym. Skuteczna profilaktyka prawna w gabinecie wymaga przyjęcia założenia, że proces leczenia i upiększania rozpoczyna się nie w momencie uruchomienia aparatury zabiegowej, lecz w chwili rzetelnego, szczerego i udokumentowanego dialogu z pacjentem.

Bibliografia

Akty prawne

Ustawa 1964 Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2023 r. poz. 1610 z późn. zm.).

Ustawa 1996 Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz. U. z 2023 r. poz. 1516 z późn. zm.).

Ustawa 2008 Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581 z późn. zm.).

Orzecznictwo

Wyrok SN

1980 Wyrok Sądu Najwyższego z dnia 5 września 1980 r., sygn. akt II CR 280/80 (OSNC 1981, nr 10, poz. 170).

2007a Wyrok Sądu Najwyższego z dnia 26 kwietnia 2007 r., sygn. akt II CSK 2/07 (OSP 2009, nr 1, poz. 6).

2007 Wyrok Sądu Najwyższego z dnia 29 maja 2007 r., sygn. akt V CSK 76/07 (OSNC 2008, nr 7-8, poz. 91).

2012 Wyrok Sądu Najwyższego z dnia 27 kwietnia 2012 r., sygn. akt V CSK 142/11 (OSP 2013, nr 6, poz. 61).

Wyrok SO w Poznaniu

2025 Wyrok Sądu Okręgowego w Poznaniu z dnia 29 maja 2025 r., sygn. akt XIV C 7/21

Literatura

Boratyńska M., Konieczniak P.
2001 *Prawa pacjenta*, Warszawa.

Fiutak A.
2021 *Prawo w medycynie*, Warszawa.

Janiszewska B.
2013 *Zgoda na udzielenie świadczenia zdrowotnego. Ujęcie wewnątrzsystemowe*, Warszawa.

Kubicki L.
2003 *Prawo medyczne*, Warszawa.

Nesterowicz M.
2019 *Prawo medyczne*, wyd. XII, Toruń.

Safjan M.
1998 *Prawo i medycyna. Ochrona praw jednostki a dylematy współczesnej medycyny*, Warszawa.

Świderska M.
2007 *Zgoda pacjenta na zabieg medyczny*, Toruń.

Zielińska E. (red.)
2022 *Ustawa o zawodach lekarza i lekarza dentysty. Komentarz*, wyd. III, Warszawa.

EXPANDED DUTY TO INFORM IN AESTHETIC MEDICINE AND THE CIVIL LIABILITY OF THE PRACTITIONER: A CASE LAW ANALYSIS

Abstract: The dynamic development of the aesthetic medicine and cosmetology market creates new challenges in the field of medical and civil law. The article addresses the issue of the patient's informed consent standard in the context of procedures whose purpose is not to save a life or restore health, but to improve external appearance. The research objective of the paper is to answer the question of whether the requirements regarding the duty to inform should be differentiated depending on the therapeutic or purely aesthetic nature of the intervention. Based on an analysis of the Supreme Court's case law and a recent judgment of the Regional Court in Poznań (case file No. XIV C 7/21), the author posits that the elective nature of aesthetic procedures forces a rigorous tightening of the duty to inform. It has been demonstrated that concealing the risk of rare complications – even if there is only a "shadow of a suspicion" of their occurrence – invalidates the patient's consent, constituting an independent basis for redress for the violation of patient rights, regardless of liability for damages for potential medical malpractice.

Keywords: aesthetic medicine, informed consent, physician's duty to inform, medical malpractice, patient rights, civil liability

Katarzyna Gurgul
Uniwersytet Wrocławski

SZARA STREFA MEDYCYNY ESTETYCZNEJ. GRANICE KOMPETENCJI LEKARZA I KOSMETOLOGA W ŚWIETLE ORZECZNICTWA SĄDOWEGO ORAZ PRAKTYKI ORGANÓW ADMINISTRACJI PAŃSTWOWEJ

Streszczenie: Artykuł podejmuje aktualną problematykę zacierania się granic między medycyną estetyczną a kosmetologią w polskim systemie prawnym. Brak ustawowej definicji zawodu kosmetologa oraz precyzyjnego podziału na procedury medyczne i kosmetyczne doprowadził do powstania niebezpiecznej dla pacjentów „szarej strefy". Autorka dokonuje analizy dogmatycznoprawnej i orzeczniczej (w tym wyroków Sądu Najwyższego oraz sądów powszechnych), wykazując, jak judykatura radzi sobie z oceną odpowiedzialności cywilnej i karnej osób wykonujących inwazyjne zabiegi bez odpowiednich uprawnień medycznych. Szczególną uwagę poświęcono kwalifikacji kwasu hialuronowego i toksyny botulinowej w świetle unijnego rozporządzenia MDR oraz Prawa farmaceutycznego. Nowością badawczą artykułu jest analiza wpływu tej luki prawnej na funkcjonowanie organów państwa, zilustrowana najnowszą praktyką Dyrektora Krajowej Informacji Skarbowej oraz Głównego Urzędu Statystycznego (2024 r.) w kontekście obniżonych stawek podatku VAT. Artykuł kończą wnioski de lege ferenda postulujące pilną potrzebę ustawowego uregulowania uprawnień w branży beauty.

Słowa kluczowe: medycyna estetyczna, kosmetologia, odpowiedzialność cywilna, błąd medyczny, wyroby medyczne, MDR, świadczenie zdrowotne, podatek VAT

Medycyna estetyczna, niegdyś zarezerwowana wyłącznie dla gabinetów lekarskich, ulega obecnie procesowi demokratyzacji, przenikając w szerokim zakresie do oferty podmiotów nieposiadających statusu placówek medycznych. Usługi kosmetologiczne coraz śmielej ingerują w strukturę tkanek poprzez zabiegi iniekcyjne,

wykorzystując preparaty o udowodnionym lub domniemanym działaniu farmakologicznym. Ten swoisty wyścig technologiczny, nierzadko podsycany agresywnym marketingiem, rodzi uzasadnione obawy o bezpieczeństwo pacjenta-konsumenta. Wobec braku aktu prawnego rangi ustawowej, który w sposób wyczerpujący i kategoryczny rozgraniczałby kompetencje lekarza od uprawnień kosmetologa, polski system prawny boryka się z problemem wyegzekwowania odpowiedzialności za błędy i powikłania powstałe w wyniku przekroczenia kompetencji zawodowych. W praktyce judykacyjnej można zaobserwować zróżnicowane podejścia do kwestii odpowiedzialności cywilnej i karnej osób wykonujących zabiegi z pogranicza medycyny i kosmetologii bez odpowiednich kwalifikacji. Celem niniejszego opracowania jest próba nakreślenia granic tych kompetencji na podstawie analizy dotychczasowego dorobku orzecznictwa, z jednoczesnym uwzględnieniem statusu stosowanych produktów (leki, wyroby medyczne). Ponadto, artykuł pokaże wymiar problemu braku regulacji, jakim jest paraliż organów administracji skarbowej i Głównego Urzędu Statystycznego w procesie kwalifikacji usług beauty na potrzeby rozliczeń podatkowych (VAT), co stanowi dobitny dowód na konieczność pilnej interwencji ustawodawcy.

Fundamentem rozważań nad dopuszczalnością wykonywania określonych zabiegów przez lekarzy i kosmetologów jest analiza obowiązujących w Polsce przepisów prawa, które kształtują zakres ich kompetencji. Trudność polega na tym, że o ile ramy wykonywania zawodu lekarza są uregulowane relatywnie precyzyjnie, o tyle status kosmetologa pozostaje w dużej mierze niezdefiniowany ustawowo, co prowadzi do wspomnianego zderzenia "dwóch światów" – uregulowanej medycyny i nieregulowanej prawnie (w aspekcie uprawnień do ingerencji w tkanki) kosmetologii.

Wyłączność lekarza do udzielania świadczeń zdrowotnych

Punktem wyjścia dla określenia kompetencji lekarza jest ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2023 r. poz. 1516 z późn. zm.). Zgodnie z art. 2 ust. 1 tej ustawy, wykonywanie zawodu lekarza polega na udzielaniu świadczeń zdrowotnych, w szczególności: badaniu stanu zdrowia, rozpoznawaniu chorób i zapobieganiu im, leczeniu i rehabilitacji chorych, udzielaniu porad lekarskich, a także wydawaniu opinii i orzeczeń lekarskich. Z kolei art. 2 ust. 2 precyzuje, że wykonywanie zawodu lekarza dentysty polega na udzielaniu świadczeń określonych w ust. 1, w zakresie chorób zębów, jamy ustnej, części twarzowej czaszki oraz okolic przyległych.

Kluczowe dla wyznaczenia granicy między medycyną a kosmetologią jest pojęcie "świadczenia zdrowotnego". Definicję legalną tego terminu zawiera ustawa z dnia

15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2023 r. poz. 991 z późn. zm.). Zgodnie z jej art. 2 ust. 1 pkt 10, świadczenie zdrowotne to działania służące zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania.

Z powołanych przepisów wynika jednoznacznie, że prawo do udzielania świadczeń zdrowotnych jest zastrzeżone wyłącznie dla osób wykonujących zawody medyczne (przede wszystkim lekarzy), a definicja ta opiera się na kryterium celu, którym musi być szeroko pojęta ochrona zdrowia. Wszelkie działania wkraczające w sferę "świadczeń zdrowotnych" podejmowane przez osoby nieuprawnione stanowią naruszenie prawa, zagrożone sankcją karną z art. 58 ust. 1 ustawy o zawodach lekarza i lekarza dentysty (udzielanie świadczeń zdrowotnych bez uprawnień).

Sąd Najwyższy w orzeczeniu z dnia 26 maja 2021 r. (sygn. akt I KK 23/21) wyraźnie zaakcentował rygoryzm ustawowych ram wykonywania zawodów medycznych, wskazując, że nawet w obrębie tych zawodów granice kompetencji są ściśle określone (np. ograniczenie obszaru działania lekarza dentysty), a certyfikaty z kursów doszkalających "nie stanowią potwierdzenia, że dana osoba posiada umiejętności stosowania preparatu" i nie nadają uprawnień wykraczających poza ustawowe ramy. Orzeczenie to ustanawia bezwzględny prymat prawa powszechnie obowiązującego nad kwalifikacjami nabywanymi poza formalnym systemem specjalizacji medycznych.

Brak ustawowej regulacji zawodu kosmetologa i kwalifikacja zabiegów estetycznych

W opozycji do zawodu lekarza, status kosmetologa w polskim systemie prawnym charakteryzuje się brakiem kompleksowej regulacji ustawowej. Kosmetolog nie jest wymieniony w ustawie o działalności leczniczej jako osoba wykonująca zawód medyczny. Jak słusznie zauważył Naczelny Sąd Administracyjny w wyroku z dnia 4 października 2016 r. (sygn. akt I FSK 878/14): „zawód kosmetologa nie jest zawodem medycznym w rozumieniu art. 18d ust. 1 pkt 1 ustawy o ZOZ [obecnie u.d.l. – przyp. aut.], a tym samym osoby posiadające kwalifikacje do jego wykonywania nie spełniają przesłanki podmiotowej do skorzystania ze zwolnienia [z VAT – przyp. aut.]". Sąd podkreślił, że mimo nabywania przez kosmetologów w toku studiów wiedzy z zakresu nauk medycznych, nie są oni uprawnieni do udzielania świadczeń opieki zdrowotnej.

Brak ustawy o zawodzie kosmetologa powoduje, że zakres jego uprawnień nie jest zdefiniowany pozytywnie (co kosmetolog może robić), lecz wyznaczany negatywnie – poprzez zakaz wkraczania w kompetencje zastrzeżone dla lekarzy (świadczenia zdrowotne, ordynowanie i stosowanie leków na receptę). Tradycyjnie przyjmuje się, że kosmetologia obejmuje nieinwazyjne zabiegi pielęgnacyjne i upiększające, działające na powierzchniowe warstwy skóry.

Główny problem pojawia się przy kwalifikacji prawnej zabiegów z pogranicza, czyli tzw. medycyny estetycznej, obejmujących procedury inwazyjne (iniekcje, lasery o dużej mocy). Kosmetolodzy często argumentują swoje prawo do ich wykonywania, powołując się na fakt, że zabiegi te – mające na celu wyłącznie poprawę urody – nie spełniają definicji "świadczenia zdrowotnego", gdyż nie służą ratowaniu czy poprawie zdrowia w sensie terapeutycznym.

Taka argumentacja znajduje częściowe odzwierciedlenie w orzecznictwie sądów administracyjnych. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 30 maja 2016 r. (sygn. akt VII SA/Wa 385/16) stwierdził, że "zabiegi z zakresu medycyny estetycznej co do zasady nie mieszczą się w pojęciu świadczenia zdrowotnego w rozumieniu przepisu art. 2 ust. 1 pkt 10 u.d.l. Mają one na ogół na celu poprawienie wyglądu zewnętrznego lub usunięcie wad urody". Sąd ten dopuścił jednak wyjątek, wskazując, że w pewnych przypadkach świadczenia te mogą służyć poprawie lub ratowaniu zdrowia (np. chirurgia rekonstrukcyjna), co wymaga indywidualnej oceny. Podobne stanowisko – różnicujące zabiegi na podstawie celu (terapeutyczny vs. wyłącznie estetyczny) – jest konsekwentnie przyjmowane przez organy podatkowe w kontekście prawa do zwolnienia z podatku VAT (np. Pismo Dyrektora Krajowej Informacji Skarbowej z dnia 30 czerwca 2021 r., znak: 0112-KDIL3.4012.99.2021.2.AK).

Z pozoru "korzystne" dla kosmetologów orzeczenia, odmawiające zabiegom estetycznym statusu świadczeń zdrowotnych, tworzą jednak iluzję legalności ich wykonywania przez osoby bez wykształcenia medycznego. O ile bowiem dany zabieg może nie być "świadczeniem zdrowotnym" w rozumieniu ustawy o działalności leczniczej, o tyle jego wykonanie nadal podlega rygorom innych aktów prawnych, przede wszystkim Prawa farmaceutycznego oraz Ustawy o wyrobach medycznych, co w praktyce czyni wykonywanie inwazyjnych procedur estetycznych przez kosmetologów działaniem sprzecznym z prawem, o czym szerzej w kolejnej części artykułu.

Podsumowując, ramy prawne w Polsce opierają się na wyłączności lekarzy do udzielania świadczeń zdrowotnych oraz braku definicji kompetencji kosmetologów. Paradoks polega na tym, że brak kwalifikacji zabiegów czysto estetycznych jako świadczeń zdrowotnych nie oznacza automatycznej legalizacji ich wykonywania

przez niemedyków, lecz przesuwa środek ciężkości analizy na status prawny używanych do tych zabiegów substancji i narzędzi.

Produkty lecznicze i wyroby medyczne

Skoro analiza samej definicji "świadczenia zdrowotnego" często prowadzi do niejednoznacznych wniosków, a brak ustawy o zawodzie kosmetologa uniemożliwia proste wyliczenie dozwolonych procedur, to gdzie w polskim systemie prawnym przebiega twarda, nieprzekraczalna granica między medycyną a kosmetologią? Odpowiedź kryje się w przepisach regulujących obrót i stosowanie substancji oraz narzędzi wykorzystywanych podczas zabiegów – mianowicie w Prawie farmaceutycznym oraz przepisach dotyczących wyrobów medycznych. To status prawny użytego produktu determinuje, kto może po niego legalnie sięgnąć.

Toksyna botulinowa (Prawo farmaceutyczne)

Najbardziej jaskrawym przykładem przekraczania kompetencji w branży beauty jest podawanie przez osoby bez wykształcenia medycznego toksyny botulinowej (potocznie zwanej botoksem). W świetle przepisów ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301 z późn. zm.), toksyna botulinowa jest bezwzględnie klasyfikowana jako produkt leczniczy (lek), a nie wyrób medyczny czy tym bardziej kosmetyk.

Kluczowe znaczenie ma tu kategoria dostępności. Wszystkie zarejestrowane w Polsce preparaty zawierające toksynę botulinową posiadają kategorię dostępności "Rp" – wydawane z przepisu lekarza. Oznacza to, że ustawodawca uznał stosowanie tego preparatu za stwarzające bezpośrednie lub pośrednie niebezpieczeństwo dla zdrowia, wymagające ordynacji i nadzoru lekarskiego. Z samego faktu, że lek wydawany jest na receptę, wynika logiczny wniosek, iż kosmetolog (nieposiadający uprawnień do wystawiania recept) nie może wejść w jego legalne posiadanie w celu komercyjnego wykorzystania w swoim gabinecie.

Ordynowanie i podawanie leku na receptę jest immanentną częścią udzielania świadczeń zdrowotnych. Proces ten obejmuje zbadanie pacjenta, postawienie diagnozy (nawet jeśli problemem jest np. bruksizm czy nadpotliwość), określenie dawki i sposobu podania. Kompetencje te są zastrzeżone wyłącznie dla lekarzy. Co więcej, w Charakterystyce Produktu Leczniczego (ChPL) – dokumencie stanowiącym podstawę dopuszczenia leku do obrotu – producenci toksyny botulinowej wprost

wskazują, że preparat może być podawany wyłącznie przez lekarza posiadającego odpowiednie kwalifikacje.

Wykonywanie zabiegów z użyciem toksyny botulinowej przez kosmetologów rodzi zatem konsekwencje prawnokarne. Po pierwsze, stanowi to naruszenie art. 58 ustawy o zawodach lekarza i lekarza dentysty (udzielanie świadczeń zdrowotnych bez uprawnień). Po drugie, ze względu na niemożność legalnego zakupu leku na receptę przez gabinet kosmetyczny, preparaty te często pochodzą z nielegalnych źródeł (np. import z Azji, podróbki). Takie działanie penalizuje art. 126b ust. 1 i 2 Prawa farmaceutycznego, wprowadzając kary pozbawienia wolności zarówno dla osoby sprzedającej lek poza legalnym łańcuchem dystrybucji, jak i dla nabywcy (kosmetologa), który kupuje produkt leczniczy z naruszeniem zakazów. Orzecznictwo sądów powszechnych potwierdza rygorystyczne podejście do nielegalnego obrotu lekami, czego przykładem jest wyrok Sądu Apelacyjnego w Warszawie z dnia 27 listopada 2018 r. (sygn. akt II AKa 228/18). Sąd ten wskazał, że do wykazania zamiaru bezpośredniego nielegalnego wprowadzania do obrotu produktu leczniczego wystarczy świadomość powszechnego zakazu handlu lekami poza aptekami.

Kwas hialuronowy i inne wypełniacze – Ustawa o wyrobach medycznych i MDR

Sytuacja prawna kwasu hialuronowego (stosowanego w iniekcjach jako wypełniacz) jest odmienna, lecz równie restrykcyjna dla osób bez wykształcenia medycznego. Preparaty te nie są lekami, lecz są klasyfikowane jako wyroby medyczne, zazwyczaj klasy III (najwyższego ryzyka).

Fundamentalną zmianę w tym obszarze przyniosło wejście w życie unijnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 (tzw. MDR – Medical Device Regulation). Rozporządzenie to, stosowane bezpośrednio od maja 2021 r., znacząco zaostrzyło wymogi dotyczące oceny zgodności, nadzoru i dokumentacji wyrobów medycznych. Co niezwykle istotne, na mocy Aneksu XVI do MDR, rygorom rozporządzenia poddano również grupy produktów niemających przewidzianego zastosowania medycznego, ale o profilu ryzyka zbliżonym do wyrobów medycznych. Należą do nich wprost m.in. substancje przeznaczone do stosowania jako wypełniacze do twarzy (wstrzykiwane podskórnie). Oznacza to, że nawet kwas hialuronowy reklamowany przez producenta wyłącznie do celów "upiększających" musi spełniać te same, rygorystyczne normy co wyrób medyczny (m.in. znak CE, odpowiednia dokumentacja).

Jak przekłada się to na granice kompetencji? Kluczem jest instrukcja używania wyrobu. Zgodnie z MDR, producent w ramach oceny ryzyka określa w instrukcji przewidziane zastosowanie wyrobu oraz kwalifikacje jego użytkownika. Na gruncie prawa krajowego, art. 63 ustawy z dnia 7 kwietnia 2022 r. o wyrobach medycznych (Dz. U. z 2022 r. poz. 974) nakłada na użytkownika bezwzględny obowiązek: wyrób powinien być używany zgodnie z przewidzianym zastosowaniem, a użytkownik jest obowiązany do przestrzegania instrukcji używania wyrobu.

Wielu producentów renomowanych wypełniaczy tkankowych (wyrobów klasy III) w swoich instrukcjach wyraźnie zastrzega, że produkt jest przeznaczony do stosowania wyłącznie przez wykwalifikowanego lekarza (lub ewentualnie przez personel medyczny pod jego ścisłym nadzorem). Stosowanie takiego wyrobu przez kosmetologa (który zgodnie z wcześniej przywołanym orzecznictwem NSA nie wykonuje zawodu medycznego) stanowi bezpośrednie naruszenie instrukcji używania, a tym samym naruszenie art. 63 ustawy o wyrobach medycznych. Stanowi to argument prawny, delegalizujący wykonywanie iniekcji kwasu hialuronowego przez osoby bez uprawnień lekarskich, niezależnie od tego, czy sam zabieg nazwiemy "świadczeniem zdrowotnym", czy też "usługą kosmetyczną". Teza wyroku Krajowej Izby Odwoławczej z dnia 16 kwietnia 2019 r. (sygn. akt KIO 573/19) potwierdza tę interpretację, wskazując, że: "Kwestię dopuszczalności używania wyrobu w określonych celach rozstrzyga dostarczana z nim dokumentacja".

Reasumując, polskie i unijne przepisy regulujące status produktów leczniczych oraz wyrobów medycznych stanowią twardą, nieprzekraczalną barierę kompetencyjną. Sam fakt zaklasyfikowania substancji jako leku na receptę (toksyna botulinowa) lub wyrobu medycznego z zastrzeżeniem w instrukcji (kwas hialuronowy) wyklucza legalność ich samodzielnego stosowania przez kosmetologów. Orzecznictwo i poglądy doktryny potwierdzają, że naruszenie tych regulacji niesie za sobą realne ryzyko odpowiedzialności karnej i cywilnej, o czym traktować będzie kolejny rozdział niniejszego opracowania.

Orzecznictwo sądowe – odpowiedzialność w praktyce (*Case Studies*)

Brak interwencji ustawodawcy w zakresie wyraźnego rozgraniczenia procedur medycznych i kosmetologicznych powoduje, że ciężar wyznaczania granic kompetencyjnych oraz standardów bezpieczeństwa został de facto przeniesiony na sądy powszechne oraz Sąd Najwyższy. Analiza judykatury z ostatniej dekady pozwala wyodrębnić kilka wyraźnych nurtów orzeczniczych, które kształtują zasady odpowiedzialności cywilnej, karnej oraz dyscyplinarnej w branży beauty.

Reżim cywilnoprawny – równanie standardów i bezwzględność wymogu staranności

W sprawach o błędy w sztuce kosmetologicznej sądy cywilne najczęściej opierają odpowiedzialność na reżimie deliktowym (art. 415 k.c.), nierzadko w zbiegu z odpowiedzialnością zwierzchnika za podwładnego (art. 430 k.c.). Fundamentalną tezę, która ukształtowała linię orzeczniczą w tym zakresie, wyraził Sąd Apelacyjny w Krakowie (wyrok z dnia 16 października 2014 r., sygn. akt I ACa 946/14). Sąd ten arbitralnie przesądził, że jeżeli podmiot niemedyczny podejmuje się wykonywania czynności ingerujących w integralność ciała (z którymi wiąże się ryzyko uszczerbku na zdrowiu), musi dochować takich samych standardów bezpieczeństwa i staranności, jakie obowiązują w profesjonalnej opiece medycznej. Orzecznictwo odrzuca zatem próbę „taryfy ulgowej" dla gabinetów kosmetycznych.

W konsekwencji zrównania standardów, sądy piętnują braki proceduralne u osób niebędących lekarzami. W wyroku Sądu Rejonowego w Toruniu (z dnia 25 czerwca 2018 r., sygn. akt I C 600/15), dotyczącym powikłań po iniekcji kwasu hialuronowego, sąd wprost orzekł, że zabieg ten ma charakter medyczny, a ukończone przez wykonawcę kursy nie nadają mu uprawnień lekarskich. Co więcej, sąd uwypuklił, że brak prowadzenia dokumentacji medycznej przez kosmetologa uniemożliwił identyfikację użytego preparatu, co zablokowało możliwość skutecznego leczenia powikłań. Brak dokumentacji i świadomej zgody w gabinetach kosmetycznych sądy traktują jako rażące niedbalstwo, skutkujące automatycznym przyjęciem winy w reżimie deliktowym.

Sądy cywilne regorystycznie oceniają również samowolne stosowanie preparatów niezgodnie z ich przeznaczeniem. W wyroku Sądu Okręgowego w Poznaniu (z dnia 15 stycznia 2021 r., sygn. akt XII C 45/18), orzekającym o solidarnej odpowiedzialności kosmetologa oraz właściciela hurtowni kosmetycznej za powikłania po mezoterapii igłowej, kluczowym argumentem było użycie przez wykonawcę kosmetyku, zamiast certyfikowanego wyrobu medycznego do iniekcji. Sąd uznał to za rażące naruszenie zasad bezpieczeństwa, skutkujące bezpośrednią odpowiedzialność odszkodowawczą.

Jednocześnie judykatura podkreśla, że nie każda niepożądana reakcja organizmu rodzi odpowiedzialność kontraktową lub deliktową. Jeżeli zabieg (nawet inwazyjny, jak korekta powiek plazmą) został wykonany prawidłowo technicznie, a pacjent został w pełni poinformowany o ryzyku i normalnych następstwach pozabiegowych (np. obrzęk, strupy), powództwa są oddalane w oparciu o instytucję wkalkulowanego

ryzyka i świadomej zgody (tak m.in. Sąd Rejonowy dla Warszawy-Śródmieścia w wyroku z dnia 9 maja 2024 r., sygn. akt VI C 515/20).

Odpowiedzialność karna – paradoks luki prawnej i problem związku przyczynowego

O ile sądy cywilne przypisują odpowiedzialność kosmetologom za przekroczenie kompetencji, o tyle na gruncie prawa karnego sytuacja jest znacznie bardziej skomplikowana. Zderzenie wymogów procesu karnego z brakiem regulacji ustawowych zawodu kosmetologa prowadzi niekiedy do orzeczeń obnażających słabość systemu prawnego.

Najbardziej jaskrawym tego przykładem jest wyrok Sądu Okręgowego w Gliwicach (z dnia 6 listopada 2019 r., sygn. akt VI Ka 581/19). W sprawie o nieumyślne spowodowanie uszczerbku na zdrowiu (art. 157 § 3 k.k.) na skutek infekcji i ropnia po podaniu kwasu hialuronowego przez kosmetyczkę, sąd utrzymał w mocy wyrok uniewinniający. Argumentacja sądu odwoławczego opierała się na dwóch filarach. Po pierwsze, ze względu na upływ czasu (infekcja rozwinęła się po 13 dniach), nie udało się ponad wszelką wątpliwość udowodnić adekwatnego związku przyczynowego między zaniechaniem kosmetyczki (brakiem antyseptyki i zaleceń pozabiegowych) a samym zakażeniem. Po drugie – co z punktu widzenia niniejszego artykułu istotne – sąd wprost wskazał, że w polskim prawie nie istnieją przepisy zakazujące osobom bez wykształcenia medycznego przerywania ciągłości skóry i wstrzykiwania kwasu hialuronowego. Orzeczenie to stanowi de facto sądowy manifest o istnieniu niebezpiecznej luki legislacyjnej, która w procesie karnym (chronionym zasadą nullum crimen sine lege) działa na korzyść oskarżonych niemedyków.

Wyjątkiem od tej reguły są sytuacje, w których bezprawność działania kosmetologa wynika z naruszenia innych ustaw, np. Prawa farmaceutycznego czy przepisów o wyrobach medycznych. Skazaniem zakończyła się sprawa kosmetyczek z Piły i Poznania, gdzie powikłania (martwica) były wynikiem wstrzyknięcia nielegalnego preparatu z Azji, nieposiadającego certyfikatu CE ani polskojęzycznej ulotki. W tym przypadku organy ścigania z sukcesem udowodniły, że użycie produktu bez legalnej dokumentacji medycznej wyczerpuje znamiona rażącego niedbalstwa, prowadząc wprost do odpowiedzialności z art. 157 k.k.

Odpowiedzialność zawodowa lekarzy wkraczających w „szarą strefę"

Problem granic kompetencji w medycynie estetycznej nie dotyczy wyłącznie kosmetologów. Orzecznictwo Sądu Najwyższego dostarcza ważnych rozstrzygnięć dyscyplinujących również przedstawicieli zawodów medycznych, którzy przekraczają swoje ustawowe uprawnienia.

Przełomowe znaczenie ma w tym kontekście postanowienie Sądu Najwyższego z dnia 26 maja 2021 r. (sygn. akt I KK 23/21). Sprawa dotyczyła lekarza dentysty, który wykonał zabieg powiększenia piersi przy użyciu preparatu Aquafilling (wyrobu medycznego klasy III). Sąd Najwyższy utrzymał w mocy orzeczenie skazujące sądu lekarskiego, formułując kluczową dla całej branży beauty tezę: ukończenie certyfikowanych szkoleń z zakresu medycyny estetycznej nie rozszerza ustawowych ram prawa wykonywania zawodu. SN podkreślił, że certyfikaty z kursów są jedynie dowodem uczestnictwa, a nie dokumentem nadającym uprawnienia. Skoro art. 2 ust. 2 ustawy o zawodach lekarza i lekarza dentysty ogranicza kompetencje dentysty do obrębu twarzoczaszki, wykonanie zabiegu na piersiach było deliktem dyscyplinarnym i działaniem bez uprawnień, niezależnie od posiadanych umiejętności technicznych. Orzeczenie to – stosowane per analogiam – jest najsilniejszym argumentem doktrynalnym obalającym mit, jakoby absolwenci kosmetologii mogli na podstawie certyfikatów z weekendowych kursów nabywać prawo do wykonywania procedur stricte medycznych.

Co więcej, Sąd Najwyższy w wyroku z dnia 10 grudnia 2020 r. (sygn. akt I KK 134/20) wskazał, że odpowiedzialność deontologiczna lekarza rozciąga się także na sferę jego aktywności poza gabinetem. Lekarz pełniący funkcję "dyrektora medycznego" w ośrodku szkolącym kosmetologów może ponosić odpowiedzialność dyscyplinarną, jeśli ośrodek ten publikuje nieprawdziwe informacje (np. sugerujące, że po kursie kosmetolodzy uzyskują uprawnienia medyczne). Sąd Najwyższy udowodnił tym samym, że legitymizowanie "szarej strefy" przez osoby z prawem wykonywania zawodu lekarza spotyka się z nieobojętną oceną samorządu i sądownictwa dyscyplinarnego.

Podsumowując analizę orzecznictwa, należy stwierdzić, że sądy powszechne i Sąd Najwyższy starają się tamować negatywne skutki braku regulacji zawodu kosmetologa poprzez rygorystyczne stosowanie przepisów ogólnych Kodeksu cywilnego oraz ustaw o produktach leczniczych i wyrobach medycznych. Niemniej jednak, z perspektywy prawa karnego, judykatura wyraźnie sygnalizuje granicę swoich możliwości interpretacyjnych, wzywając tym samym ustawodawcę do pilnej interwencji.

Nowy wymiar problemu – paraliż administracyjno-podatkowy

Problem zacierania się granic między medycyną a kosmetologią, dotychczas rozpatrywany głównie na płaszczyznach odpowiedzialności cywilnej, karnej oraz ochrony zdrowia publicznego, zyskał w 2024 roku zupełnie nowy, niespodziewany wymiar. Brak ustawowych uregulowań zawodu kosmetologa doprowadził do bezprecedensowego paraliżu organów administracji państwowej, ze szczególnym uwzględnieniem administracji skarbowej. Zjawisko to ukazuje, że luka prawna w branży beauty przestała być wyłącznie problemem bezpieczeństwa pacjenta, a stała się problemem ustrojowym, rzutującym na finanse państwa i funkcjonowanie aparatu urzędniczego.

Geneza kryzysu – obniżona stawka VAT na usługi kosmetyczne (2024 r.)

Zarzewiem obecnego kryzysu administracyjno-podatkowego stało się wejście w życie rozporządzenia Ministra Finansów z dnia 14 marca 2024 r. zmieniającego rozporządzenie w sprawie obniżonych stawek podatku od towarów i usług (Dz. U. z 2024 r. poz. 387). Akt ten, z założenia mający stanowić ulgę dla branży kosmetycznej, wprowadził preferencyjną stawkę VAT w wysokości 8% dla usług objętych m.in. grupowaniami PKWiU 96.02.13.0 („Usługi kosmetyczne, manicure i pedicure") oraz 96.02.19.0 („Pozostałe usługi kosmetyczne").

Jak wynika z uzasadnienia projektu tego rozporządzenia, intencją prawodawcy było objęcie preferencyjną stawką wyłącznie tych świadczeń, które nie wymagają posiadania specjalistycznej wiedzy lekarskiej oraz jednocześnie nie są zabiegami z kategorii inwazyjnych, opieki zdrowotnej czy chirurgii plastycznej. Ustawodawca założył zatem, że istnieje wyraźna, dająca się zdefiniować granica między nieinwazyjną kosmetologią (uprawnioną do stawki 8%) a inwazyjną medycyną estetyczną (opodatkowaną stawką podstawową 23%, chyba że zachodzą przesłanki zwolnienia z VAT dla usług medycznych o charakterze terapeutycznym).

Wprowadzenie tej regulacji wywołało lawinę wniosków o wydanie Wiążących Informacji Stawkowych (WIS) kierowanych do Dyrektora Krajowej Informacji Skarbowej (KIS). Przedsiębiorcy z branży beauty, pragnąc zabezpieczyć się przed ryzykiem karnoskarbowym, zaczęli masowo pytać o możliwość zastosowania stawki 8% VAT do szerokiego spektrum zabiegów z pogranicza medycyny i kosmetologii (m.in. lipolizy iniekcyjnej, zabiegów z użyciem stymulatorów tkankowych, nici liftingujących, iniekcji kwasu hialuronowego czy zaawansowanej laseroterapii).

Pismo Dyrektora KIS z grudnia 2024 r.

Zmasowany napływ wniosków o wydanie WIS uwidocznił fundamentalną słabość polskiego systemu prawnego – całkowity brak definicji legalnych i rozgraniczenia kompetencji w analizowanym obszarze. Skala problemu okazała się na tyle duża, że organy podatkowe de facto skapitulowały przed zadaniem klasyfikacji tych usług.

Dowodem na ten stan rzeczy jest oficjalne wystąpienie Dyrektora Krajowej Informacji Skarbowej do Ministerstwa Zdrowia z dnia 4 grudnia 2024 r. (znak: 0110-KSI2-2.509.19.2024.1.PS) z prośbą o zajęcie stanowiska w sprawie usług z sektora „beauty". W piśmie tym Dyrektor KIS wprost przyznaje się do braku kompetencji organów podatkowych do oceny charakteru inwazyjności poszczególnych procedur oraz ustalenia wymogów kwalifikacyjnych niezbędnych do ich wykonania.

W treści pisma Dyrektor KIS dokonuje szczegółowej analizy popularnych zabiegów (takich jak lipoliza iniekcyjna podbródka, podawanie stymulatorów tkankowych, zakładanie nici liftingujących czy wolumetria kwasem hialuronowym), wskazując na ich inwazyjny charakter (przerwanie ciągłości naskórka, iniekcje śródskórne i podskórne, konieczność stosowania wyrobów medycznych klasy III, wywiadu i wykluczania przeciwwskazań). Organ podatkowy wprost konstatuje: "*Ustawodawca krajowy nie określił również, które zabiegi mogą być wykonywane przez kosmetologów i kosmetyczki, a które zarezerwowane są tylko dla lekarzy medycyny estetycznej*".

Szczególnie uderzające jest stwierdzenie Dyrektora KIS, w którym organ ten – posiłkując się poglądami doktryny prawniczej (m.in. S. Wolframa) oraz klasyfikacjami Głównego Urzędu Statystycznego (GUS) – dochodzi do wniosku, że kosmetolog to podmiot o węższym zakresie wiedzy i uprawnień niż lekarz, nieposiadający specjalistycznej wiedzy medycznej niezbędnej do przeprowadzania zabiegów znacząco ingerujących w organizm (inwazyjnych).

Dyrektor KIS w swoim piśmie wyraża daleko idące obawy: "Ewentualna błędna identyfikacja zabiegu jako procedury niemedycznej lub nieinwazyjnej bądź też przyjęcie niewłaściwego oświadczenia podatnika, że wykonanie zabiegu nie wymaga posiadania specjalistycznej wiedzy medycznej, może spowodować, że Organ nieświadomie przyczyni się do wspierania działań niepożądanych – wykonywania zabiegów przez podmioty nieuprawnione, niemające wymaganego wykształcenia, kompetencji".

Konsekwencje prawne i fiskalne dla państwa

Sytuacja ta prowadzi do klinczu. Z jednej strony, ustawa o VAT i rozporządzenie wykonawcze uzależniają zastosowanie stawki obniżonej od "braku inwazyjności" i "braku wymogu specjalistycznej wiedzy medycznej". Z drugiej strony, żaden powszechnie obowiązujący akt prawny nie definiuje tych pojęć w kontekście kosmetologii, ani nie określa, które konkretnie zabiegi spełniają te kryteria.

Stanowisko Głównego Urzędu Statystycznego, przywoływane przez KIS (opinie z lutego i października 2024 r.), jedynie potwierdza ten impas. GUS stwierdza, że o klasyfikacji usług do odpowiedniego grupowania PKWiU decyduje fakt, "czy wykonywane zabiegi wymagają wiedzy medycznej w zakresie zabiegów estetycznych związanych ze specjalizacją lekarzy lub osób uprawnionych, którzy wykonują takie zabiegi". Zatem GUS, podobnie jak organy podatkowe, odsyła do nieistniejących regulacji określających te uprawnienia.

Paraliż ten ma dwa zasadnicze wymiary:

Jak zauważa Dyrektor KIS, niejasności te mogą znacząco wpłynąć na opodatkowanie, prowadzić do nadużyć (masowego, nieuzasadnionego stosowania stawki 8% VAT dla zabiegów de facto medycznych wykonywanych przez niemedyków) i w konsekwencji narazić budżet państwa na uszczuplenia.

KIS domaga się od Ministerstwa Zdrowia lub ustawodawcy podjęcia pilnych działań legislacyjnych. Organ podatkowy trafnie diagnozuje, że unormowanie pojęcia zabiegu inwazyjnego i rozgraniczenie zawodów w branży beauty jest niezbędne nie tylko dla celów podatkowych, ale przede wszystkim "dla ogólnego funkcjonowania systemu opieki zdrowotnej" oraz "zapewnienia bezpieczeństwa osób decydujących się na przeprowadzenie wskazanych zabiegów".

Zjawisko to można określić mianem swoistego paradoksu prawa podatkowego. Organy skarbowe, nie mogąc oprzeć się na klarownych regulacjach z zakresu prawa medycznego, zmuszone są do dokonywania interpretacji na pograniczu medycyny i kosmetologii, ryzykując legalizację niebezpiecznych praktyk poprzez nadawanie im statusu "usług kosmetycznych" za pomocą decyzji o stawce VAT. Pismo Dyrektora KIS z grudnia 2024 r. stanowi zatem dowód na to, że tolerowanie luki prawnej w obszarze medycyny estetycznej jest już dłużej niemożliwe z perspektywy spójności całego systemu prawnego państwa.

Podsumowanie i wnioski *de lege ferenda* (postulaty zmian w prawie)

Przeprowadzona analiza dogmatycznoprawna, orzecznicza oraz praktyki organów administracji państwowej prowadzi do jednoznacznej konkluzji: polski system prawny w obszarze medycyny estetycznej i kosmetologii znajduje się w stanie głębokiego kryzysu normatywnego. Brak kompleksowej ustawy regulującej zawód kosmetologa, połączony z niedookreślonością pojęcia "świadczenia zdrowotnego" w kontekście zabiegów o czysto estetycznym celu, stworzył niebezpieczną "szarą strefę". Strefa ta, z jednej strony, naraża pacjentów (konsumentów) na utratę zdrowia w wyniku inwazyjnych procedur przeprowadzanych przez osoby bez wykształcenia medycznego, z drugiej zaś – generuje chaos orzeczniczy i paraliżuje aparat państwowy, czego najnowszym dowodem jest apel organów administracji skarbowej o pilną interwencję ustawodawczą.

Obecny stan prawny, opierający się na wyłączności lekarzy do udzielania świadczeń zdrowotnych (art. 2 ust. 1 u.z.l.) oraz rygorystycznych przepisach Prawa farmaceutycznego i Ustawy o wyrobach medycznych, stanowi twardą, lecz często ignorowaną w praktyce barierę kompetencyjną. Orzecznictwo sądów cywilnych i lekarskich, rygorystycznie zrównujące standardy bezpieczeństwa dla wszystkich podmiotów ingerujących w integralność ciała (wyrok SA w Krakowie I ACa 946/14) oraz kwestionujące moc certyfikatów z kursów jako źródła uprawnień (postanowienie SN I KK 23/21), stara się tamować negatywne skutki tej luki. Jednakże powściągliwość sądów karnych, wprost wskazujących na brak ustawowych zakazów wykonywania określonych zabiegów przez niemedyków (wyrok SO w Gliwicach VI Ka 581/19), obnaża słabość systemu opierającego się wyłącznie na wykładni przepisów ogólnych.

Sytuacja ta wymaga natychmiastowej reakcji ustawodawcy. Wobec powyższego, formułuję następujące postulaty de lege ferenda, mające na celu uporządkowanie branży beauty i zagwarantowanie bezpieczeństwa pacjentom:

1. Ustawowe zdefiniowanie medycyny estetycznej

Kluczowym postulatem jest wprowadzenie do polskiego porządku prawnego legalnej definicji "medycyny estetycznej" (lub pojęcia równoważnego), powiązanej z precyzyjnym określeniem, że procedury o wysokim stopniu inwazyjności stanowią wyłączną domenę lekarzy (i lekarzy dentystów w ich zakresie).

2. Uregulowanie zawodu kosmetologa – ustawa kompetencyjna

Równolegle z dookreśleniem kompetencji lekarzy, niezbędne jest uchwalenie ustawy o zawodzie kosmetologa. Akt ten powinien pozytywnie zdefiniować ten

zawód (jako zawód zaufania publicznego w sferze profilaktyki zdrowotnej i estetyki), określić wymogi edukacyjne oraz, co najważniejsze, stworzyć zamknięty katalog (lub jasne kryteria) uprawnień zawodowych.

Ustawa ta powinna wyraźnie wskazywać, że kosmetolog jest specjalistą od nieinwazyjnej i minimalnie inwazyjnej pielęgnacji skóry, profilaktyki procesów starzenia i wspomagania leczenia dermatologicznego. Katalog dopuszczalnych procedur powinien obejmować m.in. peelingi chemiczne (do ściśle określonego stężenia i pH), obsługę urządzeń oraz zabiegi niewymagające znieczulenia i nienaruszające ciągłości skóry właściwej w sposób stwarzający ryzyko poważnych powikłań.

3. Kategoryzacja i certyfikacja urządzeń oraz preparatów

Ustawodawca powinien doprecyzować zasady klasyfikacji urządzeń wykorzystywanych w branży *beauty*. Konieczne jest stworzenie mechanizmów weryfikacji, czy dane urządzenie lub preparat (nawet jeśli nie jest wyrobem medycznym w rozumieniu MDR) może być bezpiecznie obsługiwane przez osobę bez wykształcenia medycznego. Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych powinien dysponować szerszymi kompetencjami kontrolnymi w odniesieniu do produktów z tzw. pogranicza.

4. Wzmocnienie nadzoru i zaostrzenie sankcji

Obecne mechanizmy kontroli (Państwowa Inspekcja Sanitarna, nadzór farmaceutyczny) są rozproszone i często nieefektywne w zwalczaniu "szarej strefy". Postuluje się powołanie wyspecjalizowanych zespołów kontrolnych lub rozszerzenie kompetencji istniejących organów o możliwość szybkiej interwencji w gabinetach kosmetycznych podejrzewanych o wykonywanie nielegalnych procedur medycznych.

Ponadto, należy rozważyć zaostrzenie sankcji karnych i administracyjnych za:

- Wykonywanie zabiegów inwazyjnych bez uprawnień lekarskich (zmiana lub doprecyzowanie art. 58 u.z.l., ewentualnie wprowadzenie nowego typu czynu zabronionego).
- Reklamę wprowadzającą konsumentów w błąd co do charakteru usług i kwalifikacji personelu (np. zakaz używania terminów "medycyna estetyczna", "klinika", "pacjent" przez podmioty niebędące podmiotami leczniczymi i niezatrudniające lekarzy).

Podsumowanie

Tolerowanie obecnego stanu prawnego, w którym granice między medycyną a kosmetologią wyznaczane są *post factum* przez sądy orzekające o odszkodowaniach za oszpecenie lub utratę zdrowia pacjentów, a organy podatkowe toną w gąszczu nierozwiązywalnych dylematów klasyfikacyjnych, jest niedopuszczalne w demokratycznym państwie prawa. Apel Dyrektora KIS z grudnia 2024 r. powinien stanowić ostateczny sygnał alarmowy dla ustawodawcy. Zapewnienie bezpieczeństwa zdrowotnego obywateli wymaga podjęcia racjonalnych prac legislacyjnych, opartych na prymacie wiedzy medycznej w odniesieniu do procedur inwazyjnych oraz jasnym zdefiniowaniu profesji kosmetologa. Każdy kolejny dzień zwłoki to zgoda na funkcjonowanie niebezpiecznej "szarej strefy", której ofiarami są pacjenci.

Bibliografia

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.U. UE. L. 2017.117.1).

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz. U. z 2023 r. poz. 1516 z późn. zm.).

Ustawa z dnia 6 września 2001 r. Prawo farmaceutyczne (t.j. Dz. U. z 2022 r. poz. 2301 z późn. zm.).

Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U. z 2023 r. poz. 991 z późn. zm.).

Ustawa z dnia 7 kwietnia 2022 r. o wyrobach medycznych (Dz. U. z 2022 r. poz. 974).

Orzecznictwo i inne dokumenty urzędowe

Pismo Dyrektora Krajowej Informacji Skarbowej z dnia 30 czerwca 2021 r., znak: 0112-KDIL3.4012.99.2021.2.AK.

Pismo Dyrektora Krajowej Informacji Skarbowej z dnia 4 grudnia 2024 r., znak: 0110-KSI2-2.509.19.2024.1.PS.

Postanowienie Sądu Najwyższego z dnia 26 maja 2021 r., sygn. akt I KK 23/21.

Wyrok Krajowej Izby Odwoławczej z dnia 16 kwietnia 2019 r., sygn. akt KIO 573/19.

Wyrok Naczelnego Sądu Administracyjnego z dnia 4 października 2016 r., sygn. akt I FSK

878/14.

Wyrok Sądu Apelacyjnego w Krakowie z dnia 16 października 2014 r., sygn. akt I ACa 946/14.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 27 listopada 2018 r., sygn. akt II AKa 228/18.

Wyrok Sądu Najwyższego z dnia 10 grudnia 2020 r., sygn. akt I KK 134/20.

Wyrok Sądu Okręgowego w Gliwicach z dnia 6 listopada 2019 r., sygn. akt VI Ka 581/19.

Wyrok Sądu Okręgowego w Poznaniu z dnia 15 stycznia 2021 r., sygn. akt XII C 45/18.

Wyrok Sądu Rejonowego dla Warszawy-Śródmieścia z dnia 9 maja 2024 r., sygn. akt VI C 515/20.

Wyrok Sądu Rejonowego w Toruniu z dnia 25 czerwca 2018 r., sygn. akt I C 600/15.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 30 maja 2016 r., sygn. akt VII SA/Wa 385/16.

Literatura

Kózka M.

2013 *Opinia Konsultanta Krajowego w dz. pielęgniarstwa w sprawie uprawnień pielęgniarki do wykonywania zabiegów z medycyny i dermatologii estetycznej, w tym iniekcji podskórnej z kwasu hialuronowego – wypełniaczy zmarszczek i bruzd*, Kraków.

Wolfram S.

2023 *Medycyna estetyczna i kosmetologia. Legalność zabiegów i zgoda pacjenta, umowa o zabieg*, Warszawa.

THE GRAY AREA OF AESTHETIC MEDICINE: BOUNDARIES OF COMPETENCE BETWEEN PHYSICIANS AND COSMETOLOGISTS IN THE LIGHT OF CASE LAW AND THE PRACTICE OF STATE ADMINISTRATION AUTHORITIES

Abstract: The article addresses the current issue of the blurring boundaries between aesthetic medicine and cosmetology in the Polish legal system. The lack of a statutory definition of the cosmetologist profession and a precise division into medical and cosmetic procedures has led to the emergence of a "gray area" that is dangerous to patients. The author conducts a dogmatic-legal and jurisprudential analysis (including judgments of the Supreme Court and common courts), demonstrating how the judiciary handles the assessment of civil and criminal liability of persons performing invasive procedures without appropriate medical qualifications. Special attention is given to the classification of hyaluronic acid and botulinum toxin in light of the EU Medical Device Regulation (MDR) and the Pharmaceutical Law. The research novelty of the article is the analysis of the impact of this legal loophole on the functioning of state authorities, illustrated by the latest practice of the Director of the National Revenue Information and Statistics Poland (2024) in the context of reduced VAT rates. The article concludes with de lege ferenda proposals postulating the urgent need for statutory regulation of professional qualifications in the beauty industry.

Keywords: aesthetic medicine, cosmetology, civil liability, medical malpractice, medical devices, MDR, healthcare service, VAT tax

Dynamiczny rozwój nowych technologii oraz zmieniające się uwarunkowania bezpieczeństwa międzynarodowego sprawiają, że współczesne państwo prawa staje wobec wyzwań o szczególnie złożonym charakterze. Niniejsza monografia podejmuje próbę wielowymiarowej analizy relacji zachodzących między postępem technologicznym, funkcjonowaniem systemów prawnych a ochroną fundamentalnych wartości demokratycznych. Zebrane opracowania tworzą spójną refleksję nad sposobami zapewnienia bezpieczeństwa państwa, ochrony infrastruktury krytycznej oraz poszanowania praw i godności jednostki w realiach postępującej transformacji cyfrowej.

ISBN 978-83-68410-79-2