Uniwersytet Mikołaja Kopernika w Toruniu

Dziedzina: nauki społeczne
Dyscyplina: nauki o bezpieczeństwie

Sylwia Osowska

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W WYBRANYCH JEDNOSTKACH SAMORZĄDU TERYTORIALNEGO W POLSCE

PERSONAL DATA SECURITY IN SELECTED LOCAL GOVERNMENT UNITS IN POLAND

Praca doktorska
wykonana pod kierunkiem naukowym promotora
dr hab. Arkadiusz Czwołek, prof. UMK

Toruń 2024

SPIS TREŚCI

SUMMARY

This dissertation has thoroughly examined the current state of personal data protection in selected local government units in Poland. The analysis, both theoretical and practical, focused on the scope of public services provided to determine whether Polish local governments can effectively protect sensitive information, namely, citizens' personal data. The author sought to answer the question of how local government institutions protect the personal data they hold, what measures they take to ensure its secure storage, and whether these measures are sufficient. Considering the current challenges and opportunities arising from the digital transformation of public services, the study aimed to identify potential gaps and shortcomings in the current public administration system to seek ways to eliminate them. This corrective goal guided the author of this dissertation. To achieve it, information was gathered through a multifaceted analysis of the research problem. The analysis included various perspectives – broadly defined – highlighting the interdisciplinary nature of personal data protection issues in local government units.

The dissertation consists of seven chapters. The first chapter presents a spectrum of issues from various fields that converge on personal data protection. The aim of this approach was to demonstrate that the security of personal data is an issue considered within the security sciences but also within many other scientific disciplines, indicating the complexity and multifaceted nature of the topic. Thus, the stereotype of discussing data protection solely from an IT perspective was broken. By presenting the perspectives of security sciences, as well as political science, administration and law, sociology, psychology, ethics, economics, and communication sciences, we can see that personal data security is one of the most important issues for information societies today. It is a significant topic, and with the advancing digitization, it is becoming part of nearly every aspect of modern human life. Therefore, when we talk about the real protection of personal data, we address a range of issues from private life to administration, legal, ethical, economic, cultural issues, and many others. We are also aware that with further digital development, this complexity will increase and become even more complicated.

The second chapter focuses on the legal dimension of personal data protection in Poland and beyond. It presents the legal regulations for personal data protection, both national and those mandated by the European Union for Poland. In this chapter, we define personal data, the General Data Protection Regulation (EU) 2016/679 of

27 April 2016 (GDPR), discuss the supervisory and control bodies resulting from these regulations, legal responsibility, and compare the EU personal data protection system with those of other countries.

The third chapter discusses the organization and structure of local government bodies in Poland. This discussion serves as an introduction to the fourth chapter – the key theoretical part of the work – which addresses the responsibilities of local government bodies resulting from GDPR, imposed by the state as part of public administration tasks. This topic is also presented in the context of public services in the fifth chapter of the dissertation.

In the fourth chapter, the role of local government bodies in personal data protection is discussed, particularly their cooperation with other entities and the conduct of training to enhance the qualifications of administrative personnel.

The separate fifth chapter is dedicated to local public services, such as educational, health, infrastructure, environmental, social, cultural, and security services. Their connection to personal data protection is undeniable, as the principles of legality, fairness, transparency, data minimization, purpose limitation, storage limitation, integrity, and confidentiality should apply in the provision of public services.

The contribution to the understanding of personal data protection issues in Poland was made through conducted research. The methodology of this research is discussed in the sixth chapter. The main research problem, which the empirical part of this work is based on, concerned the impact of local government bodies' actions on personal data protection in the context of providing public services, as well as the factors influencing the effectiveness of these actions. During the detailing of the research problem, the following hypotheses were formulated: (1) do local government organizations that invest in training and educating personnel on personal data protection achieve a higher level of compliance with regulations and effectiveness in data management? (2) does coordinated action and cooperation between local government bodies contribute to more effective personal data protection? (3) does transparent communication with citizens about the processing of their personal data increase trust in local government bodies? (4) do local government organizations that invest in the development and implementation of effective data security systems reduce the risk of personal data protection breaches? (5) to what extent do local government organizations that strictly adhere to personal data protection regulations avoid serious legal consequences related to violations of these regulations?

The collected material allowed for the verification of the hypotheses posed in the dissertation, and the conclusions from the research and theoretical analysis were formulated in the final part of the work.

WPROWADZENIE

W XXI wieku społeczeństwa stały się w dużej mierze społeczeństwami informacyjnymi. Jest to trend ogólnoświatowy wyznaczany przez państwa najbardziej rozwinięte gospodarczo i zaawansowane technologicznie. Podobnie jak wiele zmian spowodowanych rozwojem cywilizacyjnym, otwierających przed ludzkością nowe możliwości, ale także generujących potencjalne zagrożenia, rozwój i zastosowanie techniki cyfrowej wymaga dbałej uwagi ze strony państwa. Wyzwaniem stojącym dzisiaj przed administracją publiczną jest ochrona danych osobowych, które mogą zostać niezgodnie z prawem wykorzystane przez różne podmioty. W Polsce prawa ochrony danych osobowych realizują jednostki samorządu terytorialnego.

Przedmiotem niniejszej pracy jest zagadnienie ochrony danych osobowych z perspektywy funkcjonowania wybranych jednostek samorządu terytorialnego w Polsce. Podstawowym dokumentem określającym zakres ochrony danych osobowych jest *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także uchylenia dyrektywy 95/46/WE – ogólne rozporządzenie o ochronie danych*[1] (zwane w skrócie „RODO"), a obszarem badawczym jednostki samorządu terytorialnego w Polsce.

Wiele działań i usług świadczonych przez organy samorządu terytorialnego wymaga przetwarzania danych osobowych. Niezależnie od tego, czy jest to zezwolenie na budowę lub działalność gospodarczą, na organizację imprez publicznych[2] czy też inne, w zakres usług administracyjnych wchodzi przetwarzanie i zarządzanie indywidualnymi danymi. Samorządy zbierają i zarządzają danymi swoich mieszkańców w szeregu wykazach i rejestrach, takich jak: rejestr ludności, dane podatkowe, informacje o świadczeniach usług społecznych i wiele innych. Ochrona takich wrażliwych

[1] Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016 roku.

[2] Zob. *Zezwolenie na przeprowadzenie imprezy masowej*, nhttps://www.biznes.gov.pl/pl/opisy-procedur/-/proc/263 (dostęp: 02.10.2023).

informacji jest kluczowa dla zapewnienia prawa do prywatności obywateli, ale również dla ich bezpieczeństwa, ponieważ dane osobowe mogą stać się przedmiotem przestępstwa. Zapewnienie, że informacje na temat obywateli są przechowywane i przetwarzane w sposób bezpieczny i zgodny z przepisami, staje się dzisiaj niezwykle istotne i wymusza na organach administracji publicznej ścisłą ochronę danych osobowych. W ramach korzystania z technologii informatycznych, realizując skuteczną politykę ochrony danych, samorządy terytorialne zobowiązane są do zadbania o odpowiednie zabezpieczenia cyfrowe. Odrębną kwestią jest płaszczyzna działań edukacyjnych oraz informowania lokalnej społeczności o wadze ochrony danych osobowych, ponieważ organy samorządu terytorialnego są przekaźnikami danych osobowych na poziomie lokalnym, współpracując z różnymi instytucjami (służba zdrowia, placówki edukacyjne, służby socjalne).

Niniejsza publikacja koncentruje się na analizie roli i odpowiedzialności organów samorządu terytorialnego w ochronie danych osobowych w kontekście usług publicznych. Nieodłącznym elementem współczesnych usług publicznych jest przetwarzanie danych osobowych, które pozwala na dostosowanie oferowanych usług do indywidualnych potrzeb obywateli. Jednakże w obliczu stale rosnącego ryzyka naruszeń prywatności i bezpieczeństwa danych, konieczne jest dokładne zrozumienie, jakie rodzaje obowiązków i odpowiedzialności spoczywają na samorządach w zakresie ochrony tych informacji.

Pomimo stałego zwiększania się ryzyka utraty danych w wyniku braku odpowiednich zabezpieczeń, a także istotnej w tym względzie roli samorządów, niewiele jest dogłębnych badań oceniających stan wdrożenia polityki ochrony danych osobowych (RODO) w Polsce przez samorządy terytorialne. Niniejsza praca stara się w pewnym stopniu uzupełnić tę lukę.

Stan badań dotyczących ochrony danych osobowych w Polsce wskazuje na kilka istotnych wyzwań, zarówno w zakresie implementacji przepisów, jak i świadomości społecznej. Warto w tym względzie przywołać raport Fundacji Wiedza To Bezpieczeństwo, który wskazuje, że Polacy co prawda deklarują świadomość w zakresie zagrożeń dotyczących naruszeń danych osobowych, jednak nie mają pełnej wiedzy, jak się przed nimi chronić. Aż 90% aktywnych zawodowo osób deklaruje potrzebę szkoleń w zakresie ochrony danych. Jednocześnie 33% ankietowanych doświadczyło naruszenia prywatności, ale jedynie 10% zgłosiło incydent odpowiednim

instytucjom.[3]

Wyniki badania podkreślają potrzebę edukacji oraz zwiększenia świadomości prawnej w tej dziedzinie. Tym samym podjęcie badań w tym zakresie jest jak najbardziej zasadne.

Warto również odnieść się do wniosków, Prezesa Urzędu Ochrony Danych Osobowych, zawartych w sprawozdaniu z działalności w 2022 roku. Podkreśla on w nim zwiększającą się liczbę incydentów naruszenia ochrony danych osobowych oraz namnażanie się skarg od obywateli. W badaniach stwierdzono, że wiele instytucji publicznych i prywatnych nie przestrzegało w pełni przepisów RODO, co prowadziło do wzmożonych interwencji obywateli. Ważnym wnioskiem, płynącym z przedmiotowego raportu, jest konieczność kontynuowania działań edukacyjnych w zakresie ochrony danych.[4] Stanowi to kolejny asumpt do analizy w pracy doktorskiej skuteczności wdrażania przepisów RODO.

Należy podkreślić również, że Najwyższa Izba Kontroli przeprowadzając z końcem 2023 roku kontrolę danych osobowych przechowywanych w jednostkach samorządowych w formie elektronicznej stwierdziła liczne nieprawidłowości w zakresie zabezpieczeń systemów informatycznych i przestrzegania przepisów RODO. Głównymi obszarami podlegającymi sprawdzaniu były: efektywność postępowania kontrolnego, współpraca z interesariuszami w trakcie czynności kontrolnych, oczekiwanie działań naprawczych, już w trakcie czynności kontrolnych, oraz nastawienie kontroli na możliwie szybką zmianę porządku publicznego w kontrolowanym obszarze. Przeprowadzona kontrola wykazała, iż wiele jednostek nie wdrożyło odpowiednich procedur ochrony danych, co stwarzało ryzyko niekontrolowanego udostępniania danych. NIK zalecił poprawę monitorowania, szkolenia pracowników i wprowadzenie lepszych mechanizmów kontroli dostępu do danych. [5] Tym samym ujęte rekomendacje stanowią kolejny przyczynek do analizy skuteczności wdrażania RODO w administracji publicznej.

---

[3] Fundacja Wiedza to bezpieczeństwo, *Co wiemy o ochronie danych osobowych Raport 2017*, https://wtb.org.pl/files/raport_wtb_2017.pdf [dostęp: 11.03.2024].

[4] Urząd Ochrony danych Osobowych, *Sprawozdanie z działalności Prezesa UODO w roku 2022*, https://uodo.gov.pl/pl/487/2279 [dostęp: 12.03.2024].

[5] Najwyższa Izba Kontroli, *W samorządach ochrona danych osobowych bez ochrony W samorządach ochrona danych osobowych bez ochrony*, https://www.nik.gov.pl/aktualnosci/bezpieczenstwo-ochrony-danych-osobowych-w-jst.html [dostęp: 16.03.2024].

Przedmiot badań

Analiza praktyk ochrony danych osobowych w ramach samorządowych usługach publicznych powinna uwzględnić ich praktyczną realizację. Przykładowo, zgodnie z art. 6 RODO, przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy jest to konieczne do wykonania umowy, wypełnienia obowiązku prawnego, ochrony istotnych interesów, wykonywania zadań realizowanych w interesie publicznym, wykonywania zadań powierzonych administratorowi danych w ramach wykonywania władzy publicznej lub jeżeli osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych do jednego lub więcej określonych celów[6].

W praktyce samorządowej często dochodzi do przetwarzania danych w celu wypełnienia obowiązku prawnego (art. 6 ust. 1 lit. c RODO) lub wykonywania zadań realizowanych w interesie publicznym (art. 6 ust. 1 lit. e RODO). Oczywiście, to przetwarzanie musi przebiegać zgodne z zasadami przetwarzania danych osobowych określonych w art. 5 RODO[7].

Analiza praktyk ochrony danych osobowych w samorządowych usługach publicznych nie pozostawia wątpliwości, że przestrzeganie przepisów prawnych jest kluczowe dla zapewnienia praw obywateli do prywatności. Samorządy muszą również przetwarzać dane w celu świadczenia swoich usług. Znalezienie równowagi między tymi dwoma celami jest dużym wyzwaniem dla władz samorządowych.

Zgodnie z RODO, organy samorządowe jako administratorzy danych, mają obowiązek zabezpieczenia danych osobowych przed utratą, zniszczeniem, modyfikacją, nieuprawnionym dostępem lub przetwarzaniem. Istnieje wiele metod ochrony danych osobowych, które są stosowane w praktyce samorządowej. Poniżej przedstawione są wybrane z nich.

Zgodnie z art. 5 ust. 1 lit. c RODO, dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane. To oznacza, że samorządy powinny zbierać i przechowywać tylko te dane osobowe, które są niezbędne do świadczenia usług publicznych. Praktyka ta jest często określana jako „minimalizacja danych", o czym niejednokrotnie wspominano[8].

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679…
[7] Ibidem.
[8] Ibidem.

Pseudonimizacja, zgodnie z definicją zawartą w art. 4 ust. 5 RODO, polega na przetwarzaniu danych osobowych w taki sposób, że nie mogą one już być przypisane konkretnej osobie bez użycia dodatkowych informacji, które są przechowywane osobno i zabezpieczone. Pseudonimizacja może być używana do zabezpieczenia danych osobowych w sytuacji, gdy nie można zastosować całkowitej anonimizacji[9].

Artykuł 32 RODO zobowiązuje administratorów danych do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiadającego ryzyku. Może to obejmować kontrolę dostępu, szyfrowanie, systemy monitorowania, systemy backupu, procedury reagowania na incydenty, a także szkolenia dla personelu[10].

Artykuł 35 RODO wprowadza obowiązek przeprowadzania oceny skutków dla ochrony danych (DPIA) dla przetwarzania, które może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. DPIA powinna obejmować systematyczny opis przetwarzania danych, ocenę konieczności i proporcjonalności przetwarzania, ocenę ryzyk dla praw i wolności osób, które są tematem danych, oraz środki, które mają na celu zabezpieczenie danych i zminimalizować te ryzyka[11].

Jak widać, praktyki ochrony danych osobowych w samorządowych usługach publicznych, stanowiące w niniejszej pracy przedmiot badań, są złożone i wymagają uwzględnienia wielu aspektów technicznych, organizacyjnych i prawnych.

Cel badawczy

Celem pracy jest zbadanie, czy samorządy terytorialne w adekwatny sposób wypełniają swoje obowiązki w ramach polityki ochrony danych osobowych, czy są w stanie realizować wszystkie wyzwania, które stoją przed nimi w tym zakresie, a jeśli nie, to jakie zgłaszają postulaty, jakie strategie stosują obecnie w celu zapewnienia ochrony danych osobowych, a które z nich mogłyby polepszyć ochronę danych osobowych.

Badania przeprowadzone w ramach niniejszej pracy mają na celu sprawdzić na ile w praktyce możliwe jest pogodzenie kierunków wynikających z dylematu stojącego przed administracją w zakresie realizacji przepisów RODO, którym jest z jednej strony

[9] Ibidem.
[10] Ibidem.
[11] Ibidem.

rewolucja cyfrowa usług publicznych, a z drugiej prawo do prywatności danych. Celem jest nie tylko zidentyfikowanie obecnych praktyk i wyzwań, ale również wypracowanie rekomendacji, które mogą przyczynić się do lepszego zrozumienia i efektywniejszej ochrony danych osobowych w środowisku samorządowym.

Badaniom, prowadzonym na potrzeby niniejszej pracy, przyświecają następujące cele szczegółowe:

- Określenie roli organów samorządu terytorialnego w ochronie danych osobowych w kontekście usług publicznych–zrozumienie, jak organy samorządowe postrzegają swoją rolę w kontekście RODO oraz jakie obowiązki i działania podejmują w celu ochrony danych osobowych, co ma kluczowe znaczenie dla zapewnienia zgodności z przepisami i budowania zaufania obywateli;
- Zbadanie wpływu szkoleń i edukacji na kompetencje personelu organów samorządu terytorialnego w zakresie przetwarzania danych osobowych–analiza, w jaki sposób szkolenia i programy edukacyjne wpływają na wiedzę i umiejętności pracowników samorządowych w zakresie przetwarzania danych osobowych, co jest fundamentem skutecznej ochrony tych danych;
- Ocena skuteczności wdrażania systemów bezpieczeństwa danych przez organy samorządu terytorialnego– badanie, jakie systemy bezpieczeństwa są stosowane przez organy samorządowe oraz ocena ich efektywności w zapobieganiu naruszeniom danych osobowych;
- Analiza koordynacji działań pomiędzy różnymi organami samorządu terytorialnego w celu skutecznej ochrony danych–zrozumienie, jak organy samorządu współpracują między sobą oraz z innymi podmiotami w celu ochrony danych osobowych, co jest istotne dla stworzenia spójnego i efektywnego systemu ochrony;
- Badanie wpływu transparentnej komunikacji z obywatelami na zaufanie do organów samorządu terytorialnego w kontekście przetwarzania danych osobowych–ocena, jak przejrzystość procesów przetwarzania danych wpływa na postrzeganie organów samorządu przez obywateli i czy wpływa to na ich zaufanie do tych instytucji;
- Ocena zgodności działań organów samorządu terytorialnego z obowiązującymi przepisami dotyczącymi ochrony danych osobowych–analiza, czy i w jakim stopniu działania organów samorządu są zgodne z RODO i innymi przepisami

dotyczącymi ochrony danych osobowych, co ma fundamentalne znaczenie dla zapewnienia legalności przetwarzania danych i uniknięcia potencjalnych sankcji.

Stawiając sobie powyższe cele mamy nadzieję przyczynić się do wypracowania praktycznych rekomendacji, które mogą przyczynić się do zwiększenia skuteczności ochrony danych osobowych w tym sektorze.

Problem badawczy i hipotezy badawcze

W niniejszej pracy starano się zweryfikować poziom usług publicznych realizowany w zakresie ochrony danych osobowych na przestrzeni ostatnich sześciu lat – od czasu wprowadzania RODO w Polsce. Główny problem badań oscyluje wokół tematu: jaki wpływ mają działania organów samorządu terytorialnego na ochronę danych osobowych w kontekście świadczenia usług publicznych, a także jakie czynniki wpływają na skuteczność tych działań? Chcemy zwrócić uwagę na to, czy zadania stojące przed administracją publiczną w zakresie RODO nie wyzwalają sprzecznych kierunków działań jednostek samorządu terytorialnego, czy z jednej strony zwiększony proces digitalizacji danych, a z drugiej prawo do prywatności nie powoduje swoistego rozszczepienia? Weryfikujemy tezę, czy stopień zabezpieczeń w zakresie ochrony prawa do prywatności jest wystarczający oraz czy dane osobowe gromadzone przez jednostki samorządu terytorialnego są bezpieczne (w odpowiedni sposób zabezpieczone).

W procesie uszczegóławiania problemu badawczego zostały sformułowane następujące hipotezy:

- Hipoteza 1: Organizacje samorządu terytorialnego, które inwestują w szkolenia i edukację personelu z zakresu ochrony danych osobowych, osiągają wyższy poziom zgodności
  z przepisami i skuteczności w zarządzaniu danymi;
- Hipoteza 2: Skoordynowane działanie i współpraca pomiędzy organami samorządu terytorialnego przyczyniają się do skuteczniejszej ochrony danych osobowych;
- Hipoteza 3: Transparentna komunikacja z obywatelami na temat przetwarzania ich danych osobowych zwiększa zaufanie do organów samorządu terytorialnego;
- Hipoteza 4: Organizacje samorządu terytorialnego, które inwestują w rozwój i wdrażanie skutecznych systemów bezpieczeństwa danych, ograniczają ryzyko naruszenia ochrony danych osobowych;

- Hipoteza 5: Organizacje samorządu terytorialnego, które ścisłe przestrzegają przepisów dotyczących ochrony danych osobowych, unikają poważnych konsekwencji prawnych i reputacyjnych związanych z naruszeniem tych przepisów.

Metody badawcze

Z założenia niniejsza praca nie ma wyłącznie charakteru teoretycznego, ale również empiryczny. Na potrzeby realizacji celu badawczego przeprowadzono badania własne. Metodologia badań własnych opiera się na połączeniu technik jakościowych i ilościowych. Wykorzystana została między innymi analiza dokumentów, w tym aktów prawnych, dokumentacji wewnętrznej jednostek oraz naukowych publikacji przedmiotowych.

W trakcie badań prowadzonych na potrzeby niniejszej pracy zastosowano następujące metody:

- Sondaż (technika badawcza – badania ankietowe)[12] – wśród pracowników organów samorządu terytorialnego została przeprowadzona ankieta w celu zbadania ich świadomości i kompetencji w zakresie przetwarzania danych osobowych, a także oceny istniejących procedur i praktyk dotyczących ochrony danych. Wypełnione ankiety otrzymano podczas badania ankietowego wśród pracowników jednostek samorządu terytorialnego, którzy są bezpośrednio zaangażowani w procesy związane z ochroną danych osobowych. Ankiety zawierały zarówno pytania zamknięte, które ułatwiły kwantyfikację odpowiedzi, jak i pytania otwarte, pozwalające respondentom na bardziej szczegółowe wyrażenie swoich opinii i doświadczeń. Ankiety zostały zaprojektowane tak, aby uzyskać wiedzę na temat poziomu świadomości przepisów, wdrożonych procedur, napotykanych wyzwań oraz percepcji skuteczności implementacji ochrony danych osobowych. Metodologia stosowana w ramach badań dotyczących implementacji przepisów o ochronie danych osobowych

  w jednostkach samorządu terytorialnego w Polsce miała na celu zapewnienie wiarygodności i reprezentatywności wyników. W tym celu zastosowano celowy dobór próby, który umożliwił skupienie się na jednostkach, które są kluczowe z punktu

[12] *Badania ankietowe i ich rodzaje*, https://www.badania-ankietowe.com.pl/badania-ankietowe-i-ich-rodzaje [dostęp: 19.03.2024].

widzenia celów i problematyki badawczej. Próba badawcza obejmowała 57 jednostek samorządu terytorialnego, w tym 2 jednostki poziomu województwa, 5 powiatów oraz 50 gmin, w tym gminy miejskie, miejsko-wiejskie i miejskie (wykaz jednostek załączono w aneksie do niniejszej pracy). Taka próba pozwoliła uzyskać szeroki przekrój perspektyw oraz zrozumienie różnorodności praktyk w różnych typach jednostek samorządu terytorialnego.

- Studium przypadku[13] – metoda ta została zastosowana podczas analizy incydentów związanych z ochroną danych osobowych, aby zidentyfikować czynniki wpływające na skuteczność lub brak skuteczności działań organów samorządu terytorialnego w tym obszarze;
- Analiza treści – przegląd literatury przedmiotu oraz wewnętrznej dokumentacji jednostek samorządu terytorialnego w zakresie ochrony danych osobowych, pozwoliła na ocenę formalnej strony implementacji przepisów.[14] Dokonano przeglądu istotnych dokumentów wewnętrznych dostarczonych przez jednostki samorządu terytorialnego, takich jak polityki ochrony danych, procedury bezpieczeństwa, raporty z audytów, szkolenia pracowników itp. Analiza dokumentów pozwoliła na ocenę formalnej strony implementacji przepisów o ochronie danych oraz zrozumienie, jak te dokumenty są stosowane w praktyce;
- Badania porównawcze – przeprowadzono w celu analizy różnic w implementacji ochrony danych osobowych w wybranych jednostkach samorządu terytorialnego w Polsce oraz innych krajach Unii Europejskiej. Porównanie to pozwala zrozumieć, jakie czynniki wpływają na skuteczność wdrażania przepisów dotyczących ochrony danych osobowych, szczególnie w kontekście rozwoju cyfryzacji usług publicznych.
- Obserwacja uczestnicząca: W wybranych jednostkach przeprowadzono krótkie sesje obserwacji, aby zrozumieć, jak procedury ochrony danych są wdrażane na co dzień. Obserwacje te pozwoliły na uchwycenie praktycznych aspektów zarządzania danymi osobowymi, które mogłyby pozostać niezauważone w innych formach zbierania danych.

[13] Por. W. Grzegorczyk, *Studium przypadku jako metoda badawcza i dydaktyczna w naukach o zarządzaniu*, [w:] W. Grzegorczyk (red.), *Wybrane problemy zarządzania i finansów. Studia przypadków*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2015.

[14] R. Mayntz, K. Holm, P. Hübner, *Wprowadzenie do metodologii badań empirycznych*, Warszawa 1985.

Kombinacja tych metod i technik badawczych zbierania danych zapewniła wielowymiarowe podejście do badania, umożliwiając zebranie danych ilościowych dla statystycznej analizy oraz danych jakościowych, które dostarczyły kontekstu i głębi zrozumienia analizowanych zjawisk.

Specyfika obszaru badawczego

Badania prowadzone na potrzeby niniejszej rozprawy są w obszarze nauk o bezpieczeństwie[15]. Obszar badawczy sprecyzowano w oparciu o pięć kryteriów. Przedmiotem badań są dane osobowe, podmiotem jednostki samorządu terytorialnego w Polsce. Kryterium aspektowym jest bezpieczeństwo danych osobowych. Kryterium przestrzenne obejmuje jednostki samorządu terytorialnego, ze szczególnym uwzględnieniem jednostek samorządowych województw: kujawsko-pomorskiego oraz pomorskiego. Zakres temporalny rozprawy doktorskiej obejmuje lata: 2021-2022.

Wymiar etyczny badań dotyczył realizacji prawa do prywatności. Zamierzeniem rozprawy jest ukazanie, jak zachowane zostaje prawo do prywatności w tak specyficznej dziedzinie, jaką jest ochrona danych osobowych, przy okazji przetwarzania danych, a także ukazanie odstępstw od ochrony prywatności w sferze danych osobowych. Zadaniem pracy jest więc pokazanie, w jaki sposób i czy w ogóle prawo do prywatności zachowywane jest w sferze danych osobowych przy okazji chociażby przetwarzania danych czy też ich udostępniania, które to przecież niewątpliwie w ową prywatność ingerują. Problem polegający na tym, czy i jak prywatność jest chroniona w takich sytuacjach, za pomocą jakich instrumentów, jakie płyną dla niej zagrożenia i – jeśli ochrona prywatności w sferze danych osobowych w ogóle ma miejsce – ma wyraźny kontekst etyczny, a także prawny. Prawo do prywatności zaliczane jest w prawie wewnętrznym, unijnym i międzynarodowym do podstawowych praw człowieka. Uzasadnione jest stwierdzenie, że prawo to chronione jest niemal we wszystkich systemach prawnych. polską Konstytucję z 1997 r., która w art. 47 stanowi, że „Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym” oraz w art. 511, którego paragraf 1 stanowi, że „Nikt nie może być obowiązany inaczej niż na podstawie

[15] Zob. *Co to jest etyka badań naukowych i dlaczego jest ważna w badaniach społecznych?,* https://socialworlds.sgh.waw.pl/pl/ontological-section/etyka-w-badaniach-naukowych-od-wiedzy-do-praktyki-zestaw-narzedzi-do-badan [dostęp: 19.03.2024].

ustawy do ujawniania informacji dotyczących jego osoby". Mamy więc wyraźny dylemat prawno-administracyjny, ponieważ prawo do prywatności jest sprzeczne z zasady z ingerowaniem w nie podmiotów biurokratycznych, administracyjnych. Na próby rozwiązywania tej sprzeczności wskazują dokumenty prawa unijnego. Koncepcja prawa do prywatności znalazła swoje miejsce w kolejnych orzeczeniach aż do kluczowego momentu dla rozwoju ochrony praw podstawowych, a zatem i prawa do prywatności – uznania praw zawartych w Karcie praw podstawowych na mocy art. 6 Traktatu o Unii Europejskiej (TUE) w wersji traktatu z Lizbony.[16] Unia Europejska zobowiązana jest szanować prawa wynikające z art. 8 EKPC, tj. prawa do poszanowania życia prywatnego i rodzinnego obejmujące cztery sfery: ochrona życia prywatnego, rodzinnego, korespondencji, mieszkania. Prawo do prywatności chronione jest art. 7 KPP (prywatność w znaczeniu szerszym), który na mocy traktatu lizbońskiego otrzymał brzmienie: „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".[17]

Samo pojęcie „źródła prawa" jest wieloznaczne i sporne. W szczegółowych analizach odnosi się je najczęściej do źródeł poznania prawa (*fontes iuris cognoscendi*) i źródeł powstawania prawa (*fontes iuris oriundi*). Pierwsze to czynniki dostarczające informacji o prawie. Drugie są rozumiane niejednolicie i są najczęściej uznawane za czynniki wpływające na ukształtowanie się określonej treści przepisów prawa (źródła prawa w znaczeniu materialnym) lub za działania organów prawotwórczych albo efekty tej działalności (źródła prawa w znaczeniu formalnym).[18] Akty normatywne będące podstawą ochrony danych osobowych w Polsce są liczne i wymienienie ich wszystkich przekroczyłoby ramy tej pracy, jest to zresztą zbędne dla osiągnięcia założonych celów badawczych. Dlatego skupimy się tutaj na studium określonych przypadków, mogących uzmysłowić w jakim zakresie i stopniu prawo do ochrony danych jest w Polsce respektowane i realizowane.

Stan badań

Ochrona danych osobowych, szczególnie w kontekście jednostek samorządu terytorialnego, stała się jednym z kluczowych tematów w dobie wdrażania

[16] A. Gonschior, op. cit., s. 241.
[17] Ibidem.
[18] M. Błażewski, J. Behr, op. cit., s. 41-42.

ogólnego rozporządzenia o ochronie danych osobowych (RODO). W literaturze przedmiotu zgromadzono bogaty dorobek badawczy, który dotyczy głównie teoretycznych aspektów ochrony danych, regulacji prawnych oraz skutków naruszeń w obszarach publicznych i prywatnych. W szczególności wiele uwagi poświęcono interpretacji przepisów RODO, jak w pracy Pawła Fajgielskiego, „Ochrona danych osobowych w administracji publicznej”[19], gdzie omawiane są zagadnienia ochrony danych osobowych w kontekście polskiej administracji publicznej, z uwzględnieniem wyzwań wynikających z wdrożenia tychże przepisów. Autor analizuje przepisy prawne oraz praktyczne aspekty ich stosowania w urzędach administracji publicznej. Autor omawia wdrożenie RODO w Polsce oraz obowiązki, jakie wynikają z tych przepisów, ze szczególnym uwzględnieniem bezpieczeństwa przetwarzania danych. Ochrona danych jest tu ściśle związana z zapewnieniem bezpieczeństwa informacji w instytucjach publicznych, takich jak jednostki samorządu terytorialnego, które gromadzą i przetwarzają wrażliwe dane obywateli. Opracowanie to podkreśla znaczenie środków technicznych i organizacyjnych oraz ryzyka związanego z niewłaściwym zarządzaniem danymi. Praca zawiera również przegląd najważniejszych zagrożeń, takich jak cyberataki, oraz procedur, które mają na celu zapobieganie takim incydentom. Kolejną pozycją jest książka autorstwa Andrzeja Kraskiego, „Ochrona danych osobowych na podstawie RODO”[20], stanowiąca kompleksowy przegląd przepisów RODO i ich zastosowania w Polsce. Krasuski opisuje praktyczne problemy ochrony danych zarówno w obrocie tradycyjnym, jak i elektronicznym. Wartość tej publikacji wynika z omówienia kluczowych zagadnień związanych z ochroną danych osobowych, które mają znaczenie dla sektora publicznego. Inną pozycją w tym zakresie tematycznym jest opracowanie Dominika „Lubasza, RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów”[21], analizujące zmiany, jakie wprowadziło przedmiotowe przepisy w polskim systemie prawnym, porównując je z wcześniejszymi przepisami.

W szczególności zwraca uwagę na nowe obowiązki jednostek publicznych w kontekście przetwarzania danych osobowych, co jest kluczowe dla badania ochrony danych w JST. Należy również wspomnieć o pracy Justyny Boreckiej „Geneza prawnej ochrony danych

[19] P.Fajgielski, *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021.

[20] A.Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.

[21] D.Lubasz, *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018.

osobowych i pojęcie danych osobowych”[22], w której autorka skupia się na historycznym rozwoju przepisów dotyczących ochrony danych osobowych w Polsce i na świecie. Borecka omawia definicję danych osobowych oraz etapy ich ochrony prawnej, co stanowi istotne tło dla zrozumienia obecnych regulacji, takich jak RODO. Nie sposób pominąć opracowania Aleksandry Olender, „Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w podmiotach sektora publicznego”[23]**.** Autorka koncentruje się na praktycznych metodach analizy ryzyka związanych z przetwarzaniem danych osobowych w sektorze publicznym, w tym JST. Publikacja ta dostarcza narzędzi do oceny skutków wdrożonych rozwiązań dotyczących ochrony danych w kontekście obowiązujących przepisów. Istotnym znaczącym wkładem w budowanie wiedzy w przedmiotowym obszarze jest praca Macieja Błażewskiego i Jolanty Behr zatytułowanej „Środki prawne ochrony danych osobowych”. Autorzy omawiają różne środki prawne, które mają na celu podniesienia bezpieczeństwa w zakresie ochrony danych osobowych, z naciskiem na regulacje unijne i polskie. Autorzy analizują różne aspekty bezpieczeństwa prywatności w sektorze publicznym, co jest istotnym elementem badań nad wdrożeniem RODO w JST. Warto też wspomnieć o opracowaniu Lee Andrew Bygrave zatytułowanym „Data Privacy Law: An International Perspective”[24]. Książka przedstawia międzynarodowe podejście do ochrony danych osobowych, uwzględniając różnice w przepisach między krajami. Autor kładzie szczególny nacisk na unijne regulacje, co pozwala lepiej zrozumieć kontekst prawny RODO i jego wpływ na sektor publiczny w Polsce. Godnym podkreślenia jest również pozycja Jakuba Rzucidły „Prawo do prywatności i ochrona danych osobowych”[25]. Omawia on w niej kwestie bezpeczeństwa prywatności w kontekście konstytucyjnym i prawnym, a także analizuje regulacje dotyczące danych osobowych. Praca ta jest cennym źródłem informacji na temat teoretycznych podstaw prawa do ochrony danych w Polsce. Jeszcze inną pozycją wzbogacającą badany obszar jest „Introduction to Politics”[26] autorów: Roberta Garnera, Petera Ferdinand i Stephanie Lawson. Praca ta stanowi wprowadzenie do nauk

[22] J.Borecka, *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, „Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie, z. IV/2006”.

[23] A.Olender, *Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w podmiotach sektora publicznego*, „Wschód Europy”, vol. 6, 2/2020.

[24] L.A.Bygrave *Data Privacy Law: An International Perspective*, USA 2014

[25] J.Rzucidło, *Prawo do prywatności i ochrona danych osobowych,* [w:] *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym,* red. M. Jabłoński, Wrocław 2014.

[26] R.Garner, P. Ferdinand, S. Lawson, *Introduction to Politics*, Oxford 2009.

politycznych, w tym do regulacji związanych z ochroną prywatności i danymi osobowymi. Autorzy omawiają polityczne i administracyjne aspekty ochrony danych, co może być przydatne w kontekście regulacji JST.

Należy podkreślić, że wiele badań, jak te przeprowadzone przez Aleksandrę Olender, koncentruje się na kwestii analizy ryzyka w sektorze publicznym, podkreślając potrzebę lepszego przygotowania JST na zagrożenia związane z ochroną danych. Jednakże mając na względzie rozwój społeczeństwa cyfrowego istnieje jednak znacząca luka badawcza w zakresie empirycznej oceny skuteczności wdrożenia przepisów RODO w jednostkach samorządu terytorialnego. Z dostępnej literatury wynika, że choć problematyka ochrony danych osobowych jest intensywnie omawiana, brakuje szczegółowych badań na temat tego, jak JST radzą sobie z przetwarzaniem danych osobowych w praktyce. Niniejsza praca doktorska podejmuje próbę wypełnienia tej luki, poprzez analizę statystyk zgłoszonych naruszeń oraz praktyk ochrony danych w wybranych jednostkach samorządowych. Obejmuje ona ocenę procedur bezpieczeństwa danych osobowych w wybranych jednostkach samorządu terytorialnego w Polsce.

Struktura pracy

Praca składa się ze wstępu, sześciu rozdziałów, zakończenia, bibliografii, spisu wykresów oraz aneksu. We wstępie przedstawiono główne założenia metodologiczne rozprawy doktorskiej. W pierwszy rozdział poświęcony jest ochronie danych osobowych jako problemowi interdyscyplinarnemu, podkreślając jego znaczenie w kontekście społeczeństwa informacyjnego. Omawia różnorodne aspekty związane z bezpieczeństwem danych osobowych, takie jak techniczne środki zabezpieczeń, regulacje prawne (np. RODO), oraz kwestie etyczne i społeczne. W rozdziale wskazano, że ochrona danych osobowych ma wpływ na stabilność społeczną i gospodarczą, a także na zaufanie publiczne wobec instytucji. Ponadto, przedstawiono znaczenie interdyscyplinarnego podejścia, które uwzględnia technologię, prawo, ekonomię i etykę, oraz wskazano na wyzwania wynikające z rozwoju cyfrowych technologii, takich jak sztuczna inteligencja. Rozdział podkreśla również istotę danych osobowych jako zasobu ekonomicznego oraz konieczność zapewnienia ich ochrony w obliczu dynamicznie zmieniającego się środowiska technologicznego.

W rozdziale drugim poświęconym prawnym aspektom ochrony danych osobowych, koncentrowano się na całokształcie regulacji prawnych będących podstawą do realizacji polityki ochrony danych osobowych w Polsce. Uwzględniono tutaj podział na regulacje krajowe oraz unijne. W rozdziale tym poruszono także kwestię organów kontroli i nadzoru nad ochroną danych osobowych, omówiono rodzaje odpowiedzialności w kontekście ochrony danych osobowych, sankcje administracyjne i karne w przypadku naruszenia ochrony danych osobowych. Dla porównania dokonano przeglądu systemów ochrony danych osobowych obwiązujących w państwach Unii Europejskiej i poza jej granicami. Powyższe analizy porównawcze stanowią punkt wyjścia do wstępnego oszacowania stopnia ochrony danych osobowych w Polsce, a także do prognoz możliwych kierunków ewolucji systemów ochrony danych osobowych.

W rozdziale trzecim skupiano się na funkcjonowaniu organów samorządu terytorialnego w Polsce. Starano się wykazać w jaki sposób poszczególne, hierarchiczne jednostki administracji publicznej na szczeblu gminy, powiatu, województwa wykonują swoje zadania w zakresie polityki ochrony danych osobowych.

Najpełniejszym dokumentem regulującym ochronę danych osobowych w państwach członkowskich Unii Europejskiej jest wspomniane już *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku*. Obowiązki, które nakłada ono na jednostki samorządu terytorialnego w Polsce omawiano w rozdziale czwartym.

Odrębny rozdział poświęcono samorządowym usługom publicznym, takim jak: usługi edukacyjne, zdrowotne, infrastrukturalne, środowiskowe, społeczne, kulturalne i bezpieczeństwa. Ich związek z ochroną danych osobowych jest niezaprzeczalny, ponieważ właśnie w ramach świadczenia usług publicznych obowiązywać powinny zasady legalności, uczciwości i przejrzystości, minimalizacji danych, celowości, ograniczonego przechowywania, integralności i poufności. Również wymogi usług publicznych wyraźnie określają uprawnienia osób, których dane dotyczą, co zdecydowanie dookreśla właściwe praktyki administracji publicznej.

Ostatni rozdział pracy zawiera analizę praktyk ochrony danych osobowych w wybranych jednostkach samorządu terytorialnego, które zostały zgłoszone lub wykryte w jednostkach samorządu terytorialnego. Ta część pozwoliła na identyfikację najczęściej występujących newralgicznych punktów w systemie ochrony danych. Obejmuje weryfikację przypadków naruszeń danych osobowych oraz prezentację statystyk dotyczących zgłoszonych incydentów. Podrozdział *Statystyka zgłaszanych*

naruszeń ochrony danych osobowych w jednostkach samorządu terytorialnego przedstawia dane ilościowe dotyczące zgłoszeń naruszeń, umożliwiając ocenę skali problemu strukturach samorządowych samorządach. Kolejne podrozdziały szczegółowo analizują konkretne przypadki naruszeń, wskazując na zaniedbania i nieprawidłowości w procedurach zabezpieczania danych, które prowadzą do sankcji administracyjnych. W konkluzji zastanawiamy się nad konsekwencjami naruszeń prawa ochrony danych osobowych zarówno dla podmiotów samorządowych, jaki i osób, których dane zostały niewłaściwie wykorzystane. Rozdział ten zamyka podsumowująca analiza wyników uzyskanych z przeprowadzonych badań ankietowych.

Zidentyfikowanie tendencji, wzorców oraz ewentualnych odchyleń w zakresie praktyk ochrony danych osobowych w różnych jednostkach samorządu terytorialnego, będących rezultatem podjętych wysiłków badawczych, posłużyło następnie do sformułowania zaleceń, które mogą pomóc jednostkom samorządu terytorialnego w dalszym doskonaleniu swoich systemów ochrony danych osobowych. Szczególnie istotne w usługach publicznych jest wypracowanie „dobrych praktyk", mogących stanowić wzór dla jednostek dążących do doskonalenia swojej polityki ochrony danych. Poświęcamy im miejsce w końcowej części pracy, w rozdziale siódmym i zakończeniu.

Ostateczne wnioski, wynikające z nakreślonego problemu badawczego, a także weryfikacja hipotez przyjętych w pracy zostały zawarte w zakończeniu. Niemniej jednak należy zaakcentować, że weryfikacja hipotez zawartych we wstępie niniejszej pracy ma charakter mieszany. Na podstawie przeprowadzonych badań i analiz teoretycznych stwierdzono, że część założeń potwierdziła się w pełni, jednak niektóre hipotezy wymagały korekt lub nie znalazły pełnego potwierdzenia. W szczególności, badania wykazały, że organizacje samorządu terytorialnego, które inwestują w edukację personelu, osiągają lepsze wyniki w zakresie ochrony danych osobowych. Z drugiej strony, identyfikacja implementacyjnych luk w systemach ochrony danych wykazała, że nie wszystkie jednostki samorządu działają zgodnie z założeniami RODO. Celem tych wniosków jest odpowiedź na pytania dotyczące efektywności ochrony danych osobowych przez polskie samorządy terytorialne, sposobów i koniecznych działań w zakresie ochrony prywatności obywateli, a także identyfikacja ewentualnych luk implementacyjnych w istniejącym systemie organizacyjnym i prawnym oraz propozycje ich eliminacji.

ROZDZIAŁ I
BEZPIECZEŃSTWO INFORMACYJNE A OCHRONA DANYCH OSOBOWYCH

Problem bezpieczeństwa danych osobowych ma charakter interdyscyplinarny. Ochrona tego typu informacji to kwestia, wiążąca różne aspekty życia społecznego, dlatego powinna być analizowana z punktu widzenia wielu naukowych perspektyw. Zanim jednak do tego przejdziemy, spróbujmy najpierw zdefiniować czym jest społeczeństwo informacyjne i dlaczego ochrona danych osobowych jest tak ważna w życiu publicznym.

1.1. Wprowadzenie do tematu oraz uzasadnienie jego znaczenia

W dobie postępu technologii cyfrowych dane osobowe stały się jednym z istotniejszych elementem funkcjonowania współczesnych społeczeństw. Codziennie generowane są ogromne ilości informacji dotyczących jednostek, obejmujących ich preferencje zakupowe, historię zdrowotną, lokalizację, aktywność online oraz wiele innych aspektów życia. Dane te są niezwykle cenne, zarówno dla firm prywatnych, instytucji publicznych, jak i cyberprzestępców. Ochrona tych danych, czyli zapewnienie ich bezpieczeństwa, integralności oraz poufności, stała się jednym z najważniejszych wyzwań XXI wieku. Złożoność omawianego problemu sprawia, że nie może być on analizowany i rozwiązywany jedynie z perspektywy jednej dyscypliny. Konieczne jest podejście interdyscyplinarne, które uwzględnia różnorodne aspekty techniczne, prawne, etyczne, społeczne i ekonomiczne. Jak zauważa Solove: „Prywatność jest pojęciem związanym z jednostką, głęboko splecionym z autonomią osobistą i tożsamością. Jednak jest to również wartość społeczna, niezbędna dla funkcjonowania społeczeństwa.”[27]

Z technicznego punktu widzenia, ochrona danych osobowych obejmuje szereg środków i praktyk mających na celu zabezpieczenie informacji przed nieautoryzowanym dostępem, utratą czy modyfikacją. Należą do nich m.in. szyfrowanie danych, autoryzacja i uwierzytelnianie użytkowników, regularne aktualizacje oprogramowania oraz

[27] D.J. Solove, *Understanding Privacy*, Harvard University Press, 2008, s. 22.

monitorowanie sieci w celu wykrywania potencjalnych zagrożeń. Cyberbezpieczeństwo[28] jest dynamicznie rozwijającą się dziedziną, która musi nieustannie dostosowywać się do nowych zagrożeń oraz zmian w prawie. Innowacje technologiczne, takie jak sztuczna inteligencja[29] i uczenie maszynowe[30], coraz częściej znajdują zastosowanie w detekcji i neutralizacji zagrożeń. Jednocześnie stawiają one przed specjalistami nowe wyzwania.

Ochrona danych osobowych jest również regulowana przez prawo. W Unii Europejskiej kluczowym aktem prawnym jest *Rozporządzenie o Ochronie Danych Osobowych* (RODO), które wprowadza rygorystyczne wymagania dotyczące przetwarzania danych osobowych oraz surowe kary za ich naruszenie. Podobne regulacje obowiązują w wielu innych krajach, choć różnią się one szczegółami i zakresem. Przestrzeganie tych przepisów należy do obowiązku każdego podmiotu, który przetwarza dane osobowe. Wymaga to wdrożenia odpowiednich polityk i procedur, a także ciągłego monitorowania zgodności działań z obowiązującymi regulacjami. W kontekście prawnym istotne są również kwestie dotyczące międzynarodowego transferu danych oraz współpracy między jurysdykcjami w zakresie ochrony danych.

Zabezpieczenie danych osobowych to również problematyka etyczna i społeczna. Firmy oraz instytucje muszą nie tylko spełniać wymagania prawne, ale również działać zgodnie z zasadami etyki. Jest to szczególnie ważne w kontekście zaufania społecznego – użytkownicy muszą mieć pewność, że ich dane osobowe są wykorzystywane w sposób odpowiedzialny i przejrzysty. Etyczne zarządzanie danymi obejmuje m.in. zapobieganie ich nadużyciom, minimalizację zbierania danych oraz zapewnienie, że są one wykorzystywane wyłącznie do celów, na które użytkownicy wyrazili zgodę. Jest to szczególnie ważne, bowiem społeczne konsekwencje naruszeń bezpieczeństwa danych mogą być bardzo poważne. Wyciek danych może prowadzić do kradzieży tożsamości, oszustw finansowych, a także utraty reputacji i zaufania do instytucji, które były odpowiedzialne za ochronę tych informacji. Ochrona danych osobowych wywiera więc zauważalny wpływ na stabilność społeczną i gospodarkę.

[28] Zob. D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Europaen Association for Security, Kraków 2016.
[29] Zob. K. Różanowski, *Sztuczna inteligencja: rozwój, szanse i zagrożenia*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki", 2007, nr 2.
[30] Zob. K. Krawiec, J. Stefanowski, *Uczenie maszynowe i sieci neuronowe*, Poznań 2003.

Dane osobowe są także kluczowym elementem nowoczesnej gospodarki[31]. Firmy korzystają z nich do personalizacji usług, analizy rynkowej oraz tworzenia nowych produktów i usług. Wartość ekonomiczna danych osobowych jest ogromna[32], a ich odpowiednie zarządzanie może przynieść znaczące korzyści finansowe. Naruszenie bezpieczeństwa danych może prowadzić do poważnych strat finansowych, zarówno bezpośrednich, jak i pośrednich, związanych z utratą reputacji oraz zaufania klientów. Przedsiębiorstwa muszą więc inwestować w zaawansowane technologie oraz szkolenia personelu, by zapewnić wysoki poziom ochrony danych.

Bezpieczeństwo danych osobowych jest więc złożonym, interdyscyplinarnym problemem badawczym, który wymaga współpracy specjalistów z różnych dziedzin. Na tej płaszczyźnie aspekty techniczne, prawne, etyczne, społeczne i ekonomiczne przenikają się nawzajem, tworząc złożony ekosystem, w którym każde naruszenie może mieć szeroko zakrojone konsekwencje. Współczesne wyzwania związane z ochroną danych osobowych wymagają ciągłej adaptacji i innowacji, aby sprostać dynamicznie zmieniającemu się środowisku zagrożeń. Interdyscyplinarne podejście pozwala na lepsze zrozumienie tych wyzwań i wypracowanie skutecznych strategii ochrony danych, które są istotne dla zachowania prywatności i bezpieczeństwa w cyfrowym świecie.

Biorąc pod uwagę wyszczególnione wyżej aspekty, można stwierdzić, że uzasadnienie rangi problemu bezpieczeństwa danych osobowych wynika z następujących przesłanek:

- Prywatność i prawa jednostki – dane osobowe są ściśle związane z prawem do prywatności. Prawo do ochrony tych informacji należy do fundamentalnych praw człowieka. Naruszenie prywatności może prowadzić do poważnych konsekwencji, takich jak kradzież tożsamości, oszustwa czy nękanie;
- Zagrożenia cybernetyczne – wraz z rozwojem technologii, zagrożenia związane z cyberbezpieczeństwem stają się coraz bardziej powszechne. Cyberprzestępcy stosują coraz bardziej wyszukane metody, aby uzyskać dostęp do danych osobowych. Działania takie jak phishing, malware czy ransomware mogą prowadzić do masowych wycieków danych;
- Groźne następstwa – skutki naruszenia danych osobowych mogą mieć groźne następstwa nie tylko o charakterze ekonomicznym, lecz także społecznym

[31] Zob. L. Karpierz, *Ochrona danych osobowych w sektorze bankowym*, Kraków 2012.
[32] Zob. J. Kwaśnik, *Dane osobowe jako kluczowy obiekt zainteresowania cyberprzestępców*, „Annales Canonici", nr 16/2020.

i zdrowotnym. Na poziomie społecznym, naruszenia danych mogą prowadzić do erozji zaufania do instytucji publicznych i prywatnych, które są odpowiedzialne za ochronę danych. Społeczność może zacząć obawiać się korzystania z usług cyfrowych, co wiąże się z ryzykiem spowolnienia postępu technologicznego i innowacji. Naruszenia danych osobowych mogą również mieć poważne konsekwencje zdrowotne. Ofiary takich przestępstw często doświadczają wysokiego poziomu stresu, lęku oraz innych problemów psychicznych. Stres związany z kradzieżą tożsamości i koniecznością radzenia sobie z jej konsekwencjami wiąże się z ryzykiem długotrwałych problemów zdrowotnych, takich jak zaburzenia snu, depresja czy problemy kardiologiczne. W przypadku wycieku danych medycznych, niektóre osoby mogą obawiać się stygmatyzacji i dyskryminacji, co wywiera dodatkowy negatywny wpływ na ich stan psychiczny.

1.2.Charakterystyka środowiska informacyjnego

Środowisko informacyjne stanowi nieodłączny element współczesnego świata, wpływając na różne dziedziny życia, w tym gospodarkę, edukację, zdrowie, politykę i społeczeństwo. Umożliwia szybki dostęp do informacji, wspiera innowacje, ułatwia komunikację i współpracę, a także przyczynia się do podejmowania trafniejszych decyzji. Jednakże, ze względu na jego złożoność i dynamikę, wymaga ciągłej uwagi i zarządzania, aby zapewnić bezpieczeństwo, prywatność użytkowników oraz efektywność działania. Przy odpowiednim podejściu, środowisko informacyjne może wspierać rozwój i innowacje, przyczyniając się do poprawy jakości życia w skali całego globu.

1.2.1. Definicja środowiska informacyjnego

Środowisko informacyjne można zdefiniować jako złożony ekosystem składający się z ludzi, technologii, procesów, danych oraz infrastruktury, który umożliwia gromadzenie, przetwarzanie, przechowywanie, wymianę i wykorzystanie informacji. Jest to dynamiczna i interaktywna przestrzeń, w której różne elementy współdziałają, aby tworzyć, udostępniać i zarządzać informacjami w celu wspierania podejmowania decyzji, komunikacji i działań w różnych kontekstach[33]. Castells podkreśla, że „Epoka

[33] Por. M. Kisilowska, *Przestrzeń, horyzont, środowisko informacyjne… Czy wiemy, co nas otacza? Rozważania terminologiczne*, „Praktyka i Teoria Informacji Naukowej i Technicznej”, 2012, t. 20, nr 3-4.

informacyjna charakteryzuje się sieciowaniem wiedzy, a główne funkcje tego systemu to zapewnienie platformy do ciągłego uczenia się i transferu wiedzy."[34]

Środowisko informacyjne bywa definiowane zarówno w wąskim, jak i szerokim kontekście. Wąskie podejście dotyczy środowiska pojedynczych użytkowników lub lokalnych społeczności, podczas gdy szerokie podejście obejmuje wymiar globalny. Dwa podstawowe kryteria, które to determinują, to kryterium geograficzne/przestrzenne oraz „intensywność" otaczającej nas sfery informacyjnej. Badacze wyszczególniają także różne poziomy środowiska informacyjnego: indywidualne (osobowe), grupowe, zespołowe, społeczne i globalne[35].

Wiesław Babik zwraca uwagę na to, że „środowisko informacyjne (antropoinfosfera) może być rozpatrywane poprzez aspekty: społeczne, psychologiczne, socjologiczne, ekonomiczne, medyczne, edukacyjne i inne. Ważna jest przezroczystość środowiska informacyjnego człowieka. Środowisko jest przezroczyste wówczas, gdy wiadomo, kto jest nadawcą informacji, jaki ma ona status, do kogo jest skierowana, jakie nadawca ma intencje, jaki jest cel informowania, kto jest adresowanym lub potencjalnym odbiorcą informacji"[36].

Na środowisko informacyjne składają się następujące elementy:

- Użytkownicy i producenci informacji, w tym osoby indywidualne, grupy, organizacje i społeczności, biorący udział w tworzeniu, udostępnianiu i interpretowaniu informacji;
- Narzędzia i systemy informatyczne, takie jak komputery, smartfony, oprogramowanie, internet, sieci społecznościowe, które umożliwiają zbieranie, przetwarzanie, przechowywanie i wymianę informacji;
- Procedury i metody zarządzania informacjami, w tym pozyskiwanie, analiza, dystrybucja, archiwizacja oraz zabezpieczanie danych. Procesy te mają za zadanie zapewnić dostępność, wiarygodność oraz użyteczność informacji;
- Surowe fakty i liczby, które są przetwarzane w celu uzyskania informacji. Dane mogą przybierać różne formy, takie jak tekst, obraz, dźwięk, film, a także mogą pochodzić z różnych źródeł, takich jak bazy danych, media społecznościowe, czujniki czy raporty;

[34]M. Castells, *The Rise of the Network Society 1*, Wiley-Blackwell, Hoboken 1996, s. 18.
[35] W. Babik, *Ekologia informacji*, Kraków 2014, s. 37-38.
[36] Ibidem, s. 38.

- Fizyczne i wirtualne zasoby, takie jak serwery, sieci, centra danych, które wspierają funkcjonowanie technologii informacyjnych i umożliwiają przechowywanie oraz transmisję danych[37].

Współczesne środowisko informacyjne wyróżnia się następującymi cechami:

- Stała zmiana i ewolucja ze względu na szybki rozwój technologii oraz zmieniające się potrzeby i zachowania użytkowników;
- Użytkownicy działający w ramach środowiska informacyjnego mogą wchodzić w interakcje z technologią oraz z innymi użytkownikami w celu tworzenia i wymiany informacji. Interaktywność zwiększa zaangażowanie i efektywność procesów informacyjnych;
- Środowisko informacyjne obejmuje różnorodne aspekty, takie jak technologia, zarządzanie, prawo, bezpieczeństwo, etyka, które muszą być zintegrowane i zarządzane w sposób spójny;
- W ramach środowiska informacyjnego dane mogą łatwo krążyć po całym świecie, co umożliwia globalną współpracę i wymianę wiedzy[38].

Środowisko informacyjne, w którym działa dany podmiot społeczny lub ekonomiczny, wpływa na jego zdolność do działania oraz podejmowania decyzji. Jest to społeczne środowisko informacyjne. Każdy podmiot społeczny, polityczny czy ekonomiczny w ramach tego środowiska buduje swoje własne, unikalne środowisko informacyjne. Z tego społecznego otoczenia wybiera te zasoby, procesy i systemy informacyjne, które są mu aktualnie lub potencjalnie potrzebne. Wiedza o tym, jak tworzyć i kształtować indywidualne środowisko informacyjne oraz umiejętność jego tworzenia, decydują o efektywności funkcjonowania danego podmiotu w społeczeństwie, polityce i gospodarce[39].

Fritch i Mandernack wskazali na następujące cechy charakterystyczne środowiska informacyjnego:

- powszechne wykorzystanie komputerów,
- dostęp do zasobów internetowych z każdego urządzenia połączonego z siecią,

[37] Por. E.A. Matsefuk, P.V. Razbegaev*, Axiosphere as an element of the information environment*, „World of Science, Culture, Education", 6/2017.
[38] Zob. K. A. Kalyuzhny*, Information environment and information environment of science: essence and purpose*, Science Management and Scientometrics, nr 18/2015.
[39] J. Oleński, *Społeczne bezpieczeństwo informacyjne podstawą demokratycznego państwa*, „Rocznik Kolegium Analiz Ekonomicznych", 2015, nr 36, s. 13.

- różnorodność formatów publikacji,
- możliwość publikowania informacji w internecie na dowolny temat, w formie dostępnej dla każdego,
- krótkotrwałość witryn internetowych w porównaniu do źródeł drukowanych,
- ogromna rozległość i chaotyczny charakter zasobów internetowych, a także ich zróżnicowana jakość,
- brak jednolitego i uniwersalnego systemu klasyfikacji stron internetowych,
- istnienie licznych, zróżnicowanych wyszukiwarek i metod dostępu do informacji.[40]

Jak zauważa Józef Oleński: „możliwości kształtowania indywidualnego środowiska informacyjnego przez pojedynczy podmiot społeczny lub ekonomiczny są wyznaczane przez społeczne środowisko informacyjne. Co więcej, społeczne środowisko informacyjne, zwłaszcza niektóre jego zasoby, procesy i systemy, aktywnie wpływa na indywidualne środowiska informacyjne ludzi i podmiotów gospodarki narodowej, kształtując indywidualne środowiska informacyjne często w sposób nieodpowiadający rzeczywistym celom i informacyjnym potrzebom tych podmiotów”[41]. Podobne zdanie ma Richard Otlet, który uważa, że wszystkie źródła informacji a także „doświadczenia informacyjne”, stanowią część wielu oddziałujących na siebie systemów działań, które są historycznie i społecznie ukształtowanymi środowiskami informacyjnymi, w których funkcjonujemy.[42]

W warunkach globalizacji różnych aspektów życia oraz rosnącego wpływu organizacji międzynarodowych, kontrolowanych przez światowe mocarstwa i globalne instytucje finansowe, dochodzi do globalizacji społecznego środowiska informacyjnego. Globalne media i elektroniczne technologie informacyjne szeroko rozpowszechniają informacje, co skutkuje ujednoliceniem instytucji politycznych i organizacyjnych na całym świecie. Pojedyncze państwa, z wyjątkiem wielkich mocarstw, mają ograniczone możliwości kształtowania własnego środowiska informacyjnego według swoich potrzeb, często będąc zmuszane przez organizacje międzynarodowe do podporządkowania się ich interesom ekonomicznym lub politycznym. W rezultacie,

[40] J.W Fritch, S.B Mandernack, *The emerging reference paradigm: A vision of reference services in a complex information environment,* „ Library Trends”, 50 (2), 2001, s. 7.
[41] Ibidem, s. 13-14.
[42] D. Baker, W. Evans, *Trends, Discovery, and People in the Digital Age*, Woodhead Publishing Limited, Stawston 2013, s. 45-47.

krajom niebędącym mocarstwami narzucane są polityczne, ekonomiczne i kulturowe dogmaty, które często nie odpowiadają ich rzeczywistym potrzebom i interesom[43].

Charakterystyczną cechą współczesnego środowiska informacyjnego jest to, że w jego obrębie gromadzone są nie tylko informacje fachowe, specjalistyczne i naukowe, ale także osobiste i prywatne, dotyczące codziennego życia. Obecnie można stwierdzić, że środowisko informacyjne jest zaśmiecone z powodu nadmiaru informacji, które nie zawsze są istotne i rzetelne, co powoduje, że wiele osób ma trudności z rozpoznaniem informacji wartościowych[44].

Innym ważnym aspektem aktualnego środowiska informacyjnego jest to, że Internet znacząco osłabił monopol informacyjny tradycyjnych mediów, odbierając im dominującą pozycję w opiniowaniu ważnych wydarzeń. Jego powszechność stanowiła wyzwanie dla tradycyjnych mediów i ich nadawców, zmuszając ich do korzystania z różnych form przekazu jednocześnie. Obecnie każdy znaczący tytuł prasowy, stacja radiowa czy kanał telewizyjny prowadzi własną stronę internetową. Z kolei internetowe portale informacyjne rzadko rozszerzają swoją działalność na radio czy telewizję, skupiając się na zwiększaniu zakresu oferowanych usług, takich jak skrzynka pocztowa czy wirtualny dysk. Podobna sytuacja przekształciła biernych odbiorców w aktywnych użytkowników. Powstanie mediów społecznościowych stanowiło kolejny przełom w historii świata społecznego, politycznego i gospodarczego. Jak zauważa Dominik Kaznowski, media społecznościowe położyły kres monopolowi elit na płaszczyźnie kreowania i kontroli informacji, poglądów i prezentacji opinii[45].

Funkcjonowanie w środowisku informacyjnym wymaga od użytkownika posiadania kompetencji informacyjnych, czyli umiejętności skutecznego wyszukiwania, oceny, wykorzystywania i zarządzania informacjami. W obliczu ogromnej ilości dostępnych danych, niezbędne jest rozróżnianie wiarygodnych źródeł od tych mniej rzetelnych oraz krytyczne myślenie. Kompetencje informacyjne obejmują również znajomość narzędzi i technologii informacyjnych oraz umiejętność ich zastosowania w celu rozwiązywania problemów i podejmowania decyzji.

Samo pojęcie kompetencji informacyjnych (ang. *information literacy*) jest definiowane w różnorodny sposób, co wynika zarówno z szerokiego zakresu

[43] Ibidem, s. 14.
[44] M. du Vall, *Społeczne bezpieczeństwo informacyjne w erze nowych mediów*, „Bezpieczeństwo. Teorie i Praktyka", 2017, nr 4, s. 21.
[45] Ibidem.

znaczeniowego samego terminu literacy (alfabetyzm), jak i z wieloaspektowości oraz kontekstowości informacji, a także z różnych celów i metod korzystania z jej źródeł. Od czasu, gdy Paul Zurkowski w 1974 roku wprowadził to pojęcie w odniesieniu do umiejętności wykorzystywania informacji w miejscu pracy, koncepcja alfabetyzmu informacyjnego, czyli kompetencji informacyjnych, była rozwijana w różnych dziedzinach. Dotyczy to m.in. szkolnictwa wyższego (kompetencje studentów i naukowców), edukacji (kompetencje uczniów i nauczycieli), środowiska pracy (kompetencje pracowników) oraz codziennego życia (kompetencje obywateli)[46]. Jak zauważa Małgorzata Skibińska, „na przestrzeni dekad zmieniała się koncepcja kształcenia kompetencji informacyjnych – od dominujących krótkoterminowych i ściśle specjalistycznych szkoleń prowadzonych przez bibliotekarzy, do propagowania szkoleń nauczycieli akademickich i szkolnych, by ci mogli kształcić umiejętności informacyjne swoich studentów i uczniów oraz włączać je do realizacji przedmiotowych efektów kształcenia. Takie podejście ma sprzyjać rozwijaniu praktyk informacyjnych opartych na współpracy oraz efektywności i trwałości uczenia się w zakresie korzystania z informacji”[47].

Na szeroki sposób rozumienia i definiowania pojęcia kompetencji informacyjnych znacząco wpłynął postęp w zakresie technologii informacyjno-komunikacyjnych. Ich rozwój i stopniowa popularyzacja wymuszały zmiany w zachowaniach informacyjnych użytkowników. Koncepcja *information literacy* została powiązana z umiejętnością biegłego „czytania i pisania” różnych form informacji, co doprowadziło do jej łączenia z takimi terminami jak *digital literacy*, *computer literacy*, *ICT literacy*, *media literacy*, *visual literacy*, *web literacy*, *data literacy* i *metaliteracy*. Rozwój technologii Web 2.0 i pojawienie się mediów społecznościowych przyczyniły się do konwergencji mediów, co zatarło indywidualny charakter poszczególnych form informacji.

Od 2011 roku postulowano więc zrównanie kompetencji informacyjnych i medialnych. Intensywny wzrost liczby źródeł informacji i narzędzi medialnych wyznaczył nowe trendy w ewolucji koncepcji information literacy, takie jak promowanie i doskonalenie kompetencji informacyjnych w samokształceniu i edukacji zdalnej,

[46] M. Skibińska, *Kompetencje informacyjne – przegląd tendencji rozwojowych koncepcji information literacy*, „Przegląd Badań Edukacyjnych”, 2021, nr 34, s. 201.
[47] Ibidem.

uczenie krytycznej oceny źródeł informacji oraz kształtowanie kreatywnej i etycznej postawy użytkowników wobec dostępnej wiedzy[48].

Na stan i jakość środowiska informacyjnego znacząco wpływa polityka informacyjna rządu, rodzaj i dostępność technologii informacyjnych i komunikacyjnych dla obywateli, charakter i sposób działania mediów masowych, zorganizowana obsługa informacyjna, intensywność interakcji społecznych, kultura organizacyjna i informacyjna, kompetencje informacyjne i komunikacyjne osób oraz instytucji oświatowych, wiedza na temat mechanizmów informacyjnych i komunikacyjnych zachodzących w społeczeństwie, poziom organizacji życia społecznego oraz świadomość informacyjna poszczególnych obywateli i grup społecznych. Te instytucjonalno-organizacyjne warunki mogą sprzyjać swobodnemu przepływowi informacji i wiedzy, bądź go utrudniać[49].

Jednakże, to właśnie człowiek stanowi centralny element procesu informacyjnego. Fundamentalną rolę w środowisku informacyjnym, opartym na gromadzeniu, selekcjonowaniu i udostępnianiu informacji, odgrywają potrzeby i zachowania informacyjne jednostki. Potrzeby te mogą zostać zaspokojone przez informację dostarczoną w odpowiedniej formie, miejscu i czasie. Wymiana i udostępnianie informacji, niezależnie od jej zakresu i jakości, stały się możliwe dzięki środkom technicznym. Ich rozwój umożliwił łatwiejszy dostęp do informacji i wybór odpowiednich źródeł przez użytkownika. Wpływ na ten proces wywierają również czynniki ekologiczne i środowiskowe, takie jak polityka informacyjna, technologie informacyjne i komunikacyjne, media masowe, inni ludzie, Internet i biblioteki[50].

Funkcjonowanie jednostki w środowisku informacyjnym mogą utrudniać bariery informacyjne. Jolanta Sobielga wyróżniła cztery rodzaje barier, do których zaliczyła:

- fizyczne przeszkody, które utrudniają identyfikację, wyszukiwanie i wykorzystywanie informacji;
- przeszkody wynikające z działań podmiotów współpracujących z użytkownikiem podczas wyszukiwania informacji;
- trudności związane z niewystarczającymi umiejętnościami użytkowników, które ujawniają się podczas korzystania z informacji;

[48] Ibidem, s. 201-202.
[49] W. Babik, *Ekologia informacji*…, s. 25.
[50] Ibidem.

- procesy oraz stan psychiczny użytkownika, które negatywnie wpływają na korzystanie z informacji[51].

Radzenie sobie z barierami informacyjnymi wymaga różnorodnych strategii i podejść, które odpowiadają na specyficzne rodzaje przeszkód. Dla przykładu, w eliminowaniu przeszkód fizycznych może pomóc poprawa infrastruktury, polegająca na korekcie jakości oświetlenia w bibliotekach, wprowadzaniu ergonomicznych miejsc pracy, czy też ułatwianie dostępu do komputerów i innych urządzeń. Z kolei bariery wynikające ze stanu psychicznego mogą wymagać wsparcia psychologicznego dla użytkowników, którzy doświadczają stresu, lęku lub innych problemów emocjonalnych wpływających na ich zdolność do korzystania z informacji.

1.2.2. Wpływ cyfryzacji na rozwój środowiska informacyjnego

Nowoczesne komputery łączą w sobie osiągnięcia technologiczne z różnych etapów rozwoju cywilizacji. Dzięki temu możliwe stało się tworzenie, pozyskiwanie, gromadzenie, przetwarzanie i udostępnianie treści pochodzących zarówno od ludzi, jak i otoczenia. Te treści są dostosowane do ludzkich zmysłów, takich jak wzrok i słuch, szczególnie wspierając zdolności intelektualne człowieka. Dzięki temu znacząco zwiększa się szybkość i zakres wymiany danych, informacji i wiedzy. Uznaje się, że najważniejszym aspektem cyfrowej transformacji jest wspieranie intelektualnych możliwości człowieka, a oprogramowanie komputerowe stanowi niezbędne narzędzie procesu cyfryzacji[52].

Dzięki cyfryzacji pojawiły się „ogromne możliwości w zakresie przepływu informacji i jej przetwarzania, które umożliwiają organizację twórczych, interdyscyplinarnych zespołów rozwiązujących najbardziej złożone problemy społeczno-gospodarcze. W procesach gospodarczych, dzięki ich optymalizacji i racjonalnemu wykorzystaniu zasobów, cyfryzacja bezpośrednio przyczynia się do optymalizacji przepływów, zwiększenia produktywności, a tym samym przyspieszenia wzrostu gospodarczego[53].

[51] Ibidem, s. 57.
[52] L. Kowalczyk, *Cyfryzacja w procesie postępu cywilizacyjnego i jej współczesna rola w innowacyjności*, (w:) *Innowacyjność to cyfryzacja i rozwój. Zarządzanie operacyjne w teorii i praktyce organizacji biznesowych, publicznych i pozarządowych*, pod. red. L. Kowalczyka i F. Mroczko, „Prace Naukowe Wyższej Szkoły zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu", t. 43, Wałbrzych 2017, s. 19.
[53] Ibidem, s. 5.

Cyfryzacja bazuje na cyfrowej formie danych (0 i 1), będącej przekazem informacji dotyczącej ludzkiej działalności w określonej płaszczyźnie. Dzięki technologiom i specjalistycznemu oprogramowaniu, cyfrowe treści tekstowe i wizualne mogą być szybko udostępniane, duplikowane oraz wykorzystywane w interaktywnej pracy zespołowej. Stają się one dostępne dla urządzeń przechowujących określone dane, informacje i skodyfikowaną wiedzę. Praca z cyfrową treścią nie tylko przyspiesza dostęp do wiedzy i tworzenie nowej wiedzy, ale także obniża koszty (prawie do zera) i tworzy nowe możliwości dla innowacji. W ten sposób cyfryzacja i transformacja cyfrowa stają się kluczowymi czynnikami innowacyjności. Opierając się na sprzęcie i oprogramowaniu, cyfryzacja w procesie postępu cywilizacyjnego prowadzi do powstawania nowych rozwiązań technicznych i organizacyjnych, co sprzyja kreatywności i innowacyjności, przy jednoczesnym zapewnieniu odpowiedniego środowiska organizacyjnego, prawnego i kompetencyjnego[54].

Cyfryzacja bywa również rozumiana jako nieustanny proces łączenia świata rzeczywistego z wirtualnym. Taka konwergencja tworzy nowe wartości dla konsumentów, zmieniając układ sił na rynku. Ważną rolę w tym aspekcie cyfryzacji odgrywa dostęp do szybkiego Internetu, który obejmuje już nie tylko gospodarstwa domowe, instytucje i przedsiębiorstwa, ale także pojedyncze przedmioty codziennego użytku, maszyny produkcyjne, a nawet oddzielne towary przechowywane w magazynach. Przykładem technologii kształtujących dzisiejszą gospodarkę i społeczeństwo są aplikacje mobilne, przetwarzanie w chmurze, media społecznościowe, sieci czujników i duże zbiory danych. Dzięki nim gospodarka i społeczeństwo stają się "inteligentne" (ang. *smart*) – dostępne i sterowalne, wirtualne i połączone, a także angażujące i prosumenckie. W ten sposób technologie informacyjne wyszły z komputerów stacjonarnych i przeniosły się do mobilnych urządzeń obecnych niemal na każdym kroku. W konsekwencji proces cyfryzacji dotyka wszystkich sektorów gospodarki, w tym przemysłu, gdzie codzienne operacje firm coraz bardziej zależą od potrzeb i preferencji użytkowników stale przebywających w trybie „online".

Granica między wewnętrznymi procesami operacyjnymi a dynamicznym, zinformatyzowanym otoczeniem zewnętrznym staje się coraz mniej wyraźna, co wymaga od producentów ciągłego monitorowania i umiejętnego zarządzania tym otoczeniem[55].

---

[54] Ibidem, s. 9-10.

[55] K. Grzyb, *Cyfryzacja przedsiębiorstw produkcyjnych w Unii Europejskiej w perspektywie koncepcji Przemysłu 4.0*, (w:) *Innowacyjność to cyfryzacja i rozwój. Zarządzanie operacyjne w teorii i praktyce*

Cyfryzacja wywiera znaczący wpływ na środowisko informacyjne, kształtując je na wielu poziomach. W konsekwencji, zachodzą procesy i zjawiska takie jak:

- Ułatwienie dostępu do informacji: cyfryzacja umożliwia szybki i łatwy dostęp do ogromnych zasobów informacji z dowolnego miejsca na świecie. Dzięki technologiom takim jak Internet, przetwarzanie w chmurze[56] oraz mobilne aplikacje, użytkownicy mogą korzystać z informacji w czasie rzeczywistym;
- Zwiększenie przepływu informacji: technologia cyfrowa pozwala na błyskawiczne udostępnianie i wymianę informacji. To znacząco przyspiesza proces komunikacji, zarówno w życiu codziennym, jak i w sferze biznesowej i naukowej;
- Interaktywność i współpraca: narzędzia cyfrowe, takie jak media społecznościowe i platformy do współpracy online, umożliwiają interaktywne i zespołowe podejście do tworzenia i udostępniania informacji. Użytkownicy mogą współpracować na odległość, co sprzyja innowacjom i efektywności pracy zespołowej;
- Personalizacja treści: dzięki zaawansowanym algorytmom i analizie danych, cyfrowe środowisko informacyjne może dostarczać spersonalizowane treści dostosowane do indywidualnych potrzeb i preferencji użytkowników. To zwiększa efektywność przyswajania i wykorzystania informacji;
- Zwiększona przejrzystość i dostępność danych: cyfryzacja wspiera przejrzystość i dostępność danych publicznych, co wpływa na bardziej świadome podejmowanie decyzji przez obywateli oraz zwiększenie zaufania do instytucji publicznych;
- Transformacja roli mediów: tradycyjne media musiały dostosować się do nowego cyfrowego krajobrazu, co doprowadziło do zatarcia granic między różnymi formami mediów[57]. Obecnie media cyfrowe oferują różnorodne formy przekazu, co zmienia sposób konsumpcji informacji przez użytkowników;
- Zmiany ekonomiczne i społeczne: cyfryzacja wpływa na gospodarkę poprzez wprowadzanie nowych modeli biznesowych i innowacyjnych rozwiązań. Zmienia także struktury społeczne, wprowadzając nowe formy komunikacji i interakcji społecznych.

organizacji biznesowych, publicznych i pozarządowych, pod. red. L. Kowalczyka i F. Mroczko, „Prace Naukowe Wyższej Szkoły zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu", t. 43, Wałbrzych 2017, s. 89-90.

[56] Zob. M. Wyskwarski, *Przetwarzanie w chmurze z punktu widzenia małych przedsiębiorstw*, „Zeszyty Naukowe. Organizacja i Zarządzanie. Politechnika Śląska", 2014, z. 74.

[57] Zob. Katarzyna Kopecka-Piech, *Koncepcje konwergencji mediów*, „Studia Medioznawcze", 2011, nr 3.

- Wpływ na systemy edukacji: cyfrowe narzędzia edukacyjne i zasoby online zmieniają sposób, w jaki ludzie uczą się i zdobywają wiedzę[58]. Kształtują nowe kompetencje informacyjne i komunikacyjne, które są niezbędne w cyfrowym świecie;
- Zwiększenie efektywności i produktywności: automatyzacja procesów, zarządzanie danymi i inteligentne systemy wspomagają efektywność i produktywność w różnych sektorach, od przemysłu po usługi;
- Wyzwania i ryzyka: cyfryzacja niesie ze sobą również wyzwania związane z bezpieczeństwem danych, prywatnością oraz dezinformacją[59]. Z tego względu, zarówno pojedynczy użytkownicy, jak też instytucje, muszą wykazywać świadomość tych zagrożeń i podejmować odpowiednie środki zaradcze.

Omówione wyżej aspekty wskazują, że cyfryzacja znacząco przekształca środowisko informacyjne, wprowadzając zarówno liczne korzyści, jak i wyzwania, które wymagają ciągłej uwagi i adaptacji.

1.2.3. Rola bezpieczeństwa danych osobowych w erze cyfrowej

Erę cyfrową najkrócej można scharakteryzować jako: „okres historyczny cechujący się szerokim rozpowszechnieniem technologii cyfrowych w różnych aspektach działalności ludzkiej, w tym w gospodarce, polityce i wielu formach interakcji międzyludzkich. To rozpowszechnienie technologii cyfrowych skutkuje gruntowną przemianą systemów społecznych, gospodarczych i politycznych analogicznie do sposobu, w jaki silnik parowy lub elektryczność przeobraziły społeczeństwa w przeszłości”[60].

Erę cyfrową poprzedzała rewolucja cyfrowa, która polegała na gwałtownym przyspieszeniu zmian technologicznych w gospodarce, spowodowanych znacznym rozwojem zdolności do przechowywania, przetwarzania i przesyłania informacji za pomocą urządzeń elektronicznych. Choć pewne technologie i podstawy naukowe powstały już w latach 50. i 70. XX wieku, prawdziwy przełom w innowacjach i zastosowaniach technologii cyfrowych nastąpił na początku lat 70. XX wieku wraz z wynalezieniem mikroprocesora – wszechstronnego programowalnego urządzenia

[58] M. Niezgoda, *Edukacja zdalna: szansa czy zagrożenie?*, „Youth in Central and Eastern Europe”, nr 9/2022.
[59] Zob. A. Grycuk, *Fake newsy, trolle, boty i cyborgi w mediach społecznościowych*, „Analizy BAS”, 2021, nr 1.
[60] E. Fernández-Macías, *Automatyzacja, cyfryzacja i platformy: konsekwencje dla pracy i zatrudnienia*, Luksemburg 2018, s. 7.

elektronicznego do przetwarzania informacji cyfrowych. Nieustanny wzrost wydajności oraz spadek kosztów mikroprocesorów przez następne cztery dekady przyczyniły się do szybkiego upowszechnienia technologii cyfrowych, takich jak komputery osobiste, Internet i telefony komórkowe[61].

Ponieważ nowe technologie produkcji są wplecione w struktury społeczne, ich wprowadzanie początkowo napotykało na opór ze strony istniejących struktur organizacyjnych, norm kulturowych, osobistych interesów oraz uwarunkowań instytucjonalnych, które są dostosowane do już istniejących technologii produkcji. Jednak po przezwyciężeniu tego oporu, te same formy organizacyjne, interesy i instytucje mogą zacząć wspierać rozpowszechnianie i dalszy rozwój nowych technologii, które początkowo były przyjmowane z niechęcią. Czynniki technologiczne oraz społeczno-gospodarcze nadają zmianom technologicznym nieregularny rytm, podobny do zmian opisywanych chociażby przez Thomasa Kuhna w książce pt. „Struktura rewolucji naukowych" z 1962 roku[62]. W ten sposób rewolucja cyfrowa jest najnowszym przykładem serii okresowych wybuchów innowacji oraz zmian w narzędziach i metodach funkcjonujących w gospodarce. Jak wspomniano wcześniej, kluczowym czynnikiem było tutaj wynalezienie mikroprocesora i mikroczipa – technologii o wszechstronnym zastosowaniu, której koszty produkcji ciągle maleją, a możliwości stale się zwiększają. Spowodowało to pojawienie się produktów i branż o ogromnym potencjale inwestycyjnym, ale także zakłóciło istniejącą równowagę społeczno-gospodarczą. Mikroczip umożliwia tworzenie nowych form organizacji gospodarczych, które stopniowo zyskują na znaczeniu w różnych branżach i obszarach działalności, a proces ten ciągle postępuje[63].

W dobie ery cyfrowej bezpieczeństwo danych osobowych nabiera szczególnego znaczenia. W miarę jak technologia rozwija się i zbieramy coraz więcej danych w formie cyfrowej, wzrasta rola systemów ochrony tych danych. Zwiększenie się ilości przechowywanych informacji, takich jak dane o zakupach czy dane medyczne, zwiększa ryzyko ich nadużycia i kradzieży. Cybernetyczne zagrożenia (np. *phishing*, *ransomware* czy kradzież tożsamości) stały się powszechnym problemem, co czyni bezpieczeństwo danych bardziej złożonym problemem. W odpowiedzi na te wyzwania, wprowadzono przepisy prawne dotyczące ochrony danych, takie jak RODO w Unii Europejskiej czy

[61] Ibidem.
[62] Zob. T. Kuhn, *Struktura rewolucji naukowych*, tł. H. Ostromęcka, Warszawa 2009.
[63] E. Fernández-Macías, *Automatyzacja, cyfryzacja i platformy*…, s. 7-8.

CCPA w Kalifornii, które mają na celu zapewnienie odpowiedniego poziomu ochrony. Dodatkowo, bezpieczne zarządzanie danymi osobowymi stało się ważnym elementem strategii budowania i utrzymywania zaufania klientów oraz użytkowników, ponieważ incydenty związane z wyciekiem danych mogą poważnie zaszkodzić reputacji firm i instytucji[64]. W miarę jak coraz więcej usług przenosi się do Internetu, od bankowości po usługi zdrowotne, zapewnienie bezpieczeństwa danych staje się niezbędnym elementem utrzymania integralności i prywatności tych usług. W związku z tym, konieczne jest ciągłe monitorowanie, wdrażanie nowych technologii ochrony oraz przestrzeganie obowiązujących standardów i regulacji.

1.3. Społeczeństwo informacyjne a bezpieczeństwo danych osobowych

W dobie społeczeństwa informacyjnego, gdzie przepływ informacji odbywa się na niespotykaną wcześniej skalę, zagadnienia związane z bezpieczeństwem danych osobowych nabierają szczególnego znaczenia. Społeczeństwo informacyjne to rzeczywistość, w której codzienne życie, praca oraz interakcje społeczne są nierozerwalnie związane z technologiami informacyjno-komunikacyjnymi. Szeroki dostęp do Internetu, rozwój mediów społecznościowych, mobilnych aplikacji oraz systemów zarządzania danymi tworzą zarówno nowe możliwości, jak i wyzwania w kontekście ochrony prywatności. Współczesne technologie umożliwiają zbieranie, przetwarzanie i przechowywanie ogromnych ilości danych osobowych. W konsekwencji, kwestia bezpieczeństwa tych danych staje się nieodłącznym elementem funkcjonowania jednostek, firm oraz instytucji publicznych. Naruszenia prywatności i bezpieczeństwa danych mogą prowadzić do poważnych skutków, zarówno ekonomicznych, jak i społecznych.

1.3.1. Definicja społeczeństwa informacyjnego

Można powiedzieć, że współczesne polskie społeczeństwo staje się w coraz większym stopniu społeczeństwem informacyjnym. W literaturze przedmiotu terminu „społeczeństwo informacyjne" używa się do opisu wspólnot, w których informacje i technologie informacyjne odgrywają centralną rolę w życiu społecznym, gospodarczym

[64] A. Lasota-Jądrzak, *Czym grozi wyciek danych osobowych w firmie?, https://poznanrodo.pl/czym-grozi-wyciek-danych-osobowych-w-firmie* [dostęp: 29.07.2024].

i kulturalnym[65]. W takim społeczeństwie dostęp do informacji, komunikacji elektronicznej i technologii cyfrowych stanowi podstawę codziennego funkcjonowania podmiotów indywidualnych oraz rozlicznych organizacji[66]. W społeczeństwie informacyjnym obywatele mają łatwy dostęp do ogromnych ilości informacji za pośrednictwem Internetu, mediów społecznościowych, bibliotek cyfrowych oraz innych źródeł. Informacje w nich zawarte mogą być przechowywane, przetwarzane i udostępniane w sposób stosunkowo szybki i efektywny. Zapewniają to technologie informacyjne i urządzenia takie, jak komputery, smartfony, tablety czy infrastruktura telekomunikacyjna. Jak zauważa Zuboff, „Kapitalizm nadzoru jednostronnie rości sobie prawo do ludzkiego doświadczenia jako wolnego surowca do przełożenia na dane behawioralne"[67], co podkreśla nie tylko technologiczną stronę ochrony danych, ale także znaczenie ochrony prywatności w społeczeństwie informacyjnym.

We współczesnym społeczeństwie informacyjnym urządzenia tego typu są wykorzystywane do pracy, nauki albo rozrywki, ułatwiają komunikowanie się i nawiązywanie relacji interpersonalnych lub towarzyskich.

Ale społeczeństwo informacyjne jest pojęciem daleko bardziej wykraczającym poza zjawiska kulturowe. W społeczeństwie informacyjnym administracja i organizacje publiczne korzystają z technologii informacyjnych w celu usprawnienia procesów administracyjnych i organizacyjnych. W celu lepszego i efektywniejszego realizowania usług publicznych sięga się zatem po e-usługi. Wdrażanie cyfryzacji w administracji publicznej jest odbiciem współczesnych przemian technologiczno-informacyjnych, takich jak komputeryzacja, intensywny rozwój sieci internetowej czy telefonii komórkowej. Dzisiejsze społeczeństwo informatyczne, korzystające masowo z nowoczesnych technologii informacyjnych i komunikacyjnych, coraz chętniej korzysta z elektronicznej administracji i należy zakładać, że będzie to stały trend wzrostowy. Dlatego wychodząc naprzeciw oczekiwaniem i podążając z kierunkiem zmian podejmowane są działania zwiększające udział sfery IT w sektorze administracji publicznej. Cyfryzacja administracji postrzegana jest przede wszystkim jako jeden

[65] K.K. Kolin, *Information culture in the information society*, „Open Education", nr 6/2006, s. 50-51.
[66] Koncepcję społeczeństwa postprzemysłowego zaproponował na początku lat 70 XX wieku amerykański socjolog Daniel Bell [*Model społeczeństwa informacyjnego. Daniel Bell i Alvin Toffler - teoretycy społeczeństwa informacyjnego*, http://pcserwis.waw.pl/teoretycy.html (dostęp: 01.10.2023)]. Zob. R. Kluszczyński, *Społeczeństwo informacyjne. Cyberkultura. Sztuka mulimediów*, Kraków 2001.
[67] S. Zuboff, *The age of surveillance capitalism, The fight for a human future at the new frontier of power*, Profile Books, Londyn 2019, s. 35.

ze sposobów na zwiększenie efektywności sektora publicznego. Strategie wdrażania e-administracji zawarte w dyrektywach Komisji Unii Europejskiej przewidują szereg korzyści, takich jak zmniejszenie obciążenia administracyjnego przedsiębiorstw i zwykłych obywateli.[68] W porównaniu do tradycyjnej obsługi administracyjnej elektroniczne załatwianie spraw urzędowych okazuje się być szybsze, efektywniejsze, bardziej przejrzyste, wygodniejsze i tańsze zarówno z perspektywy klienta, jak i urzędu. Strategia Ministra Cyfryzacji w zakresie usług administracji publicznej zakładała już w roku 2016, że będzie ona sukcesywnie obejmowała coraz większą sferę usług w myśl zasady – każdy polski obywatel oraz przedsiębiorca powinien móc załatwić drogą elektroniczną dowolną sprawę na styku z administracją publiczną dowolnego szczebla.[69]

Pojęcie społeczeństwa informacyjnego utożsamia się niekiedy z pojęciem społeczeństwa postindustrialnego. Warto przy tym pamiętać, że społeczeństwo informacyjne i społeczeństwo postindustrialne są dwiema różnymi koncepcjami w naukach społecznych. Obie, co prawda, mają ze sobą wiele wspólnego, dlatego ich zakresy znaczeniowe często zachodzą na siebie. Mimo to określenie „społeczeństwo informacyjne" odnosi się do wspólnoty, w której informacje, technologie informacyjne i przetwarzanie danych odgrywają kluczową rolę w życiu społecznym i gospodarczym. W takim społeczeństwie informacje stanowią podstawowy zasób, a rozwój technologii komunikacyjnych i dostępu do Internetu umożliwiający łatwą wymianę informacji stanowi jego podstawową cechę. Społeczeństwo informacyjne bywa zwykle opisywane jako bardziej elastyczne i zdecentralizowane, z większym naciskiem na innowacje i wiedzę. Społeczeństwo postindustrialne, z kolei, opisuje się jako społeczeństwo, które przeszło już fazę przemysłową i opiera się na usługach, wiedzy i przetwarzaniu informacji, nie zaś na produkcji przemysłowej. Jest to etap rozwoju gospodarczego, w którym tradycyjna produkcja przemysłowa traci na znaczeniu, a gospodarka zaczyna opierać się na sektorach takich jak technologia, usługi profesjonalne, nauka, edukacja i kultura. Związek między społeczeństwem informacyjnym a społeczeństwem postindustrialnym polega na tym, że rozwijające się społeczeństwo informacyjne jest często elementem przemiany w kierunku społeczeństwa postindustrialnego. Oznacza to, że rozwijanie technologii informacyjnych, wzrost znaczenia wiedzy

[68] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Plan działania UE na rzecz administracji elektronicznej na lata 2016-2020, Przyspieszenie transformacji cyfrowej w administracji*, Bruksela 19.04.2016.
[69] *Kierunki działań strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych*, Ministerstwo Cyfryzacji 2016.

i informacji oraz zmiany w sposobie funkcjonowania gospodarki są typowe dla obu tych koncepcji. Społeczeństwo postindustrialne można uznać za jeden z etapów rozwoju społeczeństwa informacyjnego, chociaż w rzeczywistości społeczeństwa mogą istnieć na obu tych etapach rozwoju jednocześnie. Współczesne społeczeństwa rozwinięte często łączą cechy społeczeństwa informacyjnego i postindustrialnego, w zależności od dziedziny, regionu oraz dominującego sektora gospodarki.

Gospodarka współczesnych rozwiniętych państw – mamy tu na myśli przede wszystkim państwa Unii Europejskiej, USA, Kanadę, Japonię, Koreę Południową, Izrael, Australię, Nową Zelandię, Zjednoczone Emiraty Arabskie i inne – są w coraz większym stopniu związane z procesami wymiany danych, rozwojem technologii cyfrowych i e-handlem. Firmy różnych branż sięgają po technologie informatyczne w procesie zarządzania produkcją, w trakcie kampanii marketingowych, obsługi klienta oraz w wielu innych formach swojej działalności, w tym wymiany międzynarodowej[70]. Nowoczesne technologie przetwarzania informacji pozwalają bowiem wielu przedsiębiorstwom usługowym funkcjonować na dwóch podstawowych płaszczyznach: rzeczywistej i wirtualnej. Umiejętność ich połączenia w jednej strategii działania pozwala przedsiębiorstwu zdobyć przewag nad konkurencją.[71]

Społeczeństwo informacyjne rozwija edukację online, o czym mogliśmy się przekonać w trakcie pandemii Covid-19. Dostęp do zasobów edukacyjnych w sieci, który od chwili zainicjowania Internetu, dla naukowców z całego świata oznacza zdecydowanie łatwiejszy dostęp do globalnej bazy informacji naukowych, publikacji naukowych oraz wspomaga współpracę i rozwój ośrodków naukowych na międzynarodową skalę.

Oczywistym stało się dzisiaj, że technologie informacyjne zmieniły sposób, w jaki ludzie korzystają z kultury i rozrywki[72]. Strumieniowanie muzyki i filmów, gry wideo online oraz media społecznościowe stały się częścią życia kulturalnego i świata rozrywki współczesnego człowieka.

Jeśli niespotykane wcześniej możliwości koncentracji, a także kojarzenia danych znajdujących się w rozmaitych, rozproszonych, rozbudowanych i przewidzianych dla odmiennych celów zbiorów danych[73] znajdują się w użytku, należy liczyć się

[70] K.K. Kolin, *Information culture…*, s. 50-51.
[71] J. Buko, *Wprowadzenie do zarządzania informacją w przedsiębiorstwach usługowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego", nr 650, 2011, s. 14.
[72] Ibidem.
[73] K. Celarek, *Ochrona danych osobowych a rozwój społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego", nr 703, 2012, s. 722.

z wystąpieniem nadużyć. Dlatego korzystanie z informacji wymaga odpowiednich regulacji i strategii zarządzania, tak, aby potencjał technologii informacyjnych stawał się zrównoważony i pożyteczny dla człowieka, a nie szkodliwy i niebezpieczny. Wiąże się to z wieloma wyzwaniami, jednym z nich jest ochrona prywatności i bezpieczeństwo cybernetyczne („bezpieczeństwo w sieci"), całkowite wyeliminowanie lub w dużym stopniu ograniczenie nadużyć związanych z wyciekiem danych czy dezinformacją. Odrębną kwestią jest bezpieczeństwo cybernetyczne państwa, o czym piszemy więcej w kolejnym podrozdziale. Wobec zagrożeń cybernetycznych konieczne jest przyjęcie aktywnej postawy, proporcjonalnie do tego im w większym stopniu zdajemy sobie sprawę z wielkich możliwości nowego cyfrowego świata, jak też z ogromu pojawiających się zagrożeń, dlatego „Obowiązkiem świadomych uczestników dokonujących się przemian jest tworzenie takich mechanizmów, które pozwolą na wzmocnienie pozytywnych zjawisk i osłabienie negatywnych oddziaływań tak, aby przyszłe pokolenia nie mogły postawić nam zarzutu, że nie sprostaliśmy wyzwaniom dziejów i dopuściliśmy do zniewolenia ludzkości na niewyobrażalną skalę"[74].

Powyższe nakreślone tendencje rozwoju społeczeństwa informacyjnego dotyczą także Polski. Jak podaje Główny Urząd Statystyczny odsetek Polek i Polaków korzystających z technologii informatycznych systematycznie rośnie[75], a dostęp do szerokopasmowego Internetu staje się coraz powszechniejszy, zarówno w miastach, jak też na obszarach wiejskich. Jednostki samorządu terytorialnego wykorzystują technologie informacyjne do usprawnienia procesów administracyjnych i dostarczania usług publicznych online[76]. Polska staje się także rozwijającym się ośrodkiem dla branży technologicznej i informatycznej, a liczba firm działających w tej dziedzinie stale rośnie. Polskie uczelnie i placówki edukacyjne oferują coraz więcej kursów online i zasobów edukacyjnych w sieci[77]. Na terenie naszego kraju dynamicznie rozwijają się poszczególne gałęzie e-commerce, a klienci coraz częściej dokonują zakupów online[78]. Z tego względu można śmiało powiedzieć, że Polska dołączyła do globalnego społeczeństwa

[74] Ibidem.
[75] Zob. Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce w 2021 roku*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,2,11.html [dostęp: 02.10.2023].
[76] Zob. Ministerstwo Cyfryzacji, *E-usługi w administracji*, https://www.gov.pl/web/cyfryzacja/e-uslugi [dostęp: 02.10.2023].
[77] Por. *Studia online w Warszawie 2023*, https://www.otouczelnie.pl/miasto_dzial/11663/Studia-online-w-Warszawie [dostęp: 02.10.2023].
[78] ISBnews, *W 2022 roku Polacy znów chętniej korzystali z zakupów online [RAPORT]*, https://forsal.pl/biznes/handel/artykuly/8663815,ecommerce-opinionway-barometr.html [dostęp: 02.10.2023].

informacyjnego, chociaż nie w takim stopniu jak np. Japonia, Korea Południowa, Wielka Brytania czy Niemcy, zwłaszcza w sferze dostępu do edukacji online, innowacyjności w dziedzinie technologii, poziomu wykorzystania technologii, jakości infrastruktury telekomunikacyjnej i innych[79]. Jak zauważa Wojciech Traczyk, „Innowacje oraz badania i rozwój pozytywnie wpływają na postęp technologiczny, przyczyniając się do wzrostu produktywności, a tym samym wzrostu gospodarczego. W Polsce jednak ten czynnik w niewielkim stopniu wspomaga rozwój gospodarczy kraju. Jak wynika z danych Komisji Europejskiej z 2021 r., Polska plasuje się pod tym względem za większością europejskich państw (wyprzedza jedynie Rumunię, Bułgarię i Łotwę). Badanie Community Innovation Survey 2018 wykazało, że tylko 22% polskich firm innych niż mikro było innowacyjnych – co jest drugim najgorszym wynikiem w UE”[80]. Nie zmienia to generalnie wzrostu znaczenia danych osobowych oraz konieczności ich ochrony, a nawet więcej, można powiedzieć, że im większy rozwój technologiczny, tym dane są lepiej chronione. Stawia to przed polską administracją publiczną dodatkowe wyzwania, wynikające z nadrabiania zaległości.

1.3.2. Wpływ społeczeństwa informacyjnego na konieczność ochrony danych osobowych

Przyjrzyjmy się teraz dlaczego dane osobowe w społeczeństwie informacyjnym są tak cenne. Otóż dlatego, że bezpieczeństwo danych osobowych związane jest z wieloma dziedzinami życia indywidualnego i społecznego, które krzyżują się z sobą tworząc sieć wzajemnych powiązań. Spróbujmy wyszczególnić te obszary:

- prywatność: dane osobowe są związane z prywatnością jednostek. Każdy ma prawo do zachowania swojej prywatności, a dostęp do osobistych informacji bez zgody może naruszyć to prawo;
- bezpieczeństwo finansowe: dane finansowe, a więc numery kont bankowych lub informacje o kartach kredytowych są często wykorzystywane przez przestępców do kradzieży tożsamości i oszustw finansowych[81]. Chronienie tych informacji jest kluczowe dla uniknięcia strat finansowych;

[79] W. Traczyk, *Niezbędne inwestycje w poprawę produktywności*, https://magazyn przemyslowy.pl/artykuly/ niezbedne-inwestycje-w-poprawe-produktywnosci [dostęp: 02.10.2023].
[80] Ibidem.
[81] D. Wroczyński, *Co robić w przypadku kradzieży tożsamości?*, KPP w Wyszkowie, https://mazowiecka.policja.gov.pl/wwy/aktualnosci/50393,Co-zrobic-w-przypadku-kradziezy-tozsamosci.html [dostęp: 02.10.2023].

- bezpieczeństwo osobiste: dane osobowe mogą być używane do stalkingu,[82] nadużyć lub innych działań, które w sposób pośredni lub bezpośredni zagrażają bezpieczeństwu fizycznemu i/lub psychicznemu jednostek[83];
- zapobieganie dyskryminacji: niektóre dane osobowe, np. informacje o rasie, religii, orientacji seksualnej lub stanu zdrowia mogą być wykorzystywane do dyskryminacji lub prześladowania. Ochrona tych informacji może pomóc w zapobieganiu takim praktykom;
- zapobieganie przestępstwom na tle finansowym, takim jak kradzież tożsamości, oszustwa bankowe i cyberprzestępstwa, których warunkiem jest uzyskanie dostępu do danych osobowych[84]. Ochrona danych osobowych stanowi element zapobiegawczy i jest kluczowa w walce z tymi przestępstwami;
- respektowanie obowiązujących przepisów prawnych: obowiązujące przepisy i regulacje dotyczące ochrony danych osobowych, wymagają od podmiotów prawnych przestrzegania określonych standardów w zakresie zbierania, przetwarzania i przechowywania danych osobowych. Naruszenie tych przepisów może prowadzić do poważnych konsekwencji prawnych[85];
- budowanie zaufania i reputacji: organizacje, które dbają o prywatność danych osobowych swoich klientów i pracowników, zyskują ich zaufanie i budują pozytywną reputację. Z kolei zaniedbania w zakresie ochrony danych mogą prowadzić do utraty zaufania klientów oraz pracowników i w rezultacie wpłynąć negatywnie na reputację danej firmy;
- cyberbezpieczeństwo – utrzymanie odpowiednich standardów ochrony wrażliwych informacji pomaga zapobiegać naruszeniom bezpieczeństwa i wyciekom informacji, mogących znacząco wpłynąć na bezpieczeństwo infrastruktury krytycznej państwa, funkcjonowanie struktur i organów państwowych, naruszać ład publiczny, obniżać

[82] Z ang. *stalker* – natręt, osoba śledząca, podkradająca się; stalking jest jednym z najnowszych przestępstw zdefiniowanych w polskim prawie karnym, wprowadzonym w ustawie 25 lutego 2011r. Stalking definiuje się jako fizyczne lub wirtualne zbliżanie się do osoby (prześladowanej), natrętne komunikowanie się z nią wbrew jej woli, formułowanie gróźb, składanie niepożądanych propozycji, deklaracji, często także nachodzenie rodziny lub bliskich; podglądanie, śledzenie, obserwowanie miejsca zamieszkania lub pracy, itp. Inaczej stalking bywa określany mianem „nękania". Warto zauważyć, że ta forma przestępstwa może mieć wyłącznie formę wirtualną. W praktyce często stalker inicjuje swoje działania za pośrednictwem teleinformacyjnym np. przez telefon lub Internet.
[83] W. Buczkowska, *Stalking – co to jest stalking, aspekty prawne nękania, jak się bronić przed prześladowcą?*, https://portal.abczdrowie.pl/stalking [dostęp: 02.10.2023].
[84] P. Więckiel, *Cyberprzestępczość – czym jest i jak się przed tym bronić?*, https://fundacja.togatus.pl/cyberprzestepczosc-czym-jest-i-jak-sie-przed-tym-bronic/ [dostęp: 02.10.2023].
[85] Zob. *Kary za naruszenie RODO*, https://gdpr.pl/artykuly/kary-za-naruszenie-rodo [dostęp: 02.10.2023].

standardy życia, wprowadzać chaos i dezinformację, sprzyjać działaniom sabotażowym, przestępczym itp.

1.4. Reprezentatywność i umiejscowienie ochrony danych osobowych w naukach o bezpieczeństwie

Reprezentatywność i zakotwiczenie problematyki ochrony danych osobowych w naukach o bezpieczeństwie to dość złożone zagadnienie. Z tego względu należałoby zacząć je od bardziej fundamentalnych rozważań, czyli zastanowić się nie tylko nad tym, czym są nauki o bezpieczeństwie, ale również nad tym, czym jest nauka w ogóle.

Nauka, jako systematyczna działalność ludzka mająca na celu poznawanie rzeczywistości, opiera się na metodach badawczych, eksperymentach i weryfikacji hipotez. Jest to proces nieustannego poszukiwania wiedzy, który pozwala na zrozumienie i wyjaśnienie zjawisk zachodzących w świecie. Nauka dąży do obiektywności i powtarzalności wyników, co leży u podstaw jej wiarygodności i użyteczności. W jej ramach rozwijają się różne dziedziny, z których każda posiada swoje własne metody i narzędzia badawcze, a także specyficzne przedmioty badań.

Istnieje wiele definicji nauki, co wynika z różnych perspektyw badawczych, metodologicznych, filozoficznych a nawet światopoglądowych. Na potrzeby niniejszych rozważań można przytoczyć definicję Juliusza Piwowarskiego, zgodnie z którą: „Nauka jest to dziedzina kultury, która posiada badawczy charakter i łączy się ze społecznie oczekiwanymi efektami dociekań naukowych, które prowadzą uczeni; naukę tworzą:

- zespół twierdzeń i hipotez odnoszących się do badanej rzeczywistości, jej cech i rządzących nią praw;
- teorie naukowe zbudowane na podstawie w/w twierdzeń i hipotez, które dotyczą rzeczywistości i z mocy prawa mają usytuowanie instytucjonalne w obszarach, dziedzinach, dyscyplinach i specjalnościach naukowych”[86].

Piwowarski przytacza również własną definicję teorii. Według niej: „teoria jest to spójny system myślowy, oparty na zbiorze pojęć, definicji, aksjomatów i twierdzeń, pozwalających ustalić jakie są relacje pomiędzy tymi pojęciami i aksjomatami, ukazującymi wybraną, materialną lub abstrakcyjną sferę rzeczywistości”[87].

[86] J. Piwowarski, *Nauki o bezpieczeństwie. Zagadnienia elementarne*, Kraków 2017, s. 9.
[87] Ibidem.

Z powyższych definicji, zdaniem Piwowarskiego, wynika, że poważne zaangażowanie w naukę oraz związany z nią aparat teoretyczny wymaga od badacza posiadania wiedzy, która umożliwia mu rozwinięcie określonej świadomości metodologicznej. Zajmowanie się nauką, choćby w minimalnym stopniu, zobowiązuje nie tylko zawodowych naukowców, ale również każdą osobę wykształconą na uczelni, do posiadania klarowności w zakresie przemyślenia i samodzielnego formułowania podstawowych założeń naukowych o filozoficznym podłożu, które, choć nie są dowodzone, stanowią niezbędne warunki wstępne dla rozpoczęcia procesu badań naukowych[88].

Nauka nie jest tworem homogenicznym. Dzieli się ona na wiele wyspecjalizowanych rodzajów, dziedzin czy dyscyplin. Podstawą wszelkich klasyfikacji nauk są kryteria przedmiotowe, czyli przedmiot badań oraz kryteria metodologiczne, które uwzględniają różnice w metodach badawczych poszczególnych dyscyplin. Dodatkowo, klasyfikacje te są silnie uzależnione od celów, którym mają służyć. Jak podkreślają Jan Such i Małgorzata Scześniak:

„Schematy klasyfikacji nauk są zawsze zrelatywizowane do konkretnych zadań. Stąd konieczne jest uświadomienie sobie przez uczonego (historyka nauki, metodologa) celu prowadzonej klasyfikacji nauk. Może być ona przeprowadzona np. z punktu widzenia celów badawczych, polityki (strategii) badań naukowych, należytego przekazywania wiedzy naukowej nowym pokoleniom, funkcji pełnionych przez naukę w społeczeństwie, potrzeb dydaktyki czy bibliotekoznawstwa. Dla przykładu, w bibliotekoznawstwie po dziś dzień szeroko jest stosowany „system dziesiętny", zgodnie z którym całe piśmiennictwo (łącznie z literaturą piękną) dzielone jest na dziesięć działów"[89].

Aby zilustrować powyższe twierdzenie, warto przytoczyć dwa przykłady, czyli dychotomiczny podział nauk na nauki formalne i empiryczne oraz państwową klasyfikację dziedzin nauki i dyscyplin naukowych oraz dyscyplin, która obowiązuje w Polsce od roku 2022.

Podział nauk na formalne i empiryczne uznawany jest za jedną z najważniejszych klasyfikacji metodologicznych. Zgodni z nią, nauki empiryczne, zwane także doświadczalnymi, bazują na obserwacjach zmysłowych, doświadczeniach i analizie danych uzyskanych poprzez zmysły. Przede wszystkim są to nauki przyrodnicze

[88] Ibidem, s. 9-10.
[89] J. Such, M. Szcześniak, *Filozofia nauki*, Poznań 1999, s. 47.

(np. fizyka, chemia, biologia) oraz nauki społeczne (np. psychologia i socjologia). Natomiast nauki formalne opierają się na logice, matematyce i abstrakcyjnych modelach, zajmując się strukturami, wzorcami oraz abstrakcyjnymi relacjami, które nie muszą mieć związku z doświadczeniami zmysłowymi (np. matematyka i logika)[90].

Powyższy podział ma charakter metodologiczny. Z kolei polska klasyfikacja nauk z roku 2022 ma charakter administracyjny. Opiera się on na dwustopniowym, hierarchicznym podziale na dziedziny (czyli obszary szersze) oraz dyscypliny (czyli obszary węższe). Wyróżnia się tutaj dziesięć dziedzin, a w ich ramach, łącznie, wyszczególniono kilkadziesiąt dyscyplin:

- Dziedzina nauk humanistycznych. Dyscypliny: archeologia, etnologia i antropologia, kulturowa, filozofia, historia, językoznawstwo, literaturoznawstwo, nauki o kulturze i religii, nauki o sztuce, polonistyka;
- Dziedzina nauk inżynieryjno-technicznych. Dyscypliny: architektura i urbanistyka, automatyka, elektronika, elektrotechnika i technologie kosmiczne, informatyka techniczna i telekomunikacja, inżynieria bezpieczeństwa, inżynieria biomedyczna, inżynieria chemiczna, inżynieria lądowa, geodezja i transport, inżynieria materiałowa, inżynieria mechaniczna, inżynieria środowiska, górnictwo i energetyka, ochrona dziedzictwa i konserwacja zabytków;
- Dziedzina nauk medycznych i nauk o zdrowiu. Dyscypliny: biologia medyczna, nauki farmaceutyczne, nauki medyczne, nauki o kulturze fizycznej, nauki o zdrowiu.
- Dziedzina nauk o rodzinie. Dyscypliny: nauki o rodzinie;
- Dziedzina nauk rolniczych. Dyscypliny: nauki leśne, rolnictwo i ogrodnictwo, technologia żywności i żywienia, zootechnika i rybactwo;
- Dziedzina nauk społecznych. Dyscypliny: ekonomia i finanse, geografia społecznoekonomiczna i gospodarka przestrzenna, nauki o bezpieczeństwie, nauki o komunikacji społecznej i mediach, nauki o polityce i administracji, nauki o zarządzaniu i jakości, nauki prawne, nauki socjologiczne, pedagogika, prawo kanoniczne, psychologia, stosunki międzynarodowe;
- Dziedzina nauk ścisłych i przyrodniczych. Dyscypliny: astronomia, biotechnologia, informatyka, matematyka, nauki biologiczne, nauki chemiczne, nauki fizyczne, nauki o Ziemi i środowisku;
- Dziedzina nauk teologicznych. Dyscypliny: nauki biblijne, nauki teologiczne;

[90] Ibidem, s. 52.

- Dziedzina nauk weterynaryjnych. Dyscypliny: weterynaria;
- Dziedzina sztuki. Dyscypliny: sztuki filmowe i teatralne, sztuki muzyczne, sztuki plastyczne i konserwacja dzieł sztuki[91].

Powyższy podział jest szczególnie istotny z perspektywy niniejszych rozważań, bowiem w jego ramach wyróżnia się dyscyplinę nauk o bezpieczeństwie (w ramach dziedziny nauk społecznych). Nauki o bezpieczeństwie to interdyscyplinarna dziedzina, która koncentruje się na analizie zagrożeń i ryzyk, a także na opracowywaniu strategii i metod ochrony przed nimi. Zakres nauk o bezpieczeństwie obejmuje zarówno aspekty militarne i polityczne, jak i kwestie związane z bezpieczeństwem społecznym, ekonomicznym, ekologicznym oraz technologicznym. W kontekście dynamicznie zmieniającego się świata, w którym technologia odgrywa coraz większą rolę, problematyka ochrony danych osobowych staje się jednym z centralnych obszarów badań w tej dziedzinie[92].

W Polsce, nauki o bezpieczeństwie formalnie zostały wyodrębnione za sprawą *rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 roku, który dotyczył obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych* jako jedna z dyscyplin w dziedzinie nauk społecznych[93]. Jak zauważa Ewa Pogorzała: „W literaturze przedmiotu uznawano, że nauki o bezpieczeństwie stanowią w głównej mierze spuściznę nauk wojskowych oraz nauki o stosunkach międzynarodowych, ale podnoszono także problem, czy powinna to być dyscyplina czy raczej dziedzina naukowa grupująca nauki o bezpieczeństwie i jako taka powinna być wyodrębniona jako osobna dziedzina obok nauk społecznych, nie zaś jedna z dyscyplin w ramach nauk społecznych. Zmiany te spowodowały intensywną dyskusję w środowisku naukowym dotyczącą statusu dyscypliny i zasadności wprowadzonych modyfikacji. Istotna okazała się również kwestia stosunku do zachodnich studiów bezpieczeństwa (*security studies*), a w kontekście polskim także usytuowanie względem nauk o polityce”[94].

[91] Rozporządzenie Ministra Edukacji i Nauki z dnia 11 października 2022 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych, Dz.U. 2022 poz. 2202.
[92] Zob. M. Lutosański, *Idea wyodrębnienia dyscypliny naukowej „nauki o bezpieczeństwie” i jej konsekwencje*, „Historia i Polityka”, 2018, nr 25.
[93] Zob. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. 2011, poz. 1065).
[94] E. Pogorzała, *Status dyscypliny „nauki o bezpieczeństwie” a wyzwania nauczania przedmiotów metodologicznych – wstępny zarys problemu*, „Polityka i Społeczeństwo”, 2023, nr 1/21, s. 248-249.

Znaczenie bezpieczeństwa oraz badań nad tą problematyką wzrosło obecnie do niespotykanego wcześniej poziomu, a skala i intensywność niektórych zagrożeń osiągnęły bezprecedensowe rozmiary. W związku z tym współczesne państwa i ich elity wykazują coraz większe zainteresowanie wynikami badań dotyczących bezpieczeństwa. Badania te są niezwykle ważne w aspekcie prakseologicznym, który jednak nie może istnieć bez udziału teorii, niezbędnej z perspektywy nauk społecznych. Dotyczy to dziedzin interdyscyplinarnie łączących osiągnięcia nauk o bezpieczeństwie i studiów bezpieczeństwa. Obecnie szczególnie aktywnie rozwijają się badania nad kulturą bezpieczeństwa[95].

Niezwykle ważnym przedmiotem badań w ramach nauk o bezpieczeństwie jest kategoria zagrożenia. Piwowarski zaproponował następującą typologię zagrożeń:

- zagrożenia militarne;
- zagrożenia polityczne;
- zagrożenia społeczno-kulturowe, wynikające ze świadomości oraz tożsamości narodowej zarówno w wymiarze indywidualnym, jak i zbiorowym;
- zagrożenia ekonomiczne, obejmujące sferę gospodarki i finansów;
- zagrożenia prawno-administracyjne, wynikające z wadliwego stanowienia prawa, niespójności przepisów, nadmiaru regulacji, biurokratyzmu, opresyjności i arogancji urzędników;
- zagrożenia ekologiczne;
- zagrożenia związane z zasobami, obejmujące surowce dla przemysłu wytwórczego, surowce paliwowo-energetyczne oraz wodę i żywność;
- zagrożenia technogenne;
- zagrożenia cybernetyczne;
- zagrożenia zdrowotne i socjalne[96].

Dość interesujące wnioski nasuwają się w przypadku, gdy odniesiemy kwestię zagrożeń bezpieczeństwa danych osobowych do powyższej typizacji, bowiem tego rodzaju dane stanowią integralną część wielu procesów i systemów, na których opiera się współczesne społeczeństwo. W związku z tym ich nieodpowiednie wykorzystanie niesie za sobą poważne ryzyko, co można prześledzić na przykładzie konkretnych zagrożeń:

[95] J. Piwowarski, *Nauki o bezpieczeństwie. Zagadnienia elementarne*…, s. 8.
[96] Ibidem, s. 35-36.

- Zagrożenia militarne: bezpieczeństwo danych osobowych jest kluczowe w kontekście obrony narodowej i działalności wywiadowczej. Ujawnienie poufnych informacji może mieć poważne konsekwencje dla bezpieczeństwa militarnego;
- Zagrożenia polityczne: dane osobowe mogą być wykorzystywane do wpływania na procesy polityczne, np. przez kampanie dezinformacyjne czy manipulacje wyborcze. Naruszenia prywatności mogą również prowadzić do szantażu polityków;
- Zagrożenia społeczno-kulturowe: naruszenia danych osobowych mogą wpływać na tożsamość narodową i świadomość społeczną, na przykład poprzez kradzież tożsamości lub naruszanie prywatności w mediach społecznościowych;
- Zagrożenia ekonomiczne: bezpieczeństwo danych osobowych odgrywa znaczącą rolę w funkcjonowaniu gospodarki. Naruszenia mogą prowadzić do strat finansowych dla firm i jednostek, kradzieży tożsamości klientów, oszustw finansowych oraz utraty zaufania konsumentów;
- Zagrożenia prawno-administracyjne: naruszenia danych mogą wynikać z niedoskonałości prawa ochrony danych, niespójności regulacji czy biurokratycznych opóźnień w implementacji odpowiednich środków ochrony;
- Zagrożenia ekologiczne: naruszenia danych mogą wpływać na zarządzanie kryzysowe w sytuacji klęsk ekologicznych;
- Zagrożenia surowcowe: bezpieczeństwo danych osobowych może mieć wpływ na zarządzanie zasobami, np. w sektorze energetycznym, gdzie dostęp do danych jest ważny dla efektywnego zarządzania;
- Zagrożenia technogenne: bezpieczeństwo danych osobowych jest bezpośrednio związane z zagrożeniami technologicznymi, takimi jak cyberataki, które mogą prowadzić do kradzieży danych;
- Zagrożenia cybernetyczne: są one najbliżej związane z bezpieczeństwem danych osobowych. Cyberataki, hacking, phishing i inne formy cyberprzestępczości bezpośrednio zagrażają prywatności i bezpieczeństwu danych osobowych;
- Zagrożenia zdrowotne i socjalne: naruszenia danych osobowych mogą wpływać na zdrowie i bezpieczeństwo socjalne, na przykład przez kradzież danych medycznych lub socjalnych, co może pociągać za sobą ryzyko niewłaściwego leczenia lub oszustw w systemach opieki społecznej.

Powyższe zestawienie pokazuje, że w dobie cyfryzacji i globalizacji, ochrona danych osobowych stała się jednym z kluczowych elementów bezpieczeństwa

współczesnych społeczeństw. W naukach o bezpieczeństwie, ochrona ta jest nie tylko przedmiotem badań, ale również fundamentem strategii i polityk mających na celu zapewnienie stabilności i integralności systemów informacyjnych. Reprezentatywność ochrony danych osobowych oznacza, że muszą one być traktowane z najwyższą uwagą i precyzją, odzwierciedlając różnorodne zagrożenia i wyzwania stojące przed współczesnym światem.

Umiejscowienie problematyki ochrony danych osobowych w ramach nauk o bezpieczeństwie wymaga interdyscyplinarnego podejścia, które łączy w sobie aspekty prawne, technologiczne i organizacyjne. Prawo o ochronie danych osobowych, takie jak RODO w Unii Europejskiej, stanowi fundament tych działań, określając ramy prawne i standardy, które muszą być przestrzegane przez organizacje i instytucje. Jednocześnie, technologie informacyjne i komunikacyjne usprawniają proces implementacji tych zasad, oferując narzędzia i rozwiązania do zabezpieczania danych oraz monitorowania ich przetwarzania.

Ważnym aspektem ochrony danych osobowych jest również edukacja i świadomość społeczna. Zrozumienie przez jednostki znaczenia ochrony swoich danych oraz znajomość przysługujących im praw jest niezbędne do skutecznego funkcjonowania systemów ochrony danych. W tym kontekście, nauki o bezpieczeństwie pełnią rolę nie tylko w badaniu i rozwoju technologii ochronnych, ale również w promowaniu kultury bezpieczeństwa i odpowiedzialności za dane osobowe wśród obywateli.

Kolejnym istotnym wyzwaniem jest dynamiczny rozwój technologii, takich jak sztuczna inteligencja, Internet rzeczy (IoT)[97] czy blockchain[98], które z jednej strony oferują nowe możliwości, a z drugiej strony wprowadzają nowe zagrożenia i komplikacje związane z ochroną danych osobowych. Naukowcy i praktycy z zakresu bezpieczeństwa muszą stale adaptować swoje podejścia i strategie, aby sprostać tym zmieniającym się warunkom, co wymaga ciągłego monitorowania trendów technologicznych oraz aktualizacji norm i procedur ochrony danych.

[97] E. M. Kwiatkowska, *Rozwój Internetu rzeczy – szanse i zagrożenia*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" , 2014, nr 8(3), s. 61-62.
[98] Zob. H. Dikariev, M. Miłosz, *Technologia blockchain i jej zastosowania*, „Journal of Computer Sciences Institute", 2018, Vol. 6.

1.5. Bezpieczeństwo danych osobowych a inne dyscypliny naukowe

O interdyscyplinarności problematyki bezpieczeństwa danych osobowych przesądza fakt, iż może ona być badana w ramach różnych dyscyplin naukowych. W poprzednim podrozdziale przedstawiliśmy umiejscowienie tego zagadnienia w naukach o bezpieczeństwie. Jednakże warto przyjrzeć się temu zagadnieniu z perspektywy innych nauk.

Problem ochrony danych osobowych z perspektywy nauk prawnych

Dyscyplina nauk prawnych, znana również jako prawo lub nauki prawne, zajmuje się badaniem systemów prawa, instytucji prawnych oraz procesów legislacyjnych i sądowych. Obejmuje ona szeroki zakres zagadnień, a niektóre z nich to: prawo konstytucyjne[99], prawo cywilne[100], prawo karne[101], prawo administracyjne[102], prawo handlowe[103], prawo międzynarodowe[104], prawo pracy[105], prawo rodzinne[106], prawo podatkowe[107]. Na płaszczyźnie ogólnych nauk prawnych analizuje się również formalne i praktyczne aspekty zjawisk związanych z prawem, wykorzystując teorię prawa, filozofię prawa oraz rozwija się metodologię nauk prawnych[108]. Nauki prawne charakteryzują się cechami, które nadają im swoistą specyfikę. Przede wszystkim, są one interdyscyplinarne, łączące w sobie elementy z różnych dziedzin wiedzy, takich jak filozofia, socjologia, ekonomia czy historia[109]. Dynamiczność stanowi kolejny istotny aspekt nauk prawnych. Prawo podlega ciągłym zmianom i adaptacji do zmieniających się warunków społecznych, gospodarczych, politycznych i technologicznych[110]. Ważną cechą, o której warto również wspomnieć, to interpretacyjny charakter

[99] Por. S. Bożyk, *Prawo konstytucyjne*, Białystok 2014, s. 17-18.
[100] Zob. P. Kubiński, A. Wołoszko, *Wybrane zagadnienia prawa cywilnego. Stan prawny na 1 lipca 2012 r.*, Szczytno 2012.
[101] Zob. J. Lachowski, A. Marek, *Prawo karne. Zarys problematyki*, Warszawa 2021.
[102] Por. J. Frąckowiak, *Miejsce prawa handlowego w systemie prawa i sposoby jego regulacji*, Acta Universitatis Wratslaviensis, „Przegląd Prawa i Administracji CXXI", Wrocław 2020.
[103] Zob. S. Muras, *Podstawy prawa*, Warszawa 2017, s. 339.
[104] Por. J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2014, s. 1-2.
[105] Por. L. Florek, *Prawo pracy*, Warszawa 2015, s. 4-6.
[106] Por. J. Strzebinczyk, *Prawo rodzinne*, Warszawa 2013, s. 21.
[107] Zob. R. Mastalski, *Prawo podatkowe*, Warszawa 2018, s. 19.
[108] *Nauki prawne,* https://usosirk.amu.edu.pl/pl/offer/SD-2023/programme/SD-NP/?from=field:DS010507N [dostęp: 13.3.2024].
[109] Por. J. Łakomy, *Interdyscyplinarność i integracja zewnętrzna nauk prawnych w świetle postmodernistycznej krytyki*, „Archiwum Filozofii Prawa i Filozofii Społecznej", nr 1/2011.
[110] M. Pogłód, *Prawo pracy: dynamiczne czy statyczne?*, https://www.prawo.pl/prawnicy-sady/prawo-pracy-dynamiczne-czy-statyczne,27858.html [dostęp: 20.3.2024].

naukowego dyskursu prawnego[111]. Istnieje wiele różnych perspektyw odczytywania i stosowania przepisów prawnych, co prowadzi do różnorodnych interpretacji.

Ochrona danych osobowych stanowi ważny przedmiot nauk prawnych dlatego, że jest ona ściśle uregulowana w wielu jurysdykcjach na całym świecie. W Unii Europejskiej, ogólne rozporządzenie o ochronie danych (RODO) stanowi kluczową podstawę prawną dla ochrony danych osobowych[112]. Kraje nie należące do UE także mają swoje własne ustawy i regulacje dotyczące ochrony danych osobowych[113]. Badacze prawa mogą analizować te przepisy, interpretować je, wyciągać wnioski dotyczące konkretnych obowiązków, jakie nakładają na organy samorządu terytorialnego w zakresie ochrony danych.

Problem ochrony danych osobowych z perspektywy nauk technicznych

Na obecnym etapie rozwoju cywilizacyjnego nie sposób zapewnić skutecznej ochrony danych osobowych przez organy samorządu terytorialnego bez nowoczesnych technologii. Organy samorządu terytorialnego muszą dbać o to, aby ich systemy informatyczne były odporne na ataki i nieuprawniony dostęp do danych osobowych. Technologie związane z bezpieczeństwem informatycznym obejmują zabezpieczenia takie jak firewalle[114], systemy wykrywania intruzów[115], filtry antyspamowe[116], oraz procedury monitorowania i reagowania na rozliczne incydenty.

Ochrona danych osobowych związana jest z takimi dziedzinami wiedzy, jak kryptografia (nauka o zabezpieczaniu danych za pomocą szyfrów). Organy samorządu terytorialnego mogą korzystać z programów, pozwalających na skuteczne szyfrowanie danych w trakcie ich przechowywania i przesyłania. W tym celu wykorzystuje się technologie kryptograficzne, takie jak szyfrowanie SSL/TLS

[111] M. Sewastianowicz, *Rodzaje wykładni prawa*, https://www.prawo.pl/student/rodzaje-wykladni-prawa,500020.html [dostęp: 20.3.2024].
[112] *Czego dotyczy ogólne rozporządzenie o ochronie danych (RODO)?*, https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pl [dostęp: 20.10.2023].
[113] Zob. MQX Polska Sp. z o.o., *Prawo do prywatności i ochrona danych osobowych w USA*, https://ochronasygnalistow.com.pl/baza-wiedzy/prawo-prywatnosci-i-bezpieczenstwa-danych-w-usa/ [dostęp: 20.20.2023].
[114] Zob. *Co to jest firewall? Jak działa zapora sieciowa?*, https://bezpiecznyinternet.edu.pl/co-to-jest-firewall-i-jak-dziala/ [dostęp: 20.10.2023].
[115] W. Sikora-Kobyliński, *Czym są IDS?*, https://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html [dostęp: 20.10.2023].
[116] Zob. *Filtry antyspamowe,* https://www.i-host.pl/pomoc/pl/poczta_elektroniczna/filtry_antyspamowe [dostęp: 20.10.2023].

na stronach internetowych[117], a także narzędzia kryptograficzne do zabezpieczania przechowywanych danych[118]. Wdraża się także systemy zarządzania danymi, które pozwalają na kontrolowanie dostępu do danych, monitorowanie ich używania i śledzenie operacji na danych. Systemy te pomagają w egzekwowaniu polityk ochrony danych i zapewnieniu, że tylko upoważnione osoby mają do nich dostęp.

W dzisiejszych czasach istnieje wiele narzędzi i rozwiązań technologicznych, które pomagają w zabezpieczaniu poufności danych osobowych. Do tych narzędzi należą m.in. rozszerzenia przeglądarek internetowych wspierające blokowanie śledzenia (takie jak rozszerzenie AdBlock Plus[119]), narzędzia do zarządzania hasłami i narzędzia pozwalające na anonimizację danych[120]. Ponadto, istotnym elementem w procesie ochrony danych osobowych są regularne audyty technologiczne. Badacze technologii i eksperci ds. bezpieczeństwa przeprowadzają oceny systemów i infrastruktury IT organów samorządu terytorialnego w celu wykrycia potencjalnych luk w zabezpieczeniach i wyeliminowania zagrożeń.

Problem ochrony danych osobowych z perspektywy socjologii

Socjologia[121] należy do tych dziedzin nauk społecznych, która może wnosić cenne spojrzenie na problem ochrony danych osobowych. Z perspektywy socjologa, kwestia ochrony danych osobowych może być analizowany w kontekście społecznym, kulturowym i instytucjonalnym. Oto kilka aspektów, które socjologowie mogą badać w związku z tym problemem:

- Kulturowe i społeczne konteksty ochrony prywatności, czyli jak różne kultury i społeczeństwa postrzegają prywatność i ochronę danych osobowych. Ważne w tym kontekście będą próby odpowiedzi na pytanie, jakie występują różnice w podejściu do prywatności w różnych krajach i społecznościach oraz jakie czynniki kulturowe wpływają na te postawy;

[117] Zob. *Szyfrowanie połączenia (SSL/TLS)*, https://www.oki.com/printing/online-manuals-Z016/EE8001-1215/id/contents/contents/70553341.html [dostęp: 20.10.2023].
[118] *Przegląd technik kryptograficznych w zabezpieczaniu urządzeń elektronicznych*, https://elektronikab2b.pl/technika/35771-przeglad-technik-kryptograficznych-w-zabezpieczaniu-urzadzen-elektronicznych [dostęp: 20.10.2023].
[119] Zob. *Blokowanie reklam*, https://www.programosy.pl/kategoria,blokowanie_reklam,1,1.html [dostep: 20.10.2023].
[120] *Anonimizacja*, https://www.nask.pl/pl/dzialalnosc/anonimizacja/5168,Nowa-usluga-anonimizacji-dokumentow.html [dostęp: 20.10.2023].
[121] Por. Y. Ivanitska, K. Kokoszka, V. Kapcio, *Socjologia*, https://mfiles.pl/pl/index.php/Socjologia [dostęp: 20.10.2023].

- Społeczna akceptacja przepisów dotyczących ochrony danych, czyli jakie czynniki społeczne wpływają na akceptację i przestrzeganie przepisów dotyczących ochrony danych osobowych. W tym celu należałoby badać normy społeczne i zachowania w zakresie prywatności[122];
- Zagrożenia i wyzwania społeczne, takie jak nadużycia, naruszenia prywatności i ewentualne konflikty między interesami prywatności a interesami publicznymi;
- Wpływ rewolucji cyfrowej i rozwoju społeczeństwa informacyjnego na ochronę danych osobowych oraz sposób w jaki ludzie dostosowują się do nowych technologii w zakresie przetwarzania danych[123];
- Rola społeczeństwa obywatelskiego w promowaniu ochrony danych osobowych oraz w kształtowaniu przepisów i polityk związanych z prywatnością.

Socjologia dostarcza wglądu w społeczno-kulturowy kontekst problemu ochrony danych osobowych. Uczula na wyzwania i dylematy jakie wiążą się z tym zagadnieniem, a także pomaga zrozumieć reakcje konkretnych zbiorowości na kwestie związane z prywatnością. Badania socjologiczne mogą pomóc w projektowaniu bardziej skutecznych strategii ochrony danych osobowych, uwzględniając różnorodność kontekstów społecznych i kulturowych.

Problem ochrony danych osobowych w kontekście rozważań etycznych

Kategoria ochrony danych osobowych oraz prywatności należy do wartości etycznych. W aspekcie filozoficznym wartość „stanowi podstawową kategorię aksjologii oraz oznacza to wszystko, co uchodzi za ważne i cenne dla jednostki i społeczeństwa oraz jest godne pożądania. Łączy się to z pozytywnymi przeżyciami i stanowi jednocześnie cel dążeń ludzkich”[124]. Rozważanie etyczne pomagają zrozumieć niektóre aspekty znaczenia uczciwości i zaufania w kontekście gromadzenia i przetwarzania danych osobowych. Etyka nie stanowi bowiem formę oderwanego, spekulatywnego dyskursu filozoficznego[125]. Jej cel polega m.in. na rozwiązywaniu praktycznych problemów

[122] Zob. K. Jędruszczak, *Prywatność w różnych kulturach*, http://www.psychologia.net.pl/artykul.php?level=90 [dostęp: 20.10.2023].
[123] Por. Ministerstwo Cyfryzacji, *Rewolucja w systemie ochrony danych osobowych*, http://archiwum.mc.gov.pl/aktualnosci/rewolucja-w-systemie-ochrony-danych-osobowych [dostęp: 20.10.2023].
[124] I. Dudzik, S. Nowak, *Rola wartości w życiu współczesnego człowieka. Na podstawie przeprowadzonych badań własnych*, w: *Rola wartości etycznych we współczesnym świecie. Wartości etyczne współczesnego człowieka, cz I*, red. I. Dudzik, B. Czuba, K. Rejman, Jarosław 2017, s. 10.
[125] S. Rogoż, *Praktyczne aspekty kształtowania pożądanych postaw etycznych*, „Palestra”, nr 19/5-6(209-210) 1975, s. 26-27.

moralnych (bądź ich zapobieganiu), jak to ma miejsce np. w przypadku opracowywania wyspecjalizowanych etyk zawodowych. Kwestie etyczne związane z ochroną danych osobowych wiążą się także z problemem transparentności. Transparentność w działaniach organów samorządu terytorialnego, zwłaszcza w zakresie gromadzenia i przetwarzania danych osobowych, ma znaczenie etyczne[126]. Etycy mogą więc badać, jakie wymogi transparentności są istotne z perspektywy moralnej i jak organy te mogą sprostać tym wymaganiom.

Problem ochrony danych osobowych w kontekście nauk o administracji

Nauka o administracji to jedna z dyscyplin nauk społecznych[127]. Jest to dziedzina zajmująca się badaniem rozlicznych aspektów administracji publicznej, opierając się na podejściu empirycznym. Osiąga to poprzez wykorzystywanie metody rozumowania indukcyjnego, co oznacza, że wychodzi od szczegółów, a następnie generalizuje na podstawie doświadczenia i obserwacji. W swoich teoriach nauka administracji odwołuje się do różnych dziedzin, takich jak ekonomia, politologia, prakseologia, prawo, psychologia, socjologia oraz zarządzanie[128].

W gronie naukowców nie ma jednomyślności co do nazwy tej dziedziny. Zwyczajowo używają oni terminu „nauka administracji", co jest podobne do praktyki w Niemczech, gdzie stosuje się termin „Verwaltungslehre". Zdaniem Karola Dąbrowskiego, najbardziej trafne są koncepcje sugerujące wprowadzenie terminu „teoria administracji". „Podkreśla on bowiem wysoki poziom teoretyczności tej dyscypliny, poszukującej ciągle ogólnych pojęć na opisanie istniejącego stanu rzeczy w administracji publicznej. Zresztą tak, jak nie ma „nauki prawa", a istnieje dyscyplina akademicka „teoria prawa", tak nie powinno być mowy o „nauce administracji", lecz właśnie o „teorii administracji""[129].

Badania praktyk ochrony danych osobowych prowadzone przez specjalistów w zakresie teorii administracji publicznej pomaga zrozumieć, jak organy administracji publicznej zarządzają danymi osobowymi, jakie procedury są stosowane i jakie kroki

[126] *Standardy transparentności administracji publicznej w państwie demokratycznym*, https://administracjapodkontrola.pl/aktualnosci/standardy-transparentnosci-administracji-publicznej-w-panstwie-demokratycznym/ [dostęp: 20.10.2023].
[127] Zob. J. Izdebski, *Metody badań nauk społecznych w nauce prawa administracyjnego*, „Roczniki Nauk Prawnych", nr 4, 2021.
[128] K. Dąbrowski, *Nauka o administracji*, Ryki 2012, s 8.
[129] Ibidem.

podejmowane w celu ochrony prywatności jednostek[130]. Szczegółowe prace badawcze w tym zakresie mogą dotyczyć następujących aspektów:

- odpowiedzialność poszczególnych struktur i jednostek wewnętrznych organów samorządu terytorialnego w zakresie zarządzania danymi osobowymi;
- procedury stosowane w odniesieniu do danych osobowych, w tym zasady dostępu, przechowywania, usuwania i przekazywania danych;
- umiejętności i kompetencje pracowników administracji publicznej w zakresie ochrony danych;
- analiza systemów informatycznych wykorzystywanych przez organy samorządu terytorialnego w celu zarządzania danymi osobowymi oraz mechanizmy audytu i kontroli wewnętrznej[131];
- mechanizmy identyfikowania i minimalizowania potencjalnych zagrożeń związane z danymi osobowymi.

Problem ochrony danych osobowych w aspekcie nauk ekonomicznych

Analiza ekonomiczna w kontekście ochrony danych osobowych przez organy samorządu terytorialnego ma na celu zrozumienie kosztów (ale też ewentualnych korzyści) wynikających z przepisów ochrony danych oraz ich wpływu na procesy gospodarcze. Ekonomiści są w stanie przeanalizować koszta związane z wdrożeniem i przestrzeganiem przepisów dotyczących ochrony danych osobowych. To obejmuje zarówno wydatki związane z technologią i infrastrukturą (na przykład zakup i konserwację systemów ochrony danych), jak też wydatki związane z przeszkoleniem personelu oraz audytami zgodności. Badanie tych nakładów finansowych pozwala ocenić, w jakim stopniu konkretna strategia ochrona danych jest ekonomicznie uzasadniona[132].

Istotnym aspektem badań ekonomicznych jest analiza wpływu przepisów dotyczących ochrony danych na funkcjonowanie przedsiębiorstw, w tym organów samorządu terytorialnego. Eksperci muszą ustalić, czy nowe przepisy zwiększają koszty prowadzenia działalności i konkurencyjność oraz czy mają wpływ na inwestycje

[130] Zob. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych*, Warszawa 2022.
[131] Por. N. Świderska-Piksa, *Audyt RODO – Jak powinien wyglądać i kiedy go przeprowadzać*, https://rpms.pl/audyt-rodo-jak-powinien-wygladac-i-kiedy-go-przeprowadzac/ [dostęp: 20.10.2023].
[132] Zob. A. Olender, *Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w podmiotach sektora publicznego*, „Wschód Europy", vol. 6, 2/2020, s. 145-146.

w technologie i innowacje związane z ochroną danych[133]. Ekonomiczna analiza obejmuje także koszty związane z potencjalnymi naruszeniami danych, stratami finansowymi i reputacyjnymi ponoszonymi przez organy samorządu terytorialnego w wyniku incydentów naruszeń danych[134]. Problemy tego typu generują logiczne pytania o to, jakie działania można podjąć, aby zmniejszyć te wydatki.

Problem ochrony danych osobowych w kontekście nauki o komunikowaniu

Nauki o komunikowaniu to dziedzina nauk społecznych zajmująca się badaniem procesów komunikacji oraz skuteczności przekazywania informacji między różnymi jednostki oraz grupami[135]. Specjaliści z zakresu nauk o komunikowaniu mogą przeprowadzać analizy sposobu, w jaki organy samorządu terytorialnego komunikują się z różnymi grupami interesariuszy, takimi jak obywatele, firmy, organizacje pozarządowe i inne instytucje publiczne.

Skuteczna komunikacja jest niezbędna w kontekście ochrony danych osobowych, ponieważ pozwala na budowanie zaufania społecznego, skuteczne informowanie obywateli o ich prawach i obowiązkach oraz promowanie odpowiedzialnych praktyk związanych z danymi osobowymi. Specjaliści z zakresu nauk o komunikowaniu mogą dostarczyć cennych wskazówek i analiz, które pomagają organom samorządu terytorialnego w doskonaleniu swoich działań w zakresie informowania społeczności lokalnej.

Problem ochrony danych osobowych w kontekście nauk politycznych

Politologia, znana również jako nauka polityczna, to dziedzina nauk społecznych, która zajmuje się badaniem polityki, systemów politycznych, instytucji rządowych, procesów politycznych oraz zachowań politycznych jednostek i grup społecznych. Politologia ma na celu zrozumienie struktury, funkcjonowania i ewolucji systemów politycznych na różnych poziomach – od lokalnych i narodowych po międzynarodowe[136].

---

[133] P. Pałka, *Ciało obce: zasady RODO a gospodarka rynkowa*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny", nr 5(11) 2022, s. 63-64.
[134] *Prokuratura ukarana za naruszenie RODO*, https://www.rp.pl/dane-osobowe/art38453021-prokuratura-ukarana-za-naruszenie-rodo [dostęp: 20.10.2023].
[135] Zob. *Communication studies*, https://en.wikipedia.org/wiki/Communication_studies [dostęp: 15.10.2023].
[136] Y.V. Sinchuk, *Lectures on political science*, Moscow 2015, s. 5, 7, 8.

Politolodzy mogą analizować dość szerokie spektrum problematyki ochrony danych osobowych. Na przykład takie aspekty, jak:

- Analiza polityki ochrony danych osobowych, realizowanej przez organy samorządu terytorialnego;
- Wpływ przepisów ochrony danych osobowych na politykę publiczną i działania samorządów, oraz czy współgra z innymi celami polityki publicznej.
- Rola aktywizmu obywatelskiego i organizacji społeczeństwa obywatelskiego w ochronie danych osobowych,
- Porównywanie systemów politycznych i praktyk ochrony danych osobowych na poziomie lokalnym, krajowym i międzynarodowym.

Problem ochrony danych osobowych z perspektywy badań historycznych

Systemy oraz praktyki związane z zabezpieczaniem danych osobowych w jednostkach samorządu terytorialnego mogą stać się przedmiotem badań historycznych w pewnym kontekście. Przede wszystkim, badania historyczne będą przydatne podczas analizy ewolucji przepisów i praktyk związanych z ochroną danych osobowych w przeszłości. Historycy mogą również szukać odpowiedzi na pytanie, w jaki sposób wydarzenia i zmiany polityczne wpłynęły na kształtowanie obecnych ram prawnych i instytucjonalnych. Historia może dostarczyć wgląd w rozwój instytucji odpowiedzialnych za ochronę danych osobowych w jednostkach samorządu terytorialnego, takich jak biura ochrony danych czy komisje ds. prywatności itp[137]. Badania historyczne mogą pomóc zrozumieć, jak ochrona danych osobowych ewoluowała w czasie, a także jakie wydarzenia i zmiany miały wpływ na jej rozwój. Jest to cenne dla pełnego zrozumienia kontekstu i rozwoju dziedziny ochrony danych osobowych. Warto jednocześnie podkreślić, że w kontekście działań praktycznych związanych z obecnymi przepisami, badania historyczne mogą mieć ograniczone zastosowanie. Obecne przepisy o ochronie danych osobowych, takie jak RODO, skupiają się przede wszystkim na aspektach współczesnych technologii oraz mają na celu zapewnienie współczesnych standardów ochrony danych[138].

[137] Zob. J. Borecka, *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, „Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie", z. IV/2006, s. 5-7.
[138] *Czego dotyczy ogólne rozporządzenie o ochronie danych (RODO)?…*

Problem ochrony danych osobowych z perspektywy psychologii[139]

Psychologowie mogą zajmować się takimi zagadnieniami, jak: postawy ludzi wobec ochrony własnych danych osobowych, świadomość ryzyka związanego z naruszeniem prywatności, czynniki wpływające na akceptację przepisów dotyczących ochrony danych osobowych, czynniki wpływające w sposób pozytywny (bądź negatywny) na poziom zaufania wobec organów samorządu terytorialnego w zakresie gromadzenia i przetwarzania danych, przyczyny dla których obywatele decydują się udostępniać (lub odmawiają udostępniania) swoich danych, wpływ naruszeń prywatności oraz przestępczego wykorzystywania danych osobowych na zdrowie psychiczne ofiary[140], psychologiczne czynniki pływające na skuteczność strategii edukacyjnych i komunikacyjnych w podnoszeniu świadomości w zakresie ochrony danych osobowych i w promowaniu odpowiednich zachowań, czy procesy podejmowania decyzji związanych z udostępnianiem danych osobowych (np. jakie czynniki wpływają na te decyzje, jaką rolę odgrywa tutaj percepcje ryzyka, korzyści i społeczna presja). Badania psychologiczne w dziedzinie ochrony danych osobowych mogą dostarczyć informacji na temat ludzkich postaw, przekonań i reakcji wobec prywatności oraz pomóc w projektowaniu skutecznych strategii ochrony danych i edukacji społecznej w tym zakresie. Specjaliści z zakresu psychologii mogą więc wnieść cenny wkład w akademicki dyskurs wokół problemu ochrony danych osobowych, ale też zaoferować wiele praktycznych rozwiązań.

[139] A w szczególności psychologie społeczna, która skupia się na badaniu interakcji społecznych, myślenia ludzi, wpływu społecznego oraz innych aspektów związanych z zachowaniem i działaniami jednostek w kontekście społecznym. Psychologia społeczna dąży do ustalenia, jak ludzie wpływają na siebie nawzajem, jakie mechanizmy leżą u podstaw naszych przekonań, postaw, stereotypów i zachowań w kontekście społecznym. W ramach psychologii społecznej analizuje się takie zagadnienia, jak komunikacja interpersonalna, konformizm, przekonania społeczne, motywacja społeczna, społeczne uwarunkowania zachowań agresywnych, wpływ grupy na jednostkę, kwestie tożsamości społecznej i wiele innych. Psychologia społeczna stanowi ważną cześć psychologii oraz nauk społecznych, pomaga bowiem zrozumieć, dlaczego ludzie zachowują się w określony sposób w interakcjach społecznych oraz jakie czynniki wpływają na nasze społeczne decyzje i wybory [E. Aronson, T. D. Wilson, R. M. Akert, *Psychologia społeczna*, tł. J. Gilewicz, Poznań 2006, s. 29-34].

[140] Zob. P. Liwszic, *Naruszenie RODO to naruszenie prawa do prywatności – art. 82 RODO*, https://judykatura.pl/naruszenie-rodo-to-naruszenie-prawa-do-prywatnosci-art-82-rodo/ [dostęp: 20.10. 2023].

Problem ochrony danych osobowych z perspektywy nauk o zarządzaniu[141]

Nauki o zarządzaniu badają różne aspekty administrowania danymi, takie jak zarządzanie ryzykiem, zarządzanie zasobami ludzkimi, zarządzanie operacjami i wiele innych. W kontekście ochrony danych osobowych, badacze zarządzania mogą analizować, jakie procedury i strategie zarządzania są wdrażane w jednostkach samorządu terytorialnego w celu zapewnienia odpowiedniego poziomu ochrony danych osobowych, a także jakie ryzyko związane z gromadzeniem i przetwarzaniem danych jest identyfikowane i zarządzane.

[141] Pojęcie zarządzania może być definiowane na różne sposoby. Według jednych źródeł zarządzanie polega na tworzeniu warunków, które umożliwiają organizacji działać zgodnie z jej celami, misją, utrzymać spójność niezbędną do przetrwania oraz zapewnić rozwój, czyli kontynuację realizacji misji i celów w przyszłości [Zob. A.K. Koźmiński, D Jemielniak, *Zarządzanie od postaw*, Warszawa 2011, s. 18]. Natomiast według innych, istota zarządzania jako funkcji regulacyjnej wykonywanej zbiorowo przez jednostki w organizacji sprowadza się do wyznaczania celów działania, organizowania struktur poprzez planowanie oraz monitorowanie procesu realizacji tych celów [J. Zieleniewski, *Organizacja i zarządzanie*, Warszawa 1960, s. 477]. Jeśli natomiast chodzi o genezę nauk o zarządzaniu, to „zarządzanie jako działanie praktyczne istnieje od dawien dawna, jednak nauka rozwiązująca problemy występujące w tej dziedzinie ukształtowała się dopiero na przełomie XIX i XX wieku. Pierwsze przejawy powstawania tej dyscypliny wiedzy można dostrzec np. w wielkich przedsięwzięciach historycznych (budowa piramid egipskich) jak również w porzekadłach i przysłowiach a także w dziełach N. Machiavellego czy C. von Clausevitza. Za prekursorów nauki o zarządzaniu można też uznać: przemysłowca R. Owena oraz ekonomistę A. Smitha. Jednak największy wkład w rozwój tej dziedziny miała rewolucja przemysłowa, gdyż powstało wtedy mnóstwo zakładów przemysłowych, które musiały zarządzać i organizować pracę, a sposoby wcześniej wykorzystywane okazały się niewystarczające" [S. Wawak, P. Babiarz, *Zarządzanie*, (w:) *Encyklopedia Zarządzania*, https://mfiles.pl/pl/index.php/Zarz%C4%85dzanie [dostęp: 16.10.2023].

ROZDZIAŁ II
OCHRONA DANYCH OSOBOWYCH
PODSTAWY PRAWNE I ZASADY

2.1. Definicja danych osobowych

Pojęcie danych osobowych jest kluczowe w prawie ochrony prywatności. Definicja danych osobowych została w Polsce przyjęta na podstawie Rozporządzenia 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, a także uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), popularnie nazywane „RODO”[142] oraz ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych[143].

Zgodnie z art. 4 ust. 1 RODO dane osobowe to „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”.

Polska literatura prawnicza, odwołując się do przepisów RODO, często opisuje dane osobowe jako informacje, które pozwalają na zidentyfikowanie osoby fizycznej, bezpośrednio lub pośrednio, poprzez odwołanie się do jednego lub więcej czynników specyficznych dla jej tożsamości[144].

Ochrona danych osobowych odnosi się do praktyk i zasad regulujących sposób zbierania, przechowywania, udostępniania i użytkowania danych, które mogą być wykorzystane do identyfikacji osoby. Są to dane, które mogą być bezpośrednio zidentyfikowane, takie jak imię i nazwisko, adres e-mail lub numer telefonu, a także dane,

[142] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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).
[143] Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781).
[144] Ibidem.

które mogą być pośrednio zidentyfikowane, takie jak dane dotyczące lokalizacji, identyfikatory plików cookie lub innych identyfikatorów cyfrowych[145].

Pojęcie danych osobowych jest określane z uwzględnieniem dwóch elementów: informacji oraz podmiotu, który jest opisywany przez te informacje. Informacja powinna umożliwiać identyfikację podmiotu, którego dotyczy, a podmiotem tym może być wyłącznie osoba fizyczna. Jedynie spełnienie tych dwóch elementów pozwala określić, że dane mają osobowy charakter. Na takie ujęcie wskazuje definicja legalna danych osobowych, która została wyrażona w rozporządzeniu 2016/679, w którego świetle są nimi informacje o osobie fizycznej, które można przyporządkować tej osobie. Informacje te mogą dotyczyć zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której dane dotyczą. Osoba jest możliwa do identyfikacji np. na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.[146]

W omawianym temacie definicyjne ustalenia są konieczne, ponieważ nawet podstawowe pojęcie danych osobowych może rodzić wiele problemów interpretacyjnych, często prowadzących do bezprawnej ingerencji w sferę prywatności osoby, której dane dotyczą.[147]

W odniesieniu do ochrony danych osobowych kluczową rolę odgrywa dokument RODO, który wszedł w życie na terenie Unii Europejskiej w maju 2018 roku. RODO nakłada na instytucje i administrację publiczną odpowiedzialność za ochronę danych osobowych, oraz daje jednostkom (osobom i podmiotom prawnym) prawo do kontroli nad swoimi danymi. Rozporządzenie to zawiera siedem zasad ochrony danych, które organizacje muszą przestrzegać, w tym zasadę legalności, sprawiedliwości i przejrzystości, zasadę minimalizacji danych, zasadę celowości i ograniczenia przechowywania, zasadę integralności i poufności oraz zasadę odpowiedzialności[148]. Wszystkie te regulacje są ważne w kontekście cyberbezpieczeństwa państwa.

[145] L.A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press 2014.
[146] M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 28.
[147] Por. P. Fajgielski, *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021.
[148] K. Urbańska, *RODO*, [w:] *Encyklopedia Zarządzania*, https://mfiles.pl/pl/index.php/RODO [dostęp: 07.10.2023].

Zrozumienie, że ochrona danych osobowych nie dotyczy wyłącznie zapewnienia zgodności z prawem, ale także jest istotna w tworzeniu środowiska bezpieczeństwa, jest tematem podnoszącym znacznie rangę polityki ochrony danych osobowych.

Podstawą ochrony danych osobowych są prawa jednostek w kontekście ich danych osobowych. RODO określa te prawa. Obejmują one: prawo do dostępu, prawo do sprostowania, prawo do usunięcia (tzw. „prawo do bycia zapomnianym"), prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu oraz prawo do niepodlegania decyzji opartej wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu[149].

W związku z powyższym, ochrona danych osobowych obejmuje zarówno aspekty prawne, jak i techniczne, a także prawo jednostek do prywatności. Jest to obszar o złożonej naturze, wymagający ciągłej uwagi oraz czujności ze strony organizacji, które przetwarzają dane osobowe.

2.2. Ogólne rozporządzenie o ochronie danych (RODO)

Ogólne rozporządzenie o ochronie danych (RODO), znane też w języku angielskim jako *General Data Protection Regulation* (GDPR), jest ustawą Unii Europejskiej dotyczącą prywatności i ochrony danych osobowych. Jak już wcześniej wspomniano, ten akt prawny wszedł w życie 25 maja 2018 roku.

Szczegółowy opis głównych aspektów GDPR obejmuje:[150]

- Zakres: GDPR ma zastosowanie do wszystkich firm i instytucji, które przetwarzają dane osobowe mieszkańców UE, niezależnie od miejsca, w którym ta firma/instytucja działa. Dotyczy to zarówno firm oraz instytucji działających w UE, jak i poza nią;
- Prawa podmiotów danych: GDPR wprowadza szereg praw dla osób, których dane są przetwarzane, znanych jako „podmioty danych". Te prawa obejmują prawo do bycia informowanym, prawo do dostępu do swoich danych, prawo do ich poprawiania, prawo do zapomnienia, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu wobec przetwarzania i prawo do nie bycia poddanym zautomatyzowanym decyzjom, w tym profilowaniu;

[149] Ibidem.
[150] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

- Zasady przetwarzania danych: GDPR wprowadza siedem zasad przetwarzania danych, które muszą być przestrzegane. Są to zasady: legalności, uczciwości i przejrzystości; celowości; minimalizacji danych; dokładności; ograniczenia przechowywania; integralności i poufności oraz zasada odpowiedzialności;
- Rola inspektora ochrony danych (IOD): Wiele organizacji musi mianować IOD, który będzie odpowiedzialny za monitorowanie zgodności z GDPR i będzie punktem kontaktowym dla organów nadzorujących;
- Obowiązki kontrolerów i procesorów danych: Kontrolerzy i procesory danych mają określone obowiązki na mocy GDPR. Muszą zapewnić zgodność z zasadami przetwarzania danych i mogą być pociągnięci do odpowiedzialności, jeśli naruszą te zasady;
- Transfer danych międzynarodowych: GDPR zawiera szczegółowe przepisy dotyczące transferu danych osobowych poza UE. Takie transfery są dozwolone tylko w określonych okolicznościach, gdy zapewnione jest odpowiednie zabezpieczenie danych;
- Kary za naruszenie GDPR: Organizacje, które naruszają przepisy GDPR, mogą zostać ukarane grzywnami sięgającymi do 20 milionów euro lub 4% swojego globalnego obrotu rocznego, w zależności od tego, która kwota jest większa.

RODO wprowadza wiele wymagań dotyczących gromadzenia, przechowywania i przetwarzania danych osobowych, takich jak[151]:

- Zasada legalności, sprawiedliwości i przejrzystości: Dane osobowe muszą być przetwarzane legalnie, sprawiedliwie i w sposób zrozumiały dla osoby, której dane dotyczą;
- Ograniczenie celu: Dane osobowe powinny być zbierane tylko w określonych, wyraźnych i legalnych celach. Nie powinny być dalej przetwarzane w sposób niezgodny z tymi celami;
- Minimalizacja danych: Dane osobowe powinny być adekwatne, istotne i ograniczone do tego, co jest niezbędne do celów, w których są przetwarzane;
- Dokładność: Dane osobowe powinny być dokładne i, jeśli to konieczne, aktualizowane;

[151] Ibidem.

- Ograniczenie przechowywania: Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to konieczne do celów, w których są przetwarzane;
- Integralność i poufność: Dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednią ochronę danych, w tym ochronę przed nieautoryzowanym lub nielegalnym przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem, przy użyciu odpowiednich środków technicznych lub organizacyjnych;
- Odpowiedzialność: Podmiot przetwarzający dane jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie to udowodnić.

RODO wprowadza również prawo do bycia zapomnianym, co oznacza, że osoby, której dane dotyczą, mają prawo zażądać usunięcia swoich danych w określonych okolicznościach. Ponadto, podmioty przetwarzające dane muszą zgłaszać naruszenia ochrony danych do odpowiednich organów regulacyjnych i w niektórych przypadkach, do osób, których dane dotyczą[152].

2.3. Krajowe przepisy o ochronie danych osobowych

Ogólne rozporządzenie o ochronie danych (RODO) jest najistotniejszym dokumentem prawnym regulującym kwestie przetwarzania danych osobowych. Niemniej jednak, nie jest jedynym obowiązującym aktem prawnym w kwestii ochrony danych osobowych w Polsce. W polskim prawie istnieją ustawy, które są równie istotne i muszą być brane pod uwagę przez podmioty odpowiedzialne za przetwarzanie danych.

Wprowadzenie RODO (od 25 maja 2018 r.) w Polsce oznaczało, że polskie ustawy musiały od tego dnia gwarantować efektywne stosowanie regulacji RODO, nie dublując jego postanowień i nie stając w konflikcie z nim. Aby to osiągnąć, konieczne było wprowadzenie nowych regulacji oraz modyfikacji do wielu istniejących aktów prawnych.

Jako część adaptacji do wymogów RODO przyjęto ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych oraz wprowadzono zmiany w przepisach specjalistycznych, czyli zmiany w ustawach dotyczących różnych sektorów gospodarki, takich jak: HR, bankowość i ubezpieczenia, edukacja, ochrona zdrowia. Warto również

[152] Ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r., poz. 1206).

wspomnieć o ustawie z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w kontekście prewencji i zwalczania przestępczości[153]. W przeciwieństwie do wcześniej wymienionych aktów prawnych, cel tego ustawodawstwa nie był związany z implementacją regulacji RODO, ale z ustanowieniem specjalnej procedury prawnej dla przetwarzania danych w obszarze, który został wykluczony z przepisów GDPR, tj. w kontekście zapobiegania i zwalczania przestępczości.

Aktami prawnymi w prawie krajowym, które odnoszą się do przetwarzania danych osobowych, są zatem:

- Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych;
- Ustawa z dnia 26 czerwca 1974 roku – Kodeks Pracy;
- Ustawa z dnia 4 marca 1994 roku o Zakładowym Funduszu Świadczeń Socjalnych;
- Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną;
- Ustawa z dnia 16 lipca 2004 roku – Prawo Telekomunikacyjne;
- Ustawa z dnia 29 stycznia 2004 roku – Prawo Zamówień Publicznych,
- Ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w celu zapobiegania i zwalczania przestępczości.

Ustawa z 10 maja 2018 r. o ochronie danych osobowych[154]

Zakres regulacji zawartych w ustawie o ochronie danych osobowych (także nazywanej „UoODD") powstał głównie w odpowiedzi na potrzebę precyzyjniejszego zdefiniowania i dostosowania przepisów RODO do polskiego prawa. Różni się ona od wcześniej obowiązującej ustawy z 29 sierpnia 1997 roku. Uzupełniono ją m.in. o definicje pojęć prawnych: „dane osobowe", „przetwarzanie", itp.; zasady przetwarzania danych; podstawy prawne; wymagane elementy obowiązku informacyjnego; prawa przyznane osobom, których dane są przetwarzane. Wszystkie te tematy są wyłącznie przedmiotem przepisów RODO. Stąd, błędne jest odwoływanie się do ustawy o ochronie danych osobowych jako podstawy prawnej dla przetwarzania danych, na przykład w klauzuli zgody na przetwarzanie danych.

[153] Ibidem.
[154] Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. 2019 r., poz. 1781).

Co więc faktycznie zostało zawarte w regulacjach ustawy o ochronie danych osobowych? Odpowiedź na to pytanie znajdziemy w rozdziale 2 (art. 8-11a UoODD), który reguluje:

- Sposób wyznaczania inspektora ochrony danych i zawiadamiania o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych;
- Podmioty publiczne mające obowiązek wyznaczenia inspektora ochrony danych.

Z kolei rozdział 7 (art. 60-74 UoODD) reguluje kwestie procedury dotyczącej przypadków naruszenia zasad ochrony danych osobowych. Rozdział 9 (art. 78-91 UoODD) opisuje proces audytu zgodności z przepisami o ochronie danych osobowych, przeprowadzanego przez Prezesa Urzędu Ochrony Danych Osobowych. Rozdział 10 (art. 92-100 UoODD) określa procedurę sądowego dochodzenia roszczeń cywilnych wynikających z naruszeń przepisów o ochronie danych osobowych. Rozdział 11 (art. 101-108 UoODD) konkretyzuje limity wysokości administracyjnych kar finansowych nałożonych na instytucje publiczne[155].

Ustawa o ochronie danych osobowych zawiera również specyficzne wyłączenia lub restrykcje wobec pewnych zasad RODO. Wyłączenia te odnoszą się do obszarów prasy, literatury, sztuki oraz wypowiedzi naukowych (zgodnie z art. 2 UoODD), jak również do wybranych podmiotów z sektora finansów państwowych (tam, gdzie przetwarzanie informacji jest niezbędne do zapewnienia bezpieczeństwa krajowego) oraz do czynności służb specjalnych (według art. 6 UoODD). Ograniczenia w stosowaniu zasad RODO odnoszą się do administratorów realizujących zadania publiczne w zakresie spełniania obowiązków informacyjnych, zgodnie z art. 13 i 14 RODO, a także w ramach praw dostępu do informacji zgodnie z art. 15 RODO (zgodnie z art. 3-5a UoODD)[156].

UoODD jest niewątpliwie jednym z najistotniejszych dokumentów prawnych w kontekście przetwarzania informacji osobistych, tuż po RODO. Znaczenie UoODD podkreślają zawarte w nim postanowienia, które dotyczą wszystkich podmiotów, zarówno publicznych, jak i prywatnych, niezależnie od sektora lub branży, w której prowadzą swoją działalność.

[155] Ibidem.
[156] Ibidem.

Przepisy sektorowe

Efektywne wdrożenie przepisów RODO wymagało nie tylko uchwalenia ustawy o ochronie danych osobowych, ale także wprowadzenia modyfikacji w już istniejących przepisach. Te zmiany w prawach sektorowych zostały wprowadzone głównie poprzez nowelizację przyjętą wraz z ustawą z 21 lutego 2019 roku o modyfikacji niektórych ustaw w celu zapewnienia stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku, dotyczącego ochrony osób fizycznych w kontekście przetwarzania danych osobowych i swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (znanej jako „ustawa sektorowa")[157].

Zgodnie z uzasadnieniem do projektu ustawy sektorowej, głównym celem tej nowelizacji było „dostosowanie polskiego systemu prawnego do RODO, między innymi przez eliminację tych przepisów, które są sprzeczne z RODO lub które powielają rozwiązania RODO, a także dostosowanie RODO do specyficzności polskiego systemu prawnego"[158].

W ramach tej rewizji dokonano modyfikacji w przeszło 160 aktach prawnych dotyczących różnych sektorów i obszarów gospodarki, takich jak: administracja państwowa, edukacja, zasoby ludzkie, rynek telekomunikacyjny, sektor bankowy, działalność medyczna, usługi ubezpieczeniowe, działalność prawna i doradcza.

Z perspektywy pracodawców, kluczowe były modyfikacje w ustawach dotyczących prawa pracy i zagadnień kadrowych, jak na przykład Kodeks pracy czy ustawa o zakładowym funduszu świadczeń socjalnych. Dla firm prowadzących aktywność marketingową za pośrednictwem email marketingu czy telemarketingu, istotne przemiany przyniosła rewizja ustawy o świadczeniu usług drogą elektroniczną oraz ustawy o prawie telekomunikacyjnym. Dla podmiotów zaangażowanych w realizację zamówień publicznych okazały się istotne modyfikacje w ustawie Prawo zamówień publicznych.

[157] Ustawa z dnia 21 lutego 2019 roku o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego 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. z 2019 r., poz.730).

[158] 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…

Z racji zakresu ustawy sektorowej nie jest możliwe opisanie i przedstawienie wszystkich modyfikowanych aktów prawnych. Z tego względu omówione zostaną najbardziej istotne zapisy, które zostały zawarte w wyżej wymienionych ustawach.

Kodeks pracy[159] *oraz Ustawa o zakładowym funduszu świadczeń socjalnych*[160]

Przepisy kodeksu pracy (nazywanego dalej: „KP") oraz ustawy o zakładowym funduszu świadczeń socjalnych (odtąd jako: „ustawa o ZFŚS") określają liczne kluczowe dla pracodawców zasady dotyczące przetwarzania danych osobowych osób ubiegających się o pracę oraz pracowników. Te akty prawne zawierają między innymi informacje na temat:

- zakresu danych osobowych, których pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie oraz od pracownika – art.22^1 KP;
- okoliczności i zasad, w oparciu, o które pracodawca ma prawo wykorzystywać zgodę na przetwarzanie danych osobowych od osób ubiegających się o pracę oraz od pracowników, a także przetwarzać ich informacje biometryczne – art. 22^{1a} i 22^{1b} KP;
- sposobu, w jaki pracodawca powinien dopuścić pracowników do przetwarzania danych szczególnych kategorii – art. 22^{1b} KP oraz art. 8 ust. 1b ustawy o ZFŚS;
- warunków i zasad stosowania w zakładzie pracy monitoringu wizyjnego, monitoringu poczty elektronicznej pracowników oraz innych form monitorowania aktywności pracowniczej – art. 22^2 i 22^3 KP;
- sposobu, w jaki pracodawca powinien zbierać i dokumentować dane osobowe osób ubiegających się o udzielenie świadczenia z zakładowego funduszu świadczeń socjalnych, a także okresu przechowywania takich danych – art. 8 ust. 1a, 1c i 1d ustawy o ZFŚS.

Ustawa o świadczeniu usług drogą elektroniczną[161] *oraz Ustawa Prawo telekomunikacyjne*[162]

Ustawa o świadczeniu usług drogą elektroniczną (dalej nazywana: „Uśude") i Ustawa Prawo telekomunikacyjne (odtąd: „Pr. Telekom") stanowią dwa kluczowe akty

[159] Ustawa z dnia 26 czerwca 1974 roku Kodeks pracy (Dz. U. z 2023 r. poz. 1465).
[160] Ustawa z dnia 4 marca 1994 roku o zakładowym funduszu świadczeń socjalnych (Dz. U. z 2024 r., poz. 288).
[161] Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r., poz. 344).
[162] Ustawa z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz.U. z 2024 r., poz. 34).

prawne dla sektora marketingowego. Wprowadzają one wymóg zdobycia zgody odbiorcy na otrzymywanie treści marketingowych za pomocą narzędzi komunikacji, takich jak email, sms, mms i rozmowy telefoniczne (art. 10 ust. 1-2 Uśude, art. 172 ust. 1 Pr. Telekom). Ustawa sektorowa wprowadziła ważną zmianę do obu powyższych aktów prawnych, czyli konieczność stosowania przepisów o ochronie danych osobowych do uzyskania zgody marketingowej (art. 5 Uśude oraz art. 174 Pr. Telekom). To oznacza, że zgody gromadzone na podstawie Uśude i Pr. Telekom muszą być zgodne z wymogami określonymi w przepisach RODO, zwłaszcza w art. 4 pkt. 11 (definicja zgody) oraz art. 7 (warunki wyrażenia zgody) RODO.

W tym kontekście należy zwrócić uwagę na skomplikowaną kwestię zgód marketingowych. Wielu administratorów stosuje zgodę jako podstawę prawną do przetwarzania danych osobowych w celach marketingowych. Jednakże, należy mieć na uwadze, że taka zgoda nie zastępuje zgód wymaganych na mocy przepisów Uśude i Pr. Telekom. Jeżeli przetwarzanie danych osobowych będzie powiązane na przykład z wysyłaniem materiałów marketingowych na adresy email lub prowadzeniem rozmów telefonicznych, to niezależnie od „zgody z RODO", w takim przypadku będzie także wymagane uzyskanie dodatkowych zgód na podstawie przepisów Uśude i/lub Pr. Telekom.

Ustawa Prawo zamówień publicznych[163]

Problematykę związaną z ochroną danych osobowych przedstawia art. 8a ust. 1-7 PZP. Precyzuje on:

- sposób spełniania obowiązku informacyjnego;
- sposób realizacji prawa dostępu do danych z art. 15 RODO, prawa do sprostowania lub uzupełnienia danych z art.16 RODO, prawa do ograniczenia przetwarzania danych z art. 18 RODO;
- sposób poinformowania osoby o ograniczeniach związanych z realizacją praw z art. 15 oraz 18 RODO.

Artykuł 96 ust. 3a PZP reguluje kategorie danych wyłączonych z zasady jawności protokołu postępowania; art. 96 ust. 3b PZP mówi o sposobach realizacji prawa do ograniczenia przetwarzania danych z art. 18 RODO w odniesieniu do danych

[163] Ustawa z dnia 11 września 2019 roku Prawo zamówień publicznych (Dz.U. z 2023 r., poz. 1605 z późn. zm.).

zgromadzonych w protokole postępowania oraz jego załącznikach; art. 97 ust. 1a i 1b PZP konkretyzuje zasady realizacji prawa dostępu do danych z art. 15 RODO oraz prawa do sprostowania lub uzupełnienia danych z art. 16 RODO w odniesieniu do danych zgromadzonych w protokole postępowania oraz jego załącznikach.

Powyższy wykaz ilustruje ilość zobowiązań wynikających z RODO (wśród nich obowiązek informacyjny oraz spełnianie praw jednostek), które zostały uszczegółowione w ramach przepisów PZP. Znajomość tych regulacji jest fundamentalna dla właściwego wdrażania wymogów RODO przez podmioty prowadzące zamówienia publiczne.

Podobnie jak w przypadku regulacji zawartych w Kodeksie pracy, również w przepisach PZP pojawiają się klauzule dotyczące przetwarzania danych osobowych, które nie znalazły swojego miejsca w ustawie sektorowej. Przykładem jest art. 97 ust. 1 PZP definiujący okres przechowywania protokołu przebiegu procesu przyznawania zamówienia oraz dołączonych do niego dokumentów[164].

Reasumując, ochrona danych osobowych nie sprowadza się jedynie do RODO. To także całościowy system szczegółowych regulacji, które w mniejszym lub większym stopniu definiują metody i zasady obsługi informacji o osobach prywatnych. Mając to na względzie i biorąc pod uwagę specyfikę oraz podstawy funkcjonowania danej instytucji, zbiór przepisów dotyczących zagadnień ochrony danych osobowych może być bardzo obszerny. W takiej sytuacji zaleca się korzystanie z pomocy ekspertów, którzy na bieżąco śledzą zmiany w przepisach prawa o ochronie danych osobowych.

2.4. Organy nadzoru i kontroli

Na terenie Rzeczypospolitej Polskiej działa szereg instytucji odpowiedzialnych za ochronę danych osobowych i monitorowanie przestrzegania przepisów dotyczących prawa do prywatności. Poniżej zostaną omówione najważniejsze z nich.

Urząd Ochrony Danych Osobowych (UODO)

Urząd Ochrony Danych Osobowych (UODO) został powołany do nadzorowania i regulowania ochrony danych osobowych oraz wdrażania RODO. Instytucja UODO działa jako niezależny organ, co oznacza, że jest on suwerenny względem administracji

[164] Ibidem.

państwowej oraz innych instytucji publicznych[165]. Autonomiczność ta ma zagwarantować podejmowanie niezależnych decyzji i działań, które służą przede wszystkim interesom społeczeństwa w zakresie ochrony danych osobowych, nie zaś interesom administracji państwowej lub innych organizacji.

UODO posiada szeroki zakres obowiązków i kompetencji. Do jego głównych zadań należy monitorowanie i egzekwowanie przepisów RODO, a także udzielanie porad i wsparcia w zakresie ochrony danych osobowych. Instytucja ta została uprawniona do prowadzenia dochodzeń w przypadku naruszeń przepisów o ochronie danych osobowych i nakładania sankcji na organizacje, które je naruszają. UODO świadczy usługi doradcze w zakresie ochrony danych osobowych zarówno obywatelom, jak też przedsiębiorstwom i organizacjom. UODO udostępnia materiały edukacyjne i organizuje szkolenia w celu podnoszenia świadomości i kompetencji w zakresie ochrony danych osobowych[166].

Organizacje i przedsiębiorstwa przetwarzające dane osobowe są zobowiązane do zgłoszenia swoich zbiorów danych do UODO. Urząd prowadzi rejestr tych zbiorów i udostępnia go publicznie, co pozwala na transparentność i kontrolę przetwarzania danych osobowych. UODO ma prawo do nakładania sankcji i kar na organizacje i instytucje, które naruszają przepisy o ochronie danych osobowych. Sankcje te obejmują kary finansowe. UODO jest obowiązane do raportowania swoich działań Komisji Europejskiej. Komisja monitoruje skuteczność organów krajowych w egzekwowaniu przepisów RODO[167].

Przed majem 2018 roku funkcje związane z ochroną danych osobowych w Polsce znajdowały się w gestii Generalnego Inspektora Ochrony Danych Osobowych (GIODO)[168]. Na mocy nowych przepisów przekazano dotychczasowe obowiązki GIODO prezesowi UODO, który tym samym stał się także organem odpowiedzialnym za nadzorowanie przestrzegania ogólnego rozporządzenia o ochronie danych osobowych (RODO). Ponieważ UODO jest prawnym spadkobiercą GIODO, nie tylko przejął jego aktywa i zobowiązania, ale również wszczęte przez GIODO postępowania[169].

---

[165] Zob. *Urząd Ochrony Danych Osobowych*, https://uodo.gov.pl/pl (dostęp: 20.10.2023); *UODO – czym się zajmuje i kto powinien obawiać się kontroli?*, https://hsm-recycling.pl/pl/blog/czym-zajmuje-sie-uodo-i-kto-powinien-obawiac-sie-kontroli-3/ [dostęp: 20.10.2023].
[166] Ibidem.
[167] Ibidem.
[168] GIODO był poprzednikiem Urzędu Ochrony Danych Osobowych i pełnił podobną rolę w zakresie ochrony danych osobowych. Po wejściu w życie RODO, GIODO został przekształcony w UODO [*Generalny Inspektor Ochrony Danych Osobowych*, http://encyklopediaap.uw.edu.pl/index.php/Generalny_Inspektor_Ochrony_Danych_Osobowych [dostęp: 20.10.2023].
[169] *Urząd ochrony danych osobowych i jego funkcja*, https://chronpesel.pl/ochrona-danych-osobowych/urzad-ochrony-danych-osobowych-i-jego-funkcja [dostęp: 18.10.2023].

W kontekście działalności Urzędu Ochrony Danych Osobowych warto szczegółowiej omówić funkcję prezesa Urzędu Ochrony Danych Osobowych. Prezes UODO jest najważniejszym decydentem i kierownikiem Urzędu Ochrony Danych Osobowych. Jego obowiązkiem jest zarządzanie pracą urzędu, nadzorowanie jego działań oraz organizowanie działań związanych z egzekwowaniem przepisów o ochronie danych osobowych na terenie Rzeczypospolitej Polskiej. Prezes UODO jest odpowiedzialny za nadzorowanie przestrzegania przepisów o ochronie danych osobowych przez organizacje, przedsiębiorstwa i instytucje działające w Polsce. Nadzór obejmuje prowadzenie kontroli, analizowanie skarg i zgłoszeń oraz podejmowanie działań w przypadku wykrytych naruszeń. Prezes UODO pełni również rolę doradczą w zakresie ochrony danych osobowych. Zgodnie z zakresem swoich funkcji powinien on służyć wiedzą i wsparciem organizacjom, przedsiębiorstwom oraz obywatelom. W tym celu mogą oni skonsultować się z urzędem w sprawach związanych z przepisami RODO i ochroną danych osobowych. Prezes UODO posiada również uprawnienia do nakładania sankcji na podmioty naruszające przepisy o ochronie danych osobowych. Sankcje te mogą obejmować kary finansowe i/lub inne środki zaradcze, w zależności od charakteru naruszenia.

Instytucja UODO jest zaangażowana w przeciwdziałanie naruszeniom danych osobowych poprzez edukację, wydawanie zaleceń i inicjowanie działań w celu zwiększenia świadomości i przestrzegania przepisów o ochronie danych w Polsce. W tym celu współpracuje ona zarówno z organami krajowymi, takimi jak sądy i organy nadzorcze, jak też z organami międzynarodowymi w ramach wspólnego nadzoru nad ochroną danych osobowych na terenie Unii Europejskiej. Z uwagi na ten zakres działań, prezes UODO ma obowiązek składać raporty z działalności urzędu oraz całokształtu sytuacji w zakresie ochrony danych osobowych w Polsce[170].

Obecnym prezesem Urzędu Ochrony Danych Osobowych jest Mirosław Wróblewski. Sejm formalnie zatwierdził jego nominację 16 stycznia 2024 roku. Z chwilą złożenia ślubowania przed Sejmem, czyli od 26 stycznia 2024 roku, rozpoczęła się jego czteroletnia kadencja na tym stanowisku (zgodnie z przepisami ustawy o ochronie danych osobowych). Mirosław Wróblewski wcześniej był pracownikiem Biura Rzecznika Praw

[170] Zob. *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w Roku 2019*, https://uodo.gov.pl [dostęp: 20.10.2023].

Obywatelskich, był też członkiem Zarządu Agencji Praw Podstawowych Unii Europejskiej[171].

Sądy krajowe i Sąd Najwyższy

Sądy krajowe, w tym Sąd Najwyższy, odgrywają istotną rolę w systemie ochrony danych osobowych w Polsce[172]. Można przyjąć, że zagadnienia związane z zaangażowaniem sądów w ochronę danych osobowych dotyczą spraw:

- Sądy krajowe, w tym sądy rejonowe, okręgowe i Sąd Najwyższy, są uprawnione do rozstrzygania sporów związanych z ochroną danych osobowych. Osoby, których prawa zostały naruszone w wyniku nielegalnego przetwarzania ich danych osobowych, mogą składać pozwy sądowe w celu dochodzenia swoich praw;
- Zgodnie z przepisami RODO, każda osoba, której dane osobowe są przetwarzane, ma prawo do skargi do organu nadzorczego, czyli Urzędu Ochrony Danych Osobowych (UODO) w Polsce. Jednak, jeśli jej prawa w zakresie ochrony danych osobowych zostały naruszone i nie jest zadowolona z decyzji UODO, może zwrócić się do sądu w celu uzyskania zadośćuczynienia lub innych środków ochrony;
- Sądy w Polsce wydają kluczowe decyzje dotyczące ochrony danych osobowych. Sąd Najwyższy może wydawać orzeczenia, które wpływają na interpretację i stosowanie przepisów dotyczących ochrony danych osobowych w kraju. Są to precedensy, które mogą wpływać na późniejsze sprawy dotyczące ochrony danych osobowych;
- Sądy krajowe posiadają uprawnienia do przyznawania odszkodowań lub innych form zadośćuczynienia osobom, których prawa w zakresie ochrony danych osobowych zostały naruszone. To oznacza, że osoby dotknięte naruszeniem mają możliwość dochodzenia roszczeń finansowych lub innych środków naprawczych przed sądem.

Inspektor Ochrony Danych Osobowych

Inspektor Ochrony Danych Osobowych to specjalista do spraw ochrony danych osobowych w organizacji. Jego głównym zadaniem jest nadzorowanie wewnętrznego przestrzegania przepisów dotyczących ochrony danych osobowych, zarówno przepisów RODO, jak i związkowych przepisów krajowych. RODO wymaga, aby niektóre

[171] *Prezes Urzędu Ochrony Danych Osobowych*, https://uodo.gov.pl/pl/138/2973 [dostęp: 30.03.2024].
[172] Zob. P. Falkowski, *Ochrona danych osobowych w Sądzie Najwyższym*, https://www.sn.pl/informacjepraktyczne/SitePages/Ochrona_danych_osobowych.aspx [dostęp: 20.10.2023].

organizacje i przedsiębiorstwa samodzielnie powoływały własnego inspektora ochrony danych osobowych. Obowiązek ten dotyczy przede wszystkim instytucji przetwarzających duże ilości danych osobowych lub danych wrażliwych, a także podmiotów publicznych[173].

Inspektor Ochrony Danych Osobowych powinien działać niezależnie w zakresie wykonywania swoich obowiązków. Ten wymóg ma na celu zapewnienie, że inspektor będzie w stanie dokładnie monitorować przestrzeganie przepisów o ochronie danych osobowych niezależnie od jakiejkolwiek presji lub ingerencji zewnętrznej lub wewnętrznej. Inspektor Ochrony Danych Osobowych musi współpracować z Urzędem Ochrony Danych Osobowych (UODO) i powinien zgłaszać wszelkie incydenty dotyczące naruszeń danych osobowych oraz być w stałym kontakcie z UODO. Ma on również prawo do konsultowania się z organem nadzorczym w sprawach związanych z przestrzeganiem przepisów RODO[174]. Osoba pełniąca tę funkcję w organizacji jest odpowiedzialna za podnoszenie świadomości pracowniczej w zakresie ochrony danych osobowych. Jej zadaniem jest wspomaganie pracowników i członków zarządu w aktualizowaniu wiedzy dotyczącej przepisów oraz w opracowywaniu odpowiednich procedur i polityk w zakresie danych osobowych.

Oprócz tego inspektor pełni rolę pośrednika między organizacją a osobami, których dane osobowe są przetwarzane. Takie osoby mogą skontaktować się z inspektorem w przypadku pytań, wątpliwości lub skarg wynikających z nieprawidłowości. Inspektor Ochrony Danych Osobowych może być pracownikiem administratora lub podmiotu przetwarzającego dane osobowe lub wykonywać zadania na podstawie umowy o świadczenie usług.

Grupa przedsiębiorstw może wyznaczyć jednego IOD (Inspektora Ochrony Danych), jeśli jest taka możliwość. Podmiot, który wyznaczył inspektora, powinien upublicznić jego dane kontaktowe[175].

Komisja Europejska

Ponieważ RODO jest unijnym rozporządzeniem, ma zastosowanie we wszystkich państwach członkowskich Unii Europejskiej, w tym także w Polsce, która jest państwem

[173] D. Łesak, *Inspektor Ochrony Danych Osobowych - kiedy jest potrzebny?*, https://poradnik przedsiebiorcy.pl/-inspektor-ochrony-danych-osobowych-kiedy-jest-potrzebny [dostęp: 18.10.2023].
[174] Ibidem.
[175] Ibidem.

członkowskim UE od 2004 roku. Instytucje administracji publicznej Rzeczypospolitej Polskiej współpracują z instytucjami unijnymi, aby zapewnić spójne i skuteczne egzekwowanie przepisów o ochronie danych osobowych na terenie całej Unii. Komisja Europejska odgrywa naczelną rolę w nadzorze nad wdrażaniem przepisów ogólnego rozporządzenia o ochronie danych osobowych (RODO) we wszystkich państwach unijnych. Jeśli Komisja Europejska stwierdzi, że państwo członkowskie narusza przepisy RODO, może wszcząć postępowanie w tej sprawie. Jednocześnie Komisja zapewnia wsparcie i doradztwo państwom członkowskim w zakresie wdrażania przepisów RODO. Obejmuje ono pomoc w interpretacji przepisów RODO oraz wydawanie szczegółowych wytycznych i zaleceń. Komisja współpracuje z organami krajowymi do spraw ochrony danych[176]. Praca Komisji Europejskiej w nadzorze nad ochroną danych osobowych w państwach członkowskich stanowi część systemu egzekwowania przepisów RODO na szczeblu unijnym, dzięki tym działaniom możliwe jest zapewnienie jednolitego, spójnego systemu ochrony prywatności i danych osobowych na terenie całej Unii Europejskiej.

Cel ujednolicenia przepisów o ochronie danych osobowych na terenie całej Unii Europejskiej wynikał z wcześniejszych różnic legislacyjnych w poszczególnych państwach członkowskich. Przepisy krajowe w państwach UE znacznie różniły się w zakresie ochrony danych osobowych, co utrudniało zarówno funkcjonowanie organizacjom (w szczególności międzynarodowym), jak i realizację praw, których dane dotyczą. Dotychczas funkcjonujące przepisy (dyrektywa 95/46/WE) nie uwzględniały skali, na jaką obecnie przetwarzane są dane osób fizycznych. Powszechność przetwarzania danych i transgraniczny charakter tych procesów wymagał ustanowienia jednolitych zasad, zarówno w celu ochrony osób, których dane są przetwarzane, jak i podmiotów, które te operacje prowadzą.[177] Jak wskazuje już artykuł 1 RODO, celem regulacji jest nie tylko zagwarantowanie ochrony podmiotom danych, lecz jednocześnie (i równorzędnie) swoboda przepływu tego rodzaju danych w Unii. Budzi to całkiem istotne pytanie, czy nie są to cele sprzeczne, sobie przeciwstawne oraz czy osiągnięcie obu jest w ogóle możliwe. Jednakże odpowiedź na to pytanie stanowi temat na odrębne opracowanie.

[176] Zob. *Ochrona danych w UE. Ogólne rozporządzenie o ochronie danych, dyrektywa o ochronie danych w sprawach karnych i inne przepisy dotyczące ochrony danych osobowych*, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pl (dostęp: 20.20.2023).
[177] P. Wróbel, *Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia*, PME, nr 4, 2017, s. 41.

Organizacje pozarządowe

Organizacje pozarządowe odgrywają pomocniczą rolę we wzmacnianiu ochrony danych osobowych i dbaniu o skutecznie egzekwowanie przepisów RODO na poziomie krajowym. Ich działania ograniczają się do podnoszenia świadomości społecznej i promowaniu dobrych praktyk w zakresie zabezpieczania poufnych informacji dotyczących osób fizycznych. Jedną z takich organizacji jest Stowarzyszenie Inspektorów Ochrony Danych Osobowych (SIDO), które skupia profesjonalistów zajmujących się ochroną danych osobowych, przede wszystkim Inspektorów Danych Osobowych oraz wszystkie osoby, które są zainteresowane tematyką ochrony danych osobowych i RODO[178]. Główne cele Stowarzyszenia to:

- Wymiana wiedzy i doświadczeń: SIDO służy jako platforma, na której inspektorzy danych osobowych mogą wymieniać wiedzę i doświadczenia w zakresie ochrony danych osobowych, co ułatwia lepsze zrozumienie oraz skuteczniejsze wdrożenie przepisów RODO;
- Kształcenie i rozwijanie kompetencji: Stowarzyszenie organizuje szkolenia, konferencje, seminaria i inne wydarzenia mające na celu kształcenie i rozwijanie kompetencji profesjonalistów zajmujących się ochroną danych osobowych. Dzięki temu członkowie SIDO mogą być lepiej przygotowani do swoich obowiązków;
- Reprezentacja interesów Stowarzyszenia Inspektorów Ochrony Danych: stowarzyszenie reprezentuje interesy swoich członków wobec organów rządowych i innych instytucji. Organizacja dąży do wywierania wpływu na kształtowanie przepisów i regulacji związanych z ochroną danych osobowych;
- Promowanie pożytecznych praktyk: Stowarzyszenie Inspektorów Ochrony Danych stara się promować skuteczne praktyki w zakresie ochrony danych osobowych i wspiera swoich członków w stosowaniu tych praktyk w organizacjach[179].

Stowarzyszenie Inspektorów Ochrony Danych działa w oparciu o Kodeks Etyki Inspektorów Ochrony Danych przyjęty Uchwałą Nadzwyczajnego Walnego Zgromadzenia SABI – Stowarzyszenia Inspektorów Ochrony Danych w dniu 30 stycznia

[178] *Statut SABI – Stowarzyszenia Inspektorów Ochrony Danych. Tekst jednolity uwzględniający zmiany dokonane na Walnym Zgromadzeniu członków Stowarzyszenia dnia 26 maja 2010 r., dnia 24 czerwca 2010 r., dnia 30 stycznia 2018 r. i dnia 10 czerwca 2021 r*., https://sabi.org.pl/statut-sabi-stowarzyszenia-inspektorow-ochrony-danych/ (dostęp: 19.20.2023).
[179] Ibidem.

2018 roku[180]. Inspektorzy Ochrony Danych zobowiązani są do przestrzegania zasad etyki zawodowej:

- zasady legalności;
- zasady obiektywizmu;
- zasady niezależności;
- zasady profesjonalizmu;
- zasady poufności;
- zasady unikania konfliktu interesów[181].

Niżej omawiamy wyszczególnione tutaj zasady etyki zawodowej.

Działanie Inspektorów Ochrony Danych w oparciu o zasady etyki zawodowej oraz standardy postępowania ma gwarantować wysoki poziomu ochrony praw i wolności jednostek w zakresie ochrony danych osobowych. Członkowie Stowarzyszenia Inspektorów Ochrony Danych włączają przepisy kodeksu do swojej praktyki zawodowej[182].

Zasada legalności (zwana też zasadą prawości)

Zasada legalności zobowiązuje Inspektorów Danych Osobowych do wykonywania swoich zadań w sposób sumienny i profesjonalny z podkreśleniem poszanowania praw osób, których dane dotyczą oraz administratorów danych.

Zasada obiektywizmu

Inspektorzy powinni opierać swoje działania na rzeczywistym stanie badanej sprawy, uwzględniać każdy jej aspekt oraz nie ulegać naciskom z zewnątrz ani wewnątrz organizacji. Inspektorzy powinni gromadzić i oceniać informacje, które gwarantują wiarygodność ich działań, dbając o obiektywność, co oznacza korygowanie własnego stanowiska i weryfikację ocen wyłącznie na podstawie rzetelnych i sprawdzonych informacji.

[180] *Kodeks Etyki dla Inspektorów Ochrony Danych przyjęty Uchwałą Nadzwyczajnego Walnego Zgromadzenia SABI – Stowarzyszenia Inspektorów Ochrony Danych w dniu 30 stycznia 2018 r*oku, https://sabi.org.pl/kodeks-etyki/ [dostęp: 19.10.2023].
[181] Ibidem.
[182] Ibidem.

Zasada niezależności

Zgodnie z zasadą niezależności Inspektorzy Ochrony Danych powinni w swoich działaniach opierać się przede wszystkim na własnej wiedzy, umiejętnościach oraz doświadczeniu. Nie powinni przyjmować poleceń ani instrukcji dotyczących wykonywania swoich zadań od osób postronnych np. zarządu firmy. Powinni natomiast samodzielnie decydować o sposobie wypełniania swoich obowiązków.

Zasada profesjonalizmu

Inspektorzy zobowiązani są do przestrzegania zapisów obowiązującego prawa i etycznych norm oraz podejmować się tylko tych zadań, co do których posiadają odpowiednie kwalifikacje i kompetencje. Zasada profesjonalizmu wymusza nieustanne podnoszenie własnych kwalifikacji.

Zasada poufności

Zasada poufności ma szczególne znaczenie w profesji Inspektorów Danych Osobowych. Nakłada ona na inspektorów obowiązek zachowania tajemnicy dotyczącej wykonywanych zadań. Nie mogą oni zatem ujawnić informacji uzyskanych w trakcie pełnionych obowiązków, o ile zachowanie takiej dyskrecji nie narusza obowiązującego prawa. Posiadane informacje mogą zostać wykorzystywane tylko i wyłącznie w celach zawodowych. Kategorycznie zabrania się używania ich dla uzyskania osobistych korzyści lub do działań niezgodnych z prawem.

Zasada unikania konfliktu interesów

Inspektorzy Ochrony Danych powinni unikać sytuacji związanych z ryzykiem wystąpienia konfliktu interesów w ich pracy. Powinni zachować szczególną ostrożność podczas kontaktów z konkurencyjnymi podmiotami, informować ich o swojej roli i zobowiązaniach. Jeśli konflikt mimo wszystko wystąpi, inspektorzy powinni podjąć odpowiednie działania w celu jego rozwiązania[183].

[183] Ibidem.

2.5. Odpowiedzialność prawna

Zgodnie z artykułem 6 ust. 1 lit. e) Ogólnego Rozporządzenia o Ochronie Danych (RODO), organy samorządu terytorialnego są zobowiązane do przetwarzania danych osobowych w sposób zgodny z prawem, uczciwie i transparentnie. Przetwarzanie powinno być adekwatne, stosowne i ograniczone do tego, co jest konieczne do celów, w których dane są przetwarzane. Jakiekolwiek naruszenie tych zasad może skutkować odpowiedzialnością organów samorządu terytorialnego, zarówno na mocy przepisów RODO, jak i Kodeksu karnego, a także innych przepisów prawa krajowego[184].

Naruszenie RODO

W przypadku naruszenia RODO, zgodnie z art. 83 RODO, organy samorządu terytorialnego mogą podlegać karom administracyjnym nałożonym przez organ nadzorczy. Kary te mogą wynieść do 20 mln euro lub, w przypadku przedsiębiorstwa, do 4% całkowitego rocznego obrotu na skalę światową. Ponadto, na podstawie art. 82 RODO, osoba, której prawa zostały naruszone, może domagać się odszkodowania od organu samorządu terytorialnego[185].

Naruszenie prawa krajowego

Zgodnie z art. 107 kodeksu karnego, kto przetwarza dane osobowe niezgodnie z przepisami, podlega karze pozbawienia wolności do lat 2. W sytuacjach, gdy naruszenie jest szczególnie poważne, kara może być jeszcze wyższa[186]. Ponadto, osoba, której dane zostały naruszone, może domagać się odszkodowania na podstawie art. 448 Kodeksu cywilnego[187].

[184] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[185] Ibidem.
[186] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 2024 r., poz. 17 z późn. zm.).
[187] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2023 r.,poz. 610 z późn. zm.).

Środki naprawcze

Organy samorządu terytorialnego są zobowiązane do wprowadzenia odpowiednich środków naprawczych w przypadku stwierdzenia naruszenia przepisów dotyczących ochrony danych, zgodnie z art. 82 ust. 3 RODO[188] i art. 23 ustawy o ochronie danych osobowych[189].

Odpowiedzialność cywilna

Zgodnie z art. 82 RODO każda osoba, której prawa zostały naruszone w wyniku złamania przepisów o ochronie danych, ma prawo do odszkodowania za doznane szkody materialne i niematerialne. Artykuł 82 przewiduje odszkodowanie zarówno za szkody materialne, jak i niematerialne[190]. Szkody materialne to takie, które prowadzą do bezpośrednich strat finansowych – na przykład kosztów związanych z kradzieżą tożsamości. Szkody niematerialne to takie, które nie prowadzą do bezpośrednich strat finansowych, ale mogą powodować szereg negatywnych skutków, takich jak stres, strach, utrata prywatności czy negatywne skutki dla reputacji[191].

Warto jednak zauważyć, że aby otrzymać odszkodowanie, osoba pokrzywdzona musi wykazać, że doznała szkody w wyniku naruszenia przepisów o ochronie danych. Nie musi być to proces łatwy, zwłaszcza w przypadku szkód niematerialnych. Dodatkowo art. 448 Kodeksu cywilnego przewiduje odpowiedzialność cywilną za naruszenie dóbr osobistych, w tym naruszenie praw do ochrony danych osobowych[192].

Odpowiedzialność administracyjna

Zgodnie z artykułem 83 RODO organy samorządu terytorialnego mogą ponieść odpowiedzialność administracyjną za naruszenie przepisów o ochronie danych osobowych. W szczególności mogą zostać nałożone kary administracyjne do 20 mln euro

[188] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…
[189] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1781).
[190] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…
[191] Ibidem.
[192] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2023 r., poz. 610 z późn. zm.).

lub w przypadku przedsiębiorstwa do 4% całkowitego rocznego obrotu na skalę światową[193].

Odpowiedzialność karna

Zgodnie z artykułem 107 Kodeksu karnego naruszenie przepisów o ochronie danych osobowych może skutkować odpowiedzialnością karną, w tym karą pozbawienia wolności do lat 2[194]. Ponadto pracownicy samorządu terytorialnego, którzy naruszają przepisy o ochronie danych osobowych, mogą ponieść odpowiedzialność dyscyplinarną zgodnie z przepisami prawa pracy i ustawie o służbie publicznej.

Odpowiedzialność polityczna

Zgodnie z artykułem 5a Ustawy o samorządzie terytorialnym, organy samorządu terytorialnego, w tym władze wykonawcze, mogą ponieść odpowiedzialność polityczną za naruszenia przepisów o ochronie danych. Ta odpowiedzialność może obejmować konieczność rezygnacji z funkcji, a jej rezultatem może być wywołanie kryzysu politycznego, a nawet przyspieszone wybory.

Sankcje administracyjne

Zgodnie z art. 83 RODO w przypadku naruszenia przepisów o ochronie danych, organy nadzorcze mogą nałożyć na podmioty przetwarzające dane, w tym organy samorządu terytorialnego, kary administracyjne.

Kary te są dwustopniowe:

- W przypadku mniej poważnych naruszeń, takich jak brak współpracy z organem nadzorczym czy nieprzestrzeganie obowiązków związanych z prawami osób, których dane dotyczą, kara może wynieść do 10 mln euro lub w przypadku przedsiębiorstwa, do 2% całkowitego rocznego obrotu na skalę światową;
- W przypadku poważniejszych naruszeń, takich jak złamanie zasad przetwarzania danych, nieprzestrzeganie praw podstawowych osób, których dane dotyczą, lub przekroczenie zakresu przetwarzania danych osobowych, kara może wynieść

[193] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…
[194] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 2024 r., poz. 17 z późn. zm.).

do 20 mln euro lub w przypadku przedsiębiorstwa, do 4% całkowitego rocznego obrotu na skalę światową[195].

Sankcje karne

Zgodnie z art. 107 Kodeksu karnego przetwarzanie danych osobowych w sposób niezgodny z prawem może skutkować karą pozbawienia wolności do lat 2. Jeśli naruszenie przepisów o ochronie danych osobowych zostało dokonane przez osobę pełniącą publiczną funkcję, kara może zostać zaostrzona zgodnie z art. 108 kodeksu karnego, który przewiduje karę pozbawienia wolności do lat 3[196].

2.6. Konsekwencje naruszenia norm cywilnoprawnych

Zasady odpowiedzialności cywilnej

Zgodnie z art. 82 RODO każda osoba, której prawa zostały naruszone w wyniku złamania przepisów o ochronie danych ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za doznane szkody materialne i niematerialne. Oznacza to, że samorządowcy mogą ponieść odpowiedzialność cywilną za naruszenia ochrony danych osobowych. Należy podkreślić, że administrator uczestniczący w przetwarzaniu podobnych informacji odpowiada za szkody spowodowane naruszeniem wyłącznie, gdy nie dopełnił obowiązków, które rozporządzenie RODO nakłada na podmiot przetwarzający, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew instrukcjom[197].

Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający, są oni odpowiedzialni solidarnie za całość szkody. To znaczy, że poszkodowany ma prawo żądać pełnego odszkodowania od każdego z nich. Później kontroler lub procesor, który zapłacił odszkodowanie, może żądać od innych uczestników zwrotu części kosztów proporcjonalnej do ich udziału w odpowiedzialności. Jeśli administrator lub podmiot przetwarzający zapłacił pełne

[195] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…
[196] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 2024 r., poz. 17 z późn. zm.).
[197] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…

odszkodowanie, ma prawo żądać zwrotu części kosztów od pozostałych administratorów lub podmiotów przetwarzających, jeśli także byli zaangażowani w to samo przetwarzanie danych naruszające przepisy[198].

Artykuł 82 RODO posiada szczególne znaczenie dla ochrony praw osób, których dane były przetwarzane. Zasady odpowiedzialności i odszkodowań określone w tym artykule mają na celu zapewnienie, że osoby te będą mogły uzyskać odszkodowanie za szkody poniesione w wyniku naruszenia przepisów o ochronie danych[199].

Artykuł 415 Kodeksu cywilnego mówi: „kto wyrządził drugiemu szkodę z winy swojej, obowiązany jest do jej naprawienia”[200]. Jest to generalna zasada odpowiedzialności cywilnej za szkody, które obejmują również konsekwencje naruszenia przepisów RODO, choć specyfika odpowiedzialności za nieprzestrzeganie RODO jest dalej uregulowana w samym RODO.

Interpretując ten artykuł w kontekście RODO można uznać, że zwrot „Kto wyrządził drugiemu szkodę” prawdopodobnie odnosi się do kontrolera danych lub procesora danych, zajmujących się przetwarzaniem danych osobowych. Natomiast wyraz „drugiemu” może odnosić się do osoby, której dane osobowe są przetwarzane i która doznała szkody w wyniku naruszenia RODO. Wyrażenie „z winy swojej” może obejmować naruszenie wymogów RODO, takich jak niezabezpieczenie danych osobowych, niewłaściwe przetwarzanie danych osobowych lub niezastosowanie się do praw osoby, której dane dotyczą. Z kolei fragment „obowiązany jest do jej naprawienia” – w kontekście RODO, oznacza zazwyczaj wypłacenie odszkodowania pokrzywdzonej osobie.

W praktyce, art. 415 KC może być używany jako podstawa roszczeń odszkodowawczych w przypadku naruszeń RODO, ale zazwyczaj roszczenia te będą oparte na przepisach RODO, które są bardziej szczegółowe i specyficzne w kontekście przetwarzania danych osobowych[201].

Odpowiedzialność za działania podwładnych

W niektórych sytuacjach samorządowcy mogą ponieść odpowiedzialność za naruszenia ochrony danych dokonane przez ich podwładnych zgodnie z art. 430

[198] Ibidem.
[199] Ibidem.
[200] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2023 r., poz. 610 z późn. zm.).
[201] Ibidem.

Kodeksu cywilnego, który przewiduje odpowiedzialność za szkodę wyrządzoną przez osoby trzecie. Artykuł 430 Kodeksu cywilnego w Polsce mówi, że „dłużnik odpowiada za niewykonanie lub nienależyte wykonanie zobowiązania, chyba że niewykonanie lub nienależyte wykonanie zobowiązania jest następstwem okoliczności, za które nie ponosi odpowiedzialności”[202].

Jeśli przeanalizujemy ten artykuł w kontekście RODO, to wyraz „dłużnik” mógłby zostać zinterpretowany jako kontroler lub procesor danych, który ma „zobowiązanie” do przetwarzania danych zgodnie z przepisami RODO. Fragment „odpowiada za niewykonanie lub nienależyte wykonanie zobowiązania” – prawdopodobnie oznacza, iż kontroler lub procesor danych jest odpowiedzialny za niewykonanie lub nienależyte wykonanie swoich zobowiązań wynikających z RODO. Podobna forma odpowiedzialności może obejmować różne aspekty, takie jak brak zabezpieczeń, niewłaściwe przetwarzanie danych, niezastosowanie się do praw podmiotów danych, itp. Zdanie „chyba że niewykonanie lub nienależyte wykonanie zobowiązania jest następstwem okoliczności, za które nie ponosi odpowiedzialności” oznacza, że kontroler lub procesor danych może być zwolniony z odpowiedzialności, jeśli zdoła wykazać związek pomiędzy niewykonaniem lub nienależytym wykonaniem a okolicznościami, za które nie ponosi odpowiedzialności. W kontekście RODO, takie okoliczności mogą obejmować nieprzewidywalne i niekontrolowane zdarzenia, takie jak ataki hackerskie, którym nie dało się zapobiec pomimo stosowania odpowiednich środków bezpieczeństwa.

Wysokość odszkodowania

W przypadku problemów wynikających z niewłaściwej ochrony danych osobowych wysokość odszkodowania jest ustalana indywidualnie, w zależności od skutków naruszenia. Rekompensata może obejmować zarówno straty materialne, jak i niematerialne, takie jak naruszenie praw osobistych, zgodnie z art. 448 Kodeksu cywilnego. Art. 448 Kodeksu cywilnego w Polsce mówi: „Jeżeli w wyniku naruszenia dóbr osobistych powstała szkoda majątkowa, poszkodowany może żądać od sprawcy, żeby ją naprawił”[203].

[202] Ibidem.
[203] Ibidem.

W kontekście RODO, które zobowiązuje do odpowiedniego przechowywania i przetwarzania danych osobowych, wyrażenie „naruszenie dóbr osobistych" może obejmować naruszenie praw wynikających z RODO. Jeżeli dochodzi do naruszenia tych praw, na przykład w wyniku nieodpowiedniego przechowywania lub przetwarzania danych osobowych, poszkodowany ma prawo do żądania naprawienia szkody majątkowej, której doznał. Oznacza to, że jeżeli organizacja, której to dotyczy, naruszyła RODO i w rezultacie poszkodowany doznał szkody majątkowej, poszkodowany może żądać od tej organizacji naprawienia tej szkody. Jest to zgodne z artykułem 82 RODO, który stanowi, że „osoba, której prawa zostały naruszone, ma prawo do odszkodowania od podmiotu przetwarzającego"[204].Warto zauważyć, że szkoda majątkowa nie musi stanowić bezpośredniego rezultatu naruszenia RODO, tylko wynikać pośrednio, na przykład przez utratę szans na rynek pracy lub inny potencjalny dochód.

Warto również pamiętać, że odpowiedzialność za naruszenie RODO jest surowa. Oznacza to, iż podmiotowi przetwarzającemu grozi odpowiedzialność za szkody, nawet jeśli nie miał on zamiaru ich spowodować lub nie mógł przewidzieć, że do nich dojdzie.

Procedura dochodzenia roszczeń

Osoba, której dane osobowe zostały naruszone, może złożyć pozew cywilny przeciwko samorządowcom, domagając się odszkodowania. Proces ten jest regulowany przez kodeks postępowania cywilnego. W praktyce, wielu samorządowców korzysta z ubezpieczenia od odpowiedzialności cywilnej, które może pokryć koszty odszkodowań w przypadku naruszenia ochrony danych osobowych[205]. Warunki takiego ubezpieczenia są regulowane indywidualnie w umowie ubezpieczenia.

2.7. Systemy ochrony danych osobowych w krajach Unii Europejskiej i poza jej granicami – perspektywa porównawcza

W rozważaniach na temat systemu ochrony danych osobowych warto uwzględnić szerszy kontekst. Posłuży nam w tym celu metoda porównawcza (komparatystyczna).

[204] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…
[205] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2023 r., poz. 610 z późn. zm.).

Ujęcie komparatystyczne jest często stosowane w naukach społecznych w tym naukach o bezpieczeństwie jako sposób testowania uogólnionych stwierdzeń.

Porównanie systemu ochrony danych osobowych w różnych państwach może być interesujące z wielu powodów. Po pierwsze, każde państwo posiada swoje własne przepisy i regulacje dotyczące prywatności, dlatego porównanie tych praw może pomóc w zrozumieniu różnic w podejściu do ochrony danych osobowych oraz identyfikacji najlepszych praktyk. Po drugie, porównanie skuteczności tych regulacji może wykazać, które podejścia są bardziej efektywne w zapewnianiu prywatności jednostek, czy na przykład państwa, które stosują surowe kary za naruszenia przepisów, bywają bardziej skuteczne w egzekwowaniu przepisów[206].

W dobie globalizacji i Internetu, wrażliwe dane są wymieniane pomiędzy różnymi państwami. Dlatego też, porównanie praktyk ochrony danych w różnych państwach może pomóc w zrozumieniu, jakie wyzwania stwarza transgraniczny przepływ danych oraz jak różne państwa radzą sobie z tym problemem. Ponadto analiza praktyk ochrony danych może ujawnić innowacyjne metody i najlepsze praktyki, które można adaptować lub wdrożyć w odmiennych jurysdykcjach w celu poprawy ochrony prywatności.

Ważną stroną jednolitości działania systemu ochrony danych osobowych jest współpraca międzynarodowa. Porównanie regulacji dotyczących ochrony danych osobowych w różnych państwach może pomóc w identyfikacji obszarów wymagających harmonizacji dla skuteczniejszej ochrony danych na skalę globalną. Wreszcie, praktyki ochrony danych mogą być silnie związane z kontekstem kulturowym i społecznym danego kraju. Porównawcza analiza pozwala zrozumieć, jakie czynniki kulturowe wpływają na podejście do ochrony prywatności i jak można uwzględnić te różnice w opracowywaniu przepisów.

Jak już pisaliśmy, metoda komparatystyczna pozwala odkryć podobieństwa i różnice między porównywanymi procesami, zdarzeniami, tworami życia politycznego bądź instytucjami politycznymi. Odpowiedni dobór przedmiotu poznania i wyznaczenie przynajmniej dwóch porównywalnych obiektów, reprezentujących określoną klasę zjawisk, pozwala na wyjście poza opis cech jednostkowych oraz na sformułowanie uogólnień stanowiących postawę teorii. W naszych porównaniach obiektami, które

[206] Aczkolwiek doktryna prawna bazuje na teorii, zgodnie z którą do zmniejszenia przypadków naruszania przepisów przyczynia się nie tyle surowość kary, ile jej nieuchronność [R. Nogacki, *Rosną kary, mimo że przestępczość w Polsce spada*, https://kancelaria-skarbiec.pl/wzrost-kar-mimo-spadku-przestepczosci/ [dostęp: 20.03.2024].

zestawiamy jest obowiązujący w Unii Europejskiej system ochrony danych oraz systemy spoza UE. Zakładamy, że takie porównanie może przynieść wartościowe wnioski dla teorii oraz praktyki w zakresie ochrony prywatności, zapewniając bardziej wszechstronne i skuteczne podejście do tego ważnego zagadnienia.

W niniejszej analizie porównawczej pod uwagę zostaną wzięte zarówno kraje Unii Europejskiej, jak i państwa spoza Wspólnoty (m.in. USA, Japonia, Kanada, Brazylia, Indie, Chiny). Różnice w podejściu do ochrony danych osobowych między krajami UE a państwami spoza tego bloku, mogą wykazać na ile polityka RODO jest skuteczna oraz czy ujednolicenie systemu ochrony danych, które wprowadza, jest sukcesem. System ochrony danych osobowych w UE jest znacząco zdeterminowany przez RODO, które stanowi centralną część regulacji dotyczących prywatności w Unii Europejskiej[207], interesujące poznawczo jest zatem, jak radzą sobie państwa nie posiadające podobnej, nadrzędnej dyrektywy. Przepisy RODO mają zapewnić wysoki poziom ochrony danych osobowych, promując jednocześnie innowacje i rozwój gospodarczy poprzez budowanie zaufania do przetwarzania danych w ramach jednolitych i spójnych standardów. Jednocześnie, system ochrony danych osobowych w Unii Europejskiej charakteryzuje się surowymi przepisami, wprowadza jednolite standardy ochrony danych osobowych i dąży do zapewnienia skutecznej ochrony prywatności jednostek[208].

Charakterystyczne cechy systemu ochrony danych osobowych w UE, wynikające z RODO, obejmują:

- szereg obowiązków, nakładanych na podmioty przetwarzające dane, w tym obowiązek uzyskania zgody na przetwarzanie danych, obowiązek prowadzenia rejestrów przetwarzania danych, obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa danych oraz obowiązek powiadamiania organu nadzorczego i osób fizycznych w przypadku naruszenia danych[209];
- RODO nadaje jednostkom szereg praw w zakresie ochrony danych osobowych, w tym prawo do dostępu do danych, prawo do poprawiania nieprawidłowych danych, prawo

[207] B. Wolford, *What is GDPR, the EU's new data protection law*, https://gdpr.eu/what-is-gdpr/ [dostęp: 20.03.2024].
[208] Ibidem.
[209] Zob. *What are my responsibilities under the GDPR?*, https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-are-my-responsibilities-under_en [dostęp: 20.03.2024].

do usunięcia danych („prawo do bycia zapomnianym”), prawo do przenoszenia danych oraz prawo do sprzeciwu wobec przetwarzania danych[210];

- wysokie kary finansowe dla podmiotów przetwarzających dane osobowe w sposób, który naruszają przepisy o ochronie danych. Te kary mogą sięgać nawet do 4% globalnego obrotu rocznego przedsiębiorstwa lub do 20 milionów euro, w zależności od rodzaju naruszenia[211];
- RODO stosuje się do wszystkich rodzajów danych osobowych, niezależnie od sposobu ich przetwarzania i sektora działalności. Dotyczy to zarówno sektora publicznego, jak i prywatnego oraz różnorodnych form przetwarzania danych, w tym internetowych usług, handlu elektronicznego, czy też badań naukowych[212].

Pomimo wprowadzenia jednolitych standardów przez RODO, interpretacja i egzekwowanie przepisów mogą nieco się różnić w poszczególnych krajach członkowskich. Istnieją różnice w zakresie infrastruktury technologicznej, takie jak dostępność zaawansowanych narzędzi do ochrony danych osobowych i środków bezpieczeństwa informatycznego. Państwa posiadające lepiej rozwiniętą infrastrukturę technologiczną mogą łatwiej spełniać wymagania dotyczące bezpiecznego przechowywania i przetwarzania danych osobowych[213]. Ponadto, istnieją różnice w zdolności administracyjnej do nadzorowania i egzekwowania przepisów o ochronie danych osobowych. Niektóre panstwa mogą mieć lepiej wyposażone organy nadzorcze i systemy sądowe, które posiadają wyższą skuteczność w prowadzeniu dochodzeń i nakładaniu sankcji w przypadku naruszeń przepisów RODO. Z tego względu Unia Europejska pracuje nad harmonizacją i wspieraniem państw członkowskich w dostosowywaniu się do wymogów RODO, co ma na celu zapewnienie spójności i skuteczności ochrony danych osobowych we wszystkich krajach członkowskich[214].

Zasadniczo jednak przepisy RODO traktowane są w Unii Europejskiej bardzo poważnie, a wykrywalność przypadków ich naruszenia jest dość wysoka. Według danych udostępnionych przez kancelarię prawną DLA Piper, Bruksela wykazuje dość wysoką

[210] *What are 8 Data Subject rights according to the GDPR*, https://dataprivacymanager.net/what-are-data-subject-rights-according-to-the-gdpr/ [dostęp: 20.03.2024].
[211] *Kary RODO*, https://orodo.pl/kary-rodo/ [dostęp: 20.03.2024].
[212] Zob. R. Koch, *What is considered personal data under the EU GDPR?*, https://gdpr.eu/eu-gdpr-personal-data/ [dostęp: 20.03.2024].
[213] K. Sobczak, *Dr Proksa: Kłopoty z RODO to skutek naszych opóźnień*, https://www.prawo.pl/prawo/rodo-dlaczego-sa-problemy-z-wdrazaniem,313074.html [dostęp: 20.03.2024].
[214] D. Bender, *GDPR harmonization: Reality or myth?*, https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/ [dostęp: 30.03.2024].

skuteczność w egzekwowaniu przepisów dotyczących RODO. W 2021 roku unijne organy ochrony danych nałożyły kary na różne podmioty, osiągając łączną kwotę 1,25 miliarda dolarów za naruszenie prywatności. Jest to wzrost o około 180 milionów dolarów w porównaniu z rokiem 2020. Rok później liczba zgłoszeń naruszeń danych wzrosła o 8 procent, osiągając średnio 356 zgłoszeń każdego dnia. Na liście podmiotów na które nałożono najwyższe kary znalazły się m.in. Amazon (o wartości 746 milionów euro) oraz WhatsApp (o wartości 225 milionów euro)[215].

Prawnicy zwracają uwagę, że większość naruszeń wynika z dwóch głównych powodów. Po pierwsze, firmy nie dotrzymały terminu 72 godzin na powiadomienie odpowiednich organów o zagrożeniu lub wycieku danych użytkowników. Po drugie, zaistniały niedopatrzenia związane z przekazywaniem informacji o klientach między Europą a USA. Ross McKean, jeden z głównych prawników w DLA Piper zauważył, że obecne unijne przepisy stwarzają dość poważne trudności prawne dotyczące ochrony danych osobowych i ich transferu między Stanami Zjednoczonymi a Unią Europejską. Według adwokata, kwestie te wymagają pilnego rozwiązania[216].

Co istotne, Polska zajmuje 13 miejsce pod względem łącznej wysokości kar nałożonych od chwili wejścia w życie przepisów RODO w 2018 r. Wartość kar nałożonych w tym czasie przez Urząd Ochrony Danych Osobowych wyniosła prawie 2,2 mln euro. W regionie Europy Środkowo-Wschodniej wyższe łączne kary nałożył jedynie regulator w Bułgarii i wyniosły one 3,2 mln euro[217].

Analiza systemu ochrony danych osobowych w państwach nienależących do Unii Europejskiej musi uwzględniać fakt, iż państwa te znacząco różnią się pod względem rozwoju gospodarczego, społecznego czy politycznego. Dzieląc jednak świat na regiony rozwinięte i zacofane należy wykazywać się daleko idącą ostrożnością.[218] Obecnie podział na globalną Północ i Południe, który również jest dość umowny, pod

[215] *Unia Europejska pilnuje prywatności. 1,2 mld dol. kar za naruszenie RODO. Polska na 13. Miejscu*, https://www.wirtualnemedia.pl/artykul/unia-europejska-rodo-gdpr-prywatnosc-kary (dostęp: 15.03.2024).
[216] Ibidem.
[217] Ibidem.
[218] Terminologia używana do opisu państw i regionów geograficznych, która opierała się na pojęciach „Trzeci i Pierwszy Świat" lub potocznie „kraje rozwijające się i rozwinięte", nastręcza coraz większych trudności. Terminy „Trzeci i Pierwszy Świat" były używane w czasach zimnej wojny do opisu podziału świata na strefy wpływów bloku wschodniego oraz państw opierających się na gospodarce wolnorynkowej. Problem polega na tym, że wskazane terminy tracą na aktualności przede wszystkim z uwagi na ich wartościujący charakter (gdzie „pierwszy" sugeruje „lepszy", a „trzeci" „gorszy"). Podobnie, terminy „kraje rozwijające się i rozwinięte" mogą być odbierane jako wartościujące, szczególnie gdy ideę rozwoju zawęża się wyłącznie do aspektu gospodarczego – taka perspektywa jest dość nieobiektywna i uproszczona w stosunku do innych aspektów kultury i cywilizacji.

pojęciem globalnej Północy rozumie głównie kraje „Zachodu". W pierwszej kolejności są to państwa Europy i Ameryki Północnej, ale także Australia i Nowa Zelandia, które, choć znajdują się na południowej półkuli, są jednymi z najbardziej uprzemysłowionych i rozwiniętych gospodarczo państw na świecie. Z drugiej strony, globalne Południe obejmuje kraje Afryki, Azji i Ameryki Południowej, które zamieszkuje większość ludności świata – około 66% wszystkich mieszkańców planety[219]. Zgodnie z klasyfikacją Organizacji Współpracy Gospodarczej i Rozwoju (OECD) krajami rozwijającymi się nazywane są państwa, które kwalifikują się do otrzymywania Oficjalnej Pomocy Rozwojowej (ODA). Są to państwa najsłabiej rozwinięte, państwa o niskich dochodach (PKB na mieszkańca poniżej 1 006 USD), średnio-niskich dochodach (PKB na mieszkańca między 1 006 a 3 975 USD) i średnio-wysokich dochodach (PKB na mieszkańca między 3 976 a 12 275 USD). Kraje wysoko rozwinięte według klasyfikacji Banku Światowego to państwa o dochodach powyżej 12 275 USD na mieszkańca[220].

W niniejszej analizie systemu ochrony danych osobowych w krajach spoza Unii Europejskiej nie zdołamy oczywiście scharakteryzować wszystkich państw. Pod lupę zostaną wzięte tylko niektóre z nich, wybrane na podstawie wybranych kryteriów, takich jak znaczenie globalne (a więc znaczący wpływ na światową gospodarkę, politykę i technologię) bądź reprezentatywność dla swoich regionów. Spośród państw rozwiniętych zostały wybrane: Stany Zjednoczone, Japonia, Australia i Kanada; natomiast z grupy państw rozwijających się: Brazylia, Indie, Chiny i RPA (Republika Południowej Afryki)[221].

Stany Zjednoczone

Stany Zjednoczone nie posiadają jednego scentralizowanego prawa ochrony danych osobowych, analogicznego do RODO. System ochrony danych osobowych w Stanach Zjednoczonych charakteryzuje się wieloma przepisami i regulacjami na poziomie federalnym oraz stanowym, które są często skomplikowane i zróżnicowane. Jedną z charakterystycznych cech systemu ochrony danych w USA są duże kary

[219] *Unia Europejska pilnuje prywatności…*
[220] Ibidem.
[221] Zob. *Wskaźniki rozwoju społeczno-gospodarczego*, https://zpe.gov.pl/a/wskazniki-rozwoju-spoleczno-gospodarczego/DJujftdYV [dostęp: 19.03.2024].

nakładane na firmy za naruszenia ochrony danych osobowych[222]. W poszczególnych stanach obowiązują oddzielne (stanowe) przepisy dotyczące ochrony danych osobowych. Prowadzi to nierzadko do chaosu w wymaganiach dotyczących ochrony danych w poszczególnych częściach kraju, ponieważ ustawy te mogą obejmować różne wymogi, np. zgody na przetwarzanie danych, obowiązek informowania o naruszeniach danych lub zasady dotyczące marketingu internetowego. W obliczu braku jednolitej ustawy federalnej o ochronie danych osobowych, inicjatywy na poziomie federalnym mające na celu wprowadzenie bardziej spójnych przepisów, odnoszą pewien skutek. Obecnie rozważa się wprowadzenie federalnej ustawy o ochronie danych i prywatności, która mogłaby bardziej zharmonizować podejście do ochrony danych na szczeblu krajowym[223].

Warto dodać, że Stany Zjednoczone rozważają wprowadzenie „Federal Data Privacy Act", który miałby na celu harmonizację różnorodnych przepisów stanowych oraz wprowadzenie spójnych standardów ochrony danych. Główne różnice w stosunku do RODO obejmują podejście do zgody użytkownika oraz sposoby monitorowania przestrzegania przepisów.[224] Dyskusje toczą się m.in. wokół bardziej elastycznych zasad dotyczących danych wrażliwych w porównaniu z unijnym podejściem.

Japonia

Japonia posiada specjalne prawo dotyczące ochrony danych osobowych, które zostało wprowadzone w 2005 roku. Jest to „Act on the Protection of Personal Information" (APPI), który określa zasady zbierania, przetwarzania i przechowywania danych osobowych oraz prawa jednostek w związku z ich danymi[225].

W 2020 roku Japonia znowelizowała swoją ustawę o ochronie danych osobowych, dążąc do wprowadzenia podobnych rozwiązań do tych obowiązujących w Unii Europejskiej. Zmiany obejmują nową formę zgłaszania naruszeń ochrony danych,

[222] M. Hill, *The biggest data breach fines, penalties, and settlements so far*, https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html [dostęp: 20.03.2024]; M. Mango, *Understanding US Data Privacy Law Fines*, https://www.clarip.com/ blog/understanding-us-data-privacy-law-fines/ [dostęp: 20.03.2024].
[223] A. Klitenic, K. Eige, *Maybe This Time : Federal Government Proposes the American Data Privacy and Protection Act*, https://www.dataprotectionreport.com/2022/06/maybe-this-time-federal-government-proposes-the-american-data-privacy-and-protection-act/ [dostęp: 20.03.2024].
[224] L. Besemer, *Privacy and data protection*, Van Haren Publishing, 's-Hertogenbosch 2020, s. 182–195.
[225] Zob. *The Japan Act on the Protection of Personal Information Explained*, https://www.delphix.com/glossary/japan-act-protection-of-personal-information [dostęp: 16.03.2024].

która będzie wymagała wykorzystania specjalnego formularza oraz większe uprawnienia dla osób, których dane dotyczą, w zakresie dostępu, poprawiania i usuwania swoich danych. Nowe przepisy APPI wymagają również zgody na przekazywanie danych do podmiotów zewnętrznych oraz określają nowe standardy dla przetwarzania danych osobowych zgromadzonych poprzez systemy monitorujące, takie jak rozpoznawanie twarzy. Dodatkowe zmiany w ustawie dotyczą również kar, które mogą być nakładane na administratorów za naruszenia zasad ochrony danych osobowych. Japonia opracowała również kolejne zmiany w przepisach dotyczących międzynarodowego przekazywania danych osobowych, co może być inspirowane rozwiązaniami zawartymi w RODO. Po wprowadzeniu tych zmian „Kraj Kwitnącej Wiśni" stał się liderem w Azji pod względem wdrażania odpowiednich narzędzi ochrony danych osobowych, w stosunku do innych państw regionu[226].

Australia

Obecny system ochrony danych osobowych w Australii opiera się na przepisach prawnych, które wywodzą się z ustawy o ochronie prywatności z 1988 roku (Cth). Są to australijskie przepisy dotyczące prywatności danych, które mają na celu ochronę prywatności osób fizycznych i regulowanie, w jaki sposób niektóre federalne australijskie agencje rządowe i organizacje postępują z danymi osobowymi obywateli Australii. Ustawa była zmieniana na przestrzeni lat[227]. Australijska ustawa o ochronie prywatności reguluje sposób postępowania z tymi danymi przez niektóre federalne agencje rządowe oraz organizacje. Definiuje ona dane osobowe jako informacje lub opinię o zidentyfikowanej osobie, a jej zakres obejmuje większość australijskich jednostek administracji publicznej oraz organizacje o rocznych obrotach przekraczających 3 miliony dolarów, z pewnymi wyjątkami. Ustawa określa również prawa osób fizycznych, takie jak prawo dostępu do swoich danych osobowych, prawo do poprawiania danych oraz prawo do złożenia skargi w przypadku naruszeń[228].

[226] E. Woollacott, *Changes to Japan's data privacy law echo Europe's GDPR*, https://portswigger.net/daily-swig/changes-to-japans-data-privacy-law-echo-europes-gdpr?fbclid=IwAR3aoArcSCu8apJoQ6sgfXcC7Z7H-F3Qj2kteQYn6c4rYZ2_yvZJjk1d5Ys [dostęp: 16.03.2024].
[227] *Australijska Ustawa o ochronie prywatności*, https://www.atlassian.com/pl/trust/compliance/resources/australia-privacy-act [dostęp: 16.03.2024].
[228] Ibidem.

W 2023 roku Australia przygotowywała się do wprowadzenia reformy dotyczącej ochrony danych osobowych, mającej przypominać europejskie RODO. Nowe prawo ma na celu zwiększenie kontroli obywateli nad ich danymi osobowymi oraz ochronę prywatności. Zmiany obejmują prawo do całkowitej rezygnacji z targetowanych reklam oraz możliwość usunięcia danych osobowych z systemów przetwarzających. Nowe przepisy zakładają również zaostrzenie kar dla firm, które nie chronią odpowiednio danych swoich klientów. Nowe przepisy mają również na celu wzmocnienie systemu ochrony danych i prywatności dzieci oraz wprowadzenie mechanizmu zgody na gromadzenie i przetwarzanie danych osobowych. Nowe prawo ma również zostać dostosowane do potrzeb małych firm, które mają być wyłączone z niektórych zapisów, jednakże precyzyjne wytyczne w tej sprawie nie zostały jeszcze ustalone[229].

Warto przywołać raport przygotowany przez DLA Piper odnoszący się do wprowadzanych zmian w australijskim prawie ochrony prywatności w 2024. Obejmuje on m.in. wprowadzenie deliktu naruszenia prywatności, ochronę prywatności dzieci w Internecie, wyższe kary za naruszenia danych, nowe obowiązki dotyczące automatycznych decyzji, oraz mechanizmy umożliwiające bezpieczny transfer danych za granicę.[230] Wprowadzone reformy za sprawą ustawy *Privacy and Other Legislation Amendment Bill* stanowią kluczowy krok w dostosowywaniu prawa do nowoczesnych wyzwań cyfrowych.

Kanada

System ochrony danych osobowych w Kanadzie charakteryzuje się kilkoma istotnymi cechami. Po pierwsze, funkcjonuje tam prawo do prywatności, które chroni dane osobowe obywateli. Głównym aktem prawnym regulującym ochronę danych osobowych jest PIPEDA (Personal Information Protection and Electronic Documents Act). Ponadto ochrona danych osobowych podlega jurysdykcji federalnej, co oznacza, że regulacje dotyczące ochrony danych stosowane są na poziomie federalnym. PIPEDA określa zasady dotyczące zbierania, używania i ujawniania danych osobowych przez

[229] M. Fraser, *Australia szykuje reformę ochrony danych. Prywatność w rękach obywateli?*, https://cyberdefence24.pl/prywatnosc/australia-szykuje-reforme-ochrony-danych-prywatnosc-w-rekach-obywateli [dostęp: 16.03.2024].
[230] DLA Piper, *Australia: Long awaited Australian privacy reform comes to fruition,* https://privacymatters.dlapiper.com/2024/09/australia-long-awaited-australian-privacy-reform-comes-to-fruition/ [dostęp: 14.09.2024].

organizacje działające w sektorze prywatnym. Jedną z głównych zasad jest zasada zgody, która wymaga uzyskania wyraźnego pozwolenia od osób fizycznych do zbieraniem ich danych osobowych, chyba że istnieje prawny wyjątek. Osoby te mają również prawo dostępu do swoich danych osobowych przechowywanych przez organizacje oraz prawo do poprawiania nieścisłości w tych danych. Wszelkie organizacje w Kanadzie są zobowiązane do stosowania odpowiednich środków bezpieczeństwa, aby chronić dane osobowe przed nieuprawnionym dostępem, utratą lub kradzieżą. Nad przestrzeganiem PIPEDA czuwa Urząd Komisarza Ochrony Prywatności Kanady, który może prowadzić dochodzenia w przypadku naruszeń ochrony danych osobowych[231].

System ochrony danych osobowych w Kanadzie napotykał liczne problemy podczas pandemii koronawirusa. Organizacje takie jak Kanadyjskie Stowarzyszenie Swobód Obywatelskich (CCLA) wyrażały obawy co do przechowywania danych medycznych przez rząd Ontario, które zostały udostępnione policji. CCLA złożyło pozew, co skutkowało zamknięciem dostępu do tych danych przez rząd. Jednakże, pytania dotyczące celu udostępnienia tych danych nadal pozostawały bez odpowiedzi. Różne lokalne oddziały policji wykazywały różne podejścia do wykorzystania tych danych, co pokazuje różnorodność w podejściu do kwestii prywatności. Niektóre z nich, jak np. policja w Toronto, nie korzystały z tych danych, podczas gdy inne, jak np. policja regionu Durham, przeszukały bazę danych tysiące razy. Niektóre oddziały policji wyraziły obawy co do bezpieczeństwa prywatności, wskazując na duże ryzyko związane z dostępem do tych informacji[232].

Brazylia

Obecny system ochrony danych osobowych w Brazylii opiera się na Ustawie „Lei Geral de Proteção de Dados" (LGPD), która weszła w życie 16 sierpnia 2020 roku. Miała ona na celu zwiększenie bezpieczeństwa danych osobowych w Brazylii i wprowadzenie zgodności z międzynarodowymi standardami ochrony prywatności danych. Charakter tego aktu prawnego przypomina europejskie RODO. Dotyczy on przetwarzania danych osobowych użytkowników z Brazylii i ma wpływ na firmy

[231] *About the OPC*, https://www.priv.gc.ca/en/about-the-opc/ [dostęp: 20.03.2024]; *About the OPC. What we do*, https://www.priv.gc.ca/en/about-the-opc/what-we-do/ [dostęp: 20.03.2024].
[232] PAP, *Kanada: Obawy o bezpieczeństwo danych osobowych podczas pandemii*, https://www.gazetaprawna.pl/wiadomosci/artykuly/1492501,kanada-pandemia-koronawiurs-bezpieczenstwo-danych-osobowych-osob-zakazonych.html [dostęp: 16.03.2024].

działające w tym kraju. LGPD ujednolica regulacje dotyczące danych osobowych i nadaje określone uprawnienia osobom, których dane są przetwarzane. Obejmują one prawo dostępu, poprawiania danych, anonimizacji oraz przenoszenia danych do innego dostawcy usług[233].

Lei Geral de Proteção de Dados (LGPD) tworzy odpowiednie ramy prawne dla wykorzystywania danych osobowych osób fizycznych w Brazylii, niezależnie od tego, gdzie znajduje się podmiot przetwarzający dane[234]. LGPD różni się od RODO w kilku aspektach. Po pierwsze, LGPD zawiera szerszy zakres przesłanek przetwarzania danych niż RODO. Po drugie, różnice dotyczą zgłaszania naruszeń i wysokości kar finansowych za nieprzestrzeganie przepisów. Wreszcie, LGPD wymaga zatrudnienia Inspektora Ochrony Danych (DPO) przez firmy przetwarzające dane w Brazylii. Maksymalna kara finansowa za naruszenie przepisów LGPD wynosi 2% rocznego dochodu prywatnej osoby prawnej w poprzednim roku podatkowym, do kwoty 50 milionów reali (ok. 11 mln euro)[235].

Chińska Republika Ludowa

W listopadzie 2021 roku chiński Narodowy Kongres Ludowy uchwalił nową ustawę o ochronie danych osobowych Chińskiej Republiki Ludowej. Ustawa przypomina europejskie RODO pod względem poszczególnych regulacji dotyczących przetwarzania danych osobowych oraz surowych kar finansowych. Zakłada ona stworzenie spójnego systemu ochrony prywatności w Chinach, ale może także ograniczyć dostęp chińskich firm technologicznych do danych konsumentów. Podobnie jak RODO, chińska ustawa określa warunki legalnego przetwarzania danych osobowych, przykładowo wymóg uzyskania wyraźnej zgody od osób, których dane dotyczą. Interesującym elementem jest to, że zgoda ta może być wyrażona przez osoby od 14 roku życia, a zgoda rodziców jest potrzebna jedynie dla osób poniżej tego progu wiekowego. Ustawa przewiduje również surowe kary finansowe za naruszenia, sięgające nawet do 50 000 000 juanów chińskich

[233] D. Kraskowska, *Brazylijska ustawa LGPD - nowy akt prawny na temat ochrony prywatności*, https://www.politykabezpieczenstwa.pl/pl/a/brazylijska-ustawa-lgpd-nowy-akt-prawny-na-temat-ochrony-prywatnosci [dostęp: 17.03.2024].
[234] *Brazylijska ogólna ustawa o ochronie danych-LGPD*, https://www.ibm.com/docs/pl/order-management?topic=regulations-brazilian-general-data-protection-law-lgpd [dostęp: 17.03.2024].
[235] D. Kraskowska, *Brazylijska ustawa LGPD*…

(około 27 820 913,62 złotych według kursu z 17 marca 2024 roku) lub 5% rocznych przychodów administratora danych[236].

Pomimo podobieństw do RODO ustawa chińska zawiera również pewne unikalne rozwiązania, na przykład uprawnienie określonych administratorów do przetwarzania danych osobowych w celu nadzoru nad opinią publiczną, co nie jest charakterystyczne dla standardów europejskich. Jednakże, jak w przypadku RODO, organ nadzorczy ma prawo nałożyć kary zarówno na administratora danych osobowych, jak i na osoby bezpośrednio odpowiedzialne za naruszenie[237].

W ocenie Mateusza Kupca nowe chińskie przepisy z zakresu ochrony danych osobowych, na pewno przyczynią się do zwiększenia świadomości obywateli ChRL na temat przetwarzania ich danych osobowych. Europejskie przedsiębiorstwa współpracujące z chińskimi podmiotami gospodarczymi powinny mieć zatem na uwadze przepisy PIPL w szczególności z racji eksterytorialnego zakresu stosowania ustawy. Przepisy „chińskiego RODO" mają bowiem nie tylko znaczenie lokalne, lecz aktywnie przyczyniają się do tworzenia zasad dotyczących międzynarodowego transferu danych. Niemniej jednak administratorzy przekazujący dane osobowe do ChRL nadal powinni kierować się szczególną ostrożnością i odpowiednio zabezpieczyć transfer danych. Jest jeszcze zbyt wcześnie na jakąkolwiek ocenę PIPL. W Chinach nadal brakuje niestety (faktycznie) niezależnego, centralnego organu nadzorczego z zakresu danych osobowych, który mógłby skutecznie egzekwować przepisy PIPL i ustanowić jednolite standardy w zakresie ochrony prywatności. Tym samym istnieje ryzyko, że przepisy PIPL będą w praktyce egzekwowane instrumentalnie przez chińskie władze i staną się kolejnym (odstraszającym) narzędziem kontroli społeczeństwa, przedsiębiorców[238].

W tym zakresie istotnym jest przeprowadzone zastawienie podobieństw i różnic pomiędzy chińską ustawą o ochronie danych osobowych, *Personal Information Protection Law* (PIPL), oraz jej wpływie na prywatność obywateli i globalny porządek cyfrowy z unijnym RODO oraz kalifornijskim *California Consumer Privacy Act* (CCPA). Analiza przeprowadzona przez Wydawnictwo naukowe Multidisciplinary Digital Publishing Institute (MDPI) z siedzibą w Szwajcarii, wskazuje, że PIPL zbliża się do

[236] J. Strzelecki, *RODO w Chinach - polska firma będzie musiała uzyskać zgodę Chińczyka*, https://firma.rp.pl/chiny/art19049501-rodo-w-chinach-polska-firma-bedzie-musiala-uzyskac-zgode-chinczyka-dane-osobowe-chinskie-RODO [dostęp: 17.03.2024].
[237] Ibidem.
[238] *Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej*, https://www.traple.pl/ustawa-o-ochronie-danych-osobowych-chinskiej-republiki-ludowej/ [dostęp: 17.03.2024].

standardów europejskich, szczególnie pod względem ochrony danych i wymogu uzyskiwania zgody na ich przetwarzanie. RODO i PIPL są bardziej restrykcyjne niż CCPA, jednak chińska ustawa kładzie większy nacisk na kontrolę rządową i umożliwia monitorowanie opinii publicznej. CCPA ma bardziej ograniczone wymogi dotyczące zgody i mniejsze kary za naruszenia w porównaniu do PIPL i RODO.[239] Tym samym możemy przyjąć, że stworzone są silne mechanizmy ochrony danych, które przy tym umożliwiają państwu monitorowanie obywateli.

Indie

System ochrony danych osobowych w tym kraju opiera się obecnie na „Nowej ustawie o ochronie danych osobowych w Indiach", zatwierdzonej przez indyjski parlament w sierpniu 2023 roku. Ten akt prawny miał na celu uregulowanie kwestii przetwarzania cyfrowych danych osobowych w sposób zgodny z prawem, uwzględniając prawa osób fizycznych do ochrony ich prywatności oraz potrzeby legalnego przetwarzania danych osobowych. Ustawa ma zastosowanie do danych osobowych przetwarzanych na terenie Indii, a także do danych przetwarzanych poza granicami kraju przez firmy oferujące towary lub usługi na terenie Indii[240].

W projekcie omawianej ustawy, dane osobowe zdefiniowano jako informacje dotyczące osoby fizycznej, która może być zidentyfikowana na ich podstawie lub z nimi powiązana, a przetwarzanie to operacje wykonywane na tych danych. Kluczowe elementy ustawy obejmują:

- konieczność uzyskania zgody osoby, której dane dotyczą, na przetwarzanie danych osobowych zgodnie z prawem, w tym szczegółowe informacje na temat celu przetwarzania i zbieranych danych;
- podstawowe zasady przetwarzania danych osobowych, takie jak zasada zgody, legalności, przejrzystości, minimalizacji danych, prawidłowości danych, ograniczenia przechowywania i rozsądnych środków bezpieczeństwa;

[239] I. Calzada, *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law* (PIPL), https://www.mdpi.com/2624-6511/5/3/57 [dostęp: 15.09.2024].
[240] *Parlament Indii uchwala ustawę o ochronie cyfrowych danych osobowych z 2023 roku*, https://www.consentmanager.pl/wiedza/indie-ustawa-cyfrowa-o-ochronie-danych-osobowych-2023/ [dostęp: 17.03.2024].

- wzmocnienie praw osób fizycznych, takich jak prawo do informacji o przetwarzaniu danych, sprostowania i usunięcia własnych danych oraz wyznaczenia przedstawiciela do spraw ochrony danych w przypadku śmierci lub niezdolności do działania;
- środki ochrony praw dzieci, w tym zakaz przetwarzania danych, które mogą wpływać na dobro dzieci lub polegać na śledzeniu ich zachowań lub ukierunkowanej reklamie oraz konieczność uzyskania zgody rodziców na przetwarzanie danych dzieci[241].

W ocenie Magdaleny Abu Gholeh i Dominiki Kuźnickiej-Błaszkowskiej do rozwoju indyjskiego systemu ochrony danych osobowych przyczyniły się podmioty gospodarcze. Ich zdaniem charakterystyczny dla Indii ogromny rynek usług outsourcingowych powoduje, że prywatni przedsiębiorcy sami wymuszają odpowiednie zmiany w tym zakresie. Silne związki gospodarcze z przedsiębiorstwami zarejestrowanymi w krajach Unii Europejskiej powodują, że nawet w przypadku braku regulacji ustawowej, związki przedsiębiorców indyjskich dokonują swoistej samoregulacji. Nie można również zapominać o wpływie umów gospodarczych zawieranych między przedsiębiorcami z Indii i Unii Europejskiej – często to właśnie europejskie podmioty zamawiające w swoich umowach wymuszają zmiany w zakresie zabezpieczeń technicznych i organizacyjnych danych osobowych, tak aby przetwarzać dane zgodnie z wytycznymi RODO”[242].

Porównując ustawę z 2023 roku z unijnym RODO, należy dostrzec kilka istotnych różnic. Po pierwsze, indyjska ustawa obejmuje jedynie dane cyfrowe, podczas gdy RODO reguluje wszystkie dane osobowe. Po drugie, obie ustawy wymagają zgody na przetwarzanie danych, ale indyjska ustawa nie przewiduje przetwarzania na podstawie uzasadnionego interesu. Ostatnią różnicą jest to, że obie ustawy umożliwiają międzynarodowe transfery danych, jednak indyjska może ograniczać wybrane podmioty zagraniczne.[243]

[241] Ibidem.
[242] M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Ochrona danych osobowych w wybranych państwach Azji*, Wrocław 2019, s. 89.
[243] Global Privacy & Security Compliance Law Blog, *India’s Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison,* https://www.globalprivacyblog.com/2023/12/indias-digital-personal-data-protection-act-2023-vs-the-gdpr-a-comparison/ [dostęp: 12.09.2024].

RPA (Republika Południowej Afryki)

System ochrony danych osobowych w RPA warto analizować w kontekście procesów obejmujących cały kontynent. W wielu krajach afrykańskich zauważa się rosnące zainteresowanie uregulowaniem kwestii ochrony danych osobowych, szczególnie od czasu wprowadzenia RODO w Unii Europejskiej. Obecnie już połowa tych państw posiada przepisy dotyczące ochrony danych, chociaż proces ich wprowadzenia napotyka na wiele trudności, w tym brak odpowiednich środków finansowych i wykwalifikowanej kadry. W niektórych krajach, takich jak Kamerun, regulacje dotyczące ochrony danych wprawdzie zostały przyjęte, ale nie powołano przy tym odpowiednich organów nadzorujących ich egzekwowanie[244].

Specyfika afrykańskiego kontekstu sprawia, że niektóre kraje decydują się na sektorowe regulacje dotyczące ochrony danych, podobnie jak ma to miejsce w Stanach Zjednoczonych. Na przykład, regulacje dotyczące ochrony danych w sektorze finansowym zostały uchwalone przez Wspólnotę Gospodarczą Państw Afryki Środkowej. Ponadto, orzecznictwo odgrywa istotną rolę we wskazywaniu obszarów, w których państwo zajmuje się ochroną danych, gdyż niektóre firmy były karane za naruszenia przepisów. Niektóre kraje afrykańskie, takie jak Senegal czy Kenia, posiadają kompleksowe akty prawne regulujące ochronę danych osobowych. Oprócz tego, podejmowane są działania edukacyjne, nastawione na zwiększenie świadomości obywateli na temat ochrony danych. Dla przykładu, na terenie Senegalu uruchomiono stronę internetową, na której regularnie publikowane są raporty dotyczące działań organu ochrony danych[245].

Dnia 1 lipca 2020 roku w Republice Południowej Afryki weszła w życie ustawa o ochronie danych osobowych (POPIA), choć niektóre z jej przepisów zaczęły obowiązywać dopiero od 30 czerwca 2021 roku, aby dać czas organizacjom na dostosowanie się. Prace nad ustawą rozpoczęły się w 2003 roku, a inspiracją był głównie europejski wzorzec zawarty w Dyrektywie 95/46/WE Parlamentu Europejskiego. Nowe przepisy miały na celu popularyzację ochrony danych osobowych w RPA i zapewnienie prawa do prywatności, zgodnie z Kartą Praw. Ustawa nakłada obowiązek zgłaszania naruszeń ochrony danych i egzekwowania przepisów, które będą

[244] O. Modo, *Ochrona danych w Afryce*, https://gov.legalis.pl/ochrona-danych-w-afryce/ [dostęp: 17.03.2024].
[245] Ibidem.

miały pułap finansowy kar sięgający około 580 milionów dolarów. Pomimo 12-miesięcznego okresu karencji, wiele organizacji zdołało wcześniej dostosować się do wymogów ustawy, która wprowadza standardy zbliżone do globalnych i najbardziej efektywnych praktyk w zakresie ochrony danych osobowych[246].

Zdaniem Omni Modo, wzmożone zainteresowanie kwestiami dotyczącymi prawa do prywatności, nie tylko w Afryce Południowej, ale również globalnie to niewątpliwie „zasługa" pandemii COVID-19. W związku ze zjawiskiem tworzenia baz danych zawierających dane wrażliwe oraz wprowadzania aplikacji służących do śledzenia kontaktów ochrona prywatności stała się tematem znajdującym się w centrum uwagi światowych rządów[247].

Porównując systemy danych osobowych funkcjonujące w wielu państwach pozaeuropejskich, można z całą pewnością stwierdzić, że na ich tle RODO wypada całkiem dobrze, można nawet zasugerować, że jest jednym z najnowocześniejszych aktów prawnych dotyczących ochrony danych osobowych na świecie. Świadczy o tym fakt, że wiele państw wzoruje się na prawie europejskim podczas tworzenia własnych aktów regulujących kwestie związane z zabezpieczaniem danych osobowych. Widać to na przykładach ustaw w Brazylii, Chinach, Indiach czy Republice Południowej Afryki. Regulacje wprowadzane przez rządy tych państw często zawierają podobne lub zbliżone zasady i wymagania dotyczące przetwarzania danych osobowych, zgody na przetwarzanie oraz zasady karania za naruszenia oraz inne aspekty. Dlatego można uznać, że obecnie RODO stanowi punkt odniesienia dla wielu państw w opracowywaniu nowoczesnych regulacji dotyczących ochrony danych osobowych. Świadczy to również o jego skuteczności, o której można mówić po sześciu latach stosowania. Bardziej szczegółowe wnioski wymagałby dalszych porównań ustaw krajowych państw pozaeuropejskich z poszczególnymi artykułami RODO, wykracza to jednak poza temat niniejszej rozprawy.

Warto natomiast na podstawie powyższej analizy porównawczej zadać pytanie czy jakieś korzyści wynikają dla naszego kraju z przyjęcia RODO? Naszym zdaniem są to korzyści całkiem wymierne. Po pierwsze, wzrost liczby państw stosujących podobne lub zbieżne przepisy o ochronie danych osobowych może prowadzić do większej harmonizacji międzynarodowych standardów w tym zakresie. Ułatwia to wymianę

[246] O. Modo, *Republika Południowej Afryki obiera kurs na ochronę danych*, https://gov.legalis.pl/republika-poludniowej-afryki-obiera-kurs-na-ochrone-danych/ [dostęp: 17.03.2024].
[247] Ibidem.

danych osobowych między Polską a innymi krajami oraz zwiększa zaufania partnerów handlowych do polskiego systemu ochrony danych. Jako członek Unii Europejskiej, Polska jest zobowiązana do stosowania przepisów RODO, ale także musi być świadoma ewolucji międzynarodowych standardów dotyczących ochrony danych osobowych. Konieczne jest ciągłe monitorowanie i dostosowywanie krajowych regulacji do zmieniających się realiów oraz najnowszych praktyk i standardów międzynarodowych. Wzorowanie się innych państw na RODO może prowadzić do zwiększenia znaczenia roli polskiego organu nadzorczego ds. ochrony danych osobowych (UODO) w międzynarodowej przestrzeni. UODO może pełnić rolę wzorca dla innych. Gdyby tak się stało, to przyczyniłoby się to do wzmocnienia autorytetu Polski w obszarze systemów ochrony danych osobowych na arenie międzynarodowej.

2.8. Ochrona danych osobowych, a dalszy postęp cywilizacyjny – próba prognozy

Dzisiejsze prognozy dotyczące świata przeszłości obejmują w pierwszej kolejności rozważania dotyczące rozwoju nauk ścisłych i technologii. Oczywisty postęp w dziedzinie technologii przewiduje dalszą ekspansję i rozpowszechnienie się innowacji, które zmienią sposób, w jaki funkcjonuje ludzkie społeczeństwo. Szereg dziedzin technologicznych ma potencjał dalszego rozwoju, a wśród z nich wyróżnia się szczególnie sztuczna inteligencja (SI). Owa technologia stanowi obecnie jeden z najbardziej dynamicznie rozwijających się obszarów. Technologie oparte na SI, takie jak uczenie maszynowe i głębokie sieci neuronowe, znajdują zastosowanie w różnych dziedzinach, od analizy danych po automatyzację procesów przemysłowych i usprawnienie diagnostyki medycznej. Prognozuje się, że dalsze postępy w dziedzinie SI doprowadzą do powstania jeszcze bardziej zaawansowanych systemów, które będą zdolne do wykonywania skomplikowanych zadań intelektualnych[248]. Komunikacje i technologie informacyjne w postaci sieci 5G, Internetu rzeczy, rozszerzonej rzeczywistości i wirtualnej rzeczywistości to tylko niektóre z technologii, które oferują nowe możliwości w zakresie komunikacji, rozrywki, edukacji i pracy. Ekonomiczne przekształcenia, spowodowane głównie przez wzrost globalizacji i dalszy rozwój technologiczny, będą miały znaczący wpływ na strukturę gospodarczą oraz na

[248] S. A. Efimova, *Developement of artificial intelligence*, „Digital Science", nr 6/2020, s. 55-56.

sposób funkcjonowania firm i rynków. Dalszy postęp globalizacji[249] oznacza coraz większą integrację gospodarczą i handlową między krajami. Firmy mają już teraz dostęp do szerszego rynku zbytu, co stwarza możliwości zarówno dla ekspansji, jak i konkurencji. Przekształcenia w strukturze gospodarczej obejmują rozwój nowych sektorów, takich jak technologie informacyjno-komunikacyjne, biotechnologia, energia odnawialna czy usługi oparte na przepływie danych. Firmy będą musiały dostosowywać się do tych zmian, inwestując w nowe technologie i umiejętności, aby pozostać konkurencyjnymi.

Z uwagi na powyższe czynniki zmiany w dotychczasowych sposobach produkcji i dystrybucji wydają się nieuniknione. Rozwój technologii automatyzacji, robotyzacji i sztucznej inteligencji prowadzący do transformacji procesów produkcyjnych może skutkować zwiększeniem efektywności produkcji obniżeniem jej kosztów i poprawą jakości wyrobów. Równocześnie może to prowadzić do utraty miejsc pracy wśród kadr, stanowiących nisko wykwalifikowaną siłę roboczą. Firmy będą musiały zarządzać tą transformacją, aby minimalizować negatywne skutki społeczne i gospodarcze. Automatyzacja pracy[250] jest zjawiskiem, które prawdopodobnie będzie się nasilać wraz z postępem technologicznym. Robotyka, sztuczna inteligencja i maszyny uczące się będą coraz częściej zastępować ludzi w wielu obszarach, od produkcji przemysłowej po usługi klienta. To z kolei będzie wymagało przekształceń w systemie edukacji i szkoleń, aby ludzie mogli zdobyć nowe umiejętności dostosowane do coraz bardziej zautomatyzowanych miejsc pracy. Postęp technologiczny bez wątpienia ma szanse wpłynąć na rozwój ekonomii cyfrowej[251] i handlu internetowego[252] przekształcając obecne sposoby dystrybucji dóbr i usług. Firmy będą musiały dostosowywać się do preferencji klientów, którzy coraz częściej korzystają z zakupów online, co może prowadzić do zmian w modelach biznesowych i strategiach marketingowych.

Jeśli powyższe prognozy się ziszczą, to przewidywane ekonomiczne przekształcenia będą wymagały elastyczności i innowacyjności ze strony firm, instytucji oraz jednostek społecznych, aby móc skutecznie konkurować i prosperować

[249] O.B. Skorodumova, *Scientific and technological progress and globalization: achievements and risks*, „Symbol of Science", nr 2/2016, s. 39-40.
[250] M. Budka, *Automatyzacja pracy – jak wpływa na rynek zatrudnienia?*, https://www.money.pl/gospodarka/automatyzacja-pracy-jak-wplywa-na-rynek-zatrudnienia-6769823796616160a.html [dostęp: 20.03.2024].
[251] U.A. Berdieva, *Developement of the Digital economy*, „Economics And Business: Theory And Practice", nr 2-1(72)/2021, s. 31-32.
[252] Zob. M. Kawa, *Tendencje rozwoju handlu elektronicznego*, „Przedsiębiorczość – Edukacja", nr 1/2022.

w dynamicznym i coraz bardziej zglobalizowanym środowisku gospodarczym. Postęp cywilizacyjny wraz z jego wyzwaniami, ale też problemami, niewątpliwie wywrze istotny wpływ na sferę bezpieczeństwa cybernetycznego i prywatności danych. Wraz z coraz większą cyfryzacją naszego społeczeństwa, wzrasta ryzyko ataków cybernetycznych, kradzieży tożsamości i naruszeń prywatności danych. Bezpieczeństwo cybernetyczne stanie się coraz bardziej istotnym wyzwaniem dla firm, rządów i jednostek społecznych. Przyszłość systemów ochrony danych osobowych będzie silnie ukształtowana przez szereg czynników, które zostały opisane wcześniej i które dotyczą technologicznego postępu oraz zdolności adaptacji świadomości społecznej do nowych warunków. Poniżej przedstawiono kilka kierunków, w jakich mogą ewoluować systemy ochrony danych osobowych:

- Rozwój technologii bezpieczeństwa cyfrowego: w odpowiedzi na rosnące zagrożenia związane z cyberatakami[253], można się spodziewać dalszego rozwoju technologii bezpieczeństwa cyfrowego, takich jak zaawansowane systemy szyfrowania, identyfikacja biometryczna, analiza zachowań użytkowników, narzędzia do zarządzania danymi osobowymi, blokowania śledzenia online oraz anonimizacji danych. Te innowacje mogą pomóc w zabezpieczeniu danych osobowych przed nieautoryzowanym dostępem i nadużyciami;
- Regulacje prawne i normy dotyczące ochrony danych: wzrastająca świadomość i zaniepokojenie społeczne dotyczące prywatności danych osobowych mogą prowadzić do wprowadzania coraz bardziej restrykcyjnych regulacji prawnych i norm ochrony danych. Państwa mogą wprowadzać nowe ustawy o ochronie danych oraz zaostrzać kary za naruszenia przepisów, aby zwiększyć odpowiedzialność organizacji za bezpieczeństwo danych osobowych;
- Polityka prywatności i kontroli danych w przedsiębiorstwach komercyjnych: wraz z postępem technologicznym oraz zmianami prawnymi spółki prywatne będą musiały dostosować się do rosnących oczekiwań konsumentów w zakresie jakości ochrony danych;
- Globalne standardy ochrony danych: w miarę postępującej globalizacji istotne stanie się ustanowienie uniwersalnych standardów ochrony danych osobowych i współpraca

[253] *Cyberataki – co powinieneś o nich wiedzieć?*, https://szybkafaktura.pl/blog/cyberataki-co-powinienes-o-nich-wiedzec/ [dostęp: 20.03.2024].

międzynarodowa w dziedzinie cyberbezpieczeństwa[254]. Takie standardy mogą pomóc w opracowaniu spójnych norm ochrony danych na całym świecie i ułatwić wymianę informacji między poszczególnymi krajami;

- Edukacja i świadomość społeczna: adekwatny poziom świadomości społecznej w zakresie ochrony danych osobowych będzie kluczowy dla skuteczności systemu. Edukacja konsumentów na temat zagrożeń związanych z wyciekiem wrażliwych danych oraz sposobów ich zabezpieczania może pomóc w zmianie zachowań i postaw wobec prywatności online[255].

W ramach podsumowania można powiedzieć, że przyszłość systemów ochrony danych osobowych będzie kształtowana przez dynamiczny rozwój technologii, zmieniające się regulacje prawne, świadomość społeczną oraz globalną współpracę. Dążenie do zapewnienia bezpieczeństwa i prywatności danych będzie wymagało współpracy pomiędzy przedsiębiorstwami, rządami państw, organizacjami międzynarodowymi oraz konsumentami.

Prognozowanie przyszłości systemów ochrony danych jest bez wątpienia obarczone wysokim stopniem niepewności. Niemniej jednak, analizując obecne tendencje i przemiany, możemy próbować przygotować się na potencjalne wyzwania i szanse, jakie mogą pojawić się za kilkanaście lub kilkadziesiąt lat. Jedno nie ulega wątpliwości: trzeba być elastycznym i gotowym do adaptacji w obliczu zmieniających się warunków życia. Należałoby postawić w tym miejscu pytanie: na ile administracja publiczna gotowa jest do tych zmian oraz co należy brać pod uwagę w ewentualnych przygotowaniach w zakresie kształcenia kadr jednostek samorządu terytorialnego, mającego pieczę nad danymi osobowymi?

Próba odpowiedzi na to pytanie stanowi temat związany z ogólnym działaniem dobrej administracji, który wynika z konieczności praktycznej natury. Ponieważ sposób funkcjonowania administracji był i nadal pozostaje jednym z najpoważniejszych czynników wpływających zarówno na sposób funkcjonowania gospodarki oraz poziom jej rozwoju, jak i na kształt społeczeństwa.[256] Działanie administracyjne ma do spełnienia nie tylko cały szereg funkcji praktycznych, takich jak usługi, ale równolegle spełnia także wobec społeczeństwa rolę wychowawczą, kształtującą relacje społeczne.

---

[254] Zob. Ministerstwo Cyfryzacji, *Cyberbezpieczeństwo*, https://www.gov.pl/web/cyfryzacja/cyber bezpieczenstwo [dostęp: 20.03.2024].
[255] M. Lorek, A. Pieczywok, *Rola edukacji dla bezpieczeństwa w kontekście zagrożeń cyberprzestępczością*, „Edukacja – Technika – Informatyka" nr 1/2019, s. 214-215.
[256] J. Filek, *W poszukiwaniu dobrej administracji*, „Zarządzanie Publiczne", nr 2(2), 2007, s. 27.

Podmioty publiczne i niepubliczne przetwarzają informacje na ogromną skalę na przykład w postaci tak zwanego Big Data, czyli ogromnych ilości różnorodnych i zmiennych danych przetwarzanych błyskawicznie dzięki zastosowaniu nowych technologii. Umożliwia to szybkie wyciąganie wniosków, służących m.in. wprowadzaniu ulepszeń technologicznych i tworzeniu profili osobowych. Sposób i zakres przetwarzania danych i brak kontroli nad podmiotami przetwarzającymi sprawia jednak, że przetwarzanie to jest również źródłem zagrożeń, w szczególności, gdy jest ono dokonywane w niewłaściwym celu, zakresie lub przez nieuprawnione podmioty.[257] Już dzisiaj ataki cybernetyczne skutkujące wyciekiem danych do sieci, rozwój przestępczości cybernetycznej, wykradanie tożsamości, nielegalna sprzedaż danych do celów marketingowych oraz niekontrolowane i niezgodne z prawem przetwarzanie tych danych, są coraz częstszymi zjawiskami, należy więc przywidywać ich dalszy rozwój, a wraz z nimi jeszcze większe szkodliwe społecznie skutki, których eliminowanie jest w interesie publicznym. Przed administracją publiczną, i tak przeciążoną już dzisiaj, stanie jeszcze więcej zadań w zakresie funkcji policyjnej administracji, której celem jest zapewnienie porządku i bezpieczeństwa publicznego.

Koniecznym przy tak szybko postępującym rozwoju procedur cyfrowych w administracji publicznej, będzie odpowiednie przygotowanie kadrowe. Anna Łukaszuk w pracy *Problematyka kompetencji cyfrowych kadr administracji publicznej jako istotnego czynnika procesu transformacji cyfrowej jednostek samorządu terytorialnego w Polsce* zwraca uwagę: „Problem braku wysoko kwalifikowanych kadr po stronie administracji publicznej w obszarze nowoczesnych technologii ICT jest sygnalizowany od wielu lat. Podkreśla się fakt, że kompetencje cyfrowe administracji nie mogą ograniczać się do sfery czysto technicznej. Technologia nie jest celem samym w sobie. Administracja powinna zbudować kompetencje w praktycznym stosowaniu technologii cyfrowych, tak by odpowiadać na realne potrzeby, niwelować bariery, upraszczać procesy i zmniejszać koszty własnego funkcjonowania”[258] Administracja powinna zatem stale rozwijać swoje kompetencje cyfrowe tak, aby nadążyć za zmieniającym się środowiskiem. Cytowana autorka wykazuje, że to właśnie obecnie prezentowane priorytety Unii Europejskiej w zakresie transformacji cyfrowej oraz kompetencji cyfrowych, w sposób bezpośredni, chociażby w aspekcie finansowym (możliwość pozyskiwania środków na realizację założeń transformacji), kształtują sytuację polskich

[257] M. Błażewski, J. Behr, op. cit., s. 21.
[258] A. Łukaszuk, op. cit., s. 289-290.

jednostek samorządu terytorialnego. Wprowadzane przez polskiego ustawodawcę stosowne akty prawne, przyjmujące postać strategii i programów, na przykład Program Zintegrowanej Informatyzacji Państwa, Program Rozwoju Kompetencji Cyfrowych do 2030 roku, Krajowa Strategia Rozwoju Regionalnego 2030, zdają się jednak być w tej sferze niewystarczające. Zdaniem A. Łukaszuk: „Polska nie wykorzystuje potencjału technologii cyfrowych, czego wyrazem jest m.in. wartość indeksu cyfrowej gospodarki i społeczeństwa cyfrowego (DESI) plasująca nasz kraj na jednej z ostatnich pozycji wśród państw Unii Europejskiej. Na ten wynik znaczący wpływ ma niski poziom kompetencji cyfrowych. Progres w zakresie podnoszenia kompetencji cyfrowych kadr administracji publicznej jest niezadawalający i stanowi zasadniczą barierę w procesie transformacji cyfrowej jednostek samorządu terytorialnego”.[259] Sam zakres kompetencji cyfrowych obejmuje umiejętność korzystania z informacji i danych, komunikowanie się i współpracę, umiejętność korzystania z mediów, tworzenie treści cyfrowych (w tym programowanie), bezpieczeństwo (w tym komfort cyfrowy i kompetencje związane z cyberbezpieczeństwem), kwestie dotyczące własności intelektualnej, rozwiązywanie problemów i krytyczne myślenie.[260] Według zaleceń Rady Unii Europejskiej budowanie kompetencji cyfrowych jest wyzwaniem, które wymaga podjęcia szeregu działań o wymiarze strategicznym, nastawionym na realizację wieloaspektowych i długofalowych przedsięwzięć, a same kompetencje cyfrowe – obok czytania, pisania, umiejętności matematycznych i językowych – stanowią zespół fundamentalnych umiejętności współczesnego człowieka.[261] W literaturze odnoszącej się do pojęć cyfryzacji i transformacji cyfrowej pojęcie kompetencji w tym zakresie określane jest jako e-kompetencje, kompetencje cyfrowe (*digital competences*), umiejętności cyfrowe (*digital skills, e-skills*) czy alfabetyzacja cyfrowa (*digital literacy*).[262] Można więc mówić

[259] Ibidem, s. 290.
[260] Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie, https://eurlex.europa.eu/legalcontent/PL/TXT/?uri=CELEX%3A32018H0604% 2801%29 [data dostępu: 5.05.2022].
[261] Ibidem.
[262] Opracowany na zlecenie Komisji Europejskiej model DIGCOMP definiuje pięć podstawowych obszarów e-kompetencji. Kompetencje te obejmują również bardziej zaawansowane umiejętności z zakresu komunikacji, takie jak interakcje społeczne z pomocą technologii, dzielenie się informacją i treściami, partycypacja obywatelska online, współpraca online, zarządzanie tożsamością cyfrową, z zakresu współpracy, zarządzania wiedzą, uczenia się i rozwiązywania problemów technicznych, określanie potrzeb i ich rozwiązań, innowacyjność i kreatywność z pomocą technologii, określanie luk w kompetencjach cyfrowych, z zakresu treści ich tworzenia i łączenia, prawa autorskiego i licencjonowania, programowania oraz z zakresu bezpieczeństwa zabezpieczanie urządzeń, zabezpieczanie danych i tożsamości cyfrowej, ochrona zdrowia, ochrona środowiska, A. Łukaszuk, op. cit., s. 292.

o nowym, globalnym języku porozumiewania się, jakim stał się język cyfrowy oraz idące wraz z nim umiejętność posługiwania się kompetencjami, urządzeniami itd. Do szeroko definiowanych kompetencji cyfrowych zaliczane jest także tzw. myślenie komputacyjne, którym określa się zdolność znajdywania rozwiązań skomplikowanych, otwartych problemów, na ogół z wykorzystaniem technologii cyfrowych oraz analizy danych. Umiejętności te obejmują zdolność do wyszukiwania danych, krytyczną ocenę jakości źródeł, z jakich pochodzą, analizę danych oraz efektywne zarządzanie informacją, w tym także cyfrowe umiejętności graficzne. Zadania stojące przed administracją publiczną w erze cyfrowej polegać zatem będą na wprowadzaniu społeczności lokalnej w kompetencje cyfrowe (wracamy w tym miejscu do wychowawczej roli administracji publicznej). Jedynym z celów „Cyfrowego Kompasu", w ramach II Europejskiej agendy cyfrowej, które mają zostać osiągnięte do 2030 roku, jest założenie, aby wszystkie kluczowe usługi publiczne były dostępne online, wszyscy obywatele mieli dostęp do swojej elektronicznej dokumentacji medycznej, a 80% obywateli powinno korzystać z rozwiązań w zakresie tożsamości elektronicznej.[263] Jest to cel dosyć ambitny, biorąc pod uwagę polskie uwarunkowania cyfrowe (np. dostępność do Internetu). Parlament Europejski i Rada Unii w kwietniu 2021 r. wydała rozporządzenie ustanawiające program „Cyfrowa Europa" (*Digital Europe Programme* – DEP) na lata 2021–2027. Program ma zapewnić strategiczne finansowanie w celu wsparcia projektów w pięciu obszarach, z którego jeden dotyczy zaawansowanych umiejętności cyfrowych i tematyki e-administracji (*eGovernment*). Jednostkom samorządu terytorialnego takie strategiczne działania na poziomie unijnym stwarzają szanse podnoszenia kwalifikacji cyfrowych, zarówno na poziomie kadrowym, jak też świadczonych usług. Plan działania w dziedzinie edukacji cyfrowej na lata 2021–2027 jest inicjatywą polityczną mającą wspierać zrównoważone i skuteczne dostosowanie obowiązujących w państwach członkowskich Unii systemów kształcenia i szkolenia do ery cyfrowej. Aby osiągnąć te cele, w planie działania określono dwa obszary priorytetowe: wspieranie rozwoju wysoce efektywnego ekosystemu edukacji cyfrowej oraz rozwijanie kompetencji i umiejętności cyfrowych w dobie transformacji cyfrowej. Ta prospektywna strategia jest kompatybilna z implantacją praw ochrony danych osobowych przez jednostki samorządu terytorialnego w Polsce oraz konkretnymi usługami w tym zakresie.

[263] Ibidem, s. 295.

ROZDZIAŁ III
ORGANIZACJA I STRUKTURA ORGANÓW SAMORZĄDU TERYTORIALNEGO

3.1. Zarys historii struktur samorządowych na ziemiach polskich[264]

Obecnie, od 1 stycznia 2014 roku, w Polsce istnieje 16 województw, 314 powiatów i 66 miast na prawach powiatu oraz 2477 gmin (w tym 302 gminy miejskie, 711 gmin miejsko-wiejskich i 1464 gminy wiejskie).[265]

Jako istotną i ciekawą informację można podać w tym miejscu, że np. gmina może być zlikwidowana w wyniku niewypłacalności (casus gminy Ostrowice)[266].

Tradycja instytucji samorządowych w Polsce posiada bogatą historię obejmującą czasy dawnych społeczności wiejskich i plemiennych, okres zaborów i utraty niepodległości, aż do momentu odzyskiwania suwerenności i tworzenia nowoczesnych samorządów. To historia zmian w organizacji lokalnej władzy, które odgrywały istotną rolę w kształtowaniu życia społecznego i politycznego kraju.

3.2. Pojęcie samorządu terytorialnego

Pojęcie samorządu terytorialnego zostało po raz pierwszy zastosowane w literaturze niemieckiej przez G. Jellinek. Wyrażono go za pomocą niemieckiego słowa „Selbstverwaltung", które stanowi kombinację dwóch terminów: „SelbststandigeVerwaltung". Wówczas pod tą kombinacją rozumiano prawo gminy do autonomii, która pozostaje jednostką niezależną od nadzoru państwa w kwestiach związanych z zarządzaniem swoim majątkiem[267].

W 1960 roku J. Starościak pisał na temat samorządu terytorialnego, stwierdzając, że instytucja samorządu jako jednego ze sposobów decentralizacji administracji państwowej ma za sobą tak bogatą literaturę, iż dodanie jakichś nowych elementów do samego określenia tego, co jest samorządem, jest już chyba niemożliwe. Każdy z elementów gdzieś już przez kogoś był podnoszony.[268]

---

[264] Zob. J. Bardach, B. Leśnodorski, M. Pietrzak, *Historia ustroju i prawa polskiego*, Warszawa 2010.
[265] https://www.gov.pl/web/ksng/podzial-administracyjny-polski [dostęp: 12.05.2024].
[266] https://www.nist.gov.pl/wydarzenia/pierwsza-w-historii-polski-gmina-zniesiona-za-dlugi,1389.html [dostęp: 12.05.2024].
[267] Z. Bukowski, T. Jędrzejewski, P. Rączka, *Ustrój samorządu terytorialnego*,Toruń 2003, s. 28.
[268] J. Starościak, *Decentralizacja administracji*, Warszawa 1960, s. 53.

Według definicji przedstawionej przez E. Ochendowskiego, samorząd terytorialny stanowi wyodrębniony w strukturze państwa, powstały z mocy prawa, związek lokalnego społeczeństwa, powołany do samodzielnego wykonywania administracji publicznej, wyposażony w materialne środki umożliwiające realizację nałożonych nań zadań[269].

Samorząd terytorialny realizuje zadania publiczne, które nie są zarezerwowane przez konstytucję czy inne ustawy dla innych instytucji administracji publicznej. Stanowi on element władzy wykonawczej w Polsce[270].

Samorząd terytorialny można postrzegać jako jedną z kluczowych form techniki decentralizacyjnej. Technika ta ma wiele zalet, ale niesie ze sobą również pewne wady. Do korzyści płynących z techniki decentralizacyjnej, rozumianej jako usamodzielnienie jednostek lokalnych, zalicza się pobudzanie regionalnych inicjatyw oraz zwiększanie zaangażowania lokalnych społeczności w zadania administracji publicznej, a także określanie priorytetów lokalnych potrzeb. Wzrasta także znaczenie czynnika społecznego, co przekłada się na przewagę tego czynnika nad profesjonalnym w kontekście samorządu. Ten aspekt można zwykle interpretować jako demokratyzację i społecznikowanie administracji. Co więcej, jest to metoda podnoszenia poziomu kultury politycznej społeczeństwa, ponieważ samorząd terytorialny staje się szkołą gospodarowania. Samorząd umożliwia zrozumienie potrzeb, które mogą pozostawać nieznane dla organów wyższego szczebla[271].

Tendencja decentralizacji samorządu terytorialnego posiada, niestety, również swoje wady. Pierwszy mankament polega tutaj na braku jednolitości aparatu terenowego oraz (w niektórych przypadkach) na braku efektywności kosztowej wdrażania różnych rozwiązań technicznych na niższych szczeblach. Istnieje także ryzyko unikania podejmowania mało popularnych decyzji przez przedstawicieli samorządu, zwłaszcza gdy zależy im na ponownej wygranej w wyborach. Technik decentralizacji nie należy więc stosować we wszystkich formach administracji, szczególnie tych, które wymagają jednolitego działania w skalę całego kraju i gdzie występuje potrzeba szczególnego rodzaju dyscypliny. Z tego powodu technika decentralizacji nie jest stosowana w aparacie wojskowym, również w okresach wojen, odbudowy kraju ze zniszczeń, czy także w szczególnych sytuacjach, gdy zajdzie konieczność przekierowania środków

[269] E. Ochendowski, *Prawo administracyjne*, Toruń 2006, s. 331.
[270] J. Regulski, *Samorząd III Rzeczypospolitej*, Warszawa 2000, s. 369.
[271] Z. Leoński, *Samorząd*…, s. 9.

finansowych czy materiałowych, np. podczas katastrof naturalnych, itp. Również w przypadku wykonywania zadań zleconych z zakresu administracji rządowej organom samorządu, nie stosuje się w pełni techniki decentralizacji.[272]

Poprawnie działający samorząd powinien opierać się na kryterium zamieszkania na danym terytorium. Jak zauważa J. Szreniawski, zgodnie z przepisami przynależność do niego jest dla mieszkańców obowiązkowa i automatyczna, nie można zrzec się członkostwa czy zostać jego pozbawionym nawet w wypadku całkowitej bierności czy okazywanej niechęci[273]. W Polsce poszczególne jednostki samorządu terytorialnego skupiają osoby zamieszkujące na terytorium gminy, powiatu oraz województwa.

3.3. Rodzaje i funkcje organów samorządu terytorialnego

Samorząd terytorialny to struktura organizacyjna umożliwiającą lokalnym społecznościom zarządzanie swoimi sprawami. W Polsce, faktycznie, mamy do czynienia z trzema podstawowymi typami organów samorządu terytorialnego:

- Gminy– stanowią elementarne jednostki w systemie podziału administracyjnego w Polsce. Zarządzane są przez Radę Gminy, wybieraną przez obywateli gminy oraz przez Wójta, Burmistrza lub Prezydenta Miasta, w zależności od rodzaju gminy. Kluczowe zadania gminy obejmują między innymi utrzymanie publicznej infrastruktury, edukację na szczeblu podstawowym, ochronę środowiska, jak również sprawy związane z lokalnym transportem publicznym i administrowaniem nieruchomościami gminnymi[274];
- Powiaty– to struktury administracyjne drugiego szczebla. Zarządzane są przez Radę Powiatu i Zarząd Powiatu, wybieranego przez ową Radę. Powiaty odpowiadają za zadania, które wykraczają poza uprawnienia gmin, takie jak edukacja na poziomie średnim, publiczne usługi zdrowotne, zarządzanie drogami powiatowymi oraz promocja regionu[275];
- Województwa– reprezentują najwyższy poziom podziału administracyjnego w Polsce. Zarządzane są przez Sejmik Województwa, wybierany przez mieszkańców województwa oraz Marszałka Województwa, wybieranego przez Sejmik.

[272] Ibidem, s. 10.
[273] J. Szreniawski, *Prawo administracyjne. Część ogólna*, Lublin 1993, s. 168.
[274] Zob. *Co to jest Gmina?*, https://radomyslwielki.pl/informacje-o-gminie/co-to-jest-gmina.html [dostęp: 7.10.2023].
[275] Por. T. Szymaniak, *Powiat – definicja i charakterystyka. Co to jest powiat?*, https://procredito.pl/publikacje/definicje-finansowe/509-powiat [dostęp: 07.10.2023].

Województwa odpowiadają za najszerszy zakres zadań, obejmujący zarządzanie transportem regionalnym, ochronę środowiska na poziomie regionalnym, planowanie przestrzenne, a także sprawy dotyczące kultury i dziedzictwa regionalnego[276].

Opisane wyżej struktury samorządu terytorialnego mają zagwarantować, że decyzje dotyczące lokalnych społeczności podejmowane będą jak najbliżej tych społeczności, a zarządzanie publiczne będzie jak najbardziej efektywne i dostosowane do potrzeb mieszkańców.

3.3.1. Gmina

W obliczu przemian społeczno-gospodarczych, jakie zachodzą na całym świecie, coraz większą rolę zaczyna odgrywać poziom lokalny. Jak już wcześniej odnotowaliśmy, jednostką podstawową samorządu terytorialnego w Polsce jest gmina, która staje się głównym motorem rozwoju lokalnego.

Zgodnie z ustawą o samorządzie gminnym z 8 marca 1990 roku, gmina ma prawo do samostanowienia we wszystkich sprawach dotyczących społeczności lokalnej, w ramach obowiązującego prawa i przepisów prawnych[277]. Jako podstawowa jednostka samorządu terytorialnego, gmina może podejmować decyzje dotyczące wykorzystania lokalnych zasobów, infrastruktury, edukacji, ochrony zdrowia i innych spraw publicznych[278].

Zgodnie z Raportem Komisji Europejskiej „The Role of Local Government in Local Development" (2019), gminy odgrywają kluczową rolę w procesach rozwoju lokalnego, ze względu na ich bliskość do społeczności lokalnej. Ponoszą one również odpowiedzialność za tworzenie warunków sprzyjających rozwojowi lokalnemu, co obejmuje m.in. stymulowanie inwestycji, wspieranie przedsiębiorczości, tworzenie miejsc pracy, a także ochronę środowiska i promowanie zrównoważonego rozwoju[279].

Jednakże, jak podkreśla Tomasz Śmietanka, aby gmina mogła skutecznie pełnić powierzonej jej zadania, musi posiadać odpowiednie narzędzia zarządcze, finansowe i prawne. Odpowiednie narzędzia zarządcze obejmują umiejętność planowania

[276] Zob. *Województwo*, https://encyklopedia.pwn.pl/haslo/wojewodztwo;39974 32.html [dostęp: 07.10.2023].
[277] *Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym* (Dz. U. z 2023 r. poz. 40 z późn. zm.)
[278] A. Szabłowska, *Gmina jako podstawowa jednostka samorządu terytorialnego: organizacja i funkcjonowanie gminy*, Ostrołęka 2004.
[279] Commission of the European Communities (2019), *The Role of Local Government in Local Development*.

strategicznego, zarządzania projektami, a także współpracy z różnymi podmiotami. Natomiast narzędzia finansowe obejmują zdolność pozyskiwania środków na realizację projektów rozwojowych, zarówno z budżetu państwa, jak też z funduszy UE[280].

Należy zauważyć, że gmina posiada osobowość prawną, w związku z czym wykonuje zadania własne we własnym imieniu i na własną odpowiedzialność. Do zakresu działań gminy należą sprawy publiczne, które mają znaczenie lokalne, niezastrzeżone ustawami na rzecz innych podmiotów (art. 6 ustawy)[281]. Są to:

- dbanie o ład przestrzenny, gospodarowanie lokalnymi terenami i ochrona zdrowia;
- zarządzanie drogami, ulicami, mostami, placami oraz organizacja ruchu drogowego;
- zarządzanie wodociągami i kanalizacją, zapewnianie zaopatrzenia w wodę, usuwanie i oczyszczanie ścieków komunalnych, utrzymanie czystości i porządku urządzeń sanitarnych, wysypisk i unieszkodliwianie odpadów komunalnych, zaopatrzenie w energię elektryczną i cieplną oraz gaz;
- zarządzanie lokalnym transportem zbiorowym;
- zapewnianie mieszkańcom pomocy społecznej, w tym organizacja ośrodków i zakładów opiekuńczych;
- prowadzenie gminnego budownictwa lokalnego;
- zajmowanie się kwestiami oświaty, w tym organizowanie szkół podstawowych, przedszkoli i innych placówek upowszechniania kultury;
- zajmowanie się kwestiami kultury fizycznej, w tym organizowanie terenów rekreacyjnych i urządzeń sportowych;
- zarządzanie targowiskami i halami targowymi;
- zarządzanie zielenią gminną i zadrzewieniami;
- zarządzanie cmentarzami gminnymi;
- dbanie o porządek publiczny i ochronę przeciwpożarową;
- utrzymanie w należytym stanie gminnych obiektów i urządzenia użyteczności publicznej oraz obiektów administracyjnych;
- zapewnienie kobietom w ciąży opieki socjalnej, medycznej oraz prawnej[282].

[280] T. Śmietanka, *Zarządzanie rozwojem lokalnym jako współczesna determinanta jakości życia w gminach (badania pilotażowe w wybranych gminach miejsko – wiejskich w Polsce)*, Radom 2020.
[281] Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym (Dz. U. z 2023 r. poz. 40 z późn. zm.).
[282] Ibidem.

3.3.2. Powiat

W systemie administracji samorządowej w Polsce, powiat stanowi drugi, średni szczebel jednostek terytorialnych, stanowiąc istotne ogniwo między gminą a województwem[283]. Jest to jednostka samorządu terytorialnego, która odgrywa kluczową rolę w realizacji zadań publicznych na poziomie lokalnym i regionalnym.

Według ustawy o samorządzie powiatowym z dnia 5 czerwca 1998 roku, powiat jest odpowiedzialny za wiele zadań, takich jak: ochrona środowiska, gospodarka nieruchomościami, ochrona zdrowia, edukacja, kultura i ochrona dziedzictwa narodowego, transport publiczny i drogi powiatowe, a także promocja i organizacja turystyki[284].

Wielu badaczy zwraca uwagę na rolę powiatu jako jednostki koordynującej i integrującej różne działania na poziomie lokalnym. Jak wskazuje Kurowska-Pysz (2016), powiaty odgrywają kluczową rolę w procesach planowania przestrzennego i rozwoju lokalnego, ze względu na zdolność do koordynacji i integracji różnych podmiotów i interesów na ich terytorium[285].

Podobnie jak gminy, dla skutecznej realizacji zadań powiaty muszą dysponować odpowiednimi narzędziami zarządczymi, finansowymi i prawnymi. Narzędzia te obejmują umiejętność planowania strategicznego, zarządzania projektami, a także zdolność do współpracy z różnymi podmiotami na poziomie lokalnym, regionalnym, krajowym i międzynarodowym[286]. Warto też powtórzyć, że powiat jako kluczowy element samorządu terytorialnego, odgrywa istotną rolę w procesach rozwoju lokalnego i regionalnego. W celu skutecznej realizacji zadań nałożonych na powiaty, konieczne jest zapewnienie im odpowiednich narzędzi i wsparcia, zarówno na poziomie krajowym, jak i międzynarodowym.

Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym[287] określa zasady funkcjonowania powiatów. Zgodnie z art. 1 tej ustawy poprzez powiat rozumie się odpowiednie terytorium oraz lokalną wspólnotę samorządową, którą tworzą z mocy

[283] Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz. U. z 2024 r., poz. 107).
[284] Ibidem.
[285] J. Kabus, *Uwarunkowania rozwoju lokalnego na przykładzie powiatu częstochowskiego*, Częstochowa 2016, s. 56.
[286] D. Wyszkowa, *Samorząd terytorialny w ujęciu wybranych koncepcji teoretycznych*, Białystok 2018, s. 34.
[287] *Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym* (Dz. U. z 2024 r., poz. 107).

prawa mieszkańcy powiatu[288].Zgodnie z art. 4 ustawy, samorząd powiatowy wykonuje określone zadania publiczne o charakterze ponadgminnym. Należą do nich:[289]

- organizacja edukacji publicznej;
- promocja i ochrona zdrowia;
- zapewnianie pomocy społecznej;
- prowadzenie polityki prorodzinnej;
- wspieranie osób z niepełnosprawnościami;
- zarządzanie transportem i drogami publicznymi;
- wspieranie kultury i ochrona dóbr publicznych;
- promowanie kultury fizycznej oraz turystyki;
- zadania w zakresie geodezji, kartografii i katastru[290];
- gospodarowanie nieruchomościami;
- zagospodarowanie przestrzenne i nadzór budowlany;
- gospodarka wodna;
- ochrona środowiska i przyrody;
- zadania z zakresu rolnictwa, leśnictwa i rybactwa śródlądowego;
- dbanie o porządek publiczny i bezpieczeństwo obywateli;
- zapewnianie ochrony przeciwpowodziowej, przeciwpożarowej, zapobieganie innym nadzwyczajnym zagrożeniom życia i zdrowia ludzi oraz środowiska;
- przeciwdziałanie bezrobociu oraz aktywizacja lokalnego rynku pracy;
- ochrona praw konsumenta;
- utrzymanie powiatowych obiektów i urządzeń użyteczności publicznej oraz obiektów administracyjnych;
- działania z zakresu obronności;
- promocja powiatu i współpraca z organami pozarządowymi[291].

W celu wykonywania swoich zadań powiat może tworzyć jednostki organizacyjne i zawierać umowy z innymi podmiotami.

[288] Art. 1 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym.
[289] Art. 4 ust. 1 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym.
[290] Kataster nieruchomości – urzędowa, ujednolicona dla całego kraju, regularnie aktualizowana baza danych o obiektach astralnych, czyli gruntach, budynkach i lokalach. Zob. *Kataster nieruchomości*, https://encyklopedia.pwn.pl/haslo/kataster-nieruchomosci;3921129.html [dostęp: 03.10.2023].
[291] Art. 4 ust. 1 ustawy z dnia 5 czerwca 1998 roku o samorządzie powiatowym.

3.3.3. Województwo

W Polsce, województwa to największe jednostki podziału terytorialnego, będące zarówno jednostkami administracji samorządowej, jak i zdecentralizowanej administracji rządowej. Zgodnie z Konstytucją Rzeczypospolitej Polskiej z 1997 roku, województwo jest podstawową jednostką podziału administracyjnego kraju (art. 15 ust. 1)[292]. Polska obecnie składa się z 16 województw, zgodnie z reformą administracyjną przeprowadzoną w 1999 roku[293]. Każde z 16 województw w Polsce ma unikalne cechy geograficzne, historyczne, kulturalne i gospodarcze, które wpływają na jego rozwój i politykę.

Władza na poziomie wojewódzkim dzieli się na administrację samorządową i administrację rządową. Administrację samorządową reprezentuje sejmik wojewódzki, zarząd województwa oraz marszałek (ustawa o samorządzie województwa z 1998 roku). Marszałek województwa pełni funkcję przewodniczącego zarządu województwa i reprezentuje województwo na zewnątrz (art. 35 ust. 1)[294]. Natomiast administracja rządowa na poziomie województwa jest reprezentowana przez wojewodę. Wojewoda pełni funkcję przedstawiciela Rady Ministrów w województwie (art. 12 ust. 1)[295].

Województwo ma prawo tworzyć przepisy prawa miejscowego w postaci uchwał, które muszą być zgodne z prawem krajowym (Konstytucja RP, 1997, art. 94). Zgodnie z ustawą o samorządzie województwa, sejmik wojewódzki ma prawo uchwalać statut województwa (art. 18 ust. 2 pkt 1)[296].

Ustawa o samorządzie województwa z dnia 5 czerwca 1998 roku[297] mówi o tym, że województwo jest regionalną wspólnotą samorządową oraz największą jednostkę podziału samorządu terytorialnego. Jak już wcześniej wspomnieliśmy, dzięki ustawie z dnia 24 lipca 1998 roku o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego[298] państwa, utworzono z dniem 1 stycznia 1999 roku szesnaście województw. Niniejszy akt prawny określił siedziby województw i sejmików

[292] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. Nr 78, poz. 483 z późn. zm.).
[293] Ustawa z dnia 24 lipca 1998 roku o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz.U. z 1998 r. Nr 96, poz. 603 z późn zm.).
[294] Ustawa z dnia 5 czerwca 1998 roku o samorządzie województwa (Dz.U. z 2022 r., poz. 2094 z późn. zm).
[295] Ustawa z dnia 23 stycznia 2009 roku o wojewodzie i administracji rządowej w województwie (Dz.U. z 2023 r. poz. 190 z późn. zm.).
[296] Ustawa z dnia 5 czerwca 1998 roku o samorządzie województwa (Dz.U. z 2022 r., poz. 2094 z późn. zm).
[297] Ibidem.
[298] Ustawa z dnia 24 lipca 1998 roku o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz.U. z 1998 r. Nr 96, poz. 603 z późn zm.).

województw oraz wykaz gmin wchodzących w ich skład. Od tego momentu zmiana granic województw, w związku z łączeniem, tworzeniem oraz znoszeniem powiatów, może następować wyłącznie w drodze rozporządzenia Rady Ministrów[299].

Samorząd województwa wykonuje zadania publiczne określone ustawami w imieniu własnym i na własną odpowiedzialność. Do zadań samorządu wojewódzkiego należą:

- sprawy edukacji publicznej, w tym szkolnictwa wyższego;
- sprawy promocji i ochrony zdrowia;
- sprawy kultury i ochrony jej dóbr;
- sprawy pomocy społecznej;
- sprawy modernizacji terenów wiejskich;
- sprawy zagospodarowania przestrzennego;
- sprawy ochrony środowiska;
- sprawy gospodarki wodnej;
- sprawy dóbr publicznych i transportu;
- sprawy kultury fizycznej i turystyki;
- sprawy ochrony praw konsumenta;
- sprawy obronności;
- sprawy bezpieczeństwa publicznego;
- sprawy przeciwdziałania bezrobociu i aktywizacji lokalnego rynku pracy[300].

3.4. Organizacja wewnętrzna i zasady działania organów samorządu terytorialnego

Organizacja wewnętrzna i zasady działania organów samorządu terytorialnego w Polsce są określone w Konstytucji RP z 1997 roku oraz w ustawach dotyczących poszczególnych typów samorządów: gminy (ustawa z dnia 8 marca 1990 roku o samorządzie gminnym), powiatu (ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym) oraz województwa (ustawa z dnia 5 czerwca 1998 roku o samorządzie województwa).

[299] Z. Ofiarska, M. Mokrzyc, B. Rutkowski, *Reforma Samorządu Terytorialnego*, Szczecin – Zielona Góra 1998, s. 107.
[300] Art. 16 ustawy z dnia 5 czerwca 1998 roku o samorządzie województwa (Dz.U. z 2022 r., poz. 2094 z późn. zm).

Podstawowe organy samorządu terytorialnego to rada (organ stanowiący) i wójt, burmistrz albo prezydent miasta (organ wykonawczy) na szczeblu gminy, zarząd i rada powiatu na szczeblu powiatu, oraz sejmik i zarząd województwa na szczeblu województwa.

Gmina jest podstawową jednostką podziału administracyjnego w Polsce, na co zwracaliśmy uwag już wcześniej. Każdą gminą zarządza Rada Gminy, która jest wybierana w wyborach powszechnych. Rada Gminy podejmuje decyzje na temat lokalnej polityki, budżetu, a także nadzoruje działanie wójta/burmistrza/prezydenta miasta, który jest osobą odpowiedzialną za zarządzanie gminą. Na poziomie gminy, zgodnie z art. 18 ust. 2 ustawy o samorządzie gminnym, radę gminy tworzą radni wybierani w wyborach bezpośrednich. Wójt, burmistrz lub prezydent miasta, jako organ wykonawczy, jest wybierany bezpośrednio przez mieszkańców gminy (art. 30 ust. 1 tej ustawy)[301].

Powiat stanowi średni szczebel samorządu terytorialnego. Rada Powiatu jest organem stanowiącym powiatu i, podobnie jak Rada Gminy, jest wybierana w wyborach powszechnych. Starosta to główny organ wykonawczy powiatu. Na szczeblu powiatu, zgodnie z art. 15 ust. 2 ustawy o samorządzie powiatowym, rada powiatu składa się z radnych wybieranych w wyborach bezpośrednich. Zarząd powiatu jako organ wykonawczy, jest wybierany przez radę powiatu (art. 26 ust. 1 tej ustawy)[302].

Województwo jest największą jednostką podziału administracyjnego w Polsce. Zarządza nim Sejmik Województwa, wybierany w wyborach powszechnych, który podejmuje decyzje na temat polityki regionalnej. Marszałek Województwa jest organem wykonawczym, nadzorowanym przez sejmik. W odniesieniu do województwa, na podstawie art. 17 ust. 1 ustawy o samorządzie województwa, sejmik województwa składa się z radnych wybieranych w wyborach bezpośrednich. Zarząd województwa jako organ wykonawczy, jest wybierany przez sejmik (art. 33 ust. 1 tej ustawy)[303].

Każda z wymienionych jednostek samorządu terytorialnego posiada określone prawa i obowiązki, regulowane poprzez odpowiednie ustawy. Organizacja wewnętrzna tych organów, a także ich wzajemne relacje i współpraca, są kluczowe dla sprawnego funkcjonowania administracji publicznej na poziomie lokalnym i regionalnym.

[301] Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2023 r., poz. z późn. zm.).
[302] Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz.U. z 2024 r., poz. 107).
[303] Ustawa z dnia 5 czerwca 1998 rokuo samorządzie województwa (Dz.U. z 2022 r., poz. 2094 z późn. zm.).

Samorząd terytorialny w Polsce działa na podstawie regulacji określonych w Konstytucji RP, a także w szczegółowych ustawach specyficznych dla poszczególnych szczebli samorządu, takich jak ustawa o samorządzie gminnym, powiatowym czy województwie. Samorząd terytorialny składa się z trzech szczebli: gminy, powiatu i województwa.

Organizacja i zasady działania organów samorządu terytorialnego w Polsce są zdefiniowane w kilku kluczowych aktach prawnych, w tym w Konstytucji RP, Kodeksie karnym, Kodeksie postępowania karnego, a przede wszystkim w ustawach specjalnych, takich jak ustawa o samorządzie gminnym, ustawa o samorządzie powiatowym i ustawa o samorządzie województwa. Przyjrzyjmy się dokładniej tym aktom prawnym.

Konstytucja Rzeczpospolitej Polskiej[304] w art. 163 przyznaje prawo do samorządu terytorialnego, które obejmuje możliwość samodzielnego rozstrzygania o sprawach publicznych na poziomie lokalnym, zgodnie z prawem. Samorząd terytorialny wykonuje swoje zadania na podstawie i w granicach prawa (art. 16 i 17 Konstytucji RP).

Ustawa o samorządzie gminnym (1990)[305] precyzyjnie opisuje organizację i funkcjonowanie organów gminy, które są podstawową jednostką samorządu terytorialnego. Wśród organów gminy można wymienić radę gminy, wójta (burmistrza lub prezydenta miasta) i zarząd gminy. Zasada działania tych organów opiera się na trójpodziale władzy: rada gminy jest organem stanowiącym i kontrolnym, wójt (burmistrz, prezydent) jest organem wykonawczym, a zarząd gminy pełni rolę organu pomocniczego. Ustawa o samorządzie powiatowym (1998)[306] reguluje działalność organów powiatu, które obejmują radę powiatu, zarząd powiatu i starostę. Zasady ich działania są podobne do zasad działania organów gminy. Ustawa o samorządzie województwa (1998)[307] szczegółowo opisuje są zasady funkcjonowania organów województwa, w skład których wchodzą sejmik województwa, zarząd województwa i marszałek województwa. Sejmik jest organem stanowiącym i kontrolnym, zarząd wykonawczym, a marszałek reprezentuje województwo na zewnątrz.

[304] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. Nr 78, poz. 483 z późn. zm.).
[305] Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2023 r., poz. z późn. zm.).
[306] Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz.U. z 2024 r., poz. 107).
[307] Ustawa z dnia 5 czerwca 1998 rokuo samorządzie województwa (Dz.U. z 2022 r., poz. 2094 z późn. zm.).

Wspólne dla wszystkich organów samorządu terytorialnego jest zasada bezpośredniości wyborów (art. 169 Konstytucji RP) oraz zasada odpowiedzialności za działania. Organizacja i zasady działania organów samorządu terytorialnego są zgodne z zasadami demokracji, prawa do samostanowienia, jawności i odpowiedzialności za podejmowane decyzje.

Podstawowe zasady funkcjonowania organów samorządu terytorialnego obejmują:

- Dyrektywa wyborcza: Członkowie rad gmin, rad powiatów i sejmików województw są wybierani w wyborach powszechnych, równych, bezpośrednich i tajnych. Wójt (burmistrz lub prezydent miasta) jest również wybierany w wyborach bezpośrednich;
- Autonomia: Samorząd terytorialny posiada szeroką autonomię w zakresie realizacji zadań publicznych na rzecz lokalnej społeczności;
- Bimodalność: Organizacja samorządu terytorialnego opiera się na dwóch podstawowych organach: kolegialnym (rada gminy, rada powiatu, sejmik województwa) i jednoosobowym (wójt, burmistrz, prezydent miasta, zarząd powiatu, zarząd województwa);
- Kontrola: Działalność samorządu terytorialnego podlega kontroli w zakresie legalności przez wojewodę, a w zakresie gospodarności przez regionalne izby obrachunkowe;
- Zasada pomocniczości: Zgodnie z nią, zadania publiczne powinny być realizowane na najniższym możliwym szczeblu administracji, który jest w stanie je efektywnie wykonać;
- Zasada subsydiarności: Wszelkie zadania, które nie są wyraźnie zastrzeżone dla administracji rządowej, powinny być realizowane przez samorząd terytorialny;
- Zasada samofinansowania: Samorządy mają prawo do posiadania własnego majątku oraz do samodzielnego kształtowania swojego budżetu;
- Działalność gospodarcza: Samorządy mogą prowadzić działalność gospodarczą tylko wtedy, gdy jest to niezbędne do realizacji zadań, które na nich spoczywają[308].

Warto pamiętać, że konkretne procedury i zasady mogą się różnić w zależności od konkretnego poziomu samorządu terytorialnego i mogą być szczegółowo regulowane przez odpowiednie ustawy.

[308] Ibidem.

Organy samorządu terytorialnego działają zgodnie z zasadą jawności, samodzielności, bezpośredniości oraz kolegialności.

Zgodnie z art. 61 Konstytucji RP, obrady organów stanowiących samorządu terytorialnego są jawne. Jawność ta jest ograniczona jedynie w przypadkach przewidzianych w ustawach. Zasada jawności w samorządzie terytorialnym to jedna z fundamentalnych zasad demokracji lokalnej. Jest to podstawa transparentności i przejrzystości działań organów samorządowych. Zgodnie z tą zasadą, większość działań i decyzji podejmowanych przez organy samorządu terytorialnego posiada charakter publiczny, a efekty tych działań i decyzji powinny być dostępna dla mieszkańców danej gminy, powiaty czy województwa. Dotyczy to na przykład sesji rady gminy, miasta lub powiatu, które są otwarte dla publiczności. W praktyce oznacza to, że każda osoba może wziąć udział w tych spotkaniach jako obserwator[309].

Zasada jawności obejmuje również obowiązek publikacji uchwał, protokołów, planów i decyzji, tak aby mieszkańcy mieli dostęp do informacji na temat działań podejmowanych przez organy samorządu. Jednak zasada ta nie jest absolutna i istnieją pewne wyjątki, na przykład w przypadku, kiedy jawność mogłaby naruszyć prywatność osób, bezpieczeństwo państwa lub interesy publiczne. W takich sytuacjach, sesje mogą być zamknięte dla publiczności, a niektóre dokumenty mogą pozostać publicznie niedostępne[310].Zasada ta jest bardzo ważna dla budowania zaufania pomiędzy organami samorządu a obywatelami, ponieważ umożliwia kontrolę działań władzy przez społeczeństwo.

Zasada samodzielności (art. 16 ust. 2 Konstytucji RP) oznacza, że organy samorządu terytorialnego samodzielnie zarządzają swoim majątkiem i wykonywają swoje zadania[311]. Nazywana jest również autonomią. Polega ona na tym, że organy samorządu terytorialnego mają prawo do samodzielnego podejmowania decyzji w sprawach lokalnych, bez nadmiernego wpływu ze strony władz centralnych.

Zasada samodzielności obejmuje dwa główne elementy:

- Samodzielność organów: organy samorządu terytorialnego, takie jak rada gminy, burmistrz, wójt czy prezydent miasta, mają prawo do samodzielnego podejmowania decyzji i kierowania sprawami lokalnymi;

[309] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. Nr 78, poz. 483 z późn. zm.).
[310] Ibidem.
[311] Ibidem.

- Samodzielność finansowa: samorząd terytorialny ma prawo do dysponowania swoim budżetem oraz do samodzielnego decydowania o wydatkach na lokalne potrzeby[312].

Oczywiście, samodzielność samorządu terytorialnego jest ograniczona przez prawo państwowe i konieczność przestrzegania ogólnokrajowych strategii i regulacji. Samorząd musi również działać w granicach swoich kompetencji, które są określone w ustawie o samorządzie terytorialnym. W praktyce, zasada samodzielności umożliwia samorządom terytorialnym dostosowanie swoich działań do lokalnych potrzeb i oczekiwań, co przyczynia się do skuteczniejszego i bardziej efektywnego zarządzania na poziomie lokalnym.

Zasada bezpośredniości (art. 16 ust. 1 Konstytucji RP) oznacza, że organy samorządu terytorialnego są wybierane w wyborach bezpośrednich. Wyjątkiem jest zarząd powiatu i zarząd województwa, które wybiera się za pośrednictwem odpowiednich rad[313].

Zasada bezpośredniości w samorządzie terytorialnym głosi, że mieszkańcy danego obszaru samorządu terytorialnego mają bezpośredni wpływ na zarządzanie tym obszarem. Bezpośredniość manifestuje się tutaj na kilka sposobów. Po pierwsze, obywatele mają prawo do wyboru swoich przedstawicieli do organów samorządu terytorialnego (np. rady gminy, rady miasta, zarządu powiatu itp.) w wyborach lokalnych. Przedstawiciele ci są odpowiedzialni za podejmowanie decyzji dotyczących lokalnej polityki i zarządzania. Po drugie, obywatele mają prawo do udziału w bezpośrednich formach partycypacji, takich jak referenda lokalne, zgromadzenia mieszkańców, konsultacje społeczne czy budżet obywatelski. Te formy umożliwiają mieszkańcom bezpośrednie wpływanie na decyzje podejmowane na poziomie lokalnym[314].

Zasada bezpośredniości w samorządzie terytorialnym jest kluczowa dla utrzymania demokracji na poziomie lokalnym i dla zapewnienia, że decyzje podejmowane przez organy samorządu terytorialnego są zgodne z oczekiwaniami i potrzebami mieszkańców. Wzmaga także poczucie odpowiedzialności mieszkańców za sprawy ich lokalnej społeczności.

Zasada kolegialności w samorządzie terytorialnym odnosi się do procesu decyzyjnego, w którym wszystkie decyzje powinny być podejmowane przez zespół

[312] Zob. J. Szołno-Koguc, *Samodzielność dochodowa jednostek samorządu terytorialnego – aspekty teoretyczne*, „Studia BAS", nr 1/2021, s. 12-15.
[313] *Konstytucja Rzeczypospolitej Polskiej*…
[314] Zob. M. Chrzanoski, *Podstawowe zasady prawa wyborczego do organów stanowiących jednostek samorządu terytorialnego*, Białystok 2018, s. 167-179.

(np. radę gminy, radę miasta, zarząd powiatu), a nie przez jedną osobę. Każdy członek takiego organu ma prawo do głosu, a konkretna decyzja zostaje podjęta na podstawie większości głosów[315]. Zasada kolegialności podkreśla, że decyzje samorządu terytorialnego powinny być wynikiem dyskusji, współpracy i uzgodnień między różnymi członkami organu, a nie jednoosobowych decyzji. Ma to na celu zapewnienie różnorodności opinii i punktów widzenia, co może przyczynić się do lepszego i bardziej zrównoważonego procesu decyzyjnego.

Jednakże, niektóre decyzje, zwłaszcza te dotyczące bieżącego zarządzania, mogą być podejmowane przez jedną osobę, na przykład przez burmistrza, wójta lub prezydenta miasta. Taka osoba jest zwykle wybrana przez obywateli w wyborach bezpośrednich i ma pewne uprawnienia do samodzielnego podejmowania decyzji, chociaż zawsze w granicach prawa i zgodnie z uchwałami rady. Zasada kolegialności oznacza również, że decyzje organów stanowiących samorządu terytorialnego są podejmowane na posiedzeniach przez większość głosów przy obecności co najmniej połowy składu statutowego[316].

Podsumowując, organizacja wewnętrzna i zasady działania organów samorządu terytorialnego w Polsce są precyzyjnie określone w prawie. Stwarza to ramy dla demokratycznego i efektywnego zarządzania na poziomie lokalnym i regionalnym.

3.5. Rola organów samorządu terytorialnego w ochronie danych osobowych

Samorząd terytorialny jako istotny element struktury państwa odgrywa kluczową rolę w ochronie danych osobowych swoich mieszkańców. Struktura ta działa na różnych poziomach – od gmin, przez powiaty, aż do województw, tworząc kompleksowy system zabezpieczeń. Rola samorządu terytorialnego w ochronie danych osobowych polega na: zapewnianiu zgodności procedur przetwarzania danych osobowych z prawem, zarządzaniu bezpieczeństwem danych, prowadzenie działań z zakresu edukacji i świadomości społecznej oraz współpracy z organami. Przyjrzyjmy się dokładnie tym płaszczyznom:

[315] Zob. J. Jagielski, *Kolegialność i jednoosobowość w strukturach samorządu terytorialnego*, „Studia Iuridica", nr 85/2020, s. 95-103.
[316] *Ibidem*.

- Zapewnienie zgodności z prawem: Organ samorządu terytorialnego jest administratorem danych osobowych, które zbiera, przetwarza i przechowuje. Jako taki, musi przestrzegać przepisów o ochronie danych osobowych, zarówno krajowych, jak i unijnych, takich jak ogólne rozporządzenie o ochronie danych (RODO). Oznacza to, między innymi, zapewnienie transparentności procesu przetwarzania, umożliwienie dostępu do danych i ich poprawiania, a także zapewnienie bezpieczeństwa danych[317];
- Zarządzanie bezpieczeństwem danych: Samorządy terytorialne są odpowiedzialne za zabezpieczenie zgromadzonych danych osobowych. W praktyce może to obejmować zarządzanie systemami IT, które przechowują dane, zabezpieczanie fizycznych miejsc przechowywania danych, a także szkolenie personelu w zakresie bezpieczeństwa danych. Samorząd powinien także regularnie przeprowadzać audyty bezpieczeństwa, aby zapewnić ciągłą ochronę danych osobowych[318];
- Edukacja i świadomość społeczna: To jedno z zadań spoczywających na władzach samorządu terytorialnego. Edukacja społeczna i podnoszenie świadomości na temat ochrony danych osobowych można realizować choćby przez organizowanie szkoleń, warsztatów, a także publikowanie informacji na ten temat. Podobne działania powinny pomóc mieszkańcom w zrozumieniu, jakie są ich prawa względem ochrony danych osobowych i jak mogą je egzekwować[319];
- Współpraca z innymi organami. W celu skutecznej ochrony danych osobowych, samorząd terytorialny musi również współpracować z innymi organami, takimi jak Urząd Ochrony Danych Osobowych, służby bezpieczeństwa, a także innymi samorządami. Współpraca ta pozwala na wymianę doświadczeń, dobrych praktyk, a także umożliwia skoordynowane działań w przypadku zagrożeń dla danych osobowych[320].

Rola samorządu terytorialnego w ochronie danych osobowych jest więc wielowymiarowa i obejmuje zarówno aspekty prawne, techniczne, jak i edukacyjne.

[317] Zob. *Administrator danych osobowych w sektorze publicznym*, https://samorzad.infor.pl/sektor/organizacja/rodo-2018/3001763,Administrator-danych-osobowych-wsektorze-publicznym.html [dostęp: 06.10.2023].
[318] Zob. *Ochrona danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości*, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-przetwarzanych-w-zwiazku-z-zapobieganiem-i-18807130 [dostęp: 06.10.2023].
[319] Zob. K. Dzioba, *RODO - obowiązki jednostek samorządu terytorialnego*, https://www.rp.pl/zadania/art2451721-rodo-obowiazki-jednostek-samorzadu-terytorialnego [dostęp: 06.10.2023].
[320] Ibidem.

Skuteczna ochrona danych osobowych wymaga ciągłego monitorowania i aktualizowania praktyk, a także szerokiej współpracy pomiędzy różnymi organami.

3.5.1. Obowiązki organów wynikające z RODO

Wśród obowiązków organów jednostek samorządu terytorialnego można wymienić:

- Zgodność z zasadami ochrony danych: wymóg ten został określony w artykule 5 RODO. Zgodnie z tym zapisem organy samorządu terytorialnego muszą przetwarzać dane osobowe według zasad prawnego przetwarzania danych. W praktyce (co niejednokrotnie zostało już podkreślone) oznacza to, że dane powinny być przetwarzane uczciwie, przejrzyście, dla określonych, jasnych i prawnych celów, a ich przetwarzanie powinno być minimalne – ograniczone do tego, co jest konieczne dla osiągnięcia tych zamiarów[321];
- Prawo do informacji: zgodnie z artykułami 13 i 14 RODO, organy samorządu terytorialnego mają obowiązek informować osoby, których dane są przetwarzane, o tym fakcie. Informacja powinna obejmować tożsamość i dane kontaktowe administratora, cele i podstawę prawną przetwarzania, okres przechowywania danych, informacje o prawach osoby, której dane dotyczą, a także, w stosownych przypadkach, informacje o profilowaniu i automatycznym podejmowaniu decyzji[322];
- Prawa osób, których dane dotyczą: zgodnie z artykułami 15-22 RODO, organy samorządu terytorialnego muszą zapewnić realizację praw osób, których dane dotyczą. W szczególności, osoby te mają prawo do dostępu do swoich danych, ich poprawiania, usunięcia (tzw. prawo do bycia zapomnianym), ograniczenia przetwarzania, przenoszenia danych oraz sprzeciwu wobec przetwarzania. Osoba, której dane dotyczą, ma też prawo nie podlegać decyzji, która jest oparta wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu, i która wywołuje skutki prawne lub w podobny sposób istotnie na nią wpływa[323];
- Bezpieczeństwo danych: zgodnie z artykułem 32 RODO, organy samorządu terytorialnego muszą zaimplementować odpowiednie techniczne i organizacyjne

[321] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
[322] Ibidem.
[323] Ibidem.

środki, aby zapewnić odpowiedni poziom bezpieczeństwa danych, uwzględniając stan wiedzy, koszty realizacji, a także naturę, zakres, kontekst i cele przetwarzania, jak również ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze ryzyka[324];

- Meldowanie naruszeń ochrony danych: zgodnie z artykułem 33 RODO, organy samorządu terytorialnego mają obowiązek zgłaszać wszelkie naruszenia ochrony danych do odpowiedniego organu nadzorczego nie później niż 72 godziny po stwierdzeniu naruszenia, chyba że naruszenie to nie wiąże się z ryzykiem dla praw i wolności osób fizycznych. W przypadku naruszeń, które prawdopodobnie spowodują wysokie ryzyko dla praw i wolności osób fizycznych, organy te mają również obowiązek poinformować osoby, których dane dotyczą[325].

Przestrzeganie powyższych obowiązków jest kluczowe dla zgodności z RODO i może pomóc uniknąć poważnych konsekwencji prawnych, w tym kar finansowych.

3.5.2. Współpraca z innymi podmiotami

Organy samorządu terytorialnego współpracują z innymi podmiotami w zakresie ochrony danych osobowych w celu zapewnienia właściwego stosowania przepisów o ochronie danych, wymiany dobrych praktyk, zapewnienia bezpieczeństwa danych i prowadzenia edukacji w tym zakresie. Wszystkie działania współpracy powinny być zgodne z obowiązującymi przepisami prawa, w szczególności z RODO.

Organy samorządu terytorialnego powinny współpracować z organami administracji publicznej, w szczególności z organem ochrony danych, w celu wspierania i ulepszania ochrony danych osobowych. Wymiana informacji pomiędzy organami powinna odbywać się z zachowaniem pełnej ochrony danych osobowych, zgodnie z wymogami RODO[326].

Organy samorządu terytorialnego mogą współpracować z podmiotami prywatnymi, takimi jak firmy, organizacje pozarządowe, jednostki naukowe i inne instytucje, w celu promowania ochrony danych osobowych. Wszelka wymiana

[324] Ibidem.
[325] Ibidem.
[326] Zob. Ł. Wojciechowski, *Bezpieczeństwo informacji w polskim samorządzie terytorialnym na tle procesu ujednolicenia systemu ochrony danych osobowych w Unii Europejskiej*, „Rocznik Administracji Publicznej", nr 5/2019.

informacji i działania podejmowane w ramach tej współpracy powinny być zgodne z obowiązującymi przepisami o ochronie danych[327].

W ramach współpracy organy samorządu terytorialnego powinny prowadzić działania edukacyjne i informacyjne w celu podniesienia świadomości społecznej na temat ochrony danych osobowych. Działania te mogą obejmować organizację szkoleń, warsztatów, seminariów, konferencji i innych form edukacji, w tym także online. Wszelkie materiały edukacyjne i informacyjne powinny być dostosowane do różnych grup odbiorców i uwzględniać ich specyficzne potrzeby[328].

3.5.3. Realizacja praw osób, których dane dotyczą

Organy samorządu terytorialnego są zobowiązane do zapewnienia przestrzegania praw osób, których dane dotyczą. Te prawa obejmują, ale nie ograniczają się do prawa dostępu, prawa do sprostowania, prawa do usunięcia („prawo do bycia zapomnianym"), prawa do ograniczenia przetwarzania, prawa do przenoszenia danych, prawa do sprzeciwu, prawa do niepodlegania decyzji, której jedyną podstawą jest zautomatyzowane przetwarzanie, w tym profilowanie. Podczas realizacji praw osób, których dane dotyczą, organy samorządu terytorialnego powinny mieć na uwadze kilka zasad. Po pierwsze, powinny one informować osoby, których dane dotyczą, o przetwarzaniu ich danych i prawach, które z tego wynikają. Po drugie, powinny udostępniać mechanizmy umożliwiające korzystanie z tych praw, takie jak formularze wniosków czy zasady złożenia skargi. Dobrym przykładem realizacji tych praw przez organy samorządu terytorialnego może być sytuacja, w której mieszkaniec składa wniosek o dostęp do swoich danych osobowych, przetwarzanych przez organ samorządu terytorialnego. W odpowiedzi, organ powinien dostarczyć osobie, której dane dotyczą, kopię przetwarzanych danych, oraz informacje o celach przetwarzania, kategoriach danych, odbiorcach, okresie przechowywania, źródle danych, o istnieniu zautomatyzowanego podejmowania decyzji i prawach, które przysługują osobie, której dane dotyczą[329].

[327] Ibidem.
[328] Ibidem.
[329] M. Szkutnik, *Realizacja praw osób, których dane dotyczą na podstawie RODO (cz. 1)*, https://blog-daneosobowe.pl/realizacja-praw-osob-ktorych-dane-dotycza-zgodnie-z-rodo/ [dostęp: 06.10.2023].

3.5.4. Szkolenia i podnoszenie kompetencji personelu

W odpowiedzi na wzrastające znaczenie RODO, samorząd terytorialny powinien dążyć do ciągłego podnoszenia kompetencji swojego personelu. Świadomość i zrozumienie zasad RODO jest kluczowe dla zapewnienia zgodności i ochrony praw obywateli. Istnieją różne strategie szkoleniowe oraz metody podnoszenia kompetencji personelu samorządu terytorialnego w tym zakresie.

Szkolenia RODO powinny być zintegrowane z systemem szkoleń dla personelu samorządu terytorialnego. Te programy powinny zawierać moduły na różnych poziomach zaawansowania, poczynając od podstawowych zasad ochrony danych, a kończąc na szczegółowych aspektach takich jak zarządzanie incydentami dotyczącymi bezpieczeństwa danych. Ważne jest, aby programy szkoleniowe były dostosowane do różnych grup pracowników – od personelu administracyjnego, po kadry kierownicze.

Podnoszenie kompetencji to nie tylko kwestia formalnego szkolenia. Ważne jest również budowanie kultury bezpieczeństwa danych, która obejmuje zrozumienie znaczenia RODO i jego wpływu na codzienną pracę. Kampanie informacyjne, warsztaty i seminaria mogą być skutecznymi narzędziami budowania takiej kultury.

Regularna ewaluacja i monitorowanie efektów szkoleń jest niezbędne dla zapewnienia ich skuteczności. Narzędzia takie jak ankiety, testy czy audyty pomagają w ocenie stopnia zrozumienia RODO przez personel oraz identyfikacji obszarów wymagających dalszych szkoleń.

Zakres szkolenia powinien obejmować kluczowe aspekty RODO, takie jak prawa osób, które dane dotyczą, zasady przetwarzania danych osobowych, obowiązki administratora i podmiotu przetwarzającego, a także procedury reagowania na naruszenia bezpieczeństwa danych.

Korzystanie ze wsparcia zewnętrznego, takiego jak konsultanci w dziedzinie ochrony danych, może być pomocne w zapewnieniu, że szkolenia są zgodne z najnowszymi wymogami prawymi i najlepszymi praktykami. Zewnętrzni eksperci mogą również dostarczyć nowych perspektyw i pomóc w identyfikacji obszarów do poprawy.

Podsumowując, regularne szkolenia i podnoszenie kompetencji personelu samorządu terytorialnego w zakresie RODO są niezbędne do zapewnienia zgodności i ochrony praw obywateli. Wymaga to kompleksowego podejścia, które obejmuje

formalne szkolenia, budowanie kultury bezpieczeństwa danych, regularną ocenę efektywności i korzystanie ze wsparcia zewnętrznego.

ROZDZIAŁ IV
OCHRONA DANYCH OSOBOWYCH W KONTEKŚCIE SAMORZĄDOWYCH USŁUG PUBLICZNYCH

4.1. Definicja i rodzaje usług publicznych

Samorządowe usługi publiczne[330] to zestaw usług świadczonych przez jednostki samorządu terytorialnego, które mają na celu zaspokajanie potrzeb społeczności lokalnej. Te usługi obejmują szeroki zakres działań, od edukacji, poprzez ochronę zdrowia, do infrastruktury i zaopatrzenia w wodę i energię. W zależności od kraju i systemu prawnego, samorząd terytorialny może być odpowiedzialny za różne usługi publiczne.

Rodzaje samorządowych usług publicznych zależą od struktury samorządu terytorialnego danego kraju, ale często obejmują:

- Usługi edukacyjne: samorząd terytorialny często jest odpowiedzialny za zarządzanie szkołami publicznymi na swoim terytorium. Może obejmować budowę i utrzymanie szkół, zatrudnianie nauczycieli, zarządzanie programami edukacyjnymi i zapewnianie wsparcia dla uczniów;
- Usługi zdrowotne: samorząd może być odpowiedzialny za świadczenie usług zdrowotnych, takich jak zarządzanie szpitalami i klinikami, świadczenie opieki zdrowotnej dla mieszkańców, a nawet prowadzenie działań zdrowotnych, np. programów szczepień;
- Usługi infrastrukturalne: samorząd terytorialny często jest odpowiedzialny za utrzymanie infrastruktury na swoim terytorium, takiej jak drogi, mosty, transport publiczny, zaopatrzenie w wodę i kanalizację;
- Usługi środowiskowe: samorząd terytorialny może być odpowiedzialny za ochronę środowiska na swoim terytorium, w tym za gospodarowanie odpadami, ochronę przestrzeni naturalnej, utrzymanie parków i terenów zielonych;
- Usługi społeczne: samorząd może być odpowiedzialny za świadczenie różnych usług społecznych, takich jak opieka społeczna, programy dla seniorów, wsparcie dla osób z niepełnosprawnościami, programy mieszkaniowe;

[330] Por. *Usługi publiczne*, http://encyklopediaap.uw.edu.pl/index.php/Us%C5%82ugi_publiczne [dostęp: 06.10.2023].

- Usługi kulturalne: samorząd terytorialny może być odpowiedzialny za promowanie kultury i sztuki na swoim terytorium, w tym przez zarządzanie bibliotekami, muzeami, teatrami i innymi instytucjami kulturalnymi;
- Usługi bezpieczeństwa: samorząd może być odpowiedzialny za utrzymanie bezpieczeństwa publicznego, w tym przez zarządzanie lokalną policją, strażą pożarną, a nawet służbami ratowniczymi.

4.1.1. Usługi edukacyjne

Samorządowe usługi edukacyjne odnoszą się do zestawu usług świadczonych przez jednostki samorządu terytorialnego w celu zapewnienia mieszkańcom dostępu do kształcenia. Rolą samorządu jest zarówno dostarczanie, jak i koordynowanie edukacji na swoim terytorium[331]. Usługi te obejmują różne aspekty, takie jak:

- Zarządzanie szkołami: samorządy są odpowiedzialne za zarządzanie szkołami publicznymi. Ich działalność na tej płaszczyźnie obejmuje zarządzanie budżetem, zasobami, zatrudnianiem personelu, a także zarządzanie programami edukacyjnymi;
- Budowa i utrzymanie szkoły: samorządy są odpowiedzialne za budowę i utrzymanie budynków szkolnych, co obejmuje utrzymanie infrastruktury szkolnej, takiej jak klasy, biblioteki, laboratoria, sale gimnastyczne i inne;
- Wsparcie dla uczniów i rodziców: usługi edukacyjne obejmują wsparcie dla uczniów i ich rodzin. Może ono polegać na realizacji programów śniadaniowych, organizacji transportu szkolnego, pomocy w nauce dla uczniów, którzy mają trudności, jak również wsparcie dla rodziców w zakresie doradztwa edukacyjnego;
- Programy edukacyjne: samorządy są odpowiedzialne za implementację i zarządzanie programami edukacyjnymi, które mogą obejmować na przykład programy dla uczniów zdolnych, dla uczniów specjalnej troski edukacyjnej, programy edukacji dorosłych, a także programy edukacji zawodowej i technicznej;
- Nadzór nad edukacją: samorządy są odpowiedzialne za monitorowanie jakości edukacji na swoim terytorium, polegające na ocenie szkół, nauczycieli i efektywności programów edukacyjnych[332].

[331] Por. M. Adamowicz, P. Skarżyńska, *Rola samorządu lokalnego w realizacji zadań oświatowych na przykładzie samorządu gminy Szelków*, „Annales Universitatis Mariae Curie-Sklodowska, Sectio K", nr 2/2027.
[332] Por. Ł. Sobiech, *Zadania samorządu terytorialnego w działalności oświatowej*, https://samorzad.infor.pl/sektor/zadania/oswiata/388784,Zadania-samorzadu-terytorialnego-w-dzialalnosci-oswiatowej.html [dostęp: 06.10.2023].

Samorząd terytorialny jako instytucja publiczna, ma obowiązek zapewnić dostęp do edukacji na równych zasadach dla wszystkich mieszkańców. Jak wskazuje Rapacki, system edukacyjny powinien być skonstruowany tak, aby każda osoba miała możliwość kształcenia się na poziomie odpowiednim do swoich zdolności i potrzeb. Szkoły jako instytucje edukacyjne, powinny zapewniać uczniom odpowiednie warunki do nauki, a nauczyciele powinni posiadać odpowiednie przygotowanie do realizacji swoich zadań[333].

W związku z powyższym, samorządy mają duży wpływ na jakość i dostępność usług edukacyjnych. Decyzje samorządowe dotyczące edukacji są niezwykle ważne, ponieważ poziom wykształcenia rzutuje rozwój społeczności lokalnych zarówno w aspekcie zawodowym, jak też moralnym. Edukacja opiera się bowiem nie tylko na przekazywaniu wiedzy, ale także na kształtowaniu postaw obywatelskich, kultury społecznej i budowaniu społeczeństwa obywatelskiego.

W konsekwencji jakość usług edukacyjnych oferowanych przez samorządy przekłada się na ogólną jakość życia lokalnych społeczności samorząd terytorialny, poprzez swoje decyzje i działania w zakresie edukacji, ma bezpośredni wpływ na jakość życia mieszkańców oraz na kształtowanie społeczności lokalnej.

W zarządzaniu szkołami i realizacji usług edukacyjnych, przetwarzane są dane osobowe uczniów, rodziców i nauczycieli, co wymaga szczególnych środków ostrożności i zabezpieczeń.

Samorządy są zobowiązane do wdrożenia odpowiednich polityk i procedur zapewniających ochronę danych osobowych, takich jak:

- Zgody na przetwarzanie danych: zapewnienie, że przetwarzanie danych osobowych odbywa się zgodnie z uzyskanymi zgodami oraz, że są one prawidłowo udokumentowane;
- Bezpieczeństwo danych: wprowadzenie środków technicznych i organizacyjnych chroniących dane przed nieuprawnionym dostępem, utratą lub zniszczeniem;
- Prawa podmiotów danych: umożliwienie osobom, których dane są przetwarzane, korzystania z ich praw, takich jak prawo dostępu, sprostowania, usunięcia danych, ograniczenia przetwarzania oraz prawo do przenoszenia danych;

[333] J. Martuszewska, *Potrzeby edukacji dla bezpieczeństwa społeczności lokalnej – aspekt aksjologiczny, psychologiczny oraz wybrane aspekty normatywne*, Szczecin 2019.

- Edukacja i szkolenia: regularne szkolenie personelu w zakresie ochrony danych osobowych oraz podnoszenie świadomości na temat zagrożeń i najlepszych praktyk w tym zakresie.

W konsekwencji jakość usług edukacyjnych oferowanych przez samorządy przekłada się na ogólną jakość życia lokalnych społeczności. Samorząd terytorialny, poprzez swoje decyzje i działania w zakresie edukacji oraz odpowiedzialne podejście do ochrony danych osobowych, ma bezpośredni wpływ na jakość życia mieszkańców oraz na kształtowanie społeczności lokalnej.

4.1.2. Usługi zdrowotne

Samorządowe usługi zdrowotne to usługi świadczone przez jednostki samorządu terytorialnego, które mają na celu poprawę zdrowia i dobrobytu społeczności[334]. Zakres tych usług może obejmować:

- Zarządzanie placówkami zdrowia: samorządy są odpowiedzialne za zarządzanie lokalnymi placówkami służby zdrowia, takimi jak szpitale, przychodnie, centra zdrowia psychicznego, domy opieki i inne. Zarządzanie tymi placówkami obejmuje utrzymanie infrastruktury, zasobów, zatrudnianie personelu medycznego i koordynowanie świadczenia usług;
- Publiczne programy zdrowotne: samorządy często zarządzają lub koordynują publiczne programy zdrowotne, które mają na celu poprawę zdrowia społeczności. Mogą to być programy szczepień, programy kontroli chorób przewlekłych, programy zdrowia psychicznego, programy zdrowia seksualnego i reprodukcyjnego, programy zdrowia matki i dziecka, itp.;
- Edukacja i promocja zdrowia: samorządy często prowadzą działania edukacyjne i promocyjne mające na celu zwiększenie świadomości społecznej na temat różnych zagadnień zdrowotnych, promowanie zdrowego stylu życia i zapobieganie chorobom;
- Usługi ambulatoryjne i domowe: w niektórych systemach, samorządy mogą świadczyć usługi ambulatoryjne i domowe, takie jak opieka domowa, rehabilitacja, terapie dla osób starszych czy niepełnosprawnych;

[334] Por. M. Sandej, *Jednostki samorządu terytorialnego mają zadania w zakresie ochrony zdrowia*, https://www.prawo.pl/samorzad/zadania-samorzadu-terytorialnego-w-zakresie-ochrony-zdrowia,77385.html [dostęp: 06.10.2023].

- Usługi ratunkowe: samorządy mogą zarządzać usługami ratunkowymi, takimi jak ambulanse, które zapewniają natychmiastową opiekę medyczną w nagłych przypadkach;
- Nadzór nad jakością usług zdrowotnych: samorządy mogą pełnić funkcję nadzorczą nad jakością usług zdrowotnych na swoim terytorium, co obejmuje ocenę placówek medycznych i monitorowanie jakości opieki[335].

W Polsce samorządy terytorialne nie mają obowiązku zapewniania wszystkich typów usług zdrowotnych. Część świadczeń medycznych organizuje się na poziomie krajowym. Podstawowym celem samorządowych usług zdrowotnych jest promowanie i ochrona zdrowia publicznego. W realizacji tych celów, samorządy współpracują z wieloma podmiotami, w tym z lekarzami, szpitalami, instytucjami opieki zdrowotnej, organizacjami pozarządowymi i sektorem prywatnym[336].

Jednakże, kluczowym wyzwaniem dla samorządowych usług zdrowotnych pozostaje zapewnienie odpowiedniej jakości i efektywności tych usług, co wymaga skutecznego zarządzania i monitorowania. Warto też zauważyć, że samorządowe usługi zdrowotne stanowią istotny element gwarantujący prawo do opieki zdrowotnej dla wszystkich obywateli, zgodnie z Konstytucją Rzeczypospolitej Polskiej (1997).

W kontekście przestrzegania ochrony danych osobowych, samorządowe usługi zdrowotne w Polsce muszą spełniać rygorystyczne wymagania prawne i organizacyjne, aby zapewnić prywatność i bezpieczeństwo informacji medycznych pacjentów. Ochrona danych osobowych w tym obszarze jest szczególnie istotna, ponieważ dotyczy informacji wrażliwych, które mogą obejmować dane o stanie zdrowia, historię medyczną, wyniki badań, oraz inne informacje, które mogą identyfikować pacjentów.

Kluczowe aspekty ochrony danych osobowych w samorządowych usługach zdrowotnych:

- Zarządzanie placówkami zdrowia – w zarządzaniu szpitalami, przychodniami i innymi placówkami zdrowotnymi, samorządy muszą zapewnić, że dane pacjentów są chronione zgodnie z obowiązującymi przepisami prawa, w tym RODO. Konieczne jest wdrożenie odpowiednich środków technicznych i organizacyjnych,

[335] M. Leszczyński, *Samorząd terytorialny w zapewnieniu bezpieczeństwa społecznego*, Kielce 2021, s. 23.
[336] Por. W. Kuta, *Zieliński: Dobra współpraca samorządów z lekarzami POZ ułatwia skuteczną profilaktykę*, https://www.rynekzdrowia.pl/Polityka-zdrowotna/Zielinski-Dobra-wspolpraca-samorzadow-z-lekarzami-POZ-ulatwia-skuteczna-profilaktyke,233486,14.html [dostęp: 06.10.2023].

takich jak szyfrowanie danych, systemy kontroli dostępu, regularne audyty bezpieczeństwa, oraz szkolenia personelu;

- Publiczne programy zdrowotne – programy zdrowotne, takie jak szczepienia czy kontrola chorób przewlekłych, wymagają zbierania i przetwarzania danych osobowych uczestników. Samorządy muszą zapewnić, że te dane są gromadzone tylko w zakresie niezbędnym do realizacji celów programu i są przechowywane w sposób bezpieczny. Ważne jest również informowanie uczestników o celu i zakresie przetwarzania ich danych oraz o przysługujących im prawach, takich jak prawo dostępu do danych, prawo do sprostowania danych, czy prawo do wniesienia sprzeciwu;
- Edukacja i promocja zdrowia - działania edukacyjne i promocyjne często wiążą się z przetwarzaniem danych uczestników różnych kampanii i wydarzeń. W takich przypadkach samorządy muszą dbać o zgodność z zasadą minimalizacji danych i przechowywać je tylko przez czas niezbędny do realizacji danego celu;
- Usługi ambulatoryjne i domowe - w przypadku usług świadczonych bezpośrednio w domach pacjentów, szczególna uwaga musi być poświęcona zabezpieczeniu informacji wrażliwych, które mogą być przetwarzane na urządzeniach mobilnych lub przenośnych;
- Usługi ratunkowe - usługi ratunkowe, takie jak ambulanse, często wymagają szybkiego i efektywnego dostępu do danych medycznych pacjentów. Samorządy muszą zapewnić, że te dane są dostępne tylko dla uprawnionych osób i są przetwarzane zgodnie z wymogami ochrony danych;
- Nadzór nad jakością usług zdrowotnych - Samorządy pełniąc funkcję nadzorczą, muszą przetwarzać dane dotyczące jakości usług zdrowotnych świadczonych na swoim terenie. Dane te muszą być zbierane i analizowane w sposób zgodny z przepisami o ochronie danych osobowych, z uwzględnieniem zasad poufności i integralności danych.

Przestrzeganie zasad ochrony danych osobowych w samorządowych usługach zdrowotnych jest nie tylko obowiązkiem prawnym, ale również kluczowym elementem budowania zaufania społeczności do systemu opieki zdrowotnej.

4.1.3. Usługi infrastrukturalne

Samorządowe usługi infrastrukturalne odnoszą się do różnych dziedzin działalności samorządów lokalnych, które mają na celu zarządzanie, utrzymanie i rozwój infrastruktury publicznej w danej gminie, powiecie lub innym jednostkach samorządu terytorialnego. Obejmują one szeroki zakres obszarów, w tym[337]:

- Zarządzanie gospodarką wodno-ściekową: samorządowe usługi infrastrukturalne obejmują zarządzanie sieciami wodociągowymi, kanalizacyjnymi i oczyszczalniami ścieków. Samorząd lokalny jest odpowiedzialny za utrzymanie i rozwój tych systemów, zapewnienie dostępu do czystej wody pitnej oraz odbiór i oczyszczanie ścieków;
- Zarządzanie infrastrukturą drogową: samorząd gminy lub powiatu odpowiada za budowę, utrzymanie i modernizację dróg lokalnych i ulic. Obejmuje to naprawę nawierzchni, oznakowanie drogi, utrzymanie chodników, ścieżek rowerowych i innych elementów infrastruktury drogowej;
- Zarządzanie infrastrukturą komunikacyjną: samorząd terytorialny może również zarządzać infrastrukturą komunikacyjną, taką jak transport publiczny (autobusy, tramwaje), parkingi, stacje rowerowe, a także zapewnienie dostępu do Internetu szerokopasmowego;
- Zarządzanie infrastrukturą sportową i rekreacyjną: obejmuje ono utrzymanie obiektów sportowych, parków, placów zabaw, basenów, boisk, kortów tenisowych i innych miejsc do aktywności fizycznej i rekreacji;
- Zarządzanie infrastrukturą edukacyjną: samorządy lokalne są odpowiedzialne za utrzymanie i modernizację budynków szkół, przedszkoli, bibliotek i innych placówek edukacyjnych;
- Zarządzanie infrastrukturą zdrowotną: może obejmować zarządzanie i utrzymanie przychodni zdrowia, szpitali, ośrodków rehabilitacyjnych i innych obiektów służących opiece zdrowotnej;
- Zarządzanie infrastrukturą techniczną: samorządy lokalne mogą odpowiadać za zapewnienie dostępu do energii elektrycznej, gazu, ciepła i innych usług technicznych.

[337] Por. K. Witkowski, *Inwestycje infrastrukturalne w realizacji usług publicznych*, „Studia Lubuskie: prace Instytutu Prawa i Administracji Państwowej Wyższej Szkoły Zawodowej w Sulechowie", nr 7/2011.

Podmioty samorządowe odgrywają istotną rolę w dostarczaniu usług infrastrukturalnych, zwłaszcza w kontekście decentralizacji, która polega na przekazywaniu uprawnień administracyjnych, politycznych i fiskalnych do niższych szczebli rządu. W Polsce, proces ten rozpoczął się na początku lat 90. ubiegłego wieku i nadal jest kluczowy dla efektywnego funkcjonowania państwa[338].

Dostarczanie usług infrastrukturalnych przez podmioty samorządowe wiąże się z wieloma wyzwaniami. Należą do nich kwestie finansowania, efektywności, sprawiedliwości społecznej oraz zrównoważonego rozwoju[339]. Te wyzwania stanowią obszar intensywnych badań i debat politycznych. Usługi infrastrukturalne są ważnym elementem samorządowych usług publicznych, wywierają bowiem znaczący wpływ na rozwój społeczno-gospodarczy regionu.

Samorządowe usługi infrastrukturalne obejmują różne dziedziny działalności samorządów lokalnych, które mają na celu zarządzanie, utrzymanie i rozwój infrastruktury publicznej w gminach, powiatach oraz innych jednostkach samorządu terytorialnego. W ramach tych działań, samorządy przetwarzają dane osobowe mieszkańców, co wiąże się z koniecznością przestrzegania przepisów dotyczących ochrony danych osobowych, w tym RODO.

Podmioty samorządowe, zarządzając usługami infrastrukturalnymi, muszą sprostać licznym wyzwaniom związanym z ochroną danych osobowych:

- Finansowanie: Zapewnienie odpowiednich środków na zabezpieczenie systemów przetwarzających dane osobowe;
- Efektywność: Stosowanie nowoczesnych technologii do zarządzania danymi, które jednocześnie zapewniają ich bezpieczeństwo;
- Sprawiedliwość społeczna: Zapewnienie równego dostępu do usług publicznych przy jednoczesnym poszanowaniu prywatności obywateli;
- Zrównoważony rozwój: Długoterminowe planowanie inwestycji w technologie ochrony danych, które są przyjazne środowisku i efektywne energetycznie.

Reasumując, samorządowe usługi infrastrukturalne są kluczowym elementem działalności samorządów lokalnych, a przetwarzanie danych osobowych jest integralną częścią tych działań. Wymaga to odpowiedzialnego podejścia do ochrony danych

[338] P. Swianiewicz, *An Empirical Typology of Local Government Systems in Eastern Europe*, „Local Government Studies", nr 2/ 2003, s. 24-46.
[339] T. Bovaird, *Beyond Engagement and Participation: User and Community Coproduction of Public Services*, „Public Administration Review", nr 5/2007, s. 846-860.

osobowych, w tym przestrzegania przepisów RODO, implementacji odpowiednich technologii i procedur ochrony danych oraz ciągłego doskonalenia praktyk związanych z zarządzaniem danymi. Dzięki temu możliwe jest zapewnienie bezpieczeństwa i prywatności mieszkańców, co przyczynia się do zrównoważonego rozwoju społeczno-gospodarczego regionów.

4.1.4. Usługi środowiskowe

Do samorządowych usług środowiskowych zaliczamy te świadczone przez jednostki samorządu terytorialnego w celu ochrony środowiska naturalnego, utrzymania zasobów naturalnych oraz poprawy jakości życia mieszkańców. Zakres tych usług może być szeroki i zależy od specyfiki danego obszaru, ale najczęściej obejmuje[340]:

- Gospodarkę odpadami: samorządy są zazwyczaj odpowiedzialne za organizację zbierania i przetwarzania odpadów na swoim terytorium. Obejmuje to zarówno odpady komunalne, jak i specjalistyczne, takie jak odpady niebezpieczne, elektroniczne czy budowlane. Wiele samorządów prowadzi także kampanie na rzecz segregacji odpadów i recyklingu;
- Zarządzanie wodą i ściekami: samorządy mogą być odpowiedzialne za dostarczanie czystej wody do domów i firm, a także za odprowadzanie i oczyszczanie ścieków. Zajmują się także zarządzanie infrastrukturą wodociągową i kanalizacyjną;
- Ochrona powietrza: władze samorządowe często monitorują jakość powietrza i podejmują działania na rzecz jego poprawy. Mogą one obejmować regulację emisji zanieczyszczeń, promowanie czystych technologii, czy prowadzenie kampanii edukacyjnych na temat zanieczyszczenia powietrza;
- Zarządzanie zielenią miejską: samorząd terytorialny jest odpowiedzialny za zarządzanie parkami, terenami zielonymi, lasami miejskimi i innymi obszarami naturalnymi. Zajmuje się utrzymaniem i rozwijaniem tych przestrzeni, ochroną stref dzikiej przyrody oraz promowaniem bioróżnorodności;
- Edukacja środowiskowa: wiele samorządów prowadzi programy edukacyjne mające na celu zwiększenie świadomości ekologicznej mieszkańców i promowanie zrównoważonego stylu życia;

[340] *Rola samorządów terytorialnych w ochronie środowiska, w tym w ochronie klimatu*, https://www.gov.pl/web/edukacja-ekologiczna/rola-samorzadow-terytorialnych-w-ochronie-srodowiska-w-tym-w-ochronie-klimatu [dostęp: 06.10.2023].

- Planowanie przestrzenne: samorządy muszą dbać o odpowiednie planowanie przestrzenne, które ma na celu zrównoważony rozwój terytorium, ochronę zasobów naturalnych i minimalizowanie wpływu działalności człowieka na środowisko.

Świadczenie usług środowiskowych na poziomie samorządowym ma kluczowe znaczenie dla zrównoważonego rozwoju społeczno-gospodarczego. Lokalne organy samorządowe, ze względu na ich bliskość do społeczności lokalnej, znajdują się w dogodnej pozycji pozwalającej na trafniejsze identyfikowanie potrzeb społeczności i odpowiednie kształtowanie polityki. Jest to również zadanie pełne wyzwań, ze względu na potrzebę zrównoważonego zarządzania zasobami, zmieniające się preferencje społeczności, a także ograniczenia finansowe.

Sprostanie wszystkim tym wyzwaniom wymaga holistycznego podejścia, które łączy działania na poziomie lokalnym, krajowym i globalnym. Na poziomie lokalnym, istotne regularne angażowanie miejscowej społeczności w procesy decyzyjne, a także rozwój partnerstwa pomiędzy różnymi sektorami, by usługi środowiskowe były dostarczane w sposób zrównoważony i sprawiedliwy.

Powyższe rozważania można podsumować w sposób następujący: usługi środowiskowe stanowią kluczowy element usług publicznych na poziomie samorządowym. Efektywne zarządzanie na tej płaszczyźnie wymaga zintegrowanego podejścia, które uwzględnia zarówno potrzeby lokalnej społeczności, jak i globalne wyzwania związane z ochroną środowiska.

W kontekście świadczenia usług środowiskowych na poziomie samorządowym, istotne jest również przestrzeganie przepisów dotyczących ochrony danych osobowych. Samorządy, realizując swoje zadania, często przetwarzają dane osobowe mieszkańców, dlatego muszą zapewnić odpowiednie środki bezpieczeństwa w celu ochrony tych danych przed nieautoryzowanym dostępem, utratą czy zniszczeniem. Należy również pamiętać o transparentności w procesie przetwarzania danych oraz o przestrzeganiu zasad zgodności z przepisami, takich jak RODO.

4.1.5. Usługi społeczne

Samorządowe usługi społeczne[341] to usługi świadczone przez jednostki samorządu terytorialnego, które mają na celu zaspokajanie różnych społecznych potrzeb społeczności lokalnej.

[341] Por. *Czym są usługi społeczne*, https://cusmyslenice.pl/uslugi/czym-sa-uslugi-spoleczne [dostęp: 06.10.2023].

Mogą one obejmować szeroki zakres działań, takich jak:

- Opieka socjalna: samorządy świadczą usługi opieki społecznej, które mają na celu niesienie pomocy osobom i rodzinom znajdującym się w trudnej sytuacji życiowej. Takie wsparcie może to obejmować pomoc finansową, doradztwo, wsparcie dla osób bezdomnych, wsparcie dla ofiar przemocy domowej, czy pomoc dla osób uzależnionych;
- Wsparcie dla osób starszych: samorządy mogą świadczyć usługi mające na celu wspieranie seniorów poprzez organizowanie opieki domowej, realizowanie czy transportu dla osób starszych, realizację programów zdrowotnych lub ułatwianie dostępu do usług medycznych i rehabilitacyjnych;
- Wsparcie dla osób z niepełnosprawnością: samorządy mogą oferować różne usługi i programy mające na celu wspieranie osób niepełnosprawnych obejmujące rehabilitację, transport dostosowany do potrzeb osób niepełnosprawnych, programy edukacyjne, pomoc w znalezieniu zatrudnienia, czy ułatwianie dostępu do odpowiednich placówek oświatowych;
- Programy mieszkaniowe: samorządy często świadczą usługi związane z zapewnieniem mieszkań dla osób o niskich dochodach, osób seniorów, osób z niepełnosprawnością lub ludzi dotkniętych problemem bezdomności. Może to obejmować zarządzanie publicznymi mieszkaniami, pomoc w znalezieniu mieszkania czy programy subsydiów mieszkaniowych;
- Programy dla dzieci i młodzieży: samorządy mogą prowadzić różne programy dla dzieci i młodzieży, takie jak opieka przedszkolna, programy poza szkolne, programy sportowe i rekreacyjne, programy wsparcia dzieci z rodzin o niskich dochodach, czy programy profilaktyki problemów społecznych;
- Usługi dla bezdomnych: Samorządy często świadczą usługi dla osób bezdomnych, takie jak schroniska, programy żywieniowe, pomoc w znalezieniu zatrudnienia, czy wsparcie w procesie reintegracji społecznej.

Zgodnie z art. 164 Konstytucji Rzeczypospolitej Polskiej z 1997 roku, samorząd terytorialny ma prawo do decydowania o sprawach społecznych na terenie, który reprezentuje, co podkreśla ich kluczową rolę w świadczeniu usług społecznych[342].

Realizacja koncepcji usług społecznych jako samorządowych usług publicznych napotyka jednak wiele problemów. Wiąże się to z trudnościami związanymi

[342] Konstytucja Rzeczypospolitej Polskiej…

z zaspokajaniem rosnących potrzeb społeczności lokalnych w warunkach ograniczonych zasobów, co wymaga od samorządów innowacyjnego podejścia do zarządzania usługami społecznych.

W praktyce, wiele samorządów stara się znaleźć równowagę między tradycyjnym podejściem do zarządzania usługami społecznymi a podejściem, które jest bardziej ukierunkowane na obywatela i oparte na współpracy między sektorami publicznym, prywatnym i społeczeństwem obywatelskim[343]. To podejście, często określane jako zarządzanie sieciowe, może przyczynić się do zwiększenia zdolności samorządów do odpowiedzi na złożone i dynamiczne potrzeby społeczności, które reprezentują.

Rola usług społecznych jako samorządowych usług publicznych jest niezaprzeczalna. Ich skuteczne zarządzanie i dostarczanie są kluczowe dla zapewnienia dobrobytu i jakości życia obywateli.

W kontekście świadczenia samorządowych usług społecznych niezwykle istotna jest ochrona danych osobowych, gdyż dotyczy to przetwarzania dużej ilości wrażliwych informacji o mieszkańcach. Dane osobowe, takie jak imię, nazwisko, adres zamieszkania, dane kontaktowe, a także szczegółowe informacje dotyczące sytuacji życiowej, zdrowotnej czy finansowej, są gromadzone i przetwarzane przez jednostki samorządu terytorialnego w celu świadczenia odpowiednich usług.

Przykładowo, w ramach opieki socjalnej samorządy mogą przetwarzać informacje dotyczące dochodów rodziny, statusu zatrudnienia, historii zdrowia psychicznego i fizycznego, sytuacji mieszkaniowej oraz relacji rodzinnych. Wsparcie dla osób starszych może wymagać dostępu do danych medycznych, szczegółów dotyczących opieki zdrowotnej, a także informacji o stanie fizycznym i mobilności seniorów. Wsparcie dla osób z niepełnosprawnością często wymaga gromadzenia danych na temat rodzaju i stopnia niepełnosprawności, potrzeb rehabilitacyjnych oraz specyficznych wymagań dotyczących transportu i edukacji.

Dane te są niezbędne do efektywnego świadczenia usług, ale jednocześnie są one bardzo wrażliwe i wymagają szczególnej ochrony. Niedostateczne zabezpieczenie tych danych może prowadzić do poważnych konsekwencji, takich jak kradzież tożsamości, nadużycia finansowe, czy też dyskryminacja. Dlatego samorządy muszą ściśle przestrzegać przepisów dotyczących ochrony danych osobowych, aby zapobiegać takim zagrożeniom.

[343] L.M. Salamon, *The Tools of Government in the Digital Age*, Palgrave Macmillan 2015.

Przestrzeganie przepisów dotyczących ochrony danych osobowych jest kluczowe dla zapewnienia zaufania mieszkańców do samorządowych usług społecznych oraz dla ochrony prywatności i bezpieczeństwa ich danych osobowych.

Przestrzeganie przepisów dotyczących ochrony danych osobowych nie tylko zapewnia zgodność z prawem, ale także buduje zaufanie mieszkańców do samorządowych usług społecznych. Transparentność i odpowiedzialność w zarządzaniu danymi osobowymi przyczyniają się do poczucia bezpieczeństwa i pewności, że ich prywatność jest chroniona. To z kolei sprzyja większej otwartości mieszkańców na korzystanie z oferowanych usług i aktywne uczestnictwo w życiu społeczności lokalnej.

4.1.6. Usługi kulturalne

Samorządowe usługi kulturalne odnoszą się do zestawu usług oferowanych przez jednostki samorządu terytorialnego w celu promowania kultury i sztuki, zachowania dziedzictwa kulturowego oraz zaspokajania kulturalnych potrzeb mieszkańców. Takie usługi mogą obejmować[344]:

- Zarządzanie instytucjami kultury: samorządy zazwyczaj zarządzają lokalnymi instytucjami kultury, takimi jak biblioteki, muzea, galerie sztuki, teatry, centra kultury i inne. Zajmują się takimi zagadnieniami, jak utrzymanie tych instytucji, zatrudnianie personelu, organizowanie wydarzeń i zarządzanie zbiorami;
- Organizacja wydarzeń kulturalnych: samorządy często organizują lub wspierają organizację różnych wydarzeń kulturalnych, takich jak festiwale, koncerty, wystawy, warsztaty artystyczne, czy spotkania literackie;
- Edukacja kulturalna: wiele samorządów prowadzi programy edukacji kulturalnej, które mają na celu zwiększenie świadomości i zrozumienia kultury i sztuki. Może to obejmować warsztaty, wykłady, programy dla szkół, czy projekty społeczne;
- Zachowanie dziedzictwa kulturowego: samorządy mogą być odpowiedzialne za ochronę i konserwację lokalnego dziedzictwa kulturowego, takiego jak zabytki, miejsca historyczne, czy kolekcje muzealne;

[344] Zob.*Usługi publiczne w obszarze kultury finansowane przez jednostki samorządu terytorialnego w Polsce. Raport końcowy*, Główny Urząd Statystyczny, Warszawa 2018.

- Wsparcie dla artystów i twórców: samorządy często oferują różne formy wsparcia dla lokalnych artystów i twórców, takie jak granty, stypendia, przestrzenie do pracy czy możliwości wystawiania i prezentowania swojej pracy;
- Promocja kultury lokalnej: samorządy mogą podejmować działania na rzecz promowania kultury lokalnej, takie jak organizacja festiwali folklorystycznych, wsparcie dla lokalnych grup artystycznych, czy promowanie lokalnej sztuki i rzemiosła.

Zarządzanie usługami kulturalnymi na poziomie samorządowym wiąże się jednak z szeregiem wyzwań. Obejmują one zarówno kwestie finansowe, jak i kwestie dotyczące dostępu do kultury i równości. Do wyzwań finansowych należy utrzymanie infrastruktury kulturalnej i finansowanie inicjatyw kulturalnych w sytuacji ograniczonych budżetów[345]. Co do dostępu i równości, badania pokazują, że istnieje potrzeba zwiększenia dostępności i reprezentacji różnych grup społecznych w usługach kulturalnych[346].

Usługi kulturalne jako samorządowe usługi publiczne odgrywają kluczową rolę w kształtowaniu tożsamości społeczności, promowaniu różnorodności kulturowej i tworzeniu spójności społecznej. Ich zarządzanie i finansowanie stanowią jednak wyzwanie dla samorządów, które muszą radzić sobie z ograniczeniami finansowymi i dążyć do zapewnienia równego dostępu do kultury.

W ramach świadczenia samorządowych usług kulturalnych może dochodzić do przetwarzania danych osobowych. Przykłady przetwarzanych danych osobowych to dane uczestników wydarzeń kulturalnych, osób korzystających z bibliotek czy beneficjentów programów edukacyjnych. Samorządy są zobowiązane do przestrzegania przepisów dotyczących ochrony danych osobowych, w tym RODO.

4.1.7. Usługi bezpieczeństwa

Samorządowe usługi bezpieczeństwa to usługi świadczone przez jednostki samorządu terytorialnego, które mają na celu zapewnienie bezpieczeństwa i porządku publicznego na ich terytorium. Te usługi mogą obejmować[347]:

- Straż miejska: w niektórych przypadkach, samorządy mogą zarządzać lokalnymi siłami policyjnymi odpowiedzialnymi za utrzymanie porządku publicznego,

[345] A. Kangas, *Cultural policy and cultural diversity*, „International Encyclopedia of Civil Society" 2010.
[346] T. Višnić, *Access to Culture in the European Union*, „European Journal of Cultural Policy" 2017.
[347] M. Leszczyński, *Samorząd terytorialny w zapewnieniu bezpieczeństwa społecznego*…

reagowanie na incydenty kryminalne, prowadzenie śledztw, zapobieganie przestępstwom, czy współpracę z innymi służbami bezpieczeństwa;

- Straż pożarna: samorządy często zarządzają lokalnymi jednostkami straży pożarnej, które są odpowiedzialne za reagowanie na pożary, prowadzenie akcji ratowniczych, edukację przeciwpożarową, czy zapobieganie pożarom;
- Zarządzanie kryzysowe i ochrona cywilna: samorządy mogą być odpowiedzialne za planowanie i reagowanie na sytuacje kryzysowe, takie jak katastrofy naturalne, wypadki przemysłowe, czy zagrożenia terrorystyczne. Obejmuje to przygotowywanie planów zarządzania kryzysowego, koordynowanie działań różnych służb, czy edukację społeczeństwa w zakresie ochrony cywilnej;
- Ochrona mienia publicznego: na władze samorządowe nakłada się obowiązek ochrony mienia publicznego, takiego jak budynki, infrastruktura, parki czy zasoby naturalne. Ochrona polega na zapobieganiu aktom wandalizmu, kradzieży, czy innym formom uszczerbku na mieniu publicznym;
- Regulacja ruchu drogowego: samorządy często zarządzają lokalnym ruchem drogowym, a konkretnie regulacją przepływu ruchu, utrzymaniem infrastruktury drogowej, egzekwowaniem przepisów ruchu drogowego, czy edukacją drogową;
- Pomoc prawna i poradnictwo: niektóre samorządy mogą oferować usługi pomocy prawnej dla mieszkańców, takie jak doradztwo prawne, mediacje czy wsparcie dla ofiar przestępstw.

Dbanie o różne aspekty bezpieczeństwa lokalnego stanowi ważny element działalności samorządu terytorialnego. Współpraca z lokalnymi instytucjami, edukacja społeczności, a także strategiczne planowanie i reagowanie na zagrożenia to niektóre z najważniejszych aspektów tych usług.

W kontekście świadczenia powyższych usług, samorządy muszą również przestrzegać przepisów dotyczących ochrony danych osobowych. Obejmuje to:

- Zbieranie, przetwarzanie i przechowywanie danych osobowych: Samorządy muszą zapewnić, że dane osobowe są zbierane wyłącznie w zakresie niezbędnym do świadczenia usług bezpieczeństwa, przetwarzane zgodnie z przepisami prawa oraz przechowywane w sposób zabezpieczający je przed nieuprawnionym dostępem;
- Transparentność i informowanie: Mieszkańcy muszą być informowani o celu i zakresie przetwarzania ich danych osobowych oraz przysługujących im prawach, w tym prawie do dostępu do danych, ich poprawiania i usunięcia;

- Bezpieczeństwo danych: Samorządy muszą wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmianą, nieuprawnionym ujawnieniem lub dostępem;
- Zgłaszanie naruszeń: W przypadku naruszenia ochrony danych osobowych, samorządy mają obowiązek niezwłocznie zgłosić takie naruszenie odpowiednim organom nadzorczym oraz w określonych przypadkach, poinformować osoby, których dane dotyczą;
- Szkolenia i edukacja: Pracownicy samorządowi powinni być regularnie szkoleni w zakresie przepisów o ochronie danych osobowych i najlepszych praktyk związanych z ich przetwarzaniem.

Zapewnienie ochrony danych osobowych jest kluczowe dla budowania zaufania mieszkańców oraz skutecznego i zgodnego z prawem świadczenia samorządowych usług bezpieczeństwa.

4.2. Przetwarzanie danych osobowych w ramach świadczenia usług publicznych

Przetwarzanie danych osobowych stanowi nieodłączny element świadczenia usług publicznych. Umożliwia to sprawną realizację różnych zadań, od skutecznego świadczenia usług zdrowotnych po efektywne zarządzanie infrastrukturą publiczną. Takie przetwarzanie musi zawsze odbywać się zgodnie z obowiązującymi przepisami o ochronie danych osobowych, co już wielokrotnie podkreślano.

Usługi publiczne, takie jak służba zdrowia, edukacja czy zarządzanie infrastrukturą, mogą wymagać przetwarzania danych osobowych na szeroką skalę. Proces ten zawsze musi odbywać się z poszanowaniem praw jednostek, w tym prawa do prywatności i ochrony danych osobowych. Organizacje publiczne muszą zapewnić stosowne środki bezpieczeństwa, które chronią dane przed nieuprawnionym dostępem, zmianą, utratą, nieuprawnionym udostępnieniem, a także przed innymi formami nieprawidłowego przetwarzania.

Pomimo istniejących regulacji, przetwarzanie danych osobowych w ramach świadczenia usług publicznych wciąż stanowi wyzwanie. Na przykład, zasada minimalizacji danych, która zobowiązuje do przetwarzania jedynie niezbędnych informacji może okazać się trudna do zastosowania w praktyce, zwłaszcza w przypadku dużych projektów związanych z zarządzaniem infrastrukturą publiczną.

Jednocześnie, rozwój technologii cyfrowych, takich jak sztuczna inteligencja, big data czy Internet rzeczy[348], stwarza nowe możliwości, ale też nowe ryzyka dla ochrony danych osobowych. Dlatego też coraz większą rolę odgrywa rozwój technologii zorientowanych na prywatność, które pozwalają na efektywne przetwarzanie danych z zachowaniem ochrony prywatności, takich jak anonimizacja czy techniki przetwarzania federacyjnego.

Najważniejszymi regulacjami w tej dziedzinie są RODO oraz lokalne przepisy dotyczące ochrony danych. Poniżej przedstawiono kilka kluczowych zasad przetwarzania danych osobowych w ramach świadczenia usług publicznych:

- Zasada legalności, uczciwości i przejrzystości: Dane osobowe muszą być przetwarzane zgodnie z prawem, w sposób uczciwy i przejrzysty dla osoby, której dane dotyczą;
- Zasada minimalizacji danych: instytucje publiczne powinny gromadzić tylko te informacje, które są niezbędne do świadczenia usług. Nie powinny gromadzić więcej danych, niż jest to konieczne;
- Zasada celowości: dane osobowe powinny być gromadzone do określonych, wyraźnych i legalnych celów. Nie powinny być dalej przetwarzane w sposób niezgodny z tymi celami;
- Zasada ograniczenia przechowywania: dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osób, której dane dotyczą, nie dłużej, niż jest to konieczne do celów, dla których są przetwarzane;
- Zasada integralności i poufności: dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed nieuprawnionym lub nielegalnym przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

Powyższe zasady są szczególnie istotne w kontekście cyfryzacji usług publicznych, która niesie ze sobą nowe wyzwania i ryzyka związane z ochroną danych osobowych. Instytucje publiczne muszą stale monitorować i aktualizować własne systemy przetwarzania danych, aby zapewnić zgodność z obowiązującymi przepisami i działać w sposób maksymalnie efektywny.

[348] Zob. *Co to jest IoT*, https://www.oracle.com/pl/internet-of-things/what-is-iot/ [dostęp: 06.10.2023].

4.2.1.Zasada legalności, uczciwości i przejrzystości

Zasada legalności (art. 5 ust. 1 lit. a RODO) wymaga, by przetwarzanie danych osobowych odbywało się zgodnie z prawem, co oznacza, że podobne procedury muszą opierać się na jednym z prawnie uzasadnionych celów wymienionych w art. 6 RODO. W praktyce oznacza to, że organizacje przetwarzające dane osobowe muszą mieć wyraźny i legalny powód do ich gromadzenia i wykorzystania.

Zasada uczciwości (także zawarta w art. 5 ust. 1 lit. a RODO) wymaga, od administratora danych osobowych postępowania w sposób uczciwy wobec osób, których dane dotyczą[349]. To nakłada na niego obowiązek informowania osób, których dane przetwarza, o celach przetwarzania, przekazując im wszystkie niezbędne informacje w sposób zrozumiały i łatwo dostępny. W praktyce zasada uczciwości wprowadza wymóg informacyjny dla administratora danych, który musi być spełniony w odpowiedni sposób, zgodnie z art. 13 i 14 RODO[350].

Zasada przejrzystości (również zawarta w art. 5 ust. 1 lit. a RODO) nakłada na administratora danych obowiązek informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych w sposób jasny, zrozumiały i łatwo dostępny[351]. To oznacza, że wszelkie informacje i komunikacja związana z przetwarzaniem danych osobowych powinny być przekazywane w sposób prosty i zrozumiały, a także łatwo dostępne dla osób, których dane dotyczą. Zasadę przejrzystości można realizować poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, takich jak polityka prywatności czy jasne oznaczenia na stronach internetowych.

4.2.2. Zasada minimalizacji danych

Rozporządzenie o Ochronie Danych Osobowych (RODO) wprowadza szereg zasad, które muszą być przestrzegane przy przetwarzaniu danych osobowych.

Jedna z tych zasad polega na minimalizacji danych, która ma kluczowe znaczenie dla utrzymania bezpieczeństwa danych i ochrony prywatności osób, których dane dotyczą. Zgodnie z zasadą minimalizacji danych, dane osobowe powinny być „adekwatne, stosowne i ograniczone do tego, co jest niezbędne w kontekście celów,

[349] RODO, art. 5 ust. 1 lit. a.
[350] RODO, art. 13 i 14.
[351] RODO, art. 5 ust. 1 lit. a.

w których są przetwarzane" – art. 5(1)(c) RODO[352]. To oznacza, że organizacje powinny gromadzić tylko te dane osobowe, które są konieczne do osiągnięcia określonych, jasno zdefiniowanych celów.

Zasada minimalizacji danych wprowadza obowiązek dla organizacji, aby dokładnie przemyśleć, jakie informacje są im potrzebne do realizacji swoich celów, a następnie gromadzić tylko te dane i nic więcej. W praktyce oznacza to, że jeśli organizacja nie potrzebuje określonej informacji do osiągnięcia swojego celu, nie powinna jej gromadzić.

Jednym z kluczowych aspektów tej zasady jest jej wpływ na praktyki przechowywania danych. Zasada minimalizacji danych oznacza również, że organizacje nie powinny przechowywać danych osobowych dłużej, niż jest to konieczne do celów, dla których te dane zostały zebrane lub przetwarzane.

Chociaż zasada minimalizacji danych może wydawać się prosta w teorii, jej praktyczna realizacja bywa dość trudna. Organizacje muszą dokładnie zrozumieć, jakie dane są im potrzebne, w jaki sposób je wykorzystywać i jak długo powinny je przechowywać, co wymaga dokładnego, starannego planowania oraz zarządzania danymi.

4.2.3. Zasada celowości

Zasada celowości stanowi kluczowy element RODO. Ta zasada mówi, że osobiste dane muszą być zbierane dla określonych, wyraźnych i legalnych celów. Pozyskane informacje nie mogą być dalej przetwarzane w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b RODO)[353].

Zgodnie z zasadą celowości, organizacje muszą jasno określić, dla jakiego celu zbierają określone informacje. Przykładowo, cel może obejmować zarządzanie relacjami z klientami, marketing bezpośredni, zgodność z obowiązkami prawnymi itd.

To wymaga od organizacji jasnego zdefiniowania celu przetwarzania danych na etapie ich zbierania[354].Dodatkowo, zasada celowości mówi, że dane nie mogą być dalej przetwarzane w sposób niezgodny z pierwotnym celem. Oznacza to, że jeśli dane zostały zebrane dla określonego celu, nie mogą one być później używane do innych

[352] RODO, art. 5(1)(c).
[353] Ibidem, art. 5.
[354] *Podręcznik ds. Ochrony Danych*, Biuro Rzecznika Praw Obywatelskich, Warszawa 2019, s. 56.

potrzeb, chyba że osoba, której dane dotyczą, wyraziła na to zgodę lub istnieją inne legalne podstawy do takiego przetwarzania[355].

Zgodnie z RODO, organizacje muszą być w stanie wykazać zgodność z zasadą celowości. Czyli muszą dowieść, że zbierają i przetwarzają dane zgodnie z określonymi, wyraźnymi i legalnymi celami. W praktyce oznacza to utrzymanie dokładnej dokumentacji procesów przetwarzania danych i stosowanie procedur zapewniających przestrzeganie tej zasady.

4.2.4. Zasada ograniczenia przechowywania

Zasada ograniczenia przechowywania danych osobowych, znana również jako „zasada minimalizacji przechowywania"[356], jest jednym z kluczowych elementów RODO. Według tej zasady, dane osobowe powinny być przechowywane tylko przez okres niezbędny do realizacji celów, dla których dane te zostały zebrane.

Dane osobowe nie powinny być przechowywane na serwerach firmy na stałe. Należy je usuwać lub redukować, gdy cel, dla którego zostały zebrane, jest już nieaktualny i nie będą dłużej potrzebne[357].

To szczególnie ważne w przypadku danych wrażliwych, takich jak informacje o zdrowiu, orientacji seksualnej, przekonaniach religijnych lub przynależności etnicznej. Podobne informacje należy przechowywać z najwyższą ostrożnością a następnie usunąć, gdy tylko przestaną być niezbędne[358].

Jednakże, istnieją pewne wyjątki od tej zasady. Na przykład, dane mogą być przechowywane na dłużej, jeżeli są potrzebne do celów archiwizacyjnych w interesie publicznym, badań naukowych lub historycznych, lub do celów statystycznych[359].

---

[355] *Wytyczne w sprawie zasady celowości pod kątem przetwarzania danych osobowych*, Grupa Robocza ds. Ochrony Danych (Article 29 Working Party).

[356] Art. 5(1)(e) RODO stwierdza, że dane osobowe muszą być „przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, nie dłużej niż jest to niezbędne do celów, w których dane te są przetwarzane".

[357] To może obejmować różne sytuacje, takie jak zakończenie umowy z klientem, zakończenie projektu badawczego, dla którego dane zostały zebrane, lub zakończenie procesu rekrutacji, jeśli dane zostały zebrane w ramach tego procesu.

[358] Art. 9 RODO określa kategorie szczególnie wrażliwych danych osobowych, zasługujących na dodatkową ochronę.

[359] M. Milan, *Jak długo można przechowywać dane osobowe?*, https://poradnikprzedsiebiorcy.pl/-jak-dlugo-mozna-przechowywac-dane-osobowe [dostęp: 06.10.2023].

4.2.5. Zasada integralności i poufności

Zgodnie z RODO, jedną z istotnych zasad, które powinny być przestrzegane przez wszystkie organizacje przetwarzające dane osobowe, jest zasada integralności i poufności. Zasada integralności i poufności określa, że dane osobowe należy przetwarzać w sposób zapewniający odpowiednie ich zabezpieczenie, w tym ochronę przed nieautoryzowanym lub nielegalnym przetwarzaniem oraz przed przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą stosowania odpowiednich środków technicznych i organizacyjnych[360].

W praktyce oznacza to, że firmy i organizacje muszą stosować odpowiednie środki zabezpieczające, aby chronić dane, które przetwarzają. Mogą one obejmować szyfrowanie danych, zapewnienie bezpiecznego przechowywania informacji, a także zastosowanie odpowiednich procedur zarządzania ryzykiem i oceny ryzyka. Ponadto, zasada integralności i poufności wymaga również, aby firmy zatrudniały odpowiednio przeszkolony personel i stosowały procedury, które pomogą zapewnić ochronę danych[361].

RODO zobowiązuje organizacje do informowania organów nadzorczych i osób, których dane dotyczą, o naruszeniach bezpieczeństwa danych osobowych. W przypadku naruszenia integralności i poufności danych, organizacje powinny zgłosić zaistniały problem do odpowiedniego organu nadzorczego w ciągu 72 godzin po stwierdzeniu naruszenia[362].

Zasada integralności i poufności bez wątpienia stanowi jeden z kardynalnych elementów RODO i wymaga od organizacji podjęcia odpowiednich środków, aby chronić dane, które przetwarzają, przed nieautoryzowanym dostępem, utratą, zniszczeniem lub uszkodzeniem.

4.3. Wymogi techniczne i organizacyjne w ochronie danych osobowych

Ochrona danych osobowych jest kluczowym aspektem funkcjonowania współczesnych organizacji, zwłaszcza w erze cyfrowej, gdzie dane są narażone na różnorodne zagrożenia. Aby skutecznie chronić dane osobowe, organizacje muszą

[360] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych…
[361] Ibidem.
[362] Ibidem.

spełniać określone wymogi techniczne i organizacyjne. Wymogi te mają na celu zapewnienie zgodności z przepisami prawa oraz minimalizowanie ryzyka naruszeń bezpieczeństwa. Bezpieczeństwo danych osobowych obejmuje takie aspekty, jak: bezpieczeństwo fizyczne, bezpieczeństwo systemów IT, procedury organizacyjne, czy zarządzanie ryzykiem. [363]

Pierwszym krokiem w ochronie danych osobowych jest zapewnienie bezpieczeństwa fizycznego infrastruktury IT. Działania w tym zakresie obejmują zabezpieczenie infrastruktury, zabezpieczenie pomieszczeń i szaf serwerowych, w których przechowywane są serwery i inne urządzenia IT przed nieautoryzowanym dostępem.

Pierwszy obszar zabezpieczenie infrastruktury uzyskuje się zazwyczaj przez:

a) **Monitoring wizyjny** (ang. Closed-Circuit Television - CCTV) obejmujący wszystkie wejścia i krytyczne obszary budynków.
b) **Systemy alarmowe** połączone z lokalnymi służbami bezpieczeństwa oraz poprzez kontrolę dostępu fizycznego za pomocą kart dostępu, kodów PIN lub biometrii w celu ograniczenia dostępu do pomieszczeń przechowujących dane wrażliwe. [364]

Drugim obszarem w ochronie danych osobowych jest zabezpieczenie pomieszczeń i szaf serwerowych, które osiąga się poprzez:

a) **Zamykane na klucz lub kod dostępu** realizowane poprzez stosowanie zamków mechanicznych lub elektronicznych.
b) **Czujniki otwarcia drzwi**, które monitorują i alarmują o nieautoryzowanych otwarciach krytycznych obszarów. Ponadto zalecane jest prowadzenie ścisłej kontroli nad kluczami i kartami dostępu do pomieszczeń.
c) **Zasilanie awaryjne** dla zapewnienia ciągłości zasilania w przypadku przerw w dostawie energii elektrycznej. Osiąga się to z reguły poprzez stosowanie systemów zasilania awaryjnego (ang. Uninterruptible Power Supply - UPS) lub generatorów prądu.

[363] M. Kopiczko, P. Iwicka, *Jak chronić dane osobowe?*, https://www.czerwona-skarbonka.pl/jak-chronic-dane-osobowe/ [dostęp: 06.10.2023].
[364] A. Taylor, D. Alexander, A. Finch, D. Sutton, *Security Management Principles*, Swindon 2020, s. 37-52.

d) **Systemy gaśnicze** minimalizujące ryzyko uszkodzenia sprzętu IT, są niezbędnym wyposażeniem pomieszczeń i serwerowni.

e) **Monitoring temperatury i wilgotności** prowadzony dla przestrzegania warunków środowiskowych. Zazwyczaj urządzenia monitorujące są połączone z urządzeniami alarmującymi w przypadku przekroczenia dopuszczalnych wartości.

f) **Audyty i kontrola dostępu** stanowią ostatni składnik poprawnie działającego sytemu zabezpieczenia pomieszczeń i szaf serwerowych.

Stosowanie powyższych środków zabezpieczających infrastrukturę IT jest zewnętrznym zabezpieczeniem dla ochrony danych osobowych. Zapewnia to nie tylko zgodność z przepisami prawa, ale także minimalizuje ryzyko naruszeń bezpieczeństwa i buduje zaufanie wśród klientów oraz partnerów zewnętrznych.

Drugą składowa ochrony danych osobowych jest bezpieczeństwo systemów IT. Działania w tym zakresie obejmują:

a) **Szyfrowanie danych w tranzycie** sprowadzające się do zabezpieczenia danych przesyłanych przez sieci publiczne i prywatne za pomocą protokołów szyfrowania, takich jak SSL (ang. **Secure Sockets Layer)**[365] lub w nowszego TLS (ang. **Transport Layer Security)**[366], oraz **szyfrowanie danych w spoczynku,** gdzie stosuje się silne algorytmy szyfrujące dla danych przechowywanych na dyskach twardych, nośnikach przenośnych i w bazach danych SSL/TLS (to skróty od dwóch protokołów kryptograficznych używanych do zabezpieczania komunikacji w sieciach komputerowych).

b) **Kontrolę dostępu,** gdzie następuje autoryzacja użytkowników poprzez ustanowienie ścisłych polityk dostępu, zapewniających dostęp do danych tylko dla upoważnionych użytkowników oraz poprzez uwierzytelnianie

[365] **SSL (Secure Sockets Layer)** to protokół kryptograficzny, który został zaprojektowany w celu zapewnienia bezpiecznej komunikacji w sieci, głównie w Internecie. SSL szyfruje dane przesyłane między serwerem a klientem, co chroni je przed podsłuchem, fałszowaniem i innymi zagrożeniami.

[366] **TLS (Transport Layer Security)** to następca SSL i jego ulepszona wersja. TLS oferuje lepsze mechanizmy szyfrowania, większe bezpieczeństwo oraz jest bardziej odporny na różne rodzaje ataków. TLS jest obecnie standardem w zabezpieczaniu komunikacji internetowej, zastępując starszy protokół SSL.

wieloskładnikowe MFA (ang Multi-Factor Authentication)[367], wymuszające dodatkową weryfikację, przy m.in. kodu SMS lub aplikacji uwierzytelniającej.

c) **Systemy detekcji i zapobiegania włamaniom,** z reguły wykorzystywane są systemy zabezpieczeń sieciowych IDS (ang. Intrusion Detection System)[368] i IPS (ang. Intrusion Prevention System)[369], ponadto zalecane jest ciągłe monitorowanie ruchu sieciowego i działań systemowych w celu wykrywania podejrzanej aktywności. Integralną częścią tych zabezpieczeń jest reagowanie na incydenty poprzez coraz częściej automatyczne blokowanie podejrzanych działań i informowanie administratorów o potencjalnych zagrożeniach.
d) **Aktualizację oprogramowania** – poprzez regularne instalowanie aktualizacji i poprawek bezpieczeństwa dla wszystkich systemów operacyjnych, aplikacji i urządzeń sieciowych. Istotnym czynnikiem jest również proaktywne zarządzanie i szybkie wdrażanie aktualizacji zabezpieczających na nowe podatności.
e) **Kopie zapasowe** tworzone winny być regularnie, a przechowywanie ich zaleca się przetrzymywać w bezpiecznych, zdalnych lokalizacjach. Ponadto dobrą praktyką jest systematyczne testowanie procedur odzyskiwania danych z kopii zapasowych, aby zapewnić ich skuteczność w przypadku awarii.[370]

Trzecią składowa ochrony danych osobowych są procedury organizacyjne, czy zarządzanie ryzykiem. Do dobrych praktyk w tym względzie należą:

---

[367] **MFA (Multi-Factor Authentication)**, czyli uwierzytelnianie wieloskładnikowe, to metoda zabezpieczania dostępu do systemów informatycznych, która wymaga od użytkownika potwierdzenia tożsamości przy użyciu więcej niż jednego czynnika uwierzytelnienia. MFA opiera się na kombinacji co najmniej dwóch z trzech rodzajów czynników: Coś, co użytkownik wie: Hasło, PIN lub odpowiedź na pytanie zabezpieczające. Coś, co użytkownik posiada: Karta dostępu, telefon komórkowy z aplikacją generującą jednorazowe kody, token sprzętowy, klucz USB (np. YubiKey). Coś, czym użytkownik jest: Czynnik biometryczny, taki jak odcisk palca, rozpoznawanie twarzy, skan tęczówki oka lub głos.

[368] **IDS (Intrusion Detection System)** jest systemem wykrywania włamań. IDS to narzędzie monitorujące ruch sieciowy i systemy komputerowe w celu wykrywania podejrzanej aktywności, która może wskazywać na próbę ataku lub włamania. IDS analizuje ruch sieciowy i porównuje go z bazą znanych wzorców ataków (sygnatur) lub wykorzystuje metody heurystyczne do wykrywania anomalii. Główną funkcją IDS jest wykrywanie potencjalnych zagrożeń i alarmowanie administratorów o ich wystąpieniu.

[369] **IPS (Intrusion Prevention System)** jest systemem zapobiegania włamaniom. IPS działa podobnie jak IDS, ale z dodatkową funkcją – oprócz wykrywania zagrożeń, IPS może automatycznie podejmować działania mające na celu zapobieżenie atakowi. Obejmuje to blokowanie ruchu sieciowego, który został uznany za niebezpieczny, odrzucanie pakietów danych lub zamykanie połączeń. IPS nie tylko monitoruje, ale również aktywnie reaguje na wykryte zagrożenia w czasie rzeczywistym.

[370] A. Carapola, *The Data Center Builder's Bible - Book 1: Defining Your Data Center Requirements: Specifying, Designing, Building and Migrating to New Data Centers*, Washington 2018, s. 71-82.

a) **Szkolenia pracowników** realizowane poprzez regularną edukację dla całego personelu w zakresie polityk ochrony danych i najlepszych praktyk w obszarze bezpieczeństwa informacji. Dzięki systematycznie prowadzonym aktywnością następuje podnoszenie świadomości wykonujących obowiązki służbowe. Ponadto zaleca się przeprowadzenie specjalistycznych szkoleń dla pracowników IT i osób odpowiedzialnych za ochronę danych, koncentrujące się na zaawansowanych technikach i narzędziach zabezpieczeń.

b) **Polityki i procedury bezpieczeństwa,** w których zawiera się opracowanie i dokumentowanie wdrażania polityk bezpieczeństwa danych, obejmujących zarządzanie dostępem, przetwarzanie danych, reagowanie na incydenty oraz przechowywanie danych. Istotnym elementem są także procedury reagowania na incydenty, które dzięki jasno określonym wytycznym postępowania w przypadku naruszenia bezpieczeństwa, w tym zawiadamianie odpowiednich organów i zainteresowanych stron efektywnie, przyczyniają się do eliminacji zagrożeń lub minimalizacji ich skutków.

c) **Zasady minimalizacji danych** sprowadzające się do ograniczenia zbierania danych osobowych tylko do niezbędnych informacji. Jak również do przechowywanie danych tylko przez okres konieczny do realizacji celu, dla którego zostały zebrane.

d) **Regularne audyty i oceny ryzyka –** realizowane poprzez regularne przeprowadzanie audytów wewnętrznych i zewnętrznych poprzez identyfikację, ocenę i zarządzanie ryzykiem związanym z przetwarzaniem danych osobowych.

e) **Plan ciągłości działania** (ang. Business Continuity Plan - BCP) jest opracowywany celem zapewnienia ciągłości operacyjnej organizacji w przypadku awarii systemów IT lub szybkiego przywrócenia po wystąpieniu sytuacji kryzysowej, takiej jak awaria systemu, katastrofa naturalna, cyberatak, czy inne poważne zakłócenie.

f) **Plan awaryjny** (ang. Disaster Recovery Plan - DRP) będący szczegółowym planem reagowania na awarie, obejmującym procedury odzyskiwania danych i przywracania normalnego funkcjonowania systemów. Współcześnie takie palny są kluczowym elementem strategii zarządzania ciągłością działania, mającym na celu minimalizowanie skutków incydentów, które mogą zakłócić działalność danego podmiotu.

g) **Zgłaszanie i dokumentowanie incydentów**, realizowane jest poprzez obowiązkowe zgłaszanie naruszeń ochrony danych odpowiednim organom nadzorczym oraz osobom, których dane zostały naruszone oraz dokładne ewidencjonowanie wszystkich incydentów związanych z bezpieczeństwem danych.[371]

Spełnienie powyższych wymogów technicznych i organizacyjnych jest niezbędne do skutecznej ochrony danych osobowych. Podmioty organizacyjne, które inwestują w odpowiednie środki bezpieczeństwa i przestrzegają ich norm, mogą nie tylko zminimalizować ryzyko naruszeń, ale również budować zaufanie wśród klientów i partnerów biznesowych.

4.4. Uprawnienia osób, których dane dotyczą

Na mocy artykułu 13 i 14 RODO, osoby, których dane dotyczą, mają prawo być informowane o zbieraniu i przetwarzaniu ich danych osobowych. Prawo do informacji obejmuje informacje o celu przetwarzania, odbiorcach danych, okresie przechowywania oraz o prawach związanych z przetwarzaniem danych. Artykuł 15 RODO gwarantuje osobom prawo dostępu do swoich danych. Osoby mają prawo żądać od kontrolera danych kopii gromadzonych danych, co daje możliwość sprawdzenia i potwierdzenia legalności przetwarzania[372].

Artykuł 16 RODO umożliwia osobom poprawianie nieprawidłowych danych osobowych. Jeżeli dane są nieaktualne lub niepoprawne, osoby mają prawo żądać ich poprawienia. Z kolei tzw. „prawo do bycia zapomnianym", zdefiniowane w artykule 17, umożliwia żądanie usunięcia swoich danych osobowych. Kontroler danych musi usunąć dane, jeżeli nie ma już legalnego powodu do ich przetwarzania lub jeśli osoba wycofała zgodę na przetwarzanie[373].

Artykuł 18 RODO wprowadza prawo do ograniczenia przetwarzania. Oznacza to, że możemy żądać zawieszenia przetwarzania swoich danych osobowych w określonych sytuacjach, np. gdy kwestionuje dokładność danych. Prawo do przenoszenia danych, zgodnie z artykułem 20 RODO, pozwala na przeniesienie swoich danych osobowych między kontrolerami danych. To prawo jest szczególnie ważne w kontekście usług

[371] S. Hunziker, *Enterprise Risk Management*, Cham 2021, s. 23-41.
[372] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679…
[373] Ibidem.

cyfrowych, gdzie dane użytkowników często są przenoszone między różnymi usługodawcami[374].

Na mocy artykułu 21 RODO, osoby mają prawo w dowolnym momencie sprzeciwić się przetwarzaniu ich danych osobowych w przypadkach, gdy przetwarzanie jest oparte na interesie publicznym lub interesie prawnym kontrolera. Natomiast artykuł 22 RODO daje prawo do niepodlegania decyzjom, które mają istotne skutki prawne lub w inny istotny sposób na nich wpływają, a które są oparte wyłącznie na automatycznym przetwarzaniu, w tym profilowaniu[375].

Prawa osób, których dane dotyczą stanowią pewnego rodzaju fundament RODO. Wprowadzają one większą transparentność i kontrolę nad procedurami przetwarzaniem podobnych informacji, co jest szczególnie ważne w dobie ery cyfrowej, gdzie dane osobowe są często zbierane i przetwarzane na dużą skalę. Zrozumienie tych praw ma kluczowe znaczenie zarówno dla jednostek, które chcą chronić swoją prywatność, jak i dla organizacji, które przetwarzają dane osobowe.

[374] Ibidem.
[375] *Ibidem*.

ROZDZIAŁ V
ANALIZA PRAKTYK OCHRONY DANYCH OSOBOWYCH W WYBRANYCH JEDNOSTKACH ORGANIZACYJNYCH SAMORZĄDU TERYTORIALNEGO. WYNIKI BADAŃ

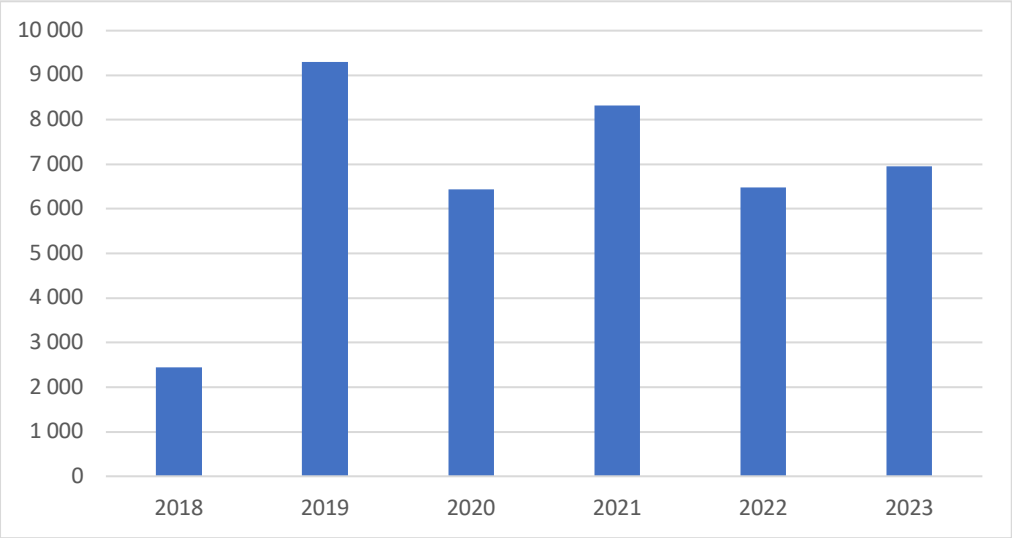
5.1. Statystyka zgłaszanych naruszeń ochrony danych osobowych w jednostkach samorządu terytorialnego

Ochrona danych osobowych w jednostkach samorządu terytorialnego (JST) w Polsce stała się istotnym wyzwaniem w ostatnich latach, szczególnie w kontekście wdrożenia ogólnego rozporządzenia o ochronie danych osobowych (RODO). W dobie intensywnej cyfryzacji oraz rosnącego znaczenia przetwarzania danych, JST – jako podmioty odpowiedzialne za przetwarzanie dużych ilości danych osobowych obywateli – muszą sprostać coraz większym wymogom prawnym i technologicznym w zakresie ochrony tych danych.

Niniejsze badania statystyczne opierają się na „Sprawozdaniach z działalności Prezesa Urzędu Ochrony Danych Osobowych za lata 2018–2023". Wybór tych sprawozdań jako głównego materiału źródłowego jest w pełni uzasadniony ze względu na ich merytoryczną wartość oraz wiarygodność. Prezentowane w nich dane dotyczące liczby skarg na naruszenia ochrony danych osobowych, zarówno w ujęciu ogólnym, jak i w sektorze publicznym, odzwierciedlają aktualny stan przestrzegania przepisów RODO w Polsce. Opracowania te stanowią oficjalny dokument, który dostarcza rzetelnych i kompleksowych informacji na temat działań podejmowanych przez UODO oraz problemów, z jakimi mierzą się podmioty przetwarzające dane osobowe, w tym jednostki samorządu terytorialnego.

Zebrane dane pozwalają na szczegółową analizę skali problemów związanych z naruszeniami ochrony danych osobowych, umożliwiając jednocześnie ocenę skuteczności wdrożonych procedur oraz identyfikację obszarów, w których JST napotykają największe trudności w przestrzeganiu przepisów RODO. W odniesieniu do niniejszej pracy pozyskane informacje posłużą jako materiał badawczy do przedstawienia skali problemów związanych z naruszeniami danych osobowych w ujęciu całkowitym ze szczególnym uwzględnieniem administracji samorządowej oraz porównaniu ich z sektorem prywatnym, finansowym wraz z ubezpieczeniami i telekomunikacją w latach 2020 – 2023.

Wykres 1. Liczba skarg, które wpłynęły do UODO w latach 2018-2023

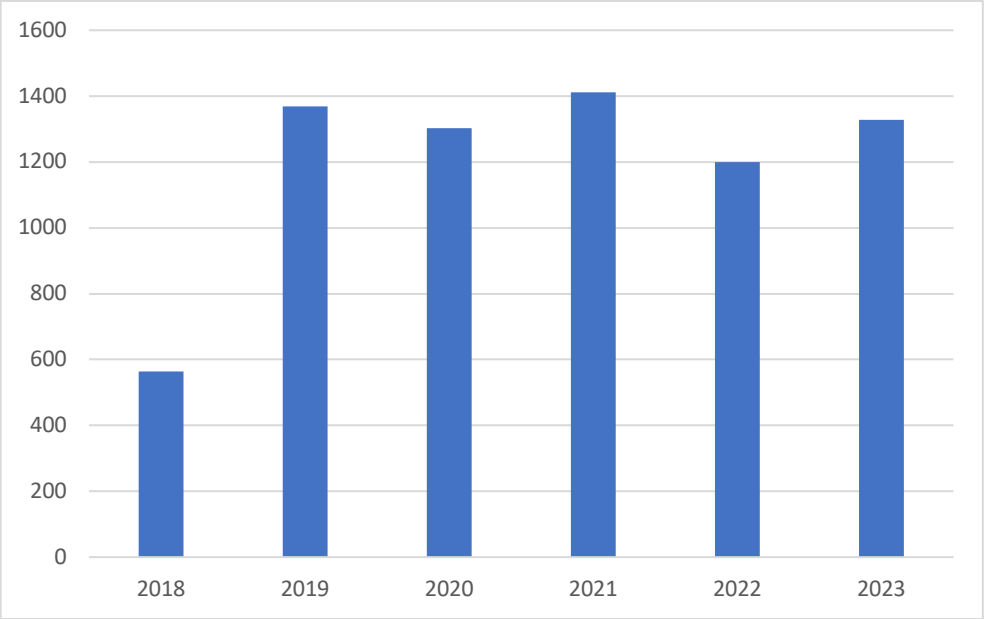


Źródło: Sprawozdania z działalności Prezesa Urzędu Danych Osobowych.[376]

W latach 2018-2023, liczba zgłaszanych naruszeń ochrony danych osobowych była znacząca. Prezes UODO regularnie otrzymywał skargi dotyczące niewłaściwego przetwarzania danych, z czego spora część dotyczyła jednostek samorządu. Analizując te naruszenia, warto zwrócić uwagę na przyczyny, wśród których dominują braki w zabezpieczeniach technicznych oraz niedostateczna świadomość pracowników administracyjnych co do wymogów prawnych ochrony danych. W 2018 roku, w pierwszym roku stosowania RODO, liczba skarg wynosiła - 2 446, natomiast już w 2019 roku liczba ta wzrosła do 9304 skarg. Zwiększona liczba zgłoszeń świadczy o rosnącej świadomości społecznej w zakresie praw związanych z ochroną danych, jak również o wzrastających wyzwaniach, przed którymi stoją zarówno organy administracji, jak i inne podmioty przetwarzające dane. Należy podkreślić, iż w latach 2022 i 2023 liczba skarg ustabilizowała się na poziomie 6479 i 6962.

[376] *Sprawozdanie z działalności Prezesa Urzędu Danych Osobowych w roku 2018,* https://uodo.gov.pl/pl/487/2279 [dostęp: 17.09.2024], *Sprawozdanie z działalności Prezesa Urzędu Danych Osobowych w roku 2019*, https://uodo.gov.pl/pl/487/2279 [dostęp: 17.09.2024], *Sprawozdanie z działalności Prezesa Urzędu Danych Osobowych w roku 2020*, https://uodo.gov.pl/pl/487/2279 [dostęp: 17.09.2024], *Sprawozdanie z działalności Prezesa Urzędu Danych Osobowych w roku 2021*, https://uodo.gov.pl/pl/487/2279 [dostęp: 17.09.2024], *Sprawozdanie z działalności Prezesa Urzędu Danych Osobowych w roku 2022*, https://uodo.gov.pl/pl/487/2279 [dostęp: 17.09.2024], *Sprawozdanie z działalności Prezesa Urzędu Danych Osobowych w roku 2023*, https://uodo.gov.pl/pl/487/2279 [dostęp: 17.09.2024].

Wykres 2. Liczba skarg, które wpłynęły do UODO w obszarze sektora publicznego w latach 2018–2023

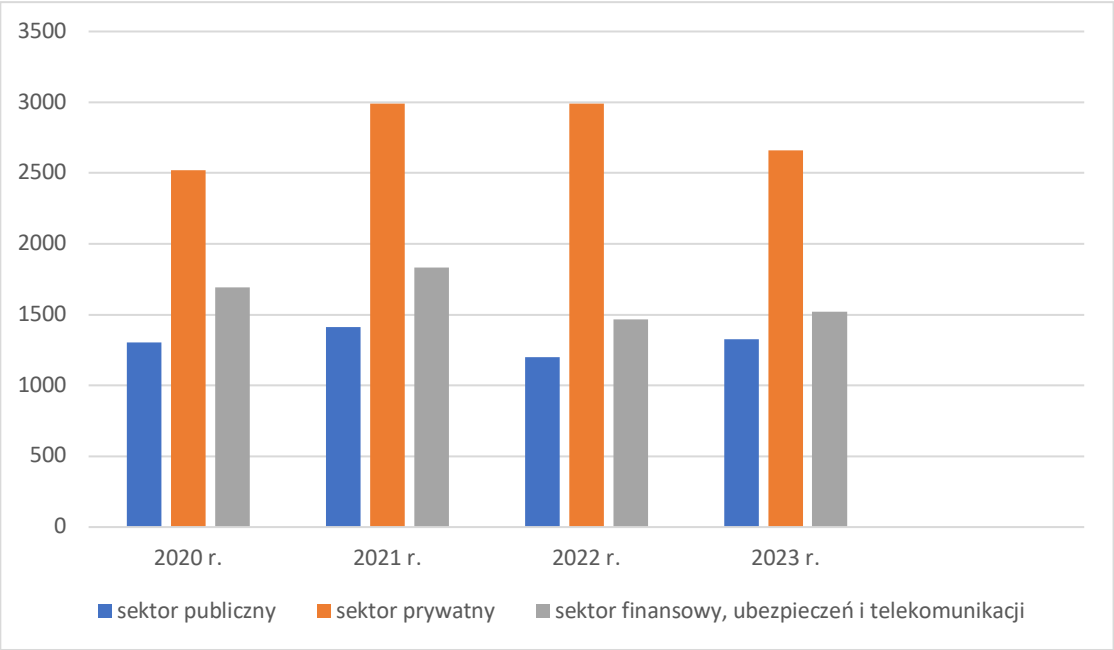


Źródło: Sprawozdania z działalności Prezesa Urzędu Danych Osobowych.[377]

W latach 2018-2023, liczba zgłaszanych naruszeń ochrony danych osobowych przez podmioty sektora publicznego jest proporcjonalnie zbliżona do całościowej liczby skarg wpływających do prezesa UDO. W 2019 roku również, w analizowanym sektorze publicznym, wzrosła ponad dwukrotnie między 2018 a 2019 rokiem (z 564 do 1369), co odzwierciedla budowanie świadomości społecznej w przedmiotowym zakresie. W kolejnych latach liczba skarg wahała się między 1199 a 1412, co pokazuje pewną stabilizację liczby zgłoszeń. Ilość wpływających skarg od 2020 roku sugeruje, że jednostki administracji publicznej wprowadziły odpowiednie procedury zarządzania danymi, choć problematyczne sytuacje wciąż się pojawiają.

[377] Tamże.

Wykres 3. Liczba skarg, które wpłynęły do UODO w obszarze sektora publicznego, prywatnego i finansowego wraz z ubezpieczeniami i telekomunikacją w latach 2020-2023



Źródło: Sprawozdania z działalności Prezesa Urzędu Danych Osobowych.[378]

Ten wykres przedstawia porównanie liczby skarg w trzech różnych sektorach – publicznym, prywatnym oraz finansowym (w tym ubezpieczeń i telekomunikacji) w latach 2020-2023. W sektorze prywatnym odnotowano wyraźny wzrost liczby skarg między 2020 a 2021 rokiem (z 2519 do 2990), co utrzymywało się na stabilnym poziomie w 2022 roku, a następnie nieznacznie spadło w 2023 (2659). Tym czasem sektor finansowy i telekomunikacyjny odnotował pewne spadki, szczególnie w 2022 roku (1466 skarg), jednak w 2023 roku liczba ta wzrosła do 1519. Widoczna jest zatem tendencja, w której liczba skarg na sektor publiczny utrzymuje się na niższym poziomie w porównaniu do sektora prywatnego oraz sektora finansowego. Większa liczba skarg w sektorze prywatnym może wynikać z różnorodności przetwarzanych danych i większej liczby podmiotów przetwarzających dane osobowe. Natomiast wahania w sektorze finansowym są zapewne efektem dynamicznych zmian w przetwarzaniu danych (np. w związku z pandemią COVID-19 i rozwojem zdalnych usług). Warto podkreślić,

[378] Tamże.

że sektor publiczny utrzymuje relatywnie stały poziom liczby skarg, co wskazuje na stabilność procedur, ale nadal wymaga dalszego doskonalenia.

Na podstawie analizy trzech wykresów, można wyciągnąć następujące wnioski:

1) **Wzrost liczby skarg po wdrożeniu RODO** w 2019 roku był spowodowany wzrostem świadomości społeczeństwa oraz koniecznością dostosowania się do nowych regulacji przez różne sektory.
2) **Stabilizacja liczby skarg** w latach 2021-2023 sugeruje, że podmioty przetwarzające dane, zwłaszcza w sektorze publicznym, wdrożyły procedury zarządzania danymi, choć nadal napotykają trudności.
3) **Sektor prywatny** oraz sektor finansowy i telekomunikacyjny wymagają szczególnej uwagi, ze względu na wyższą liczbę zgłaszanych naruszeń w porównaniu do sektora publicznego, co może wynikać z większej złożoności przetwarzania danych oraz większej liczby interakcji z klientami.

Statystyki dotyczące zgłaszanych naruszeń ochrony danych osobowych w latach 2018-2023 wskazują na konieczność dalszego wzmacniania systemu ochrony danych nie tylko w jednostkach samorządu terytorialnego. Liczba skarg zarówno ogółem, jak i w odniesieniu do sektora publicznego, ukazuje, że JST muszą podjąć działania mające na celu lepsze zarządzanie danymi osobowymi oraz wdrożenie bardziej efektywnych środków zapobiegających naruszeniom. Warto podkreślić, że głównymi problemami, jakie pojawiają się w kontekście skarg dotyczących sektora publicznego, obejmują niewłaściwe zarządzanie dostępem do danych osobowych, brak odpowiednich środków technicznych i organizacyjnych oraz nieprawidłowości w przetwarzaniu danych na poziomie lokalnym. Przykłady takich naruszeń można znaleźć w sprawozdaniach Prezesa UODO, gdzie skargi dotyczą m.in. błędów administracyjnych, wycieków danych oraz nieprzestrzegania procedur wynikających z przepisów RODO.

5.2. Analiza wybranych przypadków naruszeń ochrony danych osobowych

Zaniedbania i nieprawidłowości w ochronie danych mogą prowadzić do poważnych konsekwencji, zarówno dla jednostek, jak i dla całości systemu. Przedstawimy zatem kilka przypadków naruszeń ochrony danych w samorządowych

usługach publicznych, aby zrozumieć, jakie są najczęstsze problemy i jak można im zapobiegać.

Naruszenie 1: Kara dla Burmistrza Miasta i Gminy za nieuprawnione kopiowanie danych[379]

Burmistrz Miasta i Gminy został poddany sankcji administracyjnej w postaci grzywny wynoszącej 10 tys. zł. Jak się okazało, ten zarządzający nie stosował adekwatnych mechanizmów, które zapewniłyby adekwatne zabezpieczenie przed naruszeniem ochrony danych osobowych, które nastąpiło w wyniku nieautoryzowanego duplikowania plików zawierających informacje o charakterze osobistym. Poprzez przeprowadzenie audytu ryzyka, mógłby on skutecznie zapobiec temu incydentowi.

Burmistrz zgłosił do Urzędu Ochrony Danych Osobowych incydent naruszenia ochrony danych osobowych, który polegał na nieuprawnionym kopiowaniu danych osobowych przez pracownika z komputera służbowego na niezatwierdzony nośnik. Jak się okazało, ten zarządzający nie stosował się do mechanizmów uniemożliwiających przesyłanie danych na nieupoważniony nośnik.

W ocenie Urzędu, zważywszy na szczególne znaczenie danych osobowych przetwarzanych przez Burmistrza, które zostały skopiowane, oczekiwano od zarządzającego podjęcia działań zapewniających odpowiednie zabezpieczenia.

Implementacja zabezpieczeń adekwatnych do wcześniej zdefiniowanego poziomu ryzyka powinna brać pod uwagę specyfikę organizacji oraz stosowane technologie przetwarzania danych. Zarządzający ma obowiązek samodzielnie przeprowadzić dogłębną analizę procesów przetwarzania danych, ocenić ryzyko, a następnie wdrożyć takie procedury i środki, które będą adekwatne do zidentyfikowanego poziomu ryzyka.

Na podstawie wykonanego przez urząd nadzorujący dochodzenia wynika, że zarządzający nie dokonał oceny ryzyka dla procedury przetwarzania danych, które zostały naruszone. Tymczasem jest to działanie kluczowe do selekcji właściwych środków technicznych i procedur zarządczych.

W sytuacji, gdy zarządzający przewidział możliwość korzystania z przenośnych urządzeń pamięci, właściwa ocena ryzyka mogłaby zidentyfikować potencjalne zagrożenia związane z ich niewłaściwym użyciem, na przykład skopiowaniem przez

[379] https://uodo.gov.pl/decyzje/DKN.5131.44.2022.

pracownika informacji zapisanych na komputerze służbowym na przenośne urządzenie pamięci. Wyniki przeprowadzonej oceny ryzyka pozwoliłyby na zdefiniowanie i wdrożenie odpowiednich technicznych i zarządczych środków zabezpieczających, zapewniających ochronę tych danych.

Uzgadnianie procedur przetwarzania danych osobowych w każdym podmiocie nie powinno mieć charakteru okazjonalnego. Ochrona danych osobowych jest procesem nieustannym i wymaga regularnych aktualizacji, które są zależne od przebiegających procesów. W omawianym przypadku, zarządzający nie kontrolował ani odpowiedniości, ani efektywności zastosowanych zabezpieczeń.

Zarządzający przeprowadził szkolenia związane z ochroną danych osobowych, ale nie mógł potwierdzić, że osoba odpowiedzialna za naruszenie uczestniczyła w tych szkoleniach. Implementacja właściwych środków technicznych i organizacyjnych, a także wprowadzenie działań służących do optymalnego zabezpieczania i konfiguracji wykorzystywanych środków, narzędzi i urządzeń, powinno być regularnie testowane, oceniane i mierzone pod kątem skuteczności zastosowanych rozwiązań.

W rzeczywistości, nieprzeprowadzenie przez zarządzającego oceny ryzyka przed naruszeniem ochrony danych osobowych spowodowało, że nie mógł on potwierdzić, czy przyjęte środki faktycznie zapewniały odpowiednie zabezpieczenie. W rezultacie doszło do nieautoryzowanego użycia przenośnego urządzenia pamięci przez pracownika.

Naruszenie 2: Kara dla Wójta Gminy[380]

Prezes Urzędu Ochrony Danych Osobowych (UODO) wydał decyzję o nałożeniu sankcji finansowej w kwocie 8 tys. zł. na Wójta Gminy. Powód? Niewystarczające zabezpieczenie informacji osobistych i niedopełnienie obowiązku wdrożenia adekwatnych mechanizmów technicznych i proceduralnych.

Administrator danych zgłosił do UODO naruszenie przepisów o ochronie danych osobowych. Naruszenie to wynikało z kradzieży komputera służbowego zawierającego dane osobowe, który nie był wyposażony w odpowiednie środki ochrony, co doprowadziło do naruszenia tajemnicy tych danych. Kradzież miała miejsce poza terenem biura, gdyż laptop był przechowywany w domu przez pracownika, który go używał, a nie w miejscu pracy.

[380] *Decyzja ZSOŚS.440.136.2018*, https://uodo.gov.pl/decyzje/ZSOŚS.440.136.2018 [dostęp: 19.03.2024].

Należy zaznaczyć, że administrator wypracował adekwatne procedury i zasady dotyczące ich bezpieczeństwa oraz dokonał analizy zagrożeń, uwzględniając między innymi ryzyko kradzieży urządzeń informatycznych używanych do obróbki danych.

Administrator był świadomy zagrożeń, które niesie ze sobą utrata urządzeń komputerowych wynoszonych poza teren organizacji. Ocenił to ryzyko jako nie do zaakceptowania i w ramach swojego podejścia do zarządzania ryzykiem, określił środki ochrony, które powinny być wdrożone w celu jego minimalizacji. Jednym z proponowanych środków ochrony mających zniwelować poziom ryzyka było szyfrowanie danych.

Jednakże, jak wykazało śledztwo, skradziony laptop był chroniony przed nieautoryzowanym dostępem tylko za pomocą hasła. Zabezpieczenia, które były ustalone w procedurach, nie zostały zaimplementowane, przynajmniej w odniesieniu do tego komputera.

Dane osobowe powinny być przetwarzane w sposób gwarantujący ich właściwe zabezpieczenie, co obejmuje ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, jak również przypadkową utratą, zniszczeniem czy uszkodzeniem, przez zastosowanie adekwatnych środków technicznych lub organizacyjnych („poufność i integralność”).

RODO szczegółowo określa zasadę poufności, nakładając na administratora obowiązek wdrożenia stosownych środków technicznych i organizacyjnych. Z uwzględnieniem charakteru, zakresu, kontekstu oraz celów przetwarzania, a także ryzyka naruszenia praw lub wolności osób fizycznych o zróżnicowanym stopniu prawdopodobieństwa i wadze, administrator zobowiązany jest do wdrożenia takich środków, które umożliwią przetwarzanie danych zgodne z tym rozporządzeniem, a także umożliwią udowodnienie tej zgodności. Środki te powinny być regularnie aktualizowane i przeglądane.

Aby zminimalizować potencjalne konsekwencje naruszeń i zapobiec utracie poufności danych, administrator może zastosować dodatkowe mechanizmy ochronne, takie jak na przykład szyfrowanie dysków twardych komputerów. Określenie tych zabezpieczeń powinno wynikać z przeprowadzonej analizy ryzyka, po właściwej identyfikacji zagrożeń dla danych osobowych przetwarzanych przy użyciu laptopów wykorzystywanych poza siedzibą organizacji administratora.

W kwestii incydentu, osoba odpowiedzialna za przetwarzanie danych prowadziła adekwatną dokumentację od momentu wprowadzenia RODO, przeprowadzając również

analizę ryzyka. Można stwierdzić, że była ona świadoma konieczności wdrożenia stosownych środków technicznych i organizacyjnych, które zapewniają bezpieczeństwo przetwarzanych danych osobowych na urządzeniach przenośnych.

Niemniej jednak, dopiero po wystąpieniu naruszenia, podjęto działania zmierzające do uniknięcia podobnych sytuacji w przyszłości, poprzez szyfrowanie dysków twardych laptopów. Zatem, dopiero po incydencie, administrator dostosował się do wniosków z własnej analizy ryzyka oraz określonych w niej metod zarządzania ryzykiem.

Administrator zaniedbał pewne obowiązki, co skutkowało naruszeniem zasady poufności danych, w rezultacie nieumyślnie łamiąc przepisy o ochronie danych osobowych. Przy decydowaniu o nałożeniu sankcji finansowej uwzględniono fakt odnalezienia skradzionego komputera, oraz fakt, że przeprowadzona przez administratora analiza wykazała, iż system operacyjny laptopa nie był uruchamiany od momentu kradzieży.

W konsekwencji, mimo że administrator stracił kontrolę nad danymi osobowymi, a niepowołana osoba zyskała nielegalny dostęp, nie było podstaw do twierdzenia, że osoby, których dane dotyczą, doznały jakiejkolwiek szkody w wyniku tego naruszenia, na dzień wydania omawianej decyzji administracyjnej.

Naruszenie 3: Kara dla Ośrodka Kultury[381]

Urząd Ochrony Danych Osobowych wymierzył Centrum Kultury grzywnę administracyjną wynoszącą 2,5 tys. zł. Źródłem tego postanowienia była sytuacja, w której przekazano dane osobowe do przetwarzania, nie posiadając umowy pisemnej na ten cel oraz nie przeprowadzając kontroli która miała wykazać, czy strona przetwarzająca zapewnia odpowiednie zabezpieczenia technologiczne.

Do UODO wpłynęło zgłoszenie o potencjalnym naruszeniu ochrony danych osobowych w Centrum Kultury. W trakcie dochodzenia ustalono, że instytucja ta przekazała dane osobowe do przetwarzania bez formalnej umowy powierzenia na ten cel stronie przetwarzającej, której powierzono zadania związane z prowadzeniem księgowości, ewidencji oraz sporządzaniem raportów (w obszarach finansów, podatków oraz ubezpieczeń społecznych) lub przechowywaniem dokumentów.

[381] *DKN.5131.29.2022*, https://uodo.gov.pl/pl/314/2617 [dostęp: 31.7.2024].

Dodatkowo, instytucja nie podjęła kroków w celu weryfikacji strony przetwarzającej dane, nie sprawdzając, czy ta ostatnia daje wystarczające zabezpieczenia na poziomie technicznym i organizacyjnym, umożliwiające zgodne z RODO przetwarzanie danych osobowych.

Gdy administrator podejmuje decyzję o przekazaniu ich do przetwarzania innemu podmiotowi, winien on zatroszczyć się o to, czy ten drugi podmiot zapewnia adekwatne zabezpieczenia technologiczne i organizacyjne oraz czy przetwarzanie danych będzie zgodne z wymogami RODO i zapewni ochronę prawa jednostek, których te dane dotyczą.

Zaniedbanie obowiązku sprawdzenia podmiotu przetwarzającego oraz jego gwarancji dotyczących zgodnego z regulacjami ochrony danych osobowych przetwarzania może prowadzić do konsekwencji dla jednostek, których dane osobowe zostały powierzone na przetwarzanie, na przykład w formie utraty tych danych. Dlatego też decyzja, komu zarządzający danymi powinien przekazać je do przetwarzania, nie może być podjęta bez odpowiednich podstaw. Tylko po sprawdzeniu kwalifikacji i adekwatności wybranego podmiotu przetwarzającego, zarządzający danymi może rozpocząć proces zawarcia odpowiedniej umowy powierzenia.

W trakcie dochodzenia organ nadzorczy ustalił, że administrator nie posiadał żadnych dokumentów, które by potwierdzały weryfikację warunków współpracy z podmiotem przetwarzającym. Dodatkowo, próba skontaktowania się z tym podmiotem w celu uzyskania informacji, wyjaśnień oraz zwrotu lub udostępnienia przetwarzanych danych okazała się nieskuteczna.

Zgodnie z art. 28 RODO, administrator, kiedy decyduje się na przetwarzanie danych przez inny podmiot, korzysta tylko z usług tych podmiotów, które oferują wystarczające zabezpieczenia dotyczące wprowadzenia odpowiednich środków technicznych i organizacyjnych.

Samo przetwarzanie danych przez podmiot przetwarzający następuje na mocy umowy pisemnej zawartej między zarządzającym danymi a podmiotem przetwarzającym. Taka umowa precyzuje między innymi temat i czas przetwarzania, naturę i cel przetwarzania, typ danych osobowych oraz kategorie osób, których dane są przetwarzane, a także obowiązki i prawa zarządzającego danymi.

Zgodnie z RODO, dane osobowe muszą być przetwarzane zgodnie z prawem, uczciwie i transparentnie dla jednostki, której dane te dotyczą. Obowiązek zapewnienia bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub nielegalnym przetwarzaniem, a także przypadkową utratą, zniszczeniem

lub uszkodzeniem za pomocą odpowiednich środków technicznych czy organizacyjnych („integralność i poufność"), spoczywa na administratorze, czyli na podmiocie, który decyduje o metodach i celach przetwarzania.

W przypadku Centrum Kultury, jako że było ono zarządzającym przetwarzanymi przez siebie danymi osobowymi, to na nim spoczywał obowiązek wyboru odpowiedniego podmiotu przetwarzającego.

Biorąc pod uwagę wszystkie okoliczności, organ nadzorczy stwierdził, że nałożenie na zarządzającego danymi kary pieniężnej jest niezbędne i usprawiedliwione przez wagę oraz charakter i zakres zarzucanych temu podmiotowi naruszeń. Kara w określonej wysokości będzie skuteczna i sprawi, że zarządzający danymi, aby uniknąć dalszych sankcji, zwróci odpowiednią uwagę na przetwarzanie danych osobowych za pośrednictwem i przy współpracy z podmiotem przetwarzającym.

Naruszenie 4: Kara dla Burmistrza[382]

W 2019 roku sankcje finansowe w wysokości 40 tys. zł zostały nałożone na burmistrza za naruszenie zasad RODO, wynikające z niewłaściwego zarządzania danymi osobowymi.

Urząd Ochrony Danych Osobowych stwierdził, że brakowało odpowiednich umów z podmiotami, którym dane zostały przekazane. To zaniedbanie dotyczyło m.in. firmy zarządzającej serwerami przechowującymi informacje z Biuletynu Informacji Publicznej oraz firmy dostarczającej i obsługującej oprogramowanie dla tej platformy informacyjnej. Prezes UODO wskazał, iż w konsekwencji braku takiej umowy burmistrz dopuścił się udostępnienia danych osobowych bez podstawy prawnej, czym naruszył określone w RODO: zasadę przetwarzania danych zgodnie z prawem (art. 5 ust. 1 lit. a) oraz zasadę poufności (art. 5 ust. 1 lit. f).

UODO stwierdziło, że w Urzędzie Miejskim nie zastosowano właściwych procedur wewnętrznych dotyczących przeglądu i określenia terminu publikacji zasobów w Biuletynie Informacji Publicznej (BIP). To oznaczało, że w BIP nadal widoczne były deklaracje majątkowe urzędników z 2010 roku, choć powinny być przechowywane tylko przez sześć lat. Urząd również nieodpowiednio zarządzał nagraniami z posiedzeń rady miejskiej, umieszczając jedynie link do oficjalnego kanału YouTube w Biuletynie Informacji Publicznej, nie posiadając innej wersji tych nagrań. Analiza ryzyka związana

[382] *Decyzja ZSPU.421.3.2019*, https://uodo.gov.pl/decyzje/ZSPU.421.3.2019 [dostęp: 31.7.2024].

z publikowaniem nagrań wyłącznie na YouTube nie została przeprowadzona, co prowadzi do naruszenia zasad integralności, poufności i rozliczalności. Zasada rozliczalności została naruszona również w związku z brakami w rejestrze czynności przetwarzania. Nie było w nim np. wskazanych wszystkich odbiorców danych, a także brakowało wskazania planowanego terminu usunięcia danych dla niektórych czynności przetwarzania.

Być może Prezes UODO wykazałby bardziej wyrozumiałe podejście do tych naruszeń, gdyby nie fakt, że administrator danych, czyli Urząd Miejski nie wykazał chęci do współpracy z UODO. Pracownicy tej instytucji nie usunęli stwierdzonych nieprawidłowości, które były stopniowo wykrywane podczas kontroli, ani nie zadbali o wprowadzenie rozwiązań mających na celu zapobieganie podobnym naruszeniom w przyszłości. Można by stwierdzić, że administrator danych stał na stanowisku nieustępliwym.

Naruszenie 5: Kara dla Szkoły Podstawowej[383]

Prezes Urzędu Ochrony Danych Osobowych nałożył karę w kwocie 20 tysięcy złotych na instytucję edukacyjną. Kara została wydana za naruszenie regulacji RODO. Stołówka szkolna zainstalowała system biometryczny dla uczniów, który polegał na gromadzeniu odcisków palców. Zezwolenie od rodziców okazało się nieadekwatne.

W konsekwencji na Szkołę Podstawową została nałożona sankcja finansowa w wysokości 20 tys. zł za naruszanie ochrony danych biometrycznych[384] uczniów korzystających z usług stołówki szkolnej. Instytucja używała skanera biometrycznego do identyfikacji uczniów i sprawdzenia, czy opłata za posiłek została pokryta.

Wyniki kontroli wykazały, że gromadzenie i przetwarzanie danych biometrycznych odbywało się za pisemną zgodą opiekunów i dotyczyło 680 dzieci. Według Prezesa UODO, zgoda rodzica nie może służyć jako podstawa do legalizacji przetwarzania danych biometrycznych, zgodnie z art. 9 ust. 1 RODO.

Jak zauważył Prezes UODO, ze względu na unikalny i niezmienny charakter danych biometrycznych, które nie zmieniają się z upływem czasu, stosowanie danych

[383] *Decyzja ZSZZS.440.768.2018*, https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018 [dostęp: 31.7.2024].
[384] Dane biometryczne czyli dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne [Zob. *Dane biometryczne*, https://gdpr.pl/artykuly/dane-biometryczne [dostęp: 04.10.2023].

biometrycznych powinno następować z dużą ostrożnością i rozwagą[385]. W związku z tym, zdaniem Prezesa UODO, placówka mogła zastosować inne metody identyfikacji uczniów, które według urzędu nie naruszają prywatności dziecka w tak dużym stopniu, zwłaszcza że stołówka oferuje możliwość korzystania z jej usług za pomocą karty elektronicznej lub na podstawie nazwiska. Jak zauważył Prezes w swojej decyzji, „przetwarzanie danych biometrycznych nie jest konieczne do osiągnięcia celu, jakim jest potwierdzenie uprawnień dziecka do odebrania obiadu"[386].

Prezes UODO zwróciło również uwagę na nieprawidłowości w kolejności wprowadzania dzieci do stołówki. Na początku, dzieci z identyfikacją biometryczną miały pierwszeństwo, podczas gdy uczniowie korzystający z innych form potwierdzenia płatności czekali na końcu kolejki i byli dopuszczani do korzystania z usług dopiero na samym końcu. Według Prezesa, taka polityka wydawania posiłków w szkole prowadzi do nierównego traktowania uczniów i nieuzasadnionego ich różnicowania, ponieważ faworyzuje uczniów z identyfikacją biometryczną[387].

Dodatkowo, oprócz obowiązku zapłacenia sankcji pieniężnej, Prezes UODO nakazał placówce usunięcie przetworzonych danych osobowych przekształconych w postać cyfrowych informacji (specyficzne punkty linii papilarnych palców uczniów) oraz zaniechanie dalszego gromadzenia takich danych.

5.3. Wnioski z analizowanych naruszeń

Wnioski z naruszenia 1: Kara dla Burmistrza Miasta i Gminy za nieuprawnione kopiowanie danych

W opisanym przypadku, naruszenie ochrony danych osobowych zostało zgłoszone do Urzędu Ochrony Danych Osobowych przez Burmistrza. Wygląda na to, że pracownik skopiował dane osobowe z komputera służbowego na niezatwierdzony nośnik. Nie istniały też mechanizmy zapobiegające takim działaniom. Analizując to zgłoszenie, można wysunąć następujące wnioski:

- Zdarzenie pokazuje, że nie istniały odpowiednie środki kontroli dostępu do danych. Pracownik mógł łatwo skopiować dane osobowe bez jakichkolwiek przeszkód.

[385] https://uodo.gov.pl/decyzje/ZSZZS.440.768.2018.
[386] Ibidem.
[387] Ibidem.

Instytucje powinny wdrożyć solidne mechanizmy kontroli dostępu, takie jak autoryzacja, uwierzytelnianie i zarządzanie uprawnieniami;

- Incydent mógł wynikać z niedostatecznej świadomości pracowników na temat polityki ochrony danych i konsekwencji naruszania tych zasad. Z tego względu szkolenia z zakresu bezpieczeństwa i ochrony danych powinny być regularnie przeprowadzane;
- Wystąpił brak mechanizmów zapobiegających kopiowaniu danych na nieupoważniony nośnik pokazuje, że organizacja nie miała na miejscu odpowiednich technicznych zabezpieczeń. Tymczasem rozwiązania techniczne, takie jak blokowanie portów USB lub monitorowanie aktywności sieciowej, mogłyby pomóc zapobiegać takim incydentom;
- Sytuacja pokazuje, że instytucja nie zarządzała odpowiednio swoim ryzykiem w zakresie bezpieczeństwa danych. Należało przeprowadzić szczegółową analizę ryzyka, a następnie powinny zostać wdrożone odpowiednie środki zaradcze;
- Regularne audyty bezpieczeństwa mogą pomóc organizacji w wykrywaniu luk w zabezpieczeniach i poprawie procesów ochrony danych;
- Zaniedbania do jakich dopuszczono się w opisywanym przypadku stanowią naruszenie Rozporządzenia Ogólnego o Ochronie Danych (RODO), które wymaga od organizacji zapewnienia odpowiedniej ochrony danych osobowych. Instytucja może być narażona na poważne sankcje finansowe.

Aby zapobiec podobnym incydentom w przyszłości, organizacja powinna podjąć natychmiastowe działania w celu usunięcia istniejących luk w zabezpieczeniach i zapewnienia lepszej ochrony danych osobowych.

Wnioski z naruszenia 2: Kara dla Wójta Gminy

Z opisanego naruszenia można wysunąć następujące wnioski i zalecenia:

- Naruszenie okazało się możliwe, ponieważ komputer służbowy nie był wyposażony w odpowiednie środki ochrony danych, takie jak szyfrowanie. Szyfrowanie danych to kluczowe zabezpieczenie, które może chronić dane nawet w przypadku utraty lub kradzieży urządzenia. Bez tego, każdy kto ma dostęp do urządzenia, może potencjalnie uzyskać dostęp do zawartych na nim danych;
- Pracownik przechowywał komputer służbowy, zawierający dane osobowe, poza terenem biura. Zapobieganie podobnym incydentom wymaga wprowadzenia

szczegółowych zasad dotyczących przechowywania i zabezpieczania urządzeń poza miejscem pracy;

- Wydaje się, że przyczyna analizowanego problemu tkwiła również w braku odpowiedniego systemu monitoringu lub śledzenia urządzeń, co mogłoby pomóc w zlokalizowaniu skradzionego komputera;
- Incydent stanowi naruszenie RODO, które wymaga od administratora danych osobowych zapewnienia odpowiednich środków technicznych i organizacyjnych w celu ochrony tych danych. Administrator danych który tego nie robi naraża się na poważne sankcje finansowe;
- Zapobieganie podobnym naruszeniom wymaga przeprowadzania regularnych audytów bezpieczeństwa, które pomagają organizacjom w wykrywaniu luk w zabezpieczeniach i poprawie procesów ochrony danych;
- Odpowiednie szkolenia z bezpieczeństwa mogą pomóc pracownikom zrozumieć i przestrzegać zasad bezpieczeństwa, zwłaszcza w przypadku pracy zdalnej, gdzie istnieje większe ryzyko kradzieży urządzeń.

Aby zapobiec podobnym incydentom w przyszłości, organizacja powinna także podjąć działania mające na celu zabezpieczenia swoich urządzeń i danych, w tym szyfrowania danych, wprowadzenia zasad bezpieczeństwa dotyczących przechowywania urządzeń poza miejscem pracy, a także regularnych audytów i szkoleń z zakresu bezpieczeństwa dla pracowników.

Wnioski z naruszenia 3: Kara dla Ośrodka Kultury

Analizując zgłoszone naruszenie, możemy wyciągnąć następujące wnioski i zalecenia:

- W Ośrodku Kultury wystąpił problem braku formalnej umowy powierzenia danych: przekazanie danych osobowych do przetwarzania bez formalnej umowy powierzenia jest poważnym naruszeniem przepisów o ochronie danych osobowych, w szczególności RODO. Każda organizacja, która przekazuje dane osobowe do przetwarzania, powinna zawrzeć formalną umowę powierzenia z podmiotem przetwarzającym, która definiuje warunki przetwarzania i zabezpiecza prawa osób, których dane dotyczą;
- Analizowany incydent pokazuje, że Centrum Kultury nie miało wystarczającej kontroli nad podmiotami przetwarzającymi dane. W związku z tym, w ramach

tej instytucji powinny zostać wprowadzone procedury, które zapewnią odpowiednią kontrolę nad tymi podmiotami, w tym regularne audyty i ocena zgodności z przepisami;

- Opisane naruszenie wskazuje na brak zrozumienia lub niedostateczne stosowanie przepisów RODO przez instytucję kulturalną. Organizacje, która z racji prowadzonej działalności muszą przetwarzać dane osobowe powinny zapewnić odpowiednie szkolenia dla pracowników i zlecać audyt zgodności z RODO, aby uniknąć podobnych naruszeń w przyszłości;
- analizowany problem wskazuje także na konieczność zastosowania środków naprawczych: Centrum Kultury powinno podjąć natychmiastowe kroki, w tym zawarcie formalnej umowy powierzenia z podmiotem przetwarzającym dane oraz przeprowadzenie audytu bezpieczeństwa i zgodności z RODO;
- podobnego rodzaju naruszenia mogą narażać placówkę na sankcje finansowe nakładane przez UODO, a także do utraty zaufania ze strony osób, których dane dotyczą.

W celu zapobieżenia podobnym naruszeniom w przyszłości, instytucje powinny zawsze zawierać formalne umowy powierzenia z podmiotami przetwarzającymi dane osobowe, a także regularnie przeprowadzać audyty zgodności z RODO. Ponadto, niezbędne jest przeprowadzenie regularnych szkoleń z ochrony danych dla wszystkich pracowników.

Wnioski z naruszenia 4: Kara dla Burmistrza

Wniosek opisu naruszenia zasad RODO przez Burmistrza należy podsumować w kilku punktach:

- Brak odpowiednich umów: UODO zauważył, że Burmistrz nie zawarł odpowiednich umów z podmiotami, którym dane zostały przekazane. Bez takich umów Burmistrz udostępniał dane osobowe bez podstawy prawnej. Ta sytuacja narusza zasadę przetwarzania danych zgodnie z prawem i zasadę poufności, co jest wymagane przez RODO;
- Nieodpowiednie procedury wewnętrzne: Urząd Miejski nie zastosował właściwych procedur dotyczących przeglądu i określenia terminu publikacji zasobów w Biuletynie Informacji Publicznej (BIP). To oznaczało, że stary, nieaktualny materiał nadal był dostępny dla publiczności;

- Niewłaściwe zarządzanie danymi: Urząd nie zarządzał odpowiednio nagraniami z posiedzeń rady miejskiej. Nie było również odpowiedniej analizy ryzyka związanego z publikacją tych nagrań wyłącznie na YouTube, co narusza zasady integralności, poufności i rozliczalności;
- Naruszenie zasady rozliczalności: Rejestr czynności przetwarzania Urzędu Miejskiego był niekompletny. Brakowało informacji o wszystkich odbiorcach danych, a także o planowanym terminie usunięcia danych dla niektórych czynności przetwarzania;
- Brak współpracy: Administrator danych, czyli Urząd Miejski, nie wykazał chęci do współpracy z UODO. Nie podjął również działań w celu usunięcia stwierdzonych nieprawidłowości ani nie wprowadził rozwiązań mających na celu zapobieganie podobnym naruszeniom w przyszłości.

Na podstawie tych wniosków, jasne jest, że Urząd Miejski nie spełnia wymagań RODO w zakresie zarządzania danymi osobowymi. W konsekwencji, UODO nałożył na burmistrza sankcje finansowe w wysokości 40 tys. zł. Wszystkie podmioty przetwarzające dane osobowe muszą przestrzegać wymogów RODO, aby uniknąć podobnych sankcji.

Wnioski z naruszenia 5: Kara dla Szkoły Podstawowej

Analiza naruszeń ochrony danych biometrycznych w Szkole Podstawowej wykazała, że:

- Uzyskanie przez szkołę pisemnej zgody rodziców na przetwarzanie danych biometrycznych ich dzieci nie stanowiło wystarczającej podstawy prawnej. Zgodnie z art. 9 ust. 1 RODO, dane biometryczne stanowią kategorię szczególnie chronionych danych osobowych, a ich przetwarzanie do celów identyfikacji osoby fizycznej jest zasadniczo zabronione, chyba że spełnione są ściśle określone warunki. Prezes UODO wyjaśnił, że zgoda rodzica nie może stanowić podstawę do legalizacji przetwarzania danych biometrycznych;
- Przetwarzanie danych biometrycznych nie było konieczne do realizacji celu, jakim było potwierdzenie uprawnień dziecka do odebrania posiłku. Zamiast tego, mogły zostać wykorzystane mniej inwazyjne metody, takie jak identyfikacja za pomocą kart elektronicznych lub na podstawie nazwiska. Fakt ten podkreśla znaczenie stosowania najmniej inwazyjnej metody przetwarzania danych, która wystarczy do osiągnięcia zamierzonego celu;

- Szkoła złamała zasadę równego traktowania, faworyzując uczniów z identyfikacją biometryczną, co prowadziło do dyskryminacji części uczniów. Z tego względu wszelkie systemy identyfikacji i autoryzacji powinny być zaprojektowane i wdrożone w taki sposób, aby zapewnić równość i sprawiedliwość;
- Szkoła została wezwana do usunięcia wszelkich przetworzonych danych biometrycznych i zaprzestania ich dalszego gromadzenia. To podkreśla wagę zasady minimalizacji danych w RODO, która zobowiązuje do zbierania i przetwarzania tylko tych danych, które są bezpośrednio niezbędne do realizacji konkretnego celu.

Wnioski te podkreślają, jak ważne jest zrozumienie i przestrzeganie przepisów dotyczących ochrony danych osobowych, zwłaszcza w przypadku informacji szczególnie chronionych, takich jak dane biometryczne.

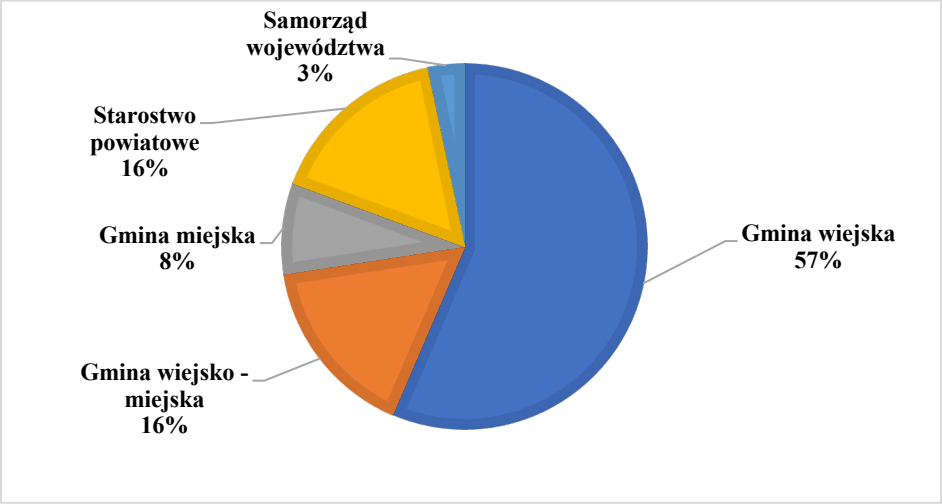
5.4. Analiza procesu implementacji przepisów o ochronie danych osobowych

W kontekście rosnącej digitalizacji i dynamicznego rozwoju technologii informacyjno-komunikacyjnych, ochrona danych osobowych stała się nieodzownym elementem działalności wszelkich instytucji, w tym jednostek samorządu terytorialnego. Przepisy o ochronie danych osobowych są zaprojektowane nie tylko z myślą o ochronie prywatności obywateli, ale także w celu zapewnienia transparentnego, bezpiecznego i zgodnego z prawem przetwarzania tych danych. Dla jednostek samorządu terytorialnego, które często są bezpośrednim łącznikiem między obywatelami a państwem, skuteczna implementacja tych przepisów jest kluczowa. Dotyczy to nie tylko zarządzania danymi mieszkańców, ale również danych pracowników oraz innych osób, z którymi jednostki te wchodzą w interakcje.

Metodologia stosowana w ramach badań dotyczących implementacji przepisów o ochronie danych osobowych w jednostkach samorządu terytorialnego w Polsce miała na celu zapewnienie wiarygodności i reprezentatywności wyników. W tym celu zastosowano celowy dobór próby, który umożliwił skupienie się na jednostkach, które są kluczowe z punktu widzenia celów i problematyki badawczej.

Próba badawcza obejmowała 57 jednostek samorządu terytorialnego, w tym 2 jednostki poziomu województwa, 5 powiatów oraz 50 gmin, w tym gminy miejskie, miejsko-wiejskie i miejskie (wykaz jednostek załączono w aneksie do niniejszej pracy). Taka próba pozwoliła uzyskać szeroki przekrój perspektyw oraz zrozumienie różnorodności praktyk w różnych typach jednostek samorządu terytorialnego.

Wykres 4. Rodzaj badanych jednostek



Źródło: opracowanie własne.

Przeważającą większość badanych jednostek stanowią gminy wiejskie, które reprezentują 57% wszystkich badanych podmiotów, ze względu na to, że tego rodzaju jednostek jest najwięcej i gminy te mają elementarne znaczenie.

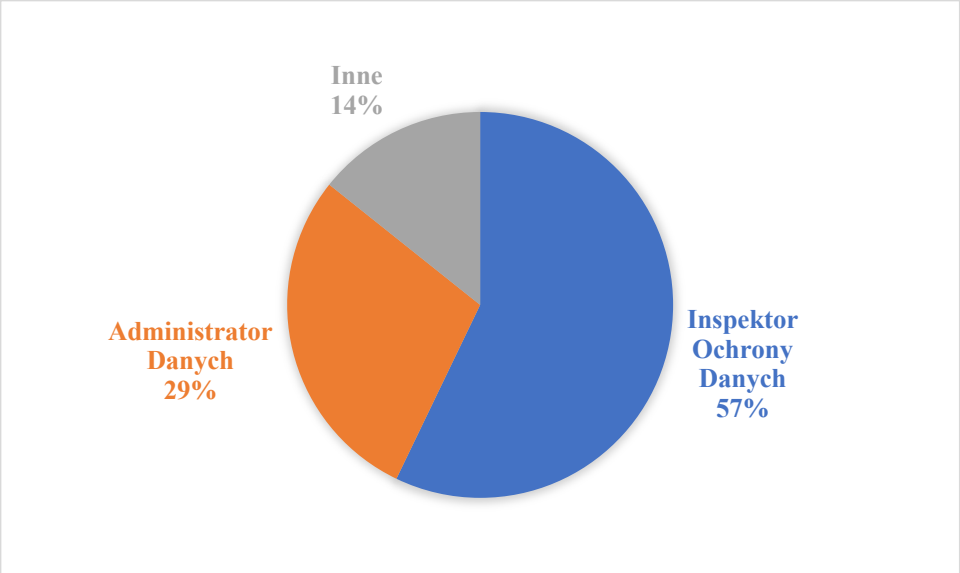
Gminy wiejsko-miejskie i starostwa powiatowe są reprezentowane równomiernie, każda z tych kategorii stanowi 16% badanych jednostek. Ukazuje to zrównoważone podejście do badań obejmujących jednostki mieszane, które łączą cechy zarówno miejskie, jak i wiejskie, a także jednostki zarządzające szerszymi obszarami powiatowymi.

Gminy miejskie, które mogą być uważane za miejsca o wyższym stopniu urbanizacji i potencjalnie większych zasobach, stanowią 8% badanych jednostek.

Samorządy województwa, będące najwyższym poziomem samorządu terytorialnego, stanowią jedynie 3% badanych jednostek.

Należy zauważyć, że badanie skupia się głównie na gminach wiejskich, których jest najwięcej w Polsce. Zróżnicowanie typów jednostek daje możliwość porównania i zrozumienia, jak różne formy organizacji samorządowej radzą sobie z wymogami ochrony danych osobowych.

Wykres 5. Zajmowane stanowisko w badanej jednostce

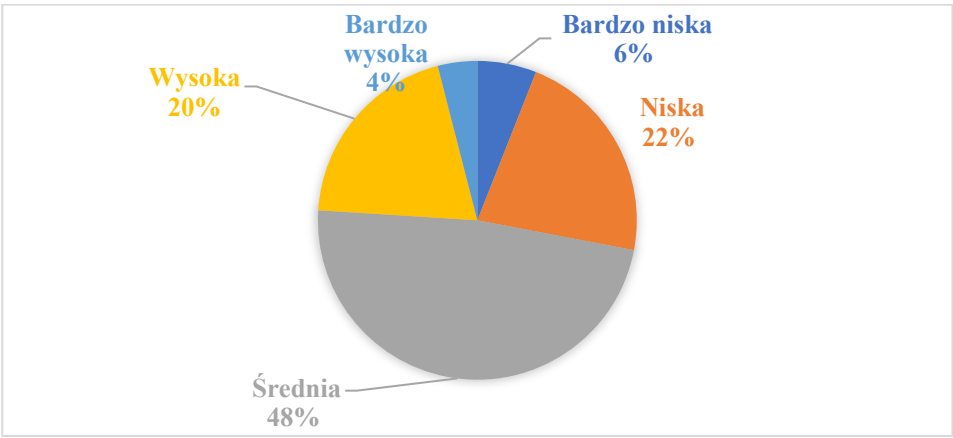


Źródło: opracowanie własne.

Większość respondentów, czyli 57%, to Inspektorzy Ochrony Danych, którzy odgrywają kluczową rolę w procesach ochrony danych w tych organizacjach. Na drugim miejscu znajdują się Administratorzy Danych, stanowiący 29% badanej grupy. Pozostałe 14% respondentów to osoby zajmujące inne stanowiska, które obejmują różne role związane z przetwarzaniem i ochroną danych osobowych, lecz nie są one bezpośrednio określone jako Inspektorzy czy Administratorzy Danych.

Ten rozkład pozwoli na zróżnicowane zaangażowanie pracowników różnych szczebli w procesy ochrony danych i wskazuje na istnienie dedykowanych ról w tej dziedzinie.

Wykres 6. Poziom świadomości przepisów RODO przed szkoleniem

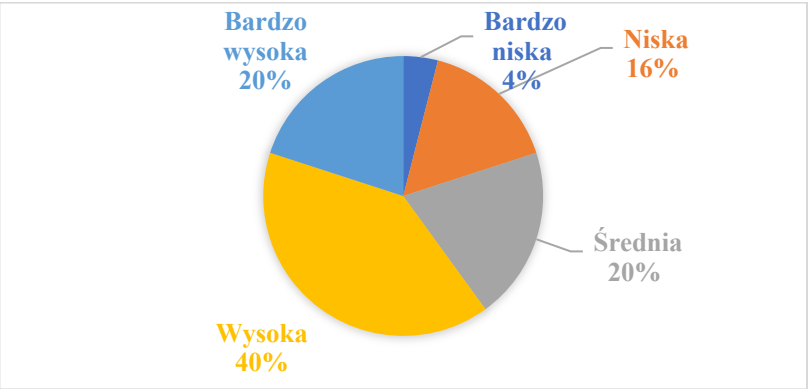


Źródło: opracowanie własne.

Badane osoby zostały zapytane o poziom świadomości RODO. Z przeprowadzonych badań wynika, że poziom świadomości RODO przed przeprowadzonymi szkoleniami w 48% oceniano jako średni. To wskazuje, że prawie połowa badanych miała podstawową znajomość RODO, ale nie czuła się w pełni pewnie w tym zakresie. Natomiast 22% respondentów oceniło swoją świadomość jako niską, co sugeruje, że ponad jedna piąta badanych dostrzegała luki w swojej wiedzy. Kolejne 20% badanych uznało, że ma wysoką świadomość przepisów, co wskazuje na dobrą znajomość RODO i komfort w jego zastosowaniu. Niewielki odsetek, 4%, ocenił swoją wiedzę jako bardzo wysoką, co sugeruje, że tylko nieliczni mieli poczucie bardzo głębokiej znajomości tematu. Grupa oceniająca swoją świadomość jako bardzo niską stanowiła 6%, co wskazuje na niewielką liczbę osób bardzo niepewnych swoich kompetencji dotyczących RODO przed szkoleniem.

Natomiast poziom świadomości RODO po przeprowadzonym szkoleniu znacząco wzrósł, tj. 40% respondentów oceniło swój poziom świadomości jako wysoki, co jest znaczącym wzrostem i świadczy o efektywności szkoleń w zwiększaniu kompetencji w zakresie RODO. 20% respondentów uznało, że ma bardzo wysoką wiedzę po odbytym szkoleniu, co pokazuje, że szkolenia przyczyniły się do znacznego podniesienia poziomu ekspertyzy wśród części uczestników. Średnia świadomość przepisów RODO została zgłoszona przez 20% badanych, co oznacza spadek w porównaniu do oceny przed szkoleniem. Odsetek osób, które oceniły swój poziom wiedzy jako niski zmniejszył się do 16%, co wskazuje na pozytywny wpływ szkolenia. Tylko 4% badanych nadal ocenia swoją świadomość jako bardzo niską, co może wskazywać na trudności niektórych osób w pełnym przyswojeniu materiału szkoleniowego.

Wykres 7. Poziom świadomości przepisów RODO po szkoleniu



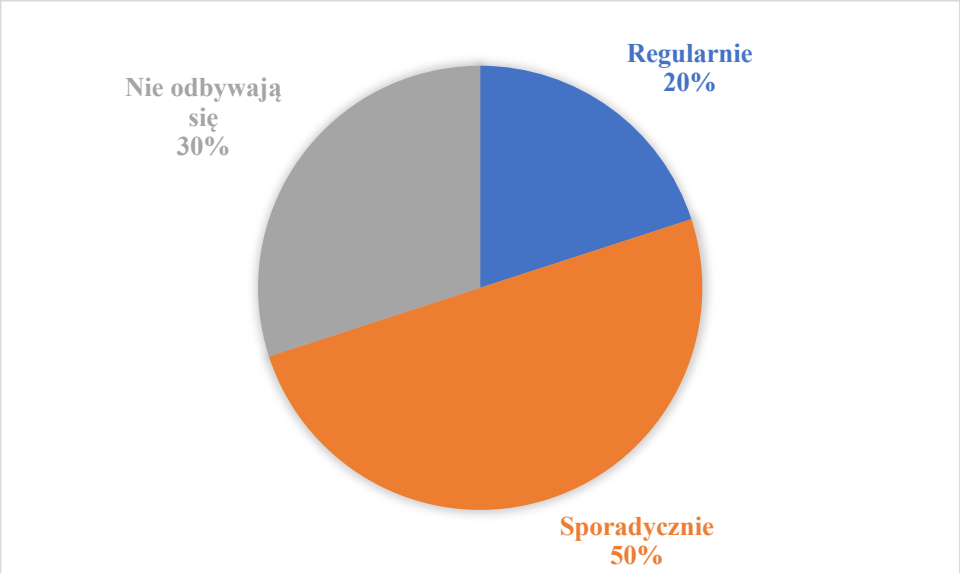
Źródło: opracowanie własne.

Podsumowując przeprowadzone badania dotyczące poziomu świadomości przepisów RODO przed i po szkoleniach, zauważamy znaczącą zmianę w poziomie wiedzy wśród respondentów.

Kolejnym badanym elementem jest częstotliwość odbywania się szkoleń z zakresu RODO. Z przeprowadzonych badań wynika, że 50% ankietowanych stwierdziło, że szkolenia z zakresu ochrony danych osobowych odbywają się sporadycznie, co sugeruje, że szkolenia nie są regularną praktyką, ale zdarzają się od czasu do czasu. Tylko 20% badanych zasygnalizowało, że szkolenia odbywają się regularnie, co wskazuje na mniejszą część jednostek mających wprowadzone stałe procedury aktualizacji wiedzy o RODO. Natomiast 30% respondentów wskazało, że szkolenia nie odbywają się wcale, co jest sygnałem, że znaczna część badanych jednostek nie przeprowadza regularnych aktualizacji wiedzy z tego zakresu, co może wskazywać na potencjalne ryzyko niezgodności z obowiązującymi przepisami o ochronie danych osobowych.

Rezultaty te wskazują na potrzebę większego nacisku na regularne szkolenia i aktualizacje wiedzy o RODO w jednostkach samorządu terytorialnego, aby zapewnić zgodność z dynamicznie zmieniającym się prawem dotyczącym ochrony danych osobowych.

Wykres 8. Jak często odbywają się szkolenia z zakresu RODO?

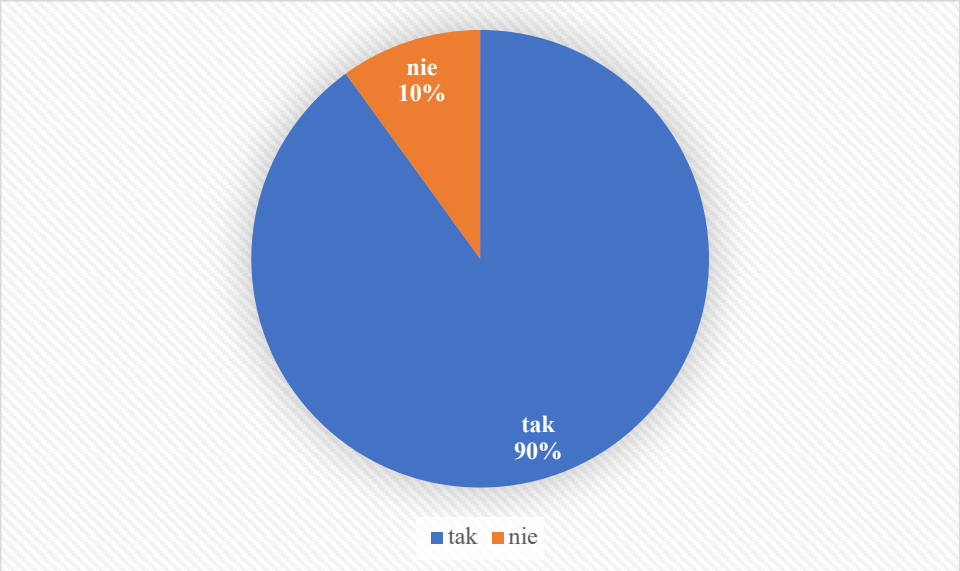


Źródło: opracowanie własne.

Dokonano analizy czy wdrożenie RODO spowodowało konieczność zatrudnienia dodatkowych pracowników, głównie Inspektorów Ochrony Danych Osobowych. Z przeprowadzonych badań wynika, że aż 90% respondentów potwierdziło, że było to konieczne, co wskazuje na wysoki wpływ wymogów RODO na zasoby ludzkie w jednostkach. Tylko 10% ankietowanych odpowiedziało, że nie było potrzeby zatrudniania dodatkowych inspektorów ochrony danych osobowych ani angażowania konsultantów.

Wyniki te świadczą o tym, że większość jednostek musiała dostosować swoje struktury organizacyjne do nowych regulacji, co często wiązało się z koniecznością pozyskania specjalistów w tej dziedzinie oraz poniesienia dodatkowych kosztów związanych z wdrażaniem.

Wykres 9. Czy wdrożenie RODO spowodowało konieczność zatrudnienia dodatkowych pracowników lub konsultantów zewnętrznych?



Źródło: opracowanie własne.

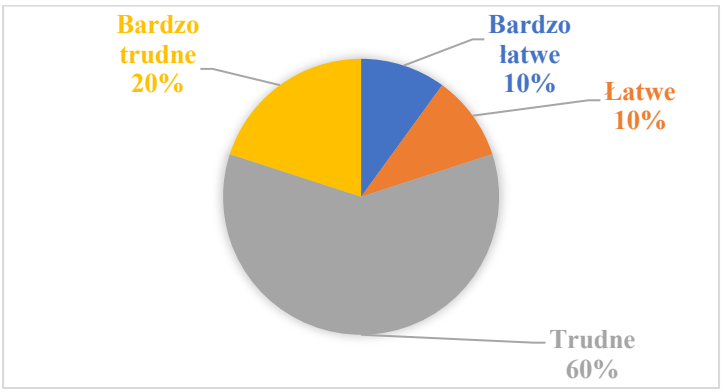
Z analizy wynika, że większość badanych jednostek doświadczyła przynajmniej pewnego stopnia trudności w procesie wdrożenia RODO. Można to wiązać z kompleksowością regulacji, wymogami dotyczącymi zabezpieczenia danych oraz koniecznością dostosowania wewnętrznych procesów. Niewielki odsetek jednostek, które wskazały, że wdrożenie było „bardzo łatwe", może sugerować, że miały one

odpowiednie zasoby, wsparcie ekspertów lub wcześniejsze doświadczenie w obszarze ochrony danych, co ułatwiło proces adaptacji do wymogów RODO.

W konkluzji dane z wykresu wskazują na to, że wdrożenie RODO jest wyzwaniem dla większości instytucji, co powinno skłonić zarówno administrację publiczną, jak też przedstawicieli prawa do dalszego badania czynników, które mogą ułatwić ten proces, oraz do rozwijania narzędzi i metod wsparcia dla jednostek mających trudności z przystosowaniem się do regulacji.

Z przeprowadzonych badań wynika, że większość badanych (60%), nie zarejestrowała poważniejszych zmian, jeśli idzie o poziom zabezpieczenia danych osobowych po wdrożeniu RODO. Może to sugerować, iż implementacja procedur bezpieczeństwa była już wcześniej na wysokim poziomie, lub też – co bardziej prawdopodobne – nowe wymogi prawne nie przyniosły zauważalnego efektu w ich percepcji bezpieczeństwa. Jedynie 24% respondentów zgłosiło „lekką poprawę" w bezpieczeństwie danych, co wskazuje na to, że wprowadzenie RODO miało pozytywny, lecz nie rewolucyjny wpływ na poziom ochrony danych w tych jednostkach. „Znacząca poprawa" została zauważona przez 10% uczestników ankiety, co może świadczyć o istotnych zmianach organizacyjnych lub technologicznych wprowadzonych w odpowiedzi na wymogi RODO, które zostały pozytywnie ocenione przez tę grupę. Jednakże 6% badanych jednostek odnotowało „pogorszenie" w poziomie bezpieczeństwa danych, co jest zaskakującym wynikiem, ponieważ RODO ma za zadanie wzmocnić ochronę danych. Może to wskazywać na wyzwania w adaptacji do nowych regulacji, niewystarczające zasoby lub błędne wdrożenie przepisów, co paradoksalnie przyczyniło się do obniżenia poziomu bezpieczeństwa.

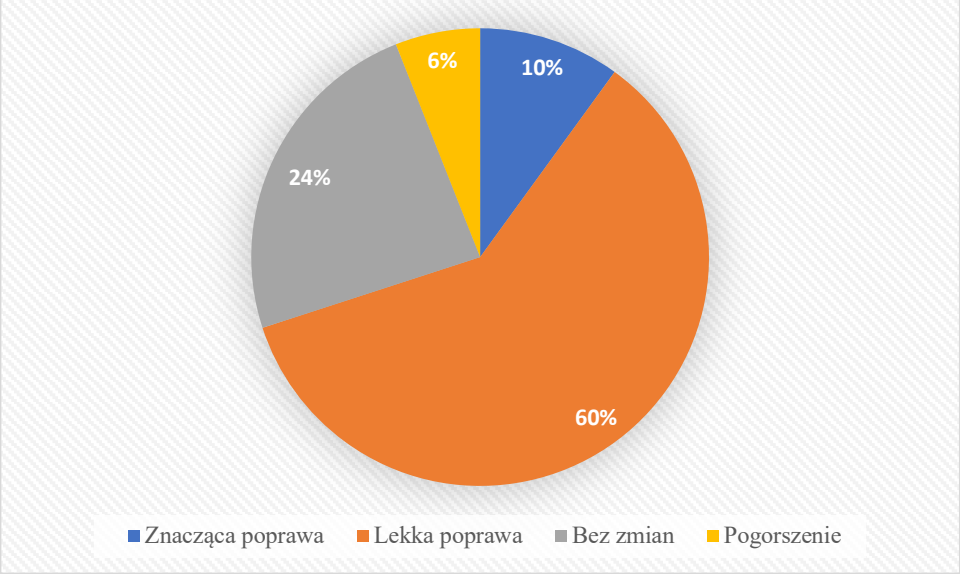
Wykres 10. Jak oceniasz poziom trudności wdrożenia RODO w Państwa jednostce?



Źródło: opracowanie własne.

Podsumowując, większość badanych jednostek nie odczuła zmian w poczuciu bezpieczeństwa danych po wdrożeniu RODO, co może stanowić punkt wyjścia do dalszej analizy skuteczności wprowadzonych przez RODO regulacji i ich realnego wpływu na organizacje. Fakt, iż część respondentów odnotowała poprawę, jest zgodny z intencją regulacji, choć stosunkowo niewielki procent „znaczącej poprawy" może sugerować, że istnieje jeszcze duże pole do usprawnień. Z kolei odsetek jednostek, które zgłosiły pogorszenie, stanowi ważny sygnał do dalszego badania potencjalnych przyczyn takiego stanu rzeczy.

Wykres 11. Czy zauważyli Państwo zmiany w poziomie bezpieczeństwa danych osobowych po wdrożeniu RODO?



Źródło: opracowanie własne.

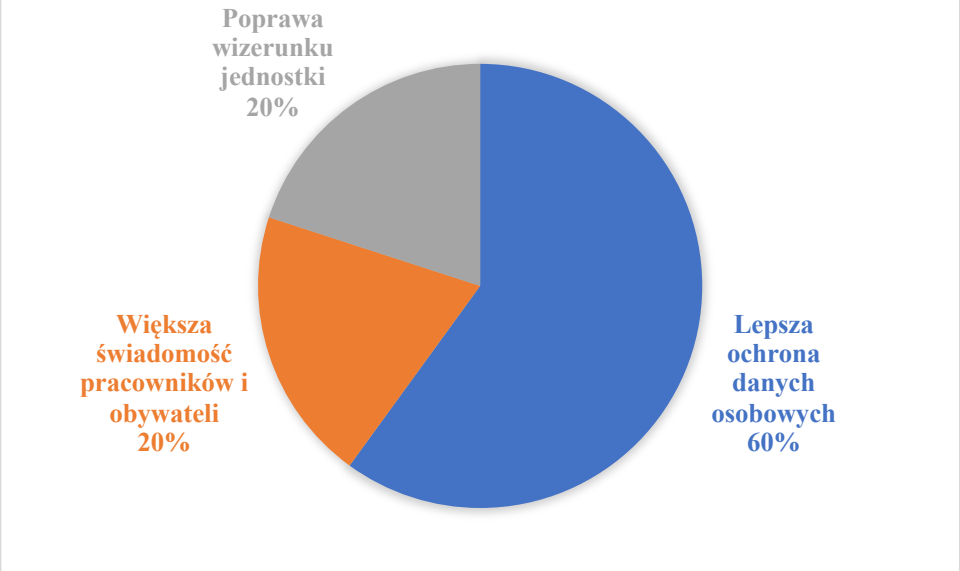
Zgodnie z przeanalizowanymi danymi, najwięcej, bo 60% respondentów uważa, że główną korzyścią wynikającą z wdrożenia RODO jest „lepsza ochrona danych osobowych". Ten wynik jest zgodny z podstawowym celem RODO, którym jest zwiększenie ochrony danych osobowych w Unii Europejskiej. Wskazuje to, iż regulacje przyczyniły się do wprowadzenia skuteczniejszych procedur i mechanizmów ochrony danych w organizacjach.

Równorzędnie 20% respondentów wskazało na „większą świadomość pracowników i obywateli" oraz „poprawę wizerunku jednostki" jako korzyści wdrożenia RODO. Zwiększona świadomość pracowników i obywateli jest niewątpliwie

koniecznym elementem w zarządzaniu prywatnością i ochroną danych, ponieważ edukacja i zrozumienie regulacji przez osoby zarządzające i przetwarzające dane osobowe ma fundamentalne znaczenie dla skuteczności całego systemu. Poprawa wizerunku jednostki z kolei odzwierciedla zaufanie do instytucji administracji publicznej oraz daje pewność, że organizacja postępuje zgodnie z przepisami prawa i dba o prywatność swoich klientów.

Podsumowując, badania wskazują, że wdrożenie RODO przyniosło wymierne korzyści w zakresie ochrony danych, edukacji i reputacji organizacji. Dominacja odpowiedzi wskazujących na lepszą ochronę danych osobowych sugeruje, że jest to najbardziej odczuwalna i bezpośrednia korzyść wdrożenia RODO. Jednocześnie równie istotne wydaje się zwiększenie świadomości oraz pozytywny wpływ na wizerunek, co może przyczyniać się do długoterminowego budowania kultury szacunku dla prywatności i danych osobowych w przestrzeni publicznej.

Wykres 12. Jakie korzyści przyniosło wdrożenie RODO w Państwa jednostce?



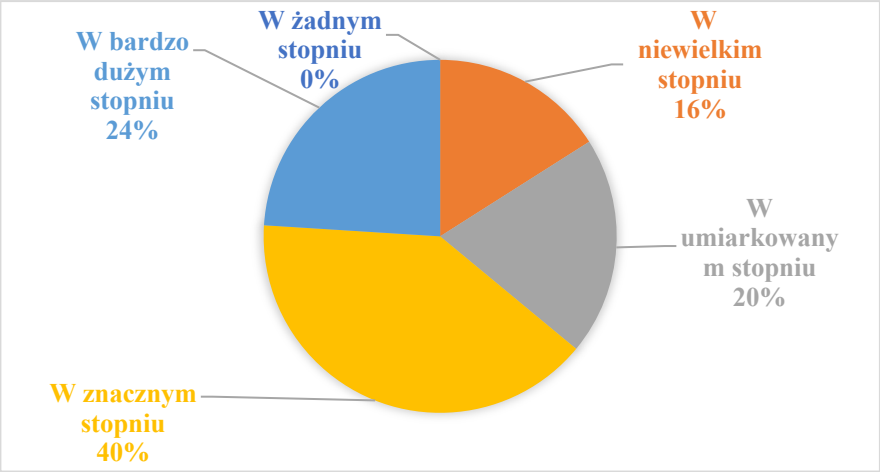
Źródło: opracowanie własne.

Z analizy wykresu wynika, że najwięcej, bo 40% respondentów, wskazało, że RODO wpłynęło na ich codzienne obowiązki „w umiarkowanym stopniu". Może to świadczyć o tym, że choć RODO wprowadziło zmiany w procedurach i wymaganiach dotyczących ochrony danych, nie były to zmiany rewolucyjne dla codziennej pracy większości pracowników. Drugą co do wielkości grupą są osoby, które

odpowiedziały, że RODO wpłynęło na ich pracę „w znacznym stopniu", stanowiąc 24% próby. Wskazuje to na istotne dostosowania w codziennych zadaniach i prawdopodobnie zwiększenie ilości obowiązków związanych z przestrzeganiem przepisów o ochronie danych. Odpowiedź „w niewielkim stopniu" została wybrana przez 20% badanych, sugerując, że dla tych pracowników wprowadzenie RODO nie miało dużego wpływu na ich codzienne obowiązki, być może ze względu na wcześniejsze wdrożenie odpowiednich praktyk lub specyfikę ich pracy, która nie wiąże się bezpośrednio z przetwarzaniem danych osobowych. Najmniejszy odsetek respondentów (16%), stwierdził, że RODO nie wpłynęło na ich obowiązki „w żadnym stopniu". To może oznaczać, że ich praca nie jest związana z przetwarzaniem danych osobowych lub że procesy w ich organizacji były już wcześniej zgodne z wymogami RODO.

Wyniki wskazują zatem, że wpływ RODO na codzienne obowiązki pracowników jest zróżnicowany, co może odzwierciedlać różnorodność stylu działania organizacji, zakresu ich działalności oraz wcześniejszego przygotowania do spełnienia wymogów ochrony danych. Brak odpowiedzi „w bardzo dużym stopniu" sugeruje, że choć RODO miało wpływ na działalność większości jednostek, nie przyczyniło się do kardynalnych zmian w rutynowych obowiązkach większości pracowników.

Wykres 13. W jakim stopniu RODO wpłynęło na Państwa codzienne obowiązki w pracy?



Źródło: opracowanie własne.

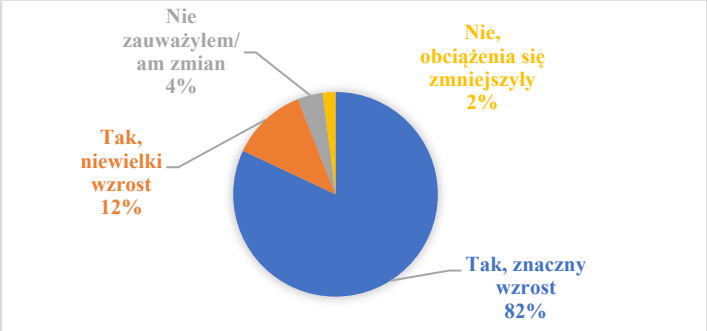
Zgodnie z pozyskanymi danymi, znaczna większość respondentów, bo aż 82%, zauważyła „znaczny wzrost" w biurokracji i obciążeniach administracyjnych

po wprowadzeniu RODO. Ten wynik sugeruje, że dla większości ankietowanych, adaptacja do wymogów RODO wiązała się z istotnym zwiększeniem pracy administracyjnej, co jest wynikiem wprowadzenia nowych procedur, konieczności szkolenia personelu, dokumentowania zgodności z przepisami oraz zarządzania zgłoszeniami i incydentami związanymi z danymi osobowymi. Odpowiedzi wskazujące na „niewielki wzrost" biurokracji zostały wybrane przez 12% respondentów. Oznacza to, że dla tej grupy wprowadzenie RODO spowodowało pewne dodatkowe wymogi administracyjne, jednakże nie były one na tyle znaczące, aby uznać je za dużo większe obciążenie. Z tego 4% badanych nie zauważyło żadnych zmian w poziomie biurokracji po wdrożeniu RODO. Może to sugerować, że te jednostki były już wcześniej dobrze przygotowane na wymogi rozporządzenia lub ich działalność nie wiązała się bezpośrednio z intensywnym przetwarzaniem danych osobowych.

Najmniejszy odsetek, bo tylko 2% respondentów zauważyło, że „obciążenia się zmniejszyły". Choć jest to niespodziewany wynik, może on odzwierciedlać sytuacje, w których procesy były optymalizowane w wyniku wdrożenia RODO, prowadząc do długoterminowej efektywności operacyjnej.

Zgromadzone informacje wskazują na to, że większość organizacji odczuła znaczne zwiększenie biurokracji po wprowadzeniu RODO. Stanowić to może ważny komunikat dla zarządzających, którzy starają się znaleźć równowagę pomiędzy spełnianiem wymogów prawnych a utrzymaniem wydajności organizacyjnej. Jednocześnie niewielki odsetek jednostek, które doświadczyły zmniejszenia obciążeń, może świadczyć o tym, że istnieje możliwość usprawnienia procesów administracyjnych w taki sposób, aby przepisy ochrony danych osobowych nie prowadziły do nadmiernej „biurokratyzacji" w negatywnym sensie.

Wykres 14. Czy zauważyli Państwo wzrost biurokracji i obciążeń administracyjnych po wprowadzeniu RODO?



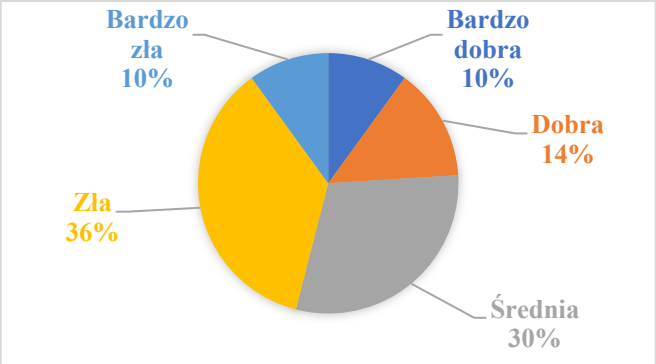
Źródło: opracowanie własne.

Z danych wynika, że największy odsetek respondentów, tj. 36% ocenił dostępność narzędzi i zasobów jako „średni". Może to wskazywać na to, że jednostki te posiadają pewne narzędzia i zasoby, lecz ich zakres lub jakość nie są w pełni satysfakcjonujące. Natomiast 30% badanych oceniło dostępność jako „dobrą", co sugeruje, że te jednostki uznają, iż dysponują odpowiednimi narzędziami i zasobami do spełnienia wymogów RODO, chociaż mogą być one niewystarczające w niektórych aspektach. 14% respondentów wskazało, że dostępność narzędzi i zasobów jest „zła", co może oznaczać, że w ich organizacjach występują znaczące luki w dostępie do odpowiednich środków niezbędnych do zapewnienia zgodności z RODO.

Respondenci, którzy uznali dostępność za „bardzo dobrą" oraz „bardzo złą", stanowią po 10% w dwu grupach badanych. Pierwsza z tych grup jest prawdopodobnie zadowolona z poziomu wsparcia, jakie otrzymuje w kontekście RODO, co może świadczyć o dobrze rozwiniętych zasobach i narzędziach. Z drugiej strony, odpowiedź „bardzo zła" wskazuje na jednostki, które mogą borykać się z poważnymi wyzwaniami w dostępie do narzędzi i zasobów, co może być przeszkodą w skutecznym przestrzeganiu RODO.

Reasumując, badania wskazują na zróżnicowanie w postrzeganiu dostępności narzędzi i zasobów do zapewnienia zgodności z RODO w różnych jednostkach. Szczególną uwagę warto zwrócić na potrzeby jednostek, które oceniły dostępność jako „średnią", „złą" lub „bardzo złą", gdyż wskazuje to na możliwe obszary wymagające ulepszenia i wsparcia.

Wykres 15. Jak oceniają Państwo dostępność narzędzi i zasobów niezbędnych do zapewnienia zgodności z RODO w Państwa jednostce?



Źródło: opracowanie własne.

Największy odsetek respondentów, tj. 66%, stwierdził, że komunikacja stała się „bardziej formalna" po wprowadzeniu RODO. Ten wynik może wskazywać na to, że jednostki zwiększyły formalność w korespondencji i interakcjach z mieszkańcami, prawdopodobnie w odpowiedzi na wymogi RODO dotyczące jasności i odpowiedzialności za przetwarzane dane osobowe. 20% badanych zauważyło, że komunikacja jest teraz „bardziej ograniczona". Może to odzwierciedlać fakt, że organizacje stały się bardziej ostrożne w udostępnianiu informacji i wchodzeniu w interakcje z obywatelami, mając na uwadze potrzebę ochrony danych osobowych zgodnie z RODO.

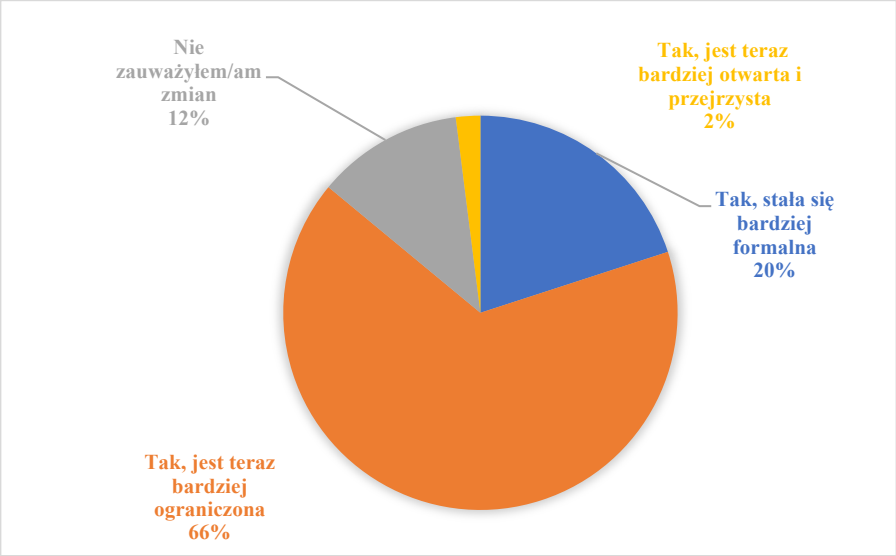
Grupa, która nie zauważyła żadnych zmian w sposobie komunikacji, stanowi zaledwie 12% respondentów. Może to oznaczać, że te jednostki nie musiały wprowadzać znaczących zmian w swoich procedurach komunikacyjnych lub uważają, że wprowadzenie RODO nie miało bezpośredniego wpływu na ich działania w tym obszarze. Jedynie 2% respondentów wskazało, że komunikacja stała się „bardziej otwarta i przejrzysta". Jest to interesujący wynik, który może sugerować, że pewne jednostki wykorzystały RODO jako okazję do poprawy jakości i transparentności komunikacji z obywatelami, co jest zgodne z duchem RODO promującym przejrzystość w przetwarzaniu danych osobowych.

Konkludując, wprowadzenie RODO miało znaczący wpływ na sposób komunikacji z mieszkańcami i obywatelami w większości jednostek. Dominacja odpowiedzi wskazujących na większą formalność i ograniczenia może odzwierciedlać zwiększone wymagania dotyczące ochrony danych osobowych i potrzebę bardziej ostrożnego podejścia do przekazywania informacji. Jednocześnie niewielki odsetek jednostek, które zauważyły poprawę w przejrzystości komunikacji, wskazuje na możliwość pozytywnego wykorzystania RODO w celu zbudowania większego zaufania i otwartości w relacjach z obywatelami.

Z przeprowadzonych badań wynika, że największy odsetek (36%) respondentów ocenił kontrole wewnętrzne jako średnio skuteczne. Są oni przekonani, że w instytucji występują pewne mechanizmy kontroli wewnętrznej, ale ich skuteczność jest tylko częściowo zadowalająca i może wymagać dodatkowych poprawek lub większej konsekwencji w egzekwowaniu. Tylko 24% badanych uznało kontrole za skuteczne, co wskazuje na to, że ich jednostki mają zaimplementowane odpowiednie procedury i systemy, które w opinii tych respondentów działają dobrze w zakresie przestrzegania RODO.

Odsetek respondentów, którzy odpowiedzieli, iż kontrole są „bardzo skuteczne", wynosi 20%. Jest to grupa jednostek, które uważają, że instytucje wdrożyły wyjątkowo efektywne i kompleksowe systemy kontroli wewnętrznych, które zapewniają wysoki poziom zgodności z RODO. Tylko 12% ankietowanych uważa, że kontrole wewnętrzne są „nieskuteczne". W takich przypadkach mogą występować luki w systemach, braki w szkoleniu personelu lub inne problemy, które przeszkadzają w efektywnym przestrzeganiu przepisów RODO. Najmniejszy odsetek (8%) uznał kontrole za „bardzo nieskuteczne". Ta krytyczna ocena może odzwierciedlać sytuacje jednostek mających poważne trudności z wdrożeniem odpowiednich procedur. Prawdopodobnie ich kontrola wewnętrzna jest niemalże nieistniejąca lub nie radzi sobie z zapewnieniem przestrzegania RODO.

Wykres 16. Czy wprowadzenie RODO wpłynęło na sposób komunikacji z mieszkańcami/obywatelami?

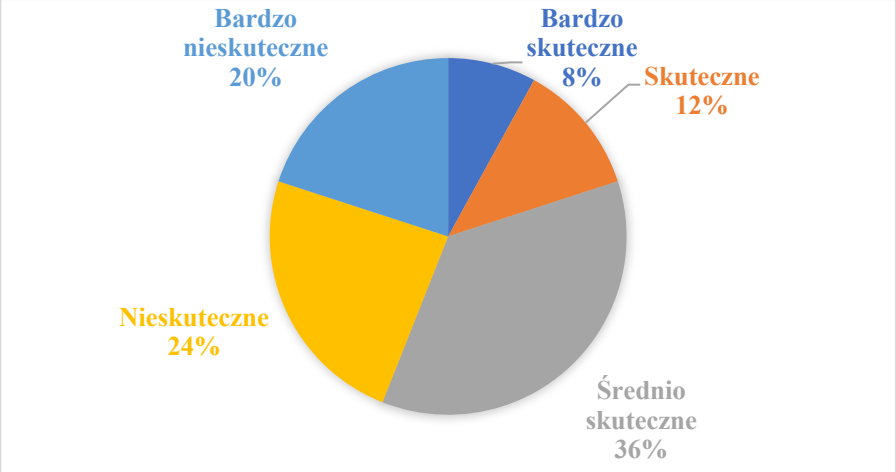


Źródło: opracowanie własne.

Tak więc wśród badanych jednostek istnieje znaczne zróżnicowanie w ocenach skuteczności kontroli wewnętrznych dotyczących przestrzegania RODO. Większość respondentów uważa, że ich systemy kontroli działają na średnim poziomie skuteczności, z mniejszą grupą wskazującą na wyższą lub niższą efektywność. Wyniki badań mogą wskazywać na potrzebę dalszego rozwijania i wzmacniania mechanizmów kontroli wewnętrznych w niektórych jednostkach, szczególnie w tych, które oceniły swoje kontrole jako nieskuteczne lub bardzo nieskuteczne. Dane wskazują

na rolę stałego monitorowania i doskonalenia procesów zgodności z RODO w celu zwiększenia poziomu ochrony danych osobowych oraz zredukowania potencjalnych ryzyk postępowań niezgodnych z prawem.

Wykres 17. Jak oceniają Państwo skuteczność kontroli wewnętrznych dotyczących przestrzegania RODO w Państwa jednostce?



Źródło: opracowanie własne.

Największy odsetek (76%) respondentów wskazało, że „nie mieliśmy do czynienia z naruszeniami", co sugeruje, że większość jednostek nie doświadczyła naruszeń danych osobowych, lub nie były one wykryte lub zgłaszane w badanym okresie. Ta odpowiedź może odzwierciedlać skuteczność wdrożonych przez nie środków ochrony danych lub niski poziom ryzyka związanego z przetwarzaniem danych w ich działalności.

Wśród respondentów, którzy doświadczyli naruszeń danych 10% stwierdziło, że „tak, zostały szybko i skutecznie rozwiązane". To wskazuje, że niektóre jednostki były w stanie efektywnie zareagować na zaistniałe naruszenia, prawdopodobnie dzięki dobrze przygotowanym procedurom reagowania na incydenty oraz zasobom niezbędnym do ich rozwiązania.

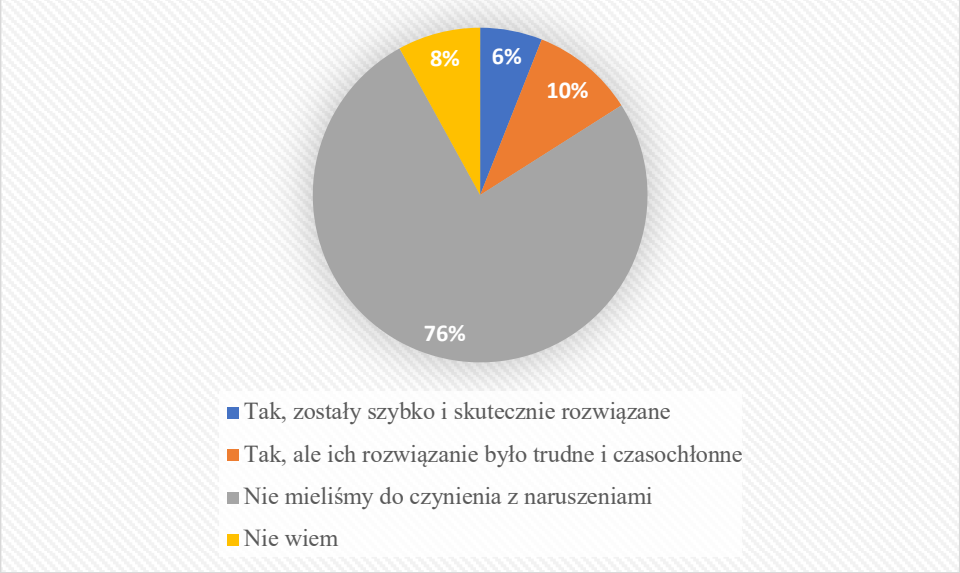
Dla 8% respondentów rozwiązanie naruszeń było „trudne i czasochłonne", co może wskazywać na wyzwania związane z identyfikacją, zgłaszaniem i naprawianiem skutków naruszeń, być może z powodu braku odpowiednich procedur, zasobów lub wiedzy specjalistycznej.

Najmniejszy odsetek (6%) odpowiedział „nie wiem", co może odzwierciedlać brak świadomości lub informacji na temat procedur zarządzania incydentami

w ich jednostkach lub niezrozumienie, jakie działania zostały podjęte w odpowiedzi na naruszenia.

Wyniki ankiety wskazują na to, że większość ankietowanych jednostek nie miała do czynienia z naruszeniami danych osobowych, co może świadczyć o wysokim poziomie ochrony danych lub braku świadomości naruszeń. Mniejszy odsetek jednostek, które doświadczyły naruszeń, zasygnalizował zdolność do skutecznego rozwiązania tych problemów, chociaż niektóre jednostki napotkały trudności. Brak informacji lub niepewność co do sposobu rozwiązania naruszeń wskazuje na potencjalne obszary do poprawy w zakresie komunikacji i edukacji pracowników na temat ochrony danych osobowych.

Wykres 18. Czy mieli Państwo do czynienia z przypadkami naruszeń danych osobowych? Jeśli tak, jak zostały one rozwiązane?



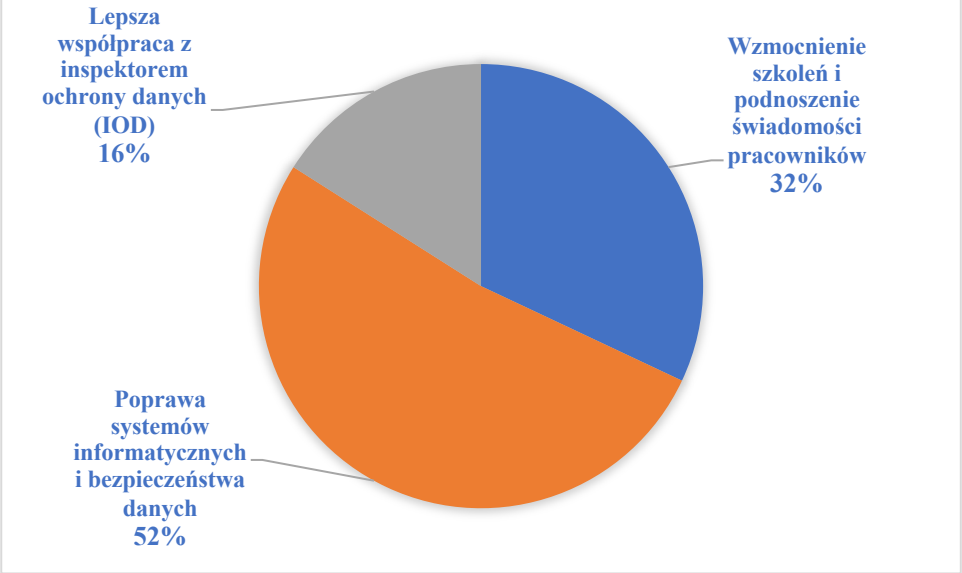
Źródło: opracowanie własne.

Największy odsetek respondentów (52%) uważa, że kluczowe jest „wzmocnienie szkoleń i podnoszenie świadomości pracowników". Wynik ten wskazuje, że edukacja i ciągłe szkolenie pracowników są fundamentem poprawy przestrzegania przepisów RODO. Może to oznaczać, że pracownicy jednostek samorządowych wymagają pogłębionej interpretacji przepisów RODO, jak również szkoleń z zakresu skutecznych praktyk w ochronie danych osobowych. Kategoria „poprawa systemów informatycznych i bezpieczeństwa danych" została wybrana przez 32% respondentów.

Infrastruktura techniczna, która musi być dostosowana do wymogów RODO, zapewnia odpowiednie zabezpieczenia techniczne i organizacyjne danych osobowych, i ten fakt potwierdzają dane. Natomiast 16% badanych sugeruje „lepszą współpracę z inspektorem ochrony danych (IOD)". Odpowiedzi podkreślają więc rolę IOD w organizacji jako kluczowego aktora w procesie zapewnienia zgodności z RODO, wskazując na potrzebę poprawy komunikacji i współdziałania pomiędzy IOD a innymi pracownikami jednostki.

Wyniki badań ankietowych wskazują, że najbardziej pożądaną metodą poprawy jest inwestycja w edukację, podnoszącą świadomość pracowników w zakresie istotności RODO. Infrastruktura IT oraz współpraca z IOD również są uznawane za ważne, ale w mniejszym stopniu. Może to sugerować, że jednostki samorządu terytorialnego widzą potrzebę kompleksowego podejścia do zagadnienia ochrony danych osobowych, biorąc pod uwagę zarówno aspekt ludzki, jak i technologiczny.

Wykres 19. Jakie są Państwa propozycje na poprawę przestrzegania RODO w jednostkach samorządu terytorialnego w Polsce?



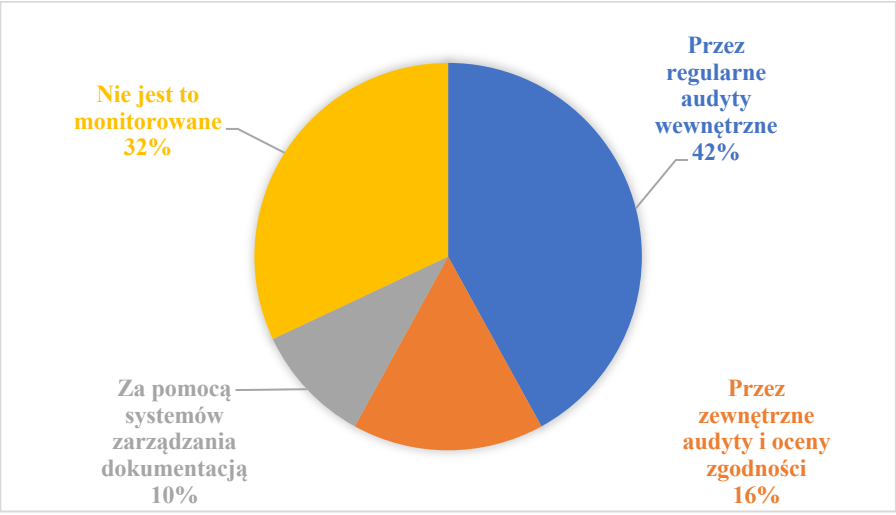
Źródło: opracowanie własne.

Z badań wynika, że 42% respondentów wskazało, że zgodność z RODO jest monitorowana „przez regularne audyty wewnętrzne". Dominacja tej metody może świadczyć o tym, że jednostki samorządu terytorialnego stosują wewnętrzne mechanizmy kontroli jako główne narzędzie zapewnienia przestrzegania przepisów RODO, co może być również wynikiem wewnętrznej polityki lub braku zasobów na zewnętrzne audyty.

Kolejne 32% badanych wykorzystuje „systemy zarządzania dokumentacją" do monitorowania zgodności z RODO, co podkreśla ważność zintegrowanych rozwiązań informatycznych w zarządzaniu procesami związanymi z ochroną danych osobowych. Zewnętrzne audyty i oceny zgodności są wykorzystywane przez 16% jednostek, co może wskazywać na to, że pewien segment jednostek samorządowych decyduje się na outsourcing tego aspektu zarządzania zgodnością z RODO, potencjalnie korzystając z wiedzy specjalistów z zewnątrz w celu uzyskania bardziej obiektywnego spojrzenia na swoje praktyki. Najmniejszy odsetek, bo 10% respondentów przyznało, że „nie jest to monitorowane". Jest to szczególnie istotne odkrycie, ponieważ wskazuje na lukę w zarządzaniu zgodnością z RODO, co może stanowić ryzyko prawne i operacyjne dla tych jednostek.

Podsumowując, wyniki ankiety podkreślają znaczenie audytów wewnętrznych oraz systemów zarządzania dokumentacją w monitorowaniu zgodności z RODO. Jednocześnie wskazują na mniejszy udział zewnętrznych audytów, który może sugerować potrzebę większego nacisku na niezależną weryfikację procedur związanych z RODO. Odkrycie, że pewna część jednostek nie monitoruje wcale swojej zgodności z RODO wskazuje na potrzebę edukacji i zwiększenia świadomości wśród pracowników oraz wprowadzenia odpowiednich procedur kontrolnych.

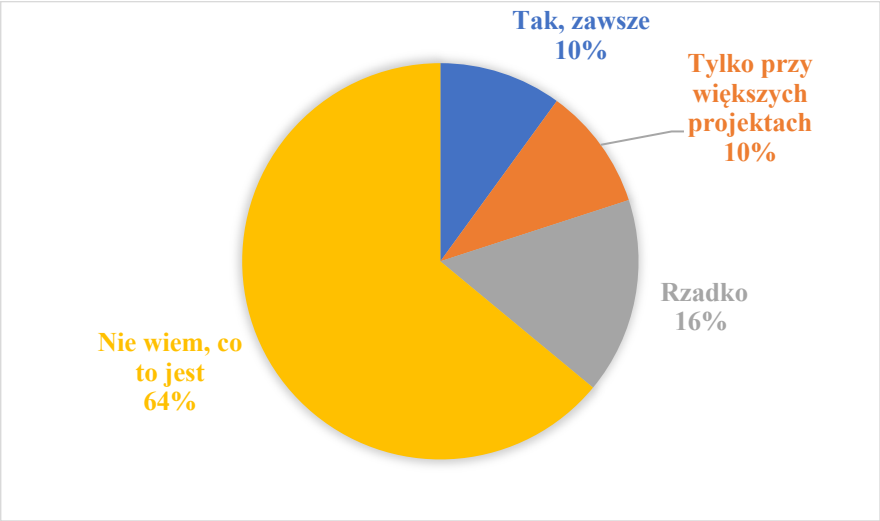
Wykres 20. Jak w Państwa jednostce jest monitorowana i dokumentowana zgodność z RODO?



Źródło: opracowanie własne.

Z przeprowadzonych analiz wynika, że większość respondentów (64%) nie jest pewna, czym jest procedura DPIA, co wskazuje na znaczący brak świadomości lub zrozumienia tej kwestii. Taki wynik może sugerować potrzebę intensywniejszych szkoleń i działań edukacyjnych na temat DPIA i ogólnie RODO wśród pracowników jednostek samorządu terytorialnego. Tylko 10% ankietowanych wskazuje, że procedury DPIA są stosowane „zawsze" przy wprowadzaniu nowych projektów, co świadczy o wysokim poziomie zgodności z najlepszymi praktykami ochrony danych. Również 10% respondentów odpowiedziało, że DPIA jest wykonywane „tylko przy większych projektach". To może oznaczać, że procedury DPIA są stosowane selektywnie, być może z uwagi na ograniczone zasoby lub percepcję, że tylko projekty o większym ryzyku dla danych osobowych wymagają takiej oceny. 16% uczestników ankiety przyznało, że procedury DPIA są stosowane „rzadko". To wskazuje na to, że w niektórych jednostkach brakuje systematycznego podejścia do oceny ryzyka związanego z przetwarzaniem danych osobowych. Podsumowując, analiza wykresu pokazuje, że w jednostkach samorządu terytorialnego w Polsce jest znaczna przestrzeń do poprawy w zakresie stosowania i zrozumienia procedur DPIA. Niewystarczająca świadomość i nieregularne stosowanie tych procedur może prowadzić do luk w ochronie danych osobowych i niezgodności z wymogami RODO.

Wykres 21. Czy w Państwa jednostce stosuje się procedury oceny skutków dla ochrony danych (DPIA) przy wprowadzaniu nowych projektów lub systemów przetwarzających dane osobowe?



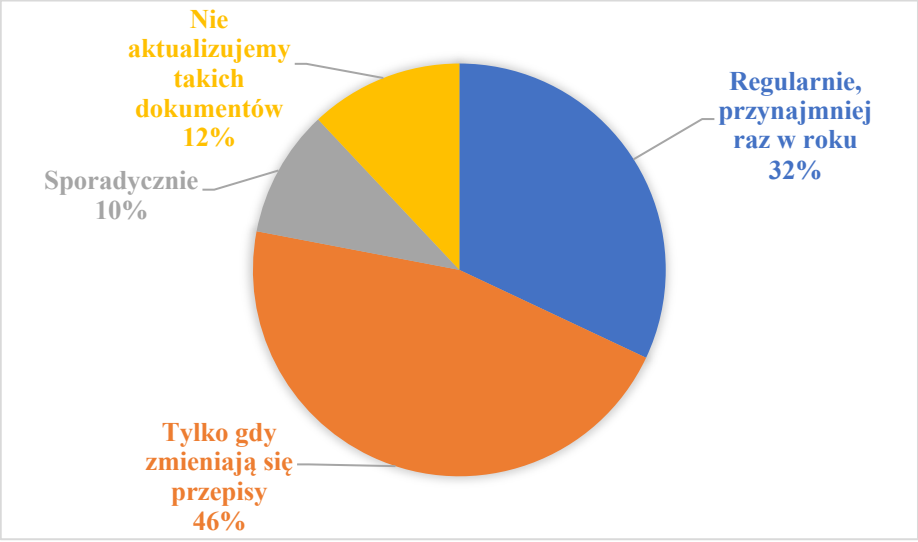
Źródło: opracowanie własne.

Z analizy wynika, że największa grupa respondentów (46%) aktualizuje swoje polityki i procedury „tylko gdy zmieniają się przepisy". Może to sugerować, że ponad połowa jednostek przyjmuje podejście reaktywne, gdzie aktualizacja następuje jedynie w odpowiedzi na zmiany legislacyjne, a nie jako część regularnego procesu przeglądu.

Aż 32% jednostek deklaruje, że aktualizuje swoje polityki i procedury „regularnie, przynajmniej raz w roku". Jest to zachęcające, jako że regularne przeglądy mogą przyczynić się do lepszego zarządzania ryzykiem i zwiększenia zgodności z aktualnymi wymogami prawymi. „Sporadycznie" aktualizacje są przeprowadzane przez 12% ankietowanych, co wskazuje na mniej systematyczne podejście do aktualizacji polityk i procedur ochrony danych. Z kolei 10% respondentów stwierdziło, że „nie aktualizujemy takich dokumentów". To może wskazywać na brak formalnych procesów zarządzania ochroną danych lub niską świadomość znaczenia takich działań.

Podsumowując, wyniki wskazują na to, że znaczący odsetek jednostek może nie być w pełni przygotowany na dynamiczne zmiany w zakresie ochrony danych osobowych, ponieważ aktualizacje polityk i procedur nie są dokonywane regularnie. Wynika z tego, że może istnieć potrzeba wprowadzenia bardziej rygorystycznych procesów aktualizacji w tych jednostkach, a także większego nacisku na edukację i budowanie świadomości dotyczącej ważności ciągłego dostosowywania się do zmieniającego się krajobrazu regulacji ochrony danych.

Wykres 22. Jak często Państwa jednostka aktualizuje polityki i procedury związane z ochroną danych osobowych?



Źródło: opracowanie własne.

Na pytanie jak jest realizowane prawo dostępu do danych, ich sprostowania, usunięcia czy przenoszenia przez mieszkańców/obywateli w Państwa jednostce, 50% ankietowanych odpowiada, że proces jest efektywny, mimo iż realizowany ręcznie. To sugeruje, że pomimo braku zautomatyzowanych systemów, jednostki te potrafią skutecznie radzić sobie z wnioskami obywateli dotyczącymi ich danych osobowych.

Aż 22% respondentów wskazało, że proces jest szybki i zautomatyzowany. Ta grupa może mieć dostęp do bardziej zaawansowanych technologicznie rozwiązań, które ułatwiają realizację praw wynikających z RODO, co zwiększa efektywność i przyspiesza obsługę wniosków. Mniejszy odsetek (18%) przyznał, że realizacja praw jest trudna i czasochłonna. To może wskazywać na problemy organizacyjne lub technologiczne, które utrudniają efektywne przetwarzanie wniosków związanych z danymi osobowymi.

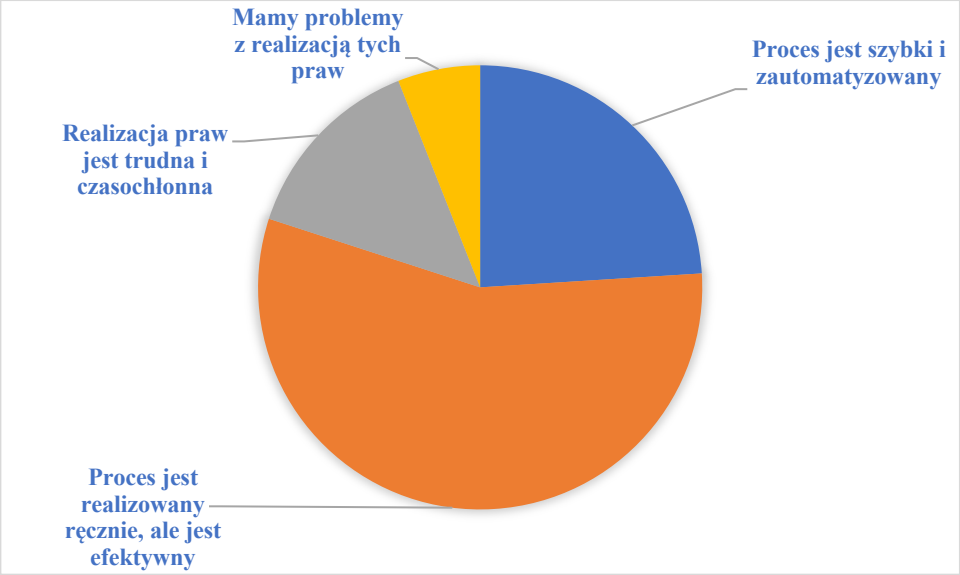
Tylko 10% respondentów doświadcza problemów z realizacją praw. Może to odzwierciedlać specyficzne wyzwania, z którymi borykają się te jednostki, takie jak ograniczone zasoby, brak odpowiedniego szkolenia lub niedostateczne systemy wsparcia.

Podsumowując, wyniki wskazują na zróżnicowanie w sposobie realizacji praw związanych z danymi osobowymi w jednostkach samorządu terytorialnego. Chociaż większość jednostek jest w stanie efektywnie radzić sobie z realizacją tych praw, znacząca część boryka się z trudnościami. Odsetek jednostek ze zautomatyzowanymi procesami może wskazywać na rosnącą tendencję do inwestycji w technologie wspierające zgodność z RODO. Niemniej jednak, dane wskazują na potrzebę dalszej optymalizacji procesów oraz na konieczność zwiększenia inwestycji w odpowiednie narzędzia (IT) oraz szkolenia pracowników podnoszące ich kwalifikacje cyfrowe.

Z dalszych badań wynika, że w zdecydowanej większości jednostek (84%) „nie było kontroli” ze strony Urzędu Ochrony Danych Osobowych. Ten wysoki odsetek może sugerować, że kontrole są rzadkie lub dane jednostki nie zostały jeszcze zbadane przez regulatora. Jedynie 12% respondentów doświadczyło kontroli, której wyniki były „pozytywne”. To wskazuje na to, że te jednostki spełniają wymogi RODO, co jest pozytywnym sygnałem wskazującym na zgodność z obowiązującymi przepisami ochrony danych osobowych. Zaledwie 2% jednostek miało kontrolę, która wykazała „pewne nieprawidłowości, ale zostały one poprawione”, a to sugeruje, że choć w trakcie kontroli zidentyfikowano pewne błędy, jednostki te podjęły kroki naprawcze w celu usunięcia stwierdzonych nieprawidłowości i prawdopodobnie poprawiły swoje procedury ochrony danych. Również 2% jednostek zgłosiło, że wyniki kontroli

były „negatywne i są wdrażane korekty”. Ta grupa stanowi jednostki, które zostały zobowiązane do przeprowadzenia istotnych zmian w swoich politykach lub procedurach, aby osiągnąć pełną zgodność z RODO.

Wykres 23. Jak jest realizowane prawo dostępu do danych, ich sprostowania, usunięcia czy przenoszenia przez mieszkańców/obywateli w Państwa jednostce?



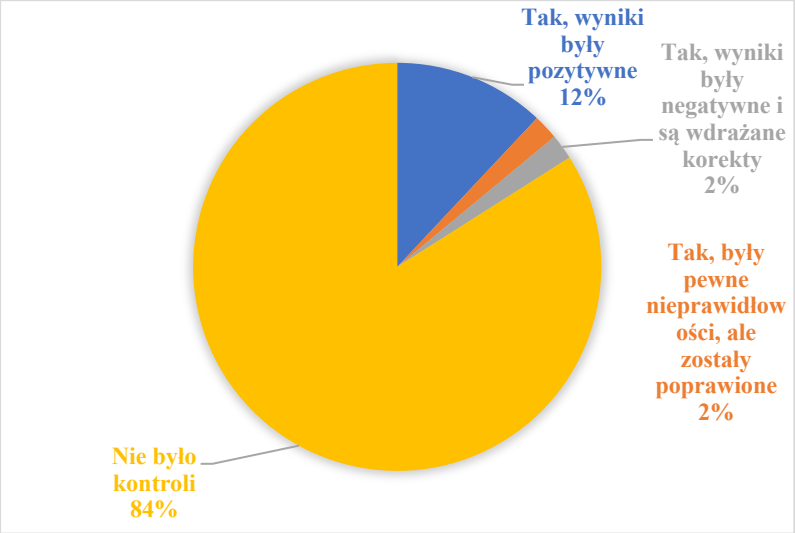
Źródło: opracowanie własne.

Powyższy wykres pokazuje, że większość jednostek nie doświadczyła kontroli UODO, co może oznaczać, że są one albo zgodne z RODO, albo że UODO koncentruje swoje zasoby na bardziej ryzykownych sektorach lub na podstawie zgłoszeń naruszeń. Wyniki kontroli w mniejszej liczbie jednostek, które doświadczyły audytów, pokazują mieszankę zgodności i potrzeby poprawek. To podkreśla znaczenie utrzymania ciągłej czujności i gotowości na kontrolę, jak również wdrażania korekt w razie stwierdzenia nieprawidłowości.

Analiza danych wskazuje, że większość pracowników, tj. 70% jest informowana „przez szkolenia i instrukcje”. To sugeruje, że w tych jednostkach preferowane są formalne metody edukacyjne, co jest zgodne z najlepszymi praktykami w zakresie zapewnienia zrozumienia i przestrzegania przepisów o ochronie danych osobowych. Kolejna grupa (22%) to pracownicy, którzy otrzymują informacje „przez bezpośrednie polecenia od przełożonych". Ten sposób komunikacji może być efektywny w mniejszych jednostkach, gdzie bezpośrednia komunikacja jest łatwiejsza, jednak może nie być tak

systematyczna jak szkolenia i instrukcje. Mniejszy odsetek pracowników (4%) jest informowany „za pomocą systemów elektronicznych (np. pop-upy przy wprowadzaniu danych)". Ta metoda, choć potencjalnie efektywna w codziennym przypominaniu o konieczności zachowania zgodności, może nie dostarczać pełnego szkolenia wymaganego przez RODO. Tylko 4% respondentów deklaruje, że „nie są informowani o tej konieczności", może to wskazywać na istotne luki w procesach informacyjnych i szkoleniowych w tych jednostkach. Jest to znaczący problem, który wymaga natychmiastowej uwagi, aby zapewnić zgodność z obowiązkami wynikającymi z RODO.

Wykres 24. Czy Państwa jednostka doświadczyła kontroli przez Urząd Ochrony Danych Osobowych? Jeśli tak, jakie były wyniki?

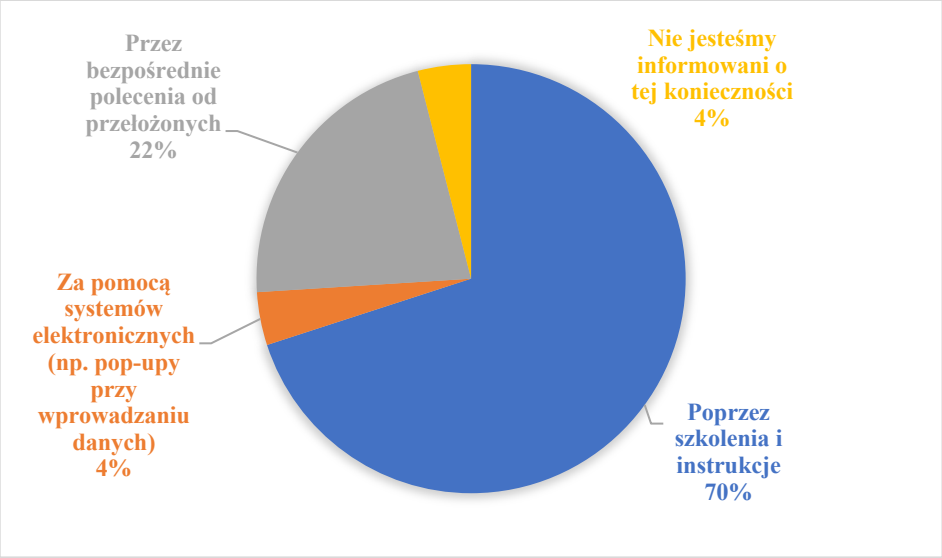


Źródło: opracowanie własne.

Podsumowując, wyniki wskazują na to, że większość jednostek stosuje formalne metody edukacji, aby informować pracowników o konieczności podpisywania klauzul RODO. Jednakże istnieje również grupa, która nie otrzymuje takich informacji, co może skutkować ryzykiem naruszeń ochrony danych osobowych.

Dla zapewnienia pełnej zgodności z RODO, ważne jest, aby wszystkie jednostki wdrażały skuteczne metody komunikacji związane z ochroną danych, w tym regularne szkolenia, jasne instrukcje oraz wykorzystanie technologii do wspierania procesów zgodności.

Wykres 25. W jaki sposób pracownicy są informowani o konieczności podpisywania klauzul RODO przy przekazywaniu danych osobowych?



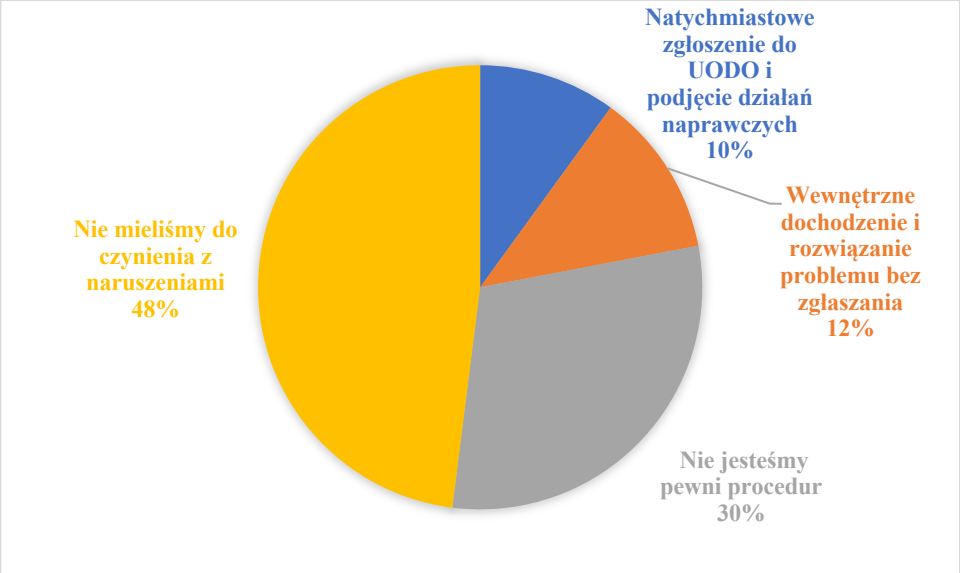
Źródło: opracowanie własne.

Znaczna większość, tj. 70%, wskazuje na to, że informowanie pracowników odbywa się „przez szkolenia i instrukcje". To świadczy o tym, że większość jednostek przywiązuje dużą wagę do formalnego przekazu wiedzy i jest to główna ścieżka edukacji pracowników w zakresie obowiązków wynikających z RODO. 22% respondentów otrzymuje informacje „przez bezpośrednie polecenia od przełożonych". Taka metoda może być bardziej osobista i pozwala na szybką komunikację, ale może nie być tak systematyczna i kompleksowa jak formalne szkolenia. „Za pomocą systemów elektronicznych" informuje 4% pracowników. Jest to najmniej popularny sposób komunikacji, co może wynikać z mniejszej dostępności technologii lub preferencji bardziej tradycyjnych metod komunikacji w jednostce.

Natomiast 4% ankietowanych stwierdziło, że „nie jesteśmy informowani o tej konieczności", co wskazuje na potencjalną lukę w procesach informacyjnych i może wskazywać na ryzyko naruszenia przepisów RODO.

Podsumowując, dane z wykresu wskazują, że większość jednostek stosuje formalne metody szkolenia, co jest pozytywnym znakiem w zakresie dbałości o przestrzeganie RODO. Jednakże istnieją jednostki, które nie informują swoich pracowników w odpowiedni sposób, co może prowadzić do nieświadomych naruszeń przepisów. Brak informacji w tych jednostkach stanowi znaczący obszar do poprawy, zwłaszcza w kontekście potencjalnych inspekcji przez UODO i związanych z tym ryzyk.

Wykres 26. Jakie kroki są podejmowane w przypadku stwierdzenia naruszenia przepisów RODO w Państwa jednostce?



Źródło: opracowanie własne.

W odpowiedzi na pytanie dotyczące wpływu wprowadzenia RODO na funkcjonowanie jednostki samorządu terytorialnego, można stwierdzić, że wprowadzenie tego rozporządzenia miało znaczący wpływ na jakość dbania o ochronę danych osobowych petentów. RODO jako kompleksowy zbiór przepisów, wymusiło na jednostkach dokładniejsze przemyślenie i wdrożenie odpowiednich procedur ochrony danych. Wprowadzenie RODO skłoniło jednostki do przeprowadzenia audytów procesów przetwarzania danych, co pozwoliło zidentyfikować i usprawnić wiele obszarów. Dzięki tym działaniom podniosła się ogólna jakość dbania o dane osobowe, co bezpośrednio przekłada się na wzrost zaufania petentów. Zintensyfikowane szkolenia i regularne aktualizacje wiedzy pracowników przyczyniły się do zwiększenia ich świadomości i odpowiedzialności w zakresie przetwarzania danych. Pracownicy są lepiej przygotowani do przestrzegania przepisów RODO, co z kolei zmniejsza ryzyko naruszeń i potencjalnych sankcji dla jednostki.

Nie można jednak pominąć wyzwań, jakie niesie ze sobą wprowadzenie RODO. Opracowanie i implementacja procedur, stałe szkolenia i monitorowanie procesów są działaniami wymagającymi zarówno zasobów finansowych, jak i zaangażowania czasowego. Niemniej jednak, pomimo tych wyzwań, RODO przyczyniło się do podniesienia standardów ochrony danych i stworzenia bardziej przejrzystego

środowiska dla obywateli w zakresie przetwarzania ich danych osobowych przez jednostki samorządowe.

W procesie wdrażania i stosowania RODO w jednostce samorządu terytorialnego największym wyzwaniem okazało się wdrożenie skutecznych procedur ochrony danych oraz edukowanie pracowników w tym zakresie. Zmiana kultury organizacyjnej i wprowadzenie nowych praktyk wymagały zaangażowania na wszystkich poziomach zarządzania, co było procesem złożonym i czasochłonnym. Szkolenia i warsztaty stały się regularną częścią kalendarza jednostki, co pozwoliło pracownikom na lepsze zrozumienie nowych obowiązków i odpowiedzialności wynikających z RODO.

Kluczowe w procesie adaptacji było także ustanowienie nowych ról w organizacji, takich jak Inspektor Ochrony Danych, który stał się głównym punktem kontaktowym dla wszelkich spraw związanych z ochroną danych osobowych. Opracowanie wewnętrznej dokumentacji, takiej jak polityki prywatności, procedury reagowania na incydenty związane z danymi, czy instrukcje postępowania w przypadku wniosków od osób, których dane dotyczą, wymagało wszechstronnej analizy procesów i identyfikacji obszarów ryzyka.

Dodatkowym wyzwaniem było zintegrowanie RODO z istniejącymi systemami IT oraz dostosowanie infrastruktury technologicznej do nowych wymagań, w tym zabezpieczenia przetwarzanych danych osobowych. Niezbędne było przeprowadzenie szczegółowych audytów bezpieczeństwa i implementacja nowych rozwiązań, takich jak szyfrowanie danych czy dwuetapowe uwierzytelnianie, aby zapewnić wyższy poziom ochrony. Na drodze do zgodności z RODO jednostki napotkały także konieczność zmiany procedur związanych z outsourcingiem i współpracą z podmiotami zewnętrznymi. Wymagało to renegocjacji umów i zapewnienia, że wszyscy partnerzy także przestrzegają przepisów RODO.

Podsumowując, mimo że wyzwania wdrożeniowe RODO były znaczące, dzięki systematycznej pracy, edukacji i zaangażowaniu personelu, jednostka zdołała z sukcesem dostosować się do nowych przepisów. Proces ten nie tylko zwiększył poziom ochrony danych osobowych petentów, ale również pozytywnie wpłynął na ogólną świadomość znaczenia prywatności i danych osobowych.

W odpowiedzi na pytanie dotyczące wprowadzania specjalnych technologii lub narzędzi w celu zapewnienia zgodności z RODO w naszej jednostce samorządu terytorialnego, można stwierdzić, że inicjalnie skupiliśmy się głównie na wdrożeniu specjalnych procedur przyjętych odpowiednimi zarządzeniami. Proces ten koncentrował

się na stworzeniu i uaktualnianiu dokumentacji, szkoleniu pracowników oraz wdrażaniu polityk bezpieczeństwa i zarządzania ryzykiem związanym z przetwarzaniem danych osobowych.

Nowoczesne technologie i narzędzia, które mogą znacznie usprawnić zgodność z RODO, nie zostały od razu wprowadzone. Dopiero po pięciu latach od wdrożenia RODO zaczęto przygotowywać grunt pod ich implementację. To opóźnienie wynikało częściowo z ograniczeń budżetowych, a częściowo z potrzeby głębszego zrozumienia i oceny dostępnych na rynku rozwiązań technologicznych.

Niemniej jednak, wprowadzone do tej pory procedury znacząco przyczyniły się do poprawy zarządzania danymi i podniosły świadomość ochrony danych wśród personelu. Regularne audyty, zwiększona kontrola nad procesami oraz systematyczne przeglądy polityk prywatności i bezpieczeństwa stały się normą. Pozwoliło to na lepszą identyfikację potencjalnych luk w ochronie danych i szybsze reagowanie na ewentualne naruszenia.

Jednostki przygotowują się obecnie do wdrożenia nowoczesnych rozwiązań technologicznych, takich jak systemy klasyfikacji danych, które automatycznie identyfikują i klasyfikują dane osobowe, czy narzędzia do zarządzania zgodnościami, które pomogą w monitorowaniu i utrzymywaniu zgodności z przepisami. Oczekuje się, że wprowadzenie tych technologii zdecydowanie usprawni procesy pracy i zwiększy poziom ochrony danych, umożliwiając między innymi automatyczne monitorowanie przepływu danych i lepsze zarządzanie incydentami związanymi z ochroną danych.

Wprowadzenie RODO wpłynęło na organizację pracy w jednostkach przede wszystkim przez wprowadzenie nowych wymogów dotyczących ochrony danych osobowych. Znaczna część badanych zauważyła po wprowadzeniu RODO większy nacisk na przestrzeganie zasad dotyczących danych osobowych, co przyczyniło się do wzrostu świadomości i odpowiedzialności pracowników w tym obszarze. Regularne szkolenia, aktualizacje polityk prywatności i procedur przetwarzania danych to tylko niektóre z działań, które zostały wprowadzone, co z kolei przyczyniło się do podniesienia poziomu bezpieczeństwa i lepszego zarządzania danymi osobowymi.

Pozytywnym aspektem tych zmian jest zwiększona ochrona przed naruszeniami danych i potencjalnymi cyberatakami. Wzmocnienie mechanizmów ochrony danych i wprowadzenie klarownych procedur przetwarzania informacji osobowych przyniosły również poprawę wizerunku jednostki jako instytucji, która poważnie podchodzi do prywatności i ochrony informacji osobistych obywateli. Natomiast z drugiej strony,

znaczna część badanych zauważyła, że wprowadzenie RODO spowodowało również wzrost biurokracji i rozbudowanie procedur. Szczególnie w początkowym okresie dostosowywania się do nowych regulacji, wiele jednostek odczuło znaczne obciążenie związane z koniecznością przeprowadzenia audytów, rewizji procedur i implementacji nowych systemów. W efekcie, te działania mogły prowadzić do początkowego spadku efektywności pracy, zwiększenia nakładu czasu na przetwarzanie wniosków oraz na zarządzanie dokumentacją.

W odpowiedzi na te wyzwania, jednostki stopniowo poszukiwały rozwiązań, które pozwoliłyby na optymalizację nowych procesów i zmniejszenie nadmiaru papierkowej roboty. Zastosowanie systemów informatycznych wspomagających zarządzanie danymi osobowymi, automatyzacja pewnych procesów i ciągłe szkolenie pracowników przyczyniają się do stopniowej poprawy efektywności pracy przy jednoczesnym zachowaniu wysokich standardów ochrony danych osobowych.

Można więc powiedzieć, że RODO przyniosło więcej pozytywów niż obciążeń dla organizacji pracy w jednostce. Po początkowych trudnościach związanych z dostosowaniem się do nowych regulacji, obserwujemy ciągły rozwój procedur i metod pracy, które mają na celu utrzymanie równowagi między ochroną danych osobowych a efektywnością operacyjną. W procesie wdrożenia i przestrzegania RODO w jednostkach samorządu terytorialnego kluczowym aspektem, który mógłby przynieść znaczącą poprawę, jest ujednolicenie procedur i zasad. Obecnie obserwuje się, że niedoprecyzowane przepisy i brak standardów wykonawczych mogą prowadzić do interpretacyjnego chaosu i co za tym idzie, nieprawidłowego wdrażania przepisów RODO. Pierwszym krokiem powinno być stworzenie jasnych, ogólnokrajowych wytycznych, które pomogą jednostkom samorządowym zrozumieć swoje obowiązki i stosować najlepsze praktyki w zakresie ochrony danych osobowych. Ustandaryzowanie podejścia nie tylko usprawni proces wdrażania RODO, ale także zapewni większą konsekwencję w działaniach różnych jednostek.

Ponadto, jednostki samorządu terytorialnego mogłyby skorzystać z bardziej szczegółowych przewodników lub wzorów dokumentacji, które mogłyby być adaptowane do specyficznych warunków i potrzeb lokalnych. Takie narzędzia umożliwiłyby łatwiejsze i bardziej efektywne wdrożenie wymaganych procedur oraz mogłyby pomóc w uniknięciu niejasności interpretacyjnych. Niezmiernie istotna jest również ciągła edukacja i szkolenie pracowników, co zapewnieni, że wszyscy zrozumieją i będą w stanie przestrzegać przepisów o ochronie danych osobowych.

Regularne szkolenia i aktualizacje wiedzy są niezbędne, by utrzymać wysoką świadomość znaczenia i konsekwencji RODO, szczególnie w świetle ciągłych zmian w technologii i metodach przetwarzania danych. Jednostki mogą również rozważyć wprowadzenie dedykowanych ról, takich jak Inspektor Ochrony Danych, który nie tylko nadzorowałby przestrzeganie RODO, ale także służył wsparciem i radą dla innych pracowników.

Ważne jest, aby jednostki samorządowe miały możliwość dzielenia się doświadczeniami i „dobrymi praktykami" poprzez tworzenie platform wymiany wiedzy, regularne warsztaty i seminaria, a także poprzez tworzenie sieci współpracy między jednostkami. Lepsze wdrożenie i przestrzeganie RODO w jednostkach samorządu terytorialnego wymaga jasnych, ustandaryzowanych procedur, edukacji i komunikacji oraz możliwości współpracy i wymiany wiedzy. Implementacja tych rekomendacji może przyczynić się do zwiększenia zgodności z przepisami RODO i podniesienia poziomu ochrony danych osobowych w jednostkach samorządu terytorialnego.

5.5. Interpretacja i ocena wyników badań

Wnioski z przeprowadzonych badań empirycznych na temat roli i odpowiedzialności organów samorządu terytorialnego w ochronie danych osobowych w kontekście usług publicznych potwierdziły kluczową rolę w ochronie danych osobowych obywateli w zakresie usług publicznych.

Wpływ na ochronę prywatności

Władze samorządowe ponoszą odpowiedzialność za gromadzone, przechowywane i wykorzystywane tych informacji zgodnie z przepisami o ochronie danych. Badania empiryczne na temat wpływu na ochronę prywatności potwierdzają istotną rolę organów samorządu terytorialnego w zapewnianiu ochrony danych osobowych obywateli i rola ta, jak i świadomość odpowiedzialności stale wzrasta. W praktyce oznacza to, że organy samorządu terytorialnego powinny wprowadzić odpowiednie procedury i praktyki zarządzania danymi, w tym mechanizmy zabezpieczające, szkolenia dla personelu i regularne audyty. W przypadku naruszenia ochrony prywatności, powinny one również mieć plany reagowania.

Z badań wynika konieczność zwiększenia świadomości w zakresie znaczenia ochrony prywatności w kontekście usług publicznych zarówno pracowników organów samorządu terytorialnego, jak też obywateli.

Potrzeba edukacji i szkolenia

Badania wykazały, że personel organów samorządu terytorialnego często nie ma odpowiednich umiejętności lub wiedzy na temat prawidłowego postępowania z danymi osobowymi. Potrzeba szkolenia i edukacji w tej dziedzinie jest więc wyraźna i konieczna. Badania empiryczne wskazały istotne luki w kompetencjach personelu organów samorządu terytorialnego w zakresie przetwarzania danych osobowych. To oznacza, że często pracownicy samorządu nie posiadają odpowiedniej wiedzy i umiejętności, które pozwoliłyby im na prawidłowe zarządzanie danymi osobowymi, a co za tym idzie – na zapewnienie ochrony prywatności i bezpieczeństwa osobom, których dane przetwarzają. Badania potwierdzają zatem istotną potrzebę szkoleń dla personelu organów samorządu terytorialnego w zakresie przetwarzania danych osobowych. Badania sugerują, że poprawa takich kompetencji może wymagać nie tylko jednorazowych szkoleń, ale także ciągłego doskonalenia umiejętności, aktualizowania wiedzy w obliczu dynamicznie zmieniających się regulacji i technologii związanych z ochroną danych osobowych.

Wdrożenie systemów bezpieczeństwa

Wyniki wskazują, że organy samorządu terytorialnego powinny inwestować w rozwijanie i wdrażanie efektywnych systemów bezpieczeństwa danych, gdyż dotychczasowe jest niewystarczające. Zapewnienie najnowocześniejszych środków ochrony zmniejsza ryzyko naruszenia ochrony danych. Badania empiryczne wskazują na potrzebę inwestycji we wdrażanie skutecznych systemów bezpieczeństwa danych przez organy samorządu terytorialnego. Najnowsze technologie ochrony danych mogą znacznie zmniejszyć ryzyko wycieku danych, poprzez zapewnienie różnorodnych mechanizmów, takich jak szyfrowanie, zabezpieczenia przed nieautoryzowanym dostępem, detekcja i odpowiedź na incydenty bezpieczeństwa, a także regularne tworzenie kopii zapasowych i procedury przywracania danych.

Wyniki badań potwierdzają, że inwestycje w systemy bezpieczeństwa nie są jedynie kwestią zgodności z przepisami, ale mogą przyczynić się do znacznego ograniczenia ryzyka naruszenia ochrony danych. Wszelkie naruszenia wiążą się, co oczywiste, z poważnymi konsekwencjami, zarówno prawnymi, jak też reputacyjnymi, dla organów samorządu terytorialnego. Stąd zaleca się, by organy

samorządu terytorialnego aktywnie inwestowały w rozwijanie i wdrażanie skutecznych systemów bezpieczeństwa danych. Takie systemy muszą być dostosowane do specyfiki przetwarzanych danych oraz do rozmiaru i struktury organizacji. W tym kontekście warto powtórzyć, że odpowiednie szkolenia personelu odgrywają kluczową rolę w utrzymaniu bezpieczeństwa danych – nawet najbardziej zaawansowany system bezpieczeństwa może nie zadziałać, jeśli pracownicy nie mają świadomości, jak z niego prawidłowo korzystać.

Skoordynowane działanie

Badania pokazują, że skoordynowane działanie pomiędzy różnymi organami samorządu terytorialnego mają pierwszorzędne znaczenie dla skutecznej ochrony danych. Wymiana najlepszych praktyk i regularna komunikacja to rzecz niezbędna dla zapewnienia ciągłości ochrony.

Przeanalizowane przypadki wskazują, że skuteczność ochrony danych nie zależy przede wszystkim od ich współpracy i koordynacji. Skuteczność ochrony danych jest wyższa, gdy różne organy samorządu terytorialnego działają w sposób skoordynowany. Badania wykazały, że organy samorządu terytorialnego mogą skuteczniej chronić dane, gdy dzielą się swoimi doświadczeniami i najlepszymi praktykami. Podobna strategia może obejmować różne aspekty, od technicznych rozwiązań, przez regulacje prawne, aż po strategie zarządzania i edukacji. Wymiana informacji, dyskusje i ciągły dialog między różnymi organami samorządu terytorialnego. Taki dialog pomaga w utrzymaniu ciągłości i skuteczności ochrony danych. Regularna komunikacja ułatwia również bieżące monitorowanie sytuacji, co pozwala na szybsze reagowanie na nowe zagrożenia i wyzwania.

Komunikacja z obywatelami

Obserwacje poczynione w ramach opisywanych badań dowodzą, że organy samorządu terytorialnego powinny aktywnie informować obywateli o tym, jak są przetwarzane ich dane osobowe i jakie mają prawa w tym zakresie. Transparentność w tym obszarze zwiększa zaufanie do instytucji publicznych i pomaga w budowaniu pozytywnego stosunku z obywatelami. Badania wskazują także na kluczową rolę komunikacji i transparentności ze strony organów samorządu terytorialnego w zakresie przetwarzania danych osobowych obywateli.

Instytucje publiczne muszą nie tylko przestrzegać regulacji dotyczących prywatności i ochrony danych, ale także podjąć dodatkowe wysiłki, aby zapewnić, że obywatele są świadomi tych praktyk. Może to obejmować wyjaśnianie, jakie dane są gromadzone, jak są przechowywane, kto ma do nich dostęp, jak są wykorzystywane i jak długo są przechowywane. Obywatele mają prawo wiedzieć, jakie są ich prawa, takie jak prawo do dostępu do swoich danych, prawo do ich poprawiania, do zapomnienia, czy do ograniczenia przetwarzania. Wiedza na ten temat umożliwia obywatelom skuteczne korzystanie z tych praw.

Warto także zwrócić uwagę związek między transparentnością a zaufaniem do instytucji publicznych. Badania wykazały, że gdy organy samorządu terytorialnego są transparentne w zakresie przetwarzania danych osobowych, zaufanie obywateli do tych instytucji wzrasta. Wzrost zaufania może również przyczynić się do budowania pozytywnych relacji między organami samorządu terytorialnego a obywatelami, co jest decydujące dla efektywnej administracji publicznej. Aktywna komunikacja i transparentność ze strony organów samorządu terytorialnego w zakresie przetwarzania danych osobowych to istotny element budowy zaufania obywateli i tworzenia pozytywnych relacji.

Zgodność z prawem

Badania potwierdzają, że organy samorządu terytorialnego muszą ściśle przestrzegać przepisów dotyczących ochrony danych, takich jak RODO. Naruszenia tych przepisów mogą prowadzić do poważnych konsekwencji, czyli kar finansowych i spadku zaufania publicznego. Ochrona danych osobowych i usługi publiczne to obszar, który wymaga ciągłego szkolenia, inwestycji w systemy bezpieczeństwa, skoordynowanego działania, transparentności oraz ścisłego przestrzegania przepisów prawa.

Omawiane badania wskazują także na konieczność bezwzględnego przestrzegania przez organy samorządu terytorialnego przepisów dotyczących ochrony danych. Jakiekolwiek naruszenie tych regulacji może prowadzić do poważnych konsekwencji, zarówno prawno-finansowych, jak też wizerunkowych.

Ze względu na ciągłe zmiany w regulacjach oraz rosnące zagrożenia związane z cyberbezpieczeństwem, organy samorządu terytorialnego powinny systematycznie szkolić swoje personel i inwestować w najnowsze systemy bezpieczeństwa w celu zapewnienia skutecznej ochrony danych. W celu zapewnienia skutecznej ochrony danych

niezbędna jest też koordynacja działań między różnymi organami samorządu terytorialnego, a także innymi instytucjami zajmującymi się ochroną danych. Organy samorządu terytorialnego muszą regularnie monitorować i udoskonalać swoje praktyki dotyczące ochrony danych, aby upewnić się, że są one zgodne z prawem.

W wyniku przeprowadzonych badań potwierdzono założone hipotezy. Zatem możemy potwierdzić, że organizacje samorządu terytorialnego, które inwestują w szkolenia i edukację personelu z zakresu ochrony danych osobowych, osiągają wyższy poziom zgodności z przepisami i skuteczności w zarządzaniu danymi, ponieważ pracownicy mają zdecydowanie większą świadomość konieczności ochrony danych osobowych, podwyższają swoje kompetencje prawno-administracyjne i kompetencje cyfrowe. Na zakres oraz poziom bezpieczeństwa cyfrowego danych ma niewątpliwie wpływ skoordynowanie działań administracji publicznej, zwłaszcza współpraca pomiędzy organami samorządu terytorialnego. Przesyłanie danych między takimi instytucjami odbywa się według obowiązujących standardów (w tym zabezpieczeń cyfrowych). Transparentna komunikacja z obywatelami na temat przetwarzania ich danych osobowych zwiększa zaufanie do organów samorządu terytorialnego, podnosi jakość usług publicznych, zwiększa także ogólną świadomość społeczną na temat roli organów samorządu lokalnego, poziomu bezpieczeństwa ich danych osobowych oraz stopnia bezpieczeństwa cyfrowego państwa. Organizacje samorządu terytorialnego, które inwestują w rozwój i wdrażanie skutecznych systemów bezpieczeństwa danych, ograniczają ryzyko naruszenia ochrony danych osobowych, a taka inwestycja mówiąc najprościej zwraca się stosunkowo szybko. Rewolucja cyfrowa, której jako obywatele doświadczamy, niesie z sobą wiele nowych możliwości, ale też zagrożeń. Mówienie w takim kontekście o odpowiednich zabezpieczeniach jest więc w zasadzie oczywistością. W obliczu zwiększających się niebezpieczeństw ataków cyfrowych na Polskę, które pogłębiły się na skutek agresywnej polityki Federacji Rosyjskiej, stopień zabezpieczeń cyfrowych musi być stale wzmacniany. Dotyczy to również działań na poziomie regionalnym. Tak więc rola samorządów w tym zakresie będzie zwiększała swój udział w polityce bezpieczeństwa cyfrowego. Dostrzeganie konieczności ścisłej implementacji przepisów prawnych przez organy samorządu terytorialnego w Polsce jest stosunkowo wysokie. Organizacje samorządu terytorialnego, które ścisłe przestrzegają przepisów dotyczących ochrony danych osobowych, unikają poważnych konsekwencji prawnych i reputacyjnych związanych z naruszeniem tych przepisów, i możemy to z całą mocą potwierdzić na podstawie przeprowadzonych badań.

ZAKOŃCZENIE

W ramach niniejszej rozprawy przeanalizowano i rozważono kluczowe aspekty dotyczące roli i odpowiedzialności organów samorządu terytorialnego w ochronie danych osobowych w kontekście usług publicznych w Polsce. Wnioski te odnoszą się do prawnych, etycznych i praktycznych zagadnień, ukazując wyzwania, przed którymi stoją te instytucje. Weryfikacja postawionych hipotez miała charakter mieszany, co potwierdziły wyniki badań. Pierwsza hipoteza, dotycząca wpływu inwestycji w szkolenia i edukację personelu na skuteczność ochrony danych, została w pełni potwierdzona. Samorządy inwestujące w edukację osiągały lepsze wyniki zgodności z RODO oraz efektywniejsze zarządzanie danymi osobowymi. Druga hipoteza, mówiąca o korzyściach z koordynacji działań między jednostkami samorządowymi, również została potwierdzona – współpracujące organy samorządowe skuteczniej chroniły dane. Trzecia hipoteza, zakładająca, że transparentna komunikacja z obywatelami buduje większe zaufanie, przyniosła mieszane wyniki. Chociaż otwartość sprzyjała budowaniu zaufania, potrzebne są dalsze działania, by poprawić komunikację. Weryfikacja czwartej hipotezy wykazała, że jednostki inwestujące w systemy bezpieczeństwa skuteczniej minimalizowały ryzyko naruszeń, co potwierdza znaczenie nowoczesnych rozwiązań technologicznych w ochronie danych. Ostatnia hipoteza, mówiąca o unikaniu poważnych konsekwencji prawnych przez organizacje przestrzegające przepisów, również znalazła potwierdzenie – badane jednostki, które rygorystycznie przestrzegały RODO, unikały sankcji oraz utraty zaufania społecznego. Wnioski z tej pracy mogą stanowić punkt odniesienia do dalszej dyskusji nad praktyczną stroną wdrażania ochrony danych osobowych w Polsce.

Poczynione w pracy spostrzeżenia ujawniły znaczący zakres odpowiedzialności spoczywającej na organach samorządu terytorialnego w zakresie ochrony danych osobowych. Wiele aktualnych wyzwań z jakimi na bieżąco się spotykają nie znajduje jednak adekwatnych praktycznych rozwiązań, stanowiąc dla nich „biurokratyczne" obciążenie.

W dobie postępującej digitalizacji, zarządzanie informacjami staje się coraz bardziej skomplikowane, a konsekwencje nieprzestrzegania obowiązujących standardów prawnych oraz technologicznych, mogą nieść z sobą niezwykle poważne konsekwencje administracyjne. Zależy to nie tylko od świadomości urzędników zatrudnionych

w strukturach organów samorządowych, lecz w dużej mierze od społecznej edukacji. Stąd też należy systematycznie prowadzić wszelkiego rodzaju działania oświatowe, szkolenia i warsztaty, aby zapewnić ciągłe doskonalenie w zakresie bezpieczeństwa informacyjnego.

Badania przeprowadzone na potrzeby niniejszej rozprawy udowodniły, że egzekwowanie i stosowanie w praktyce zasad ochrony danych często pozostawia wiele do życzenia. Dlaczego tak jest, mogą wyjaśnić dalsze pogłębione badania. Przyczyn tego stanu rzeczy należy upatrywać w stosunkowo późnym, w porównaniu do innych państw unijnych, procesie cyfryzacji administracji publicznej, a co za tym idzie także niskim poziomie kompetencji cyfrowych na poziomie kadr instytucji państwowych, ale także społeczeństwa polskiego. Jednakowoż poziom ten nie był przedmiotem szczegółowych badań niniejszej pracy. Interesowało nas natomiast czy i na ile organy samorządu terytorialnego dążą do doskonalenia procedur związanych z ochroną danych.

Idea autonomii jednostki oraz prawa do prywatności zakłada, że każda osoba ma prawo do kontroli swoich danych osobowych oraz do podejmowania decyzji odnośnie ich gromadzenia, przetwarzania i wykorzystania. To prawo do samostanowienia dotyczy zarówno danych, które są uważane za wrażliwe (takie jak dane medyczne czy informacje o preferencjach seksualnych), jak i ogólnych danych osobowych. Niesie to określone konsekwencje na poziomie etycznym, a więc etyki zawodowej osób zajmujących się zbieraniem, gromadzeniem oraz przetwarzaniem tego typu informacji. Organizacje zaangażowane w powyższe procedury powinny uzyskać zgodę od osób, których dane dotyczą, zanim zaczną dane gromadzić lub przetwarzać w celach określonych w polityce prywatności. Ale, co najistotniejsze, zgoda ta powinna być dobrowolna, świadoma, jednoznaczna i łatwa do wycofania. W związku z tym tworzenie systemów, aplikacji i usług z myślą o ochronie prywatności (tzw. *„privacy by design”*) jest ważnym trybem w poszanowaniu praw człowieka i praw obywatela państwa demokratycznego, stanowi więc potwierdzenie jednej z fundamentalnych wartości humanistycznych, jaką jest wolność. Zgodnie definicją wolność jednostki polega na jej zdolności do podejmowania niezależnych decyzji i wyborów. W kontekście ochrony danych osobowych jednostka ma prawo wybierać, jakie informacje o sobie chce ujawnić, komu i w jakim celu. To daje jej kontrolę nad swoją prywatnością i tożsamością. Ochrona danych osobowych zabezpiecza jednostkę przed nadmiernym nadzorem i ingerencją ze strony organizacji lub władz, jest więc wartością i zdobyczą demokracji. Dlatego dobrze stało się, że prawa te są respektowane zarówno na poziomie krajowym, jak i unijnym.

Płaszczyzna wolności i płaszczyzna prywatności są ściśle ze sobą powiązane. Jednostka ma prawo do własnej przestrzeni prywatnej, co wiąże się również z ochroną danych osobowych, może ona decydować, które informacje na jej temat są dostępne publicznie, a które pozostają prywatne. Poszanowanie autonomii jednostki w zakresie danych osobowych chroni ją przed manipulacją i wpływem innych osób lub organizacji. Dzięki temu dana osoba może podejmować niezależne decyzje, niezakłócone przez nieodpowiednie wykorzystanie jej danych. Jest to niezwykle istotne w kontekście współczesnych technologii i systemów gromadzenia danych, które generują tak liczne zagrożenia ograniczenia wolności. Chociaż etyczny wymiar ochrony danych osobowych nie był głównym przedmiotem niniejszej pracy, akcentujemy go jako niezwykle potrzebny w uwzględnianiu całości podejmowanej problematyki.

Ważnym humanistycznym aspektem przetwarzania danych osobowych jest ochrona wrażliwych informacji dotyczących takich zagadnień, jak np. wyznanie, kolor skóry, orientacja seksualna czy stan zdrowia. Dbanie o poufność ma tutaj ogromne znaczenie w celu zapobiegania przypadkom dyskryminacji, prześladowania czy innego rodzaju nadużyć, na które mogłaby być narażona dana jednostka przypadku ujawnienia takich informacji. Gromadzenie i wykorzystywanie danych osobowych wrażliwych w celach dyskryminacyjnych (lub przestępczych) stanowi przykład rażącego naruszenia zasad etycznych i moralnych. Szantaż oparty na wrażliwych informacjach wiąże się z ryzykiem poważnej szkody emocjonalnej jego ofiary. Świadomość, iż nasze prywatne informacje zostały ujawnione lub są zagrożone ujawnieniem, może powodować duży stres, lęk i depresję. Stąd tak ważne jest, by organizacje i osoby, które gromadzą i przetwarzają wrażliwe dane osobowe, przestrzegały ścisłych standardów prawnych i etycznych. W ramach tych standardów należy zapewnić bezpieczeństwo danych oraz respektować prywatność jednostek. Ponadto, ofiary szantażu powinny być świadome swoich praw, a także wiedzieć o możliwości szukania pomocy oraz wsparcia, jak również zgłaszania tych spraw odpowiednim organom ścigania lub organizacjom zajmującym się prawami człowieka. Szantaż oparty na wrażliwych informacjach jest niezgodny z prawem i narusza podstawowe prawa jednostki.

Ochrona wrażliwych informacji jest więc niezwykle ważna w odniesieniu do ładu społecznego i bezpieczeństwa państwa. Pozwala ona na minimalizowanie ryzyka poważnych przestępstw, ale też nierówności oraz dyskryminacji. Daje także jednostkom sposobność do uczestnictwa w życiu społecznym bez obawy o negatywne konsekwencje wynikające z ujawnienia kontrowersyjnych stron własnej tożsamości czy biografii.

Łamiąc (czy to wskutek niedbalstwa, czy celowo) zasady RODO jednostki samorządu terytorialnego nie tylko narażają się na wysokie kary finansowe, ale także na utratę zaufania społeczności lokalnej. Ta ostatnia konsekwencja jest szczególnie niekorzystna, bowiem organy samorządowe działają na mocy zaufania i akceptacji mieszkańców. Po pierwsze, znacząca utrata zaufania może prowadzić do zaniku legitymizacji tych władz, co znacząco utrudnia realizację ich zadań i projektów. Brak zaufania mieszkańców wiąże się również z ryzykiem bojkotu programów i inicjatyw władz samorządowych. Po drugie, nieufni mieszkańcy mogą być sceptyczni lub niechętni współpracy, co utrudni wdrażanie ważnych projektów. Po trzecie, spadek zaufania społeczności może obniżyć zdolność władz samorządowych do pozyskiwania środków finansowych i przyciągania inwestycji stymulujących rozwój regionu. Przedsiębiorcy mogą być niechętni inwestycjom na obszarach, gdzie brakuje stabilności, a zasady etyczne nie są respektowane. Negatywny wizerunek władz samorządowych obniża reputację regionu odstraszając nie tylko w oczach potencjalnych przedsiębiorców, ale też nowych mieszkańców. Może też powodować odpływ dotychczasowych mieszkańców oraz firm. Jednostka samorządu terytorialnego postrzegana negatywnie nierzadko styka się także z trudnościami w przyciąganiu kompetentnych pracowników do swoich struktur, co w sposób negatywny przekłada się na jakość świadczonych usług. Podobne zaniedbania, w dłuższej perspektywie czasu, narażają gminę na problemy w realizacji celów strategicznych. Stąd tak ważne jest, by jednostki samorządu terytorialnego przestrzegały przepisów RODO i dbały o ochronę danych osobowych mieszkańców, co sprzyja budowaniu zaufania i dobrych relacji ze społecznością lokalną. Zaufanie stanowi jeden z fundamentalnych elementów kapitału społecznego, który umożliwia poprawne funkcjonowanie organów samorządowych.

Rozważania wokół problematyki ochrony danych pozwalają dostrzec potencjalne konflikty wartości, jakie mogą zaistnieć przy okazji przetwarzania tego typu informacji. Konflikt może zaistnieć na płaszczyźnie ścierania się interesów prywatnych oraz interesu ogółu, np. w sytuacji, gdy powstaje napięcie między prywatnością jednostki a dobrem wspólnym. Powstaje tutaj dylemat, czy i w jakim zakresie naruszanie prywatności jednostek da się uzasadnić w imię dobra wspólnego pod postacią bezpieczeństwa publicznego lub innych celów społecznych. Centralnym elementem rozważań w tym obszarze jest znalezienie właściwej równowagi między dwiema ważnymi wartościami: prywatność jednostki i dobro wspólne. Dobro wspólne odnosi się do ogólnych korzyści i interesów społeczeństwa. Pojęcie to może obejmować sferę bezpieczeństwa

publicznego, zdrowia publicznego i wielu innych obszarów, w których działania władz centralnych lub organizacji samorządowych służą ogólnemu dobru. Rozstrzygnięcie tego dylematu wymaga znalezienia odpowiedzi na szereg pytań: na przykład czy naruszenie prywatności w danym przypadku jest proporcjonalne do pożądanego celu społecznego? Innymi słowy, czy środki podjęte w celu ochrony dobra wspólnego są uzasadnione w kontekście naruszenia prywatności? Czy działania podejmowane w imię dobra wspólnego są niezawodne i przejrzyste? Czy są odpowiednio regulowane i nadzorowane? Jakie środki są podejmowane, aby chronić prawa i wolności jednostki w przypadku naruszania prywatności? Czy istnieją mechanizmy odwoławcze i kontrole, które zapewniają, że naruszenia są minimalizowane i nadzorowane? Czy istnieje społeczny konsensus lub szerokie poparcie dla naruszania prywatności w celu ochrony tego konkretnego dobra wspólnego? Czy decyzje w tym konkretnym przypadku zostały podjęte w sposób demokratyczny i partycypacyjny? Czy dysponujemy nowoczesnymi technologiami i narzędziami, pozwalającymi ochronić dobro wspólne bez konieczności naruszania prywatności? Powyższy dylemat stanowi przykład skomplikowanego i kontrowersyjnego zagadnienia, które jest przedmiotem wielu debat oraz dyskusji zarówno na poziomie etycznym, jak też prawnym. Oczywiście nie jesteśmy w stanie odpowiedzieć na nie tutaj w zadowalający sposób, sugerujemy jedynie dalsze kierunki dyskusji nad omawianą problematyką.

Podobnie zagadnieniem otwartym jest przyszłość ochrony danych osobowych w kontekście dalszego postępu technologicznego, na przykład sztucznej inteligencji. Sztuczna inteligencja może również pomóc w: tworzeniu bardziej zaawansowanych metod szyfrowania danych oraz w ich monitorowaniu w celu zapewnienia, że pozostają one bezpieczne przed nieautoryzowanym dostępem; identyfikowaniu ryzyka związanego z przechowywaniem danych w tzw. chmurze; zarządzaniu dostępem do danych w czasie rzeczywistym; zaawansowanej identyfikacji i uwierzytelniania użytkowników (np. poprzez rozpoznawanie twarzy, biometryczne metody uwierzytelniania czy analizę zachowań użytkowników w celu wykrywania nieprawidłowości);w wykrywaniu nadużyć i oszustw, zarówno w sferze finansowej, jak i handlowej (np. poprzez analizę transakcji, monitorowanie zachowań klientów czy wykrywanie fałszywych informacji); edukowaniu użytkowników i pracowników na temat ochrony danych osobowych, identyfikacji potencjalnych zagrożeń oraz praktyk bezpieczeństwa. W miarę ewolucji sztucznej inteligencji jej rola w ochronie danych osobowych będzie prawdopodobnie się zwiększać. Dlatego jej modernizowanie i wykorzystywanie w strategicznych obszarach

życia państwa musi być prowadzone w sposób etyczny i zgodny z przepisami prawnymi, aby zapewnić skuteczną ochronę interesu społecznego.

Przedstawione analizy nie wyczerpują oczywiście całej złożoności poruszanego problemu, a stanowią jedynie wstęp do dalszych badań. Znalezienie skutecznych, niezawodnych metod radzenia sobie z wyzwaniami związanymi z ochroną danych osobowych w stale zmieniającym się świecie nowych technologii wymaga ogromnej pracy specjalistów, reprezentujących różne dyscypliny naukowe. Bez wątpienia więc istnieje potrzeba dalszych badań, które skupią się na wpływie nowych technologii na ochronę danych osobowych oraz na praktycznych konsekwencjach zmian w polityce bezpieczeństwa publicznego.

BIBLIOGRAFIA

Akty prawne:

Urząd Ochrony Danych Osobowych, https://uodo.gov.pl/pl (dostęp: 20.10.2023).

Ustawa z dnia 14 czerwca 1960 roku Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572).

Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej, https://www.traple.pl/ustawa-o-ochronie-danych-osobowych-chinskiej-republiki-ludowej/ (dostęp: 17.03.2024).

Ustawa z dnia 23 kwietnia 1964 roku Kodeks cywilny (Dz.U. z 2023 r., poz. 610 z późn. zm.).

Ustawa z dnia 26 czerwca 1974 roku Kodeks pracy (Dz.U. z 2023 r., poz. 1465).

Ustawa z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2023 r., poz. 40 z późn. zm.).

Ustawa z dnia 4 marca 1994 roku o zakładowym funduszu świadczeń socjalnych (Dz.U. z 2024 r., poz. 288).

Ustawa z dnia 6 czerwca 1997 roku Kodeks karny (Dz.U. z 2024 r., poz. 17 z późn. zm.).

Ustawa z dnia 5 czerwca 1998 roku o samorządzie powiatowym (Dz.U. z 2024 r., poz. 107).

Ustawa z dnia 5 czerwca 1998 roku o samorządzie województwa (Dz.U. z 2022 r. poz. 2094 z późn. zm.).

Ustawa z dnia 24 lipca 1998 roku o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz.U. Nr 96, poz. 603 z późn. zm.).

Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r., poz. 344).

Ustawa z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz.U. z 2024 r., poz. 34).

Ustawa z dnia 23 stycznia 2009 roku o wojewodzie i administracji rządowej w województwie (Dz.U. z 2023 r., poz. 190).

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

Ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r., poz. 1206).

Ustawa z dnia 21 lutego 2019 roku o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego 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. z 2019 r., poz.730).

Ustawa z dnia 11 września 2019 roku Prawo zamówień publicznych (Dz.U. z 2023 r., poz. 1605 z późn. zm.).

Ustawa z dnia 11 marca 2022 roku o obronie Ojczyzny (Dz. U. z 2024 r., poz. 248 z późn. zm.).

Rozporządzenie Ministra Edukacji i Nauki z dnia 11 października 2022 roku w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2022 r., poz. 2202 z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz. Urz. UE L 119.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, a także uchylenia dyrektywy 95/46/WE – ogólne rozporządzenie o ochronie danych (Dz.U.UE.L.2016.119.1 z dnia 4 maja 2016 roku).

Literatura:

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Ochrona danych osobowych w wybranych państwach Azji*, Wrocław 2019.

Adamowicz M., Skarżyńska P., *Rola samorządu lokalnego w realizacji zadań oświatowych na przykładzie samorządu gminy Szelków*, „Annales Universitatis Mariae Curie-Sklodowska, Sectio K", nr 2/2027.

Antipov G.A., *Traditions, innovations and social evolution*, „Scientific notes of the Crimean Federal University named after V.I. Vernadsky. Philosophy. Political science. Culturology", nr 1/2015.

Aronson E., Wilson T. D., Akert R. M., *Psychologia społeczna*, tł. J. Gilewicz, Poznań 2006.

Bajer J., *Badania porównawcze w politologii: zagadnienia metodologiczne*, „Studia Politicae Universitatis Silesiensis", nr 8/2012.

Baker D., Evans W., *Trends, Discovery, and People in the Digital Age*, Woodhead Publishing Limited, Stawston 2013.

Bardach J., Leśnodorski B., Pietrzak M., *Historia ustroju i prawa polskiego*, Warszawa 2010.

Barcik J., Srogosz T., *Prawo międzynarodowe publiczne*, Warszawa 2014.

Besemer L., *Privacy and data protection*, Van Haren Publishing, 's-Hertogenbosch 2020.

Berdieva U.A., *Developement of the Digital economy*, „Economics And Business: Theory And Practice", nr 2-1(72)/2021.

Bielecki J., *Poczucie pewności siebie i potrzeba bezpieczeństwa u jąkających się przed terapią i po terapii*, „Studia Psychologica", nr 2/2001.

Błażewski M., J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018.

Borecka J., *Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych*, „Zeszyty Naukowe Instytutu Administracji Akademii im. Jana Długosza w Częstochowie, z. IV/2006".

Brzeziński B., *Complexity of Tax Law: The Anglosaxon Point of View,* „Comparative Law Review", nr 16/2016.

Bożyk S., *Prawo konstytucyjne*, Białystok 2014.

Buko J., *Wprowadzenie do zarządzania informacją w przedsiębiorstwach usługowych*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego", nr 650, 2011.

Bukowski Z., Jędrzejewski T., Rączka P., *Ustrój samorządu terytorialnego*, Toruń 2003.

Bygrave, L.A., *Data Privacy Law: An International Perspective*, Oxford University Press 2014.

Carapola A., *The Data Center Builder's Bible - Book 1: Defining Your Data Center Requirements: Specifying, Designing, Building and Migrating to New Data Centers*, Washington 2018.

Castells M., *The Rise of the Network Society 1*, Wiley-Blackwell, Hoboken 1996.

Celarek K., *Ochrona danych osobowych a rozwój społeczeństwa informacyjnego*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego", nr 703, 2012.

Celarek K., *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego,* Warszawa 2013.

Chrzanoski M., *Podstawowe zasady prawa wyborczego do organów stanowiących jednostek samorządu terytorialnego*, Białystok 2018.

Commission of the European Communities (2019), *The Role of Local Government in Local Development*,.

Dąbrowski K., *Nauka o administracji*, Ryki 2012.

Dudzik I., Nowak S., *Rola wartości w życiu współczesnego człowieka. Na podstawie przeprowadzonych badań własnych*, [w:] I. Dudzik, B. Czuba, K. Rejman (red.), *Rola wartości etycznych we współczesnym świecie. Wartości etyczne współczesnego człowieka, część I*, Jarosław 2017.

Duran V.C., *Environmental degradation in the world and measures taken by the world community to prevent it*, „Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences", nr 1/2000.

Europejski Kodeks Dobrej Administracji, przyjęty przez Parlament Europejski w dniu 6 września 2001 r., [w:] B. Jastrzębski (red.), *Z teorii i praktyki funkcjonowania administracji publicznej w III RP*, Płock 2007.

Fajgielski P., *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych*, Warszawa 2022.

Filek J., *W poszukiwaniu dobrej administracji*, „Zarządzanie Publiczne", nr 2(2), 2007.

Florek L., *Prawo pracy*, Warszawa 2015.

Frąckowiak J., *Miejsce prawa handlowego w systemie prawa i sposoby jego regulacji*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji", CXXI, Wrocław 2020.

Fritch J.W. , Mandernack S.B. , *The emerging reference paradigm: A vision of reference services in a complex information environment,, Library Trends, 50 (2), 2001.*

Goban-Klas T., *Media i komunikowanie masowe: teorie i analizy prasy, radia, telewizji i Internetu,*Warszawa 2005.

Garner R., P. Ferdinand, S. Lawson, *Introduction to Politics*, Oxford 2009.

Golka M., *Dokąd zmierza cywilizacja zachodnia?*, „Przegląd Zachodni", nr 4/2017.

Gonschior A., *Ochrona danych osobowych a prawo do prywatności w Unii Europejskiej,* [w:] *Aktualne problemy Unii Europejskiej i prawa międzynarodowego – aspekty teoretyczne i praktyczne,* red. D. Kombis-Romanowska, Wrocław 2017.

Hebda J., *Z sołtysem i wójtem przez wieki. Opowieść o dziejach urzędu sołtysa i wójta w Polsce*, Tarnów–Warszawa 2016.

Hunziker S., *Enterprise Risk Management*, Cham 2021.

Isaev V.A., *Medicine of the future and healthcare*, „Vladimir farmer", nr 3/2011.

Izdebski J., *Metody badań nauk społecznych w nauce prawa administracyjnego*, „Roczniki Nauk Prawnych", nr 4.2021.

Jagielski J., *Kolegialność i jednoosobowość w strukturach samorządu terytorialnego*, „Studia Iuridica", nr 85/2020.

Janosiewicz W., *Samorząd terytorialny w Polsce – zarys historyczny*, „Homo Politicus", nr 13/2018.

Jastrzębski B., *Z teorii i praktyki funkcjonowania administracji publicznej w III RP*, Płock 2007.

Juszczyk G., Lubiński R., *Scenariusze w ochronie zdrowia w Europie w latach 2012-2030*, [w:] M. Pasowicz (red.), *Zdrowie i medycyna – wyzwania przyszłości*, Kraków 2013.

Kawa M., *Tendencje rozwoju handlu elektronicznego*, „Przedsiębiorczość – Edukacja", nr 1/2022.

Kabus J., *Uwarunkowania rozwoju lokalnego na przykładzie powiatu częstochowskiego*, Częstochowa 2016.

Kangas A., *Cultural policy and cultural diversity*, International Encyclopedia of Civil Society 2010.

Kierunki działań strategicznych Ministra Cyfryzacji w obszarze informatyzacji usług publicznych, Ministerstwo Cyfryzacji 2016.

Kiselev V.A., *About future Wars*, „Military Thought", nr 2/2008.

Kluszczyński R., *Społeczeństwo informacyjne. Cyberkultura. Sztuka mulimediów*, Rabid, Kraków 2001.

Kolin K.K., *Information culture in the information society*, „Open Education", nr 6/2006.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku (Dz.U. Nr 78, poz. 483 z późn. zm.).

Kot S. M., *Nierówności ekonomiczne i społeczne a zasady sprawiedliwości dystrybutywnej*, „Nierówności Społeczne a Wzrost Gospodarczy", nr 4/2004.

Koźmiński A. K., Jemielniak D., *Zarządzanie od postaw*, Warszawa 2011.

Kożusznik B., *Zachowania człowieka w organizacji*, Warszawa 2014.

Krasuski A., *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy,* Warszawa 2012.

Krasuski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018.

Kubiński P., Wołoszko A., *Wybrane zagadnienia prawa cywilnego. Stan prawny na 1 lipca 2012 r.*, Szczytno 2012.

Lachowski J., Marek A., *Prawo karne. Zarys problematyki*, Warszawa 2021.

Leoński Z., *Samorząd terytorialny w RP*, Warszawa 2001.

Leszczyński M., *Samorząd terytorialny w zapewnieniu bezpieczeństwa społecznego*, Kielce 2021.

Lorek M., Pieczywok A., *Rola edukacji dla bezpieczeństwa w kontekście zagrożeń cyberprzestępczością*, „Edukacja – Technika – Informatyka" nr 1/2019.

Lubasz D., *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Warszawa 2018.

Łakomy J., *Interdyscyplinarność i integracja zewnętrzna nauk prawnych w świetle postmodernistycznej krytyki*, „Archiwum Filozofii Prawa i Filozofii Społecznej, nr 1/2011.

Łukaszuk A., *Problematyka kompetencji cyfrowych kadr administracji publicznej jako istotnego czynnika transformacji cyfrowej jednostek samorządu terytorialnego w Polsce*, „Studia Prawnoustrojowe", nr 58, 2022.

Martuszewska J., *Potrzeby edukacji dla bezpieczeństwa społeczności lokalnej – aspekt aksjologiczny, psychologiczny oraz wybrane aspekty normatywne*, Szczecin 2019.

Mastalski R., *Prawo podatkowe*, Warszawa 2018.

Matwiejuk J., *Samorząd terytorialny w Polsce*, [w:] M. Perkowski, J. Szymański, M. Zdanowicz (red.), *Człowiek i prawo międzynarodowe. Księga dedykowana Profesorowi Bogdanowi Wierzbickiemu*, Białystok 2014.

Melnikova E.V., *The influence of stressful situations on human health,* „Bulletin of Magistracy", nr 4/2022.

Muras S., *Podstawy prawa*, Warszawa 2017.

Ndreca A., *Poczucie bezpieczeństwa a relacje interpersonalne u małżonków*, Nowy Sącz 2013.

Ochendowski E., *Prawo Administracyjne*, Toruń 2006.

Olender A., *Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w podmiotach sektora publicznego*, „Wschód Europy", vol. 6, 2/2020.

Pałka P., *Ciało obce: zasady RODO a gospodarka rynkowa*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny", nr 5(11)/2022.

Plan działania UE na rzecz administracji elektronicznej na lata 2016-2020, Przyspieszenie transformacji cyfrowej w administracji, Bruksela 19.04.2016.

Podrez E., *Sprawiedliwość – między utopią i kompromisem,* [w:] *Czy sprawiedliwość jest możliwa?* red. D. Probucka, Kraków 2008.

Podręcznik ds. Ochrony Danych, Biuro Rzecznika Praw Obywatelskich, Warszawa 2019.

Regulski J., *Samorząd III Rzeczypospolitej*, Warszawa 2000.

Rogoż S., *Praktyczne aspekty kształtowania pożądanych postaw etycznych*, „Palestra", nr 19/5-6(209-210) 1975.

Rzucidło J., *Prawo do prywatności i ochrona danych osobowych,* [w:] *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym,* red. M. Jabłoński, Wrocław 2014.

Salamon L.M., *The Tools of Government in the Digital Age*, Palgrave Macmillan 2015.

Sikorski Cz., *Kultura organizacyjna. Efektywne wykorzystanie możliwości swoich pracowników*, Warszawa 2006.

Sinchuk Y.V., *Lectures on political science*, Moscow 2015.

Skorodumova O.B., *Scientific and technological progress and globalization: achievements and risks*, „Symbol of Science", nr 2/2016.

Sobota J., *Klęska futurologii*, „Szkice Humanistyczne" nr 1-2/2003.

Solove D.J., *Understanding Privacy*, Harvard University Press, 2008.

Stawicki R., *Samorząd terytorialny w II Rzeczypospolitej – zarys prawno-historyczny*, Kancelaria Senatu, Warszawa 2015.

Stoiński A., *Idea sprawiedliwości społecznej. Wstępna klasyfikacja znaczeń*, Wydawnictwo UWM, Olsztyn.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2020.

Strzebinczyk J., *Prawo rodzinne*, Warszawa 2013.

Starościak J., *Decentralizacja administracji*, Warszawa 1960.

Sun Zi i jego Sztuka wojny. Filozofia i praktyka oddziaływania na bieg zdarzeń, red. P. Plebanek, Kraków 2020.

Szabłowska A., *Gmina jako podstawowa jednostka samorządu terytorialnego: organizacja i funkcjonowanie gminy*, Ostrołęka 2004.

Szołno-Koguc J., *Samodzielność dochodowa jednostek samorządu terytorialnego – aspekty teoretyczne*, „Studia BAS", nr 1/2021.

Szreniawski J., *Prawo administracyjne. Część ogólna*, Lublin 1993.

Tarno J., *Samorząd terytorialny po reformie ustrojowej państwa*, [w:] A. Sobkow-Haber (red.), *Projekty konstytucyjne 1989-1991*, Warszawa 2000.

Śmietanka T., *Zarządzanie rozwojem lokalnym jako współczesna determinanta jakości życia w gminach (badania pilotażowe w wybranych gminach miejsko – wiejskich w Polsce)*, Radom 2020.

Taylor A., Alexander D., Finch A., Sutton D., *Security Management Principles*, Swindon 2020.

Vinogradova M., Ayzler P.P., *Outlook on mastering of kosmos*, „Norwegian Journal of Development of the International Science", nr 56 /2021.

Višnić T., *Access to Culture in the European Union*, „European Journal of Cultural Policy" 2017.

Wilkin J., *Komu potrzebne są nauki społeczne? Nauki społeczne w polskiej i europejskiej przestrzeni badawczej oraz w rozwiązywaniu problemów rozwoju*, „Nauka", nr 4/2012.

Witkowski K., *Inwestycje infrastrukturalne w realizacji usług publicznych*, „Studia Lubuskie: prace Instytutu Prawa i Administracji Państwowej Wyższej Szkoły Zawodowej w Sulechowie", nr 7/2011.

Wojciechowski L., *Bezpieczeństwo informacji w polskim samorządzie terytorialnym na tle procesu ujednolicenia systemu ochrony danych osobowych w Unii Europejskiej*, „Rocznik Administracji Publicznej", nr 5/2019.

Wróbel P., *Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia*, PME, nr 4, 2017.

Wojtaszczyk K.A., *Granice nauki o polityce jako dyscypliny naukowej*, „Politeja", nr 4 (36) 2015.

Wyszkowa D., *Samorząd terytorialny w ujęciu wybranych koncepcji teoretycznych*, Białystok 2018.

Zieleniewski J., *Organizacja i zarządzanie*, Warszawa 1960.

Zuboff S., *The age of surveillance capitalism, The fight for a human future at the new frontier of power*, Profile Books, Londyn 2019.

Żebrowski W., *Metody badawcze stosowane w politologii*, „Szkice Humanistyczne", t. XII, nr 2, 2012.

Źródła internetowe:

About the OPC, https://www.priv.gc.ca/en/about-the-opc/ [dostęp: 20.03.2024].

About the OPC. What we do, https://www.priv.gc.ca/en/about-the-opc/what-we-do/ [dostęp: 20.03.2024].

Administrator danych osobowych w sektorze publicznym, https://samorzad.infor.pl/sektor/organizacja/rodo-2018/3001763,Administrator-danych-osobowych-wsektorze-publicznym.html [dostęp: 06.10.2023].

Anonimizacja, https://www.nask.pl/pl/dzialalnosc/anonimizacja/5168,Nowa-usluga-anonimizacji-dokumentow.html [dostęp: 20.10.2023].

Australijska Ustawa o ochronie prywatności, https://www.atlassian.com/pl/trust/compliance/resources/australia-privacy-act [dostęp: 16.03.2024].

Bender D., *GDPR harmonization: Reality or myth?*, https://iapp.org/news/a/gdpr-harmonization-reality-or-myth/ [dostęp: 30.03.2024].

DLA Piper, *Australia: Long awaited Australian privacy reform comes to fruition,* https://privacymatters.dlapiper.com/2024/09/australia-long-awaited-australian-privacy-reform-comes-to-fruition/ [dostęp: 14.09.2024].

Blokowanie reklam, https://www.programosy.pl/kategoria,blokowanie_reklam,1,1.html [dostęp: 20.10.2023].

Brazylijska ogólna ustawa o ochronie danych-LGPD, https://www.ibm.com/docs/pl/order-management?topic=regulations-brazilian-general-data-protection-law-lgpd [dostęp: 17.03.2024].

Buczkowska W., *Stalking - co to jest stalking, aspekty prawne nękania, jak się bronić przed prześladowcą?*, https://portal.abczdrowie.pl/stalking [dostęp: 02.10.2023].

Calzada I., *Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law* (PIPL), https://www.mdpi.com/2624-6511/5/3/57 [dostęp: 15.09.2024].

Co to jest firewall? Jak działa zapora sieciowa?, https://bezpiecznyinternet.edu.pl/co-to-jest-firewall-i-jak-dziala/ [dostęp: 20.10.2023].

Co to jest Gmina?, https://radomyslwielki.pl/informacje-o-gminie/co-to-jest-gmina.html [dostęp: 07.10.2023].

Co to jest IoT, https://www.oracle.com/pl/internet-of-things/what-is-iot/ [dostęp: 06.10.2023].

Communication studies, https://en.wikipedia.org/wiki/Communication_studies [dostęp: 15.10.2023].

Cyberataki – co powinieneś o nich wiedzieć?, https://szybkafaktura.pl/blog/cyberataki-co-powinienes-o-nich-wiedzec/ [dostęp: 20.03.2024].

Czego dotyczy ogólne rozporządzenie o ochronie danych (RODO)?, https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_pl [dostęp: 20.10.2023].

Czym są usługi społeczne, https://cusmyslenice.pl/uslugi/czym-sa-uslugi-spoleczne [dostęp: 06.10.2023].

Dane biometryczne, https://gdpr.pl/artykuly/dane-biometryczne [dostęp: 04.10.2023].

E-usługi w administracji, [w:] Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/e-uslugi [dostęp: 02.10.2023].

Falkowski P., *Ochrona danych osobowych w Sądzie Najwyższym*, https://www.sn.pl/informacjepraktyczne/SitePages/Ochrona_danych_osobowych.aspx [dostęp: 20.10.2023].

Filtry antyspamowe, https://www.i-host.pl/pomoc/pl/poczta_elektroniczna/filtry_antyspamowe [dostęp: 20.10.2023].

Fraser M. , *Australia szykuje reformę ochrony danych. Prywatność w rękach obywateli?*, https://cyber defence24.pl/prywatnosc/australia-szykuje-reforme-ochrony-danych-prywatnosc-w-rekach-obywateli [dostęp: 16.03.2024].

Generalny Inspektor Ochrony Danych Osobowych, http://encyklopediaap.uw.edu.pl/index.php/Generalny_Inspektor_Ochrony_Danych_Osobowych [dostęp: 20.10.2023].

Global Privacy & Security Compliance Law Blog, *India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison,* https://www.globalprivacyblog.com/2023/12/indias-digital-personal-data-protection-act-2023-vs-the-gdpr-a-comparison/ [dostęp: 12.09. 2024].

Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce w 2021 roku*, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2021-roku,2,11.html [dostęp: 02.10.2023].

Hill M., *The biggest data breach fines, penalties, and settlements so far*, https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html [dostęp: 20.03.2024].

ISBnews, *W 2022 roku Polacy znów chętniej korzystali z zakupów online [RAPORT]*, https://forsal.pl/biznes/handel/artykuly/8663815,ecommerce-opinionway-barometr.html [dostęp: 02.10.2023].

Ivanitska Y., Kokoszka K., Kapcio V., *Socjologia*, https://mfiles.pl/pl/index.php/Socjologia [dostęp: 20.10.2023].

Jędruszczak K., *Prywatność w różnych kulturach*, http://www.psychologia.net.pl/artykul.php?level=90 [dostęp: 20.10.2023].

Kary RODO, https://orodo.pl/kary-rodo/ [dostęp: 20.03.2024].

Kary za naruszenie RODO, https://gdpr.pl/artykuly/kary-za-naruszenie-rodo [dostęp: 02.10.2023].

Kataster nieruchomości, https://encyklopedia.pwn.pl/haslo/kataster-nieruchomosci; 3921129.html [dostęp: 03.10.2023].

Kawecki M., *Ochrona danych osobowych nową dziedziną prawa?* „Europejski Przegląd Sądowy", nr 5, 2017, https://www.prawo.pl/prawnicy-sady/ochrona-danych-osobowych-nowa-dziedzina-prawa,70908.html [dostęp 28.05.2024].

Klitenic A., Eige K., *Maybe This Time: Federal Government Proposes the American Data Privacy and Protection Act*, https://www.dataprotectionreport.com/ 2022/06/maybe-this-time-federal-government-proposes-the-american-data-privacy-and-protection-act/ [dostęp: 20.03.2024].

Koch R., *What is considered personal data under the EU GDPR?*, https://gdpr.eu/eu-gdpr-personal-data/ [dostęp: 20.03.2024].

Kodeks Etyki dla Inspektorów Ochrony Danych przyjęty Uchwałą Nadzwyczajnego Walnego Zgromadzenia SABI – Stowarzyszenia Inspektorów Ochrony Danych w dniu 30 stycznia 2018 r., https://sabi.org.pl/kodeks-etyki/ [dostęp: 19.10.2023].

Kraskowska D., *Brazylijska ustawa LGPD - nowy akt prawny na temat ochrony prywatności*, https://www.politykabezpieczenstwa.pl/pl/a/brazylijska-ustawa-lgpd-nowy-akt-prawny-na-temat-ochrony-prywatnosci [dostęp: 17.03.2024].

Kuta W., *Zieliński: Dobra współpraca samorządów z lekarzami POZ ułatwia skuteczną profilaktykę*, https://www.rynekzdrowia.pl/Polityka-zdrowotna/Zielinski-Dobrawspolpraca-samorzadow-z-lekarzami-POZ-ulatwia-skuteczna-profilaktyke,233486,14.html [dostęp: 06.10.2023].

Liwszic P., *Naruszenie RODO to naruszenie prawa do prywatności – art. 82 RODO*, https://judykatura.pl/naruszenie-rodo-to-naruszenie-prawa-do-prywatnosci-art-82-rodo/ [dostęp: 20.10.2023].

Łesak D., *Inspektor Ochrony Danych Osobowych – kiedy jest potrzebny?*, https://poradnikprzedsiebiorcy.pl/-inspektor-ochrony-danych-osobowych-kiedy-jest-potrzebny [dostęp: 18.10.2023].

Mango M., *Understanding US Data Privacy Law Fines*, https://www.clarip.com/blog/understanding-us-data-privacy-law-fines/ [dostęp: 20.03.2024].

Ministerstwo Cyfryzacji, *Cyberbezpieczeństwo*, https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo [dostęp: 20.03.2024].

Ministerstwo Cyfryzacji, *Rewolucja w systemie ochrony danych osobowych*, http://archiwum.mc.gov.pl/aktualnosci/rewolucja-w-systemie-ochrony-danych-osobowych [dostęp: 20.10.2023].

Model społeczeństwa informacyjnego. Daniel Bell i Alvin Toffler – teoretycy społeczeństwa informacyjnego, http://pcserwis.waw.pl/teoretycy.html [dostęp: 01.10.2023].

Modo O., *Ochrona danych w Afryce*, https://gov.legalis.pl/ochrona-danych-w-afryce/ [dostęp: 17.03.2024].

Modo O., *Republika Południowej Afryki obiera kurs na ochronę danych*, https://gov.legalis.pl/republika-poludniowej-afryki-obiera-kurs-na-ochrone-danych/ [dostęp: 17.03.2024].

MQX Polska Sp. z o.o., *Prawo do prywatności i ochrona danych osobowych w USA*, https://ochronasygnalistow.com.pl/baza-wiedzy/prawo-prywatnosci-i-bezpieczenstwa-danych-w-usa/ [dostęp: 20.20.2023].

Nauki prawne, https://ususirk.amu.edu.pl/pl/offer/SD-2023/programme/SD-NP/?from=field: DS010507N [dostęp: 13.3.2024].

Ochrona danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-przetwarzanych-w-zwiazku-z-zapobieganiem-i-18807130 [dostęp: 06.10.2023].

Ochrona danych osobowych: podobieństwa i różnice w europejskim prawie, https://www.rp.pl/prawo-w-firmie/art3063051-ochrona-danych-osobowych-podobienstwa-i-roznice-w-europejskim-prawie [dostęp: 20.10.2023].

Ochrona danych w UE. Ogólne rozporządzenie o ochronie danych, dyrektywa o ochronie danych w sprawach karnych i inne przepisy dotyczące ochrony danych osobowych, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_pl [dostęp: 20.10.2023].

PAP, *Kanada: Obawy o bezpieczeństwo danych osobowych podczas pandemii*, https://www.gazetaprawna.pl/wiadomosci/artykuly/1492501,kanada-pandemia-

koronawiurs-bezpieczenstwo-danych-osobowych-osob-zakazonych.html [dostęp: 16.03.2024].

Parlament Indii uchwala ustawę o ochronie cyfrowych danych osobowych z 2023 r., https://www.consentmanager.pl/wiedza/indie-ustawa-cyfrowa-o-ochronie-danych-osobowych-2023/ [dostęp: 17.03.2024].

Pogłód M., *Prawo pracy: dynamiczne czy statyczne?*, https://www.prawo.pl/prawnicy-sady/prawo-pracy-dynamiczne-czy-statyczne,27858.html [dostęp: 20.03.2024].

Prezes Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl/544/996 [dostęp: 18.10.2023].

Prokuratura ukarana za naruszenie RODO, https://www.rp.pl/dane-osobowe/art38453021-prokuratura-ukarana-za-naruszenie-rodo [dostęp: 20.10.2023].

Przegląd technik kryptograficznych w zabezpieczaniu urządzeń elektronicznych, https://elektronikab2b.pl/technika/35771-przeglad-technik-kryptograficznych-w-zabezpieczaniu-urzadzen-elektronicznych [dostęp: 20.10.2023].

Sandej M., *Jednostki samorządu terytorialnego mają zadania w zakresie ochrony zdrowia*, https://www.prawo.pl/samorzad/zadania-samorzadu-terytorialnego-w-zakresie-ochrony-zdrowia,77385.html [dostęp: 06.10.2023].

Sewastianowicz M., *Rodzaje wykładni prawa*, https://www.prawo.pl/student/rodzaje-wykladni-prawa,500020.html [dostęp: 20.03.2024].

Sikora-Kobyliński W., *Czym są IDS?*, https://students.mimuw.edu.pl/SO/Projekt04-05/temat5-g2/sikora-kobylinski/idsips.html [dostęp: 20.10.2023].

Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, http://www.repozytorium.uni.wroc.pl/Content/66149/32_Wieslaw_Smolski.pdf [dostęp: 22.01.2022].

Sobczak K., *Dr Proksa: Kłopoty z RODO to skutek naszych opóźnień*, https://www.prawo.pl/prawo/rodo-dlaczego-sa-problemy-z-wdrazaniem,313074.html [dostęp: 20.03.2024].

Sobiech L., *Zadania samorządu terytorialnego w działalności oświatowej*, https://samorzad.infor.pl/sektor/zadania/oswiata/388784,Zadania-samorzadu-terytorialnego-w-dzialalnosci-oswiatowej.html [dostęp: 06.10.2023].

Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)*, https://core.ac.uk/download/pdf/33187346.pdf [dostęp: 30.05.2024].

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019, https://uodo.gov.pl [dostęp: 20.10.2023].

Standardy transparentności administracji publicznej w państwie demokratycznym, https://administracjapodkontrola.pl/aktualnosci/standardy-transparentnosci-administracji-publicznej-w-panstwie-demokratycznym/ [dostęp: 20.10.2023].

Starzenie się społeczeństwa – wyzwanie dla rynku pracy, aktywizacja pracowników 50+. Raport tematyczny, https://www.parp.gov.pl/storage/publications/pdf/Starzenie_sie_spoleczenstw.pdf [dostęp: 20.03.2024].

Statut SABI – Stowarzyszenia Inspektorów Ochrony Danych. Tekst jednolity uwzględniający zmiany dokonane na Walnym Zgromadzeniu członków Stowarzyszenia dnia 26 maja 2010 r., dnia 24 czerwca 2010 r., dnia 30 stycznia 2018 r. i dnia 10 czerwca 2021 roku, https://sabi.org.pl/statut-sabi-stowarzyszenia-inspektorow-ochrony-danych/ [dostęp: 19.20.2023].

Strzelecki J., *RODO w Chinach - polska firma będzie musiała uzyskać zgodę Chińczyka*, https://firma.rp.pl/chiny/art19049501-rodo-w-chinach-polska-firma-bedzie-musiala-uzyskac-zgode-chinczyka-dane-osobowe-chinskie-RODO [dostęp: 17.03.2024].

Studia online w Warszawie 2023, https://www.otouczelnie.pl/miasto_dzial/11663/Studia-online-w-Warszawie [dostęp: 02.10.2023].

Subbotina L.Y., *What is meant by the state of personal security*, https://psy.su/feed/10218/ [dostęp: 06.10.2023].

Szyfrowanie połączenia (SSL/TLS), https://www.oki.com/printing/online-manuals-Z016/EE8001-1215/id/contents/contents/70553341.html [dostęp: 20.10.2023].

Szymaniak T., *Powiat – definicja i charakterystyka. Co to jest powiat?*, https://procredito.pl/publikacje/definicje-finansowe/509-powiat [dostęp: 07.10.2023].

Świderska-Piksa N., *Audyt RODO – Jak powinien wyglądać i kiedy go przeprowadzać*, https://rpms.pl/audyt-rodo-jak-powinien-wygladac-i-kiedy-go-przeprowadzac/ [dostęp: 20.10.2023].

The Japan Act on the Protection of Personal Information Explained, https://www.delphix.com/glossary/japan-act-protection-of-personal-information [dostęp: 16.03.2024].

Traczyk W., *Niezbędne inwestycje w poprawę produktywności*, https://magazynprzemyslowy.pl/artykuly/niezbedne-inwestycje-w-poprawe-produktywnosci [dostęp: 02.10.2023].

Unia Europejska pilnuje prywatności. 1,2 mld dol. kar za naruszenie RODO. Polska na 13. Miejscu, https://www.wirtualnemedia.pl/artykul/unia-europejska-rodo-gdpr-prywatnosc-kary [dostęp: 15.03.2024].

UODO – czym się zajmuje i kto powinien obawiać się kontroli?, https://hsm-recycling.pl/pl/blog/czym-zajmuje-sie-uodo-i-kto-powinien-obawiac-sie-kontroli-3/ [dostęp: 20.10.2023].

Urbańska K, *RODO*, [w:] *Encyklopedia Zarządzania*, https://mfiles.pl/pl/index.php/RODO [dostęp: 07.10.2023].

Urząd ochrony danych osobowych i jego funkcja, nhttps://chronpesel.pl/ochrona-danych-osobowych/urzad-ochrony-danych-osobowych-i-jego-funkcja [dostęp: 18.10.2023].

Wawak S., Babiarz P., *Zarządzanie*, [w:] *Encyklopedia Zarządzania*, https://mfiles.pl/pl/index.php/Zarz%C4%85dzanie [dostęp: 16.10.2023].

What are 8 Data Subject rights according to the GDPR, https://dataprivacymanager.net/what-are-data-subject-rights-according-to-the-gdpr/ [dostęp: 20.03.2024].

What are my responsibilities under the GDPR?, https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-are-my-responsibilities-under_en [dostęp: 20.03.2024].

Więckiel P., *Cyberprzestępczość – czym jest i jak się przed tym bronić?*, https://fundacja.togatus.pl/cyberprzestepczosc-czym-jest-i-jak-sie-przed-tym-bronic/ [dostęp: 02.10.2023].

Województwo, Encyklopedia PWN, https://encyklopedia.pwn.pl/haslo/wojewodztwo;3997432.html [dostęp: 07.10.2023].

Wolford B., *What is GDPR, the EU's new data protection law*, https://gdpr.eu/what-is-gdpr/ [dostęp: 20.03.2024].

Woollacott E., *Changes to Japan's data privacy law echo Europe's GDPR*, https://portswigger.net/daily-swig/changes-to-japans-data-privacy-law-echo-europes-gdpr?fbclid=IwAR3aoArcSCu8apJoQ6sgfXcC7Z7H-F3Qj2kteQYn6c4rYZ2_yvZJjk1d5Ys [dostęp: 16.03.2024].

Wroczyński D., *Co robić w przypadku kradzieży tożsamości?*, KPP w Wyszkowie, https://mazowiecka.policja.gov.pl/wwy/aktualnosci/50393,Co-zrobic-w-przypadku-kradziezy-tozsamosci.html [dostęp: 02.20.2023].

Wskaźniki rozwoju społeczno-gospodarczego, https://zpe.gov.pl/a/wskazniki-rozwoju-spoleczno-gospodarczego/DJujftdYV [dostęp: 19.03.2024].

Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie, https://eurlex.europa.eu/legalcontent/PL/TXT/?uri=CELEX%3A32018H0604%2801%29 [dostęp: 5.05.2022].

Zezwolenie na przeprowadzenie imprezy masowej, https://www.biznes.gov.pl/pl/opisy-procedur/-/proc/263 [dostęp: 02.10.2023].

SPIS WYKRESÓW

ANEKS

ANKIETA

Instrukcja: *Prosimy o uważne przeczytanie każdego pytania i zaznaczenie odpowiedzi, która najlepiej odzwierciedla Państwa doświadczenia lub opinie. Wasze odpowiedzi są anonimowe i będą wykorzystywane wyłącznie do celów badawczych.*

SEKCJA 1: INFORMACJE OGÓLNE

1. **W jakiej jednostce samorządu terytorialnego Państwo pracują?**
   a. Gmina
   b. Powiat
   c. Województwo
   d. Inna (proszę określić): _____
2. **Na jakim stanowisku Państwo pracują?**
   a. Administracja
   b. Kierownictwo
   c. Specjalista ds. ochrony danych
   d. Inne (proszę określić): _____

SEKCJA 2: ŚWIADOMOŚĆ I SZKOLENIA

3. **Jak oceniasz swoją świadomość przepisów RODO przed szkoleniami (jeśli takie miały miejsce)?**
   a. Bardzo niska
   b. Niska
   c. Średnia
   d. Wysoka
   e. Bardzo wysoka
4. **Jak oceniasz swoją świadomość przepisów RODO po szkoleniach (jeśli takie miały miejsce)?**
   a. Bardzo niska
   b. Niska
   c. Średnia
   d. Wysoka
   e. Bardzo wysoka

5. **Jak często odbywają się szkolenia aktualizacyjne z zakresu RODO?**
    a. Regularnie
    b. Sporadycznie
    c. Nie odbywają się

SEKCJA 3: WDRAŻANIE RODO

6. **Czy wdrożenie RODO spowodowało konieczność zatrudnienia dodatkowych pracowników lub konsultantów zewnętrznych?**
    a. Tak
    b. Nie
7. **Jak oceniasz poziom trudności wdrożenia RODO w Państwa jednostce?**
    a. Bardzo łatwe
    b. Łatwe
    c. Trudne
    d. Bardzo trudne

SEKCJA 4: EFEKTY WDROŻENIA

8. **Czy zauważyli Państwo zmiany w poziomie bezpieczeństwa danych osobowych po wdrożeniu RODO?**
    a. Znacząca poprawa
    b. Lekka poprawa
    c. Bez zmian
    d. Pogorszenie
9. **Jakie korzyści przyniosło wdrożenie RODO w Państwa jednostce?**
    a. Lepsza ochrona danych osobowych
    b. Większa świadomość pracowników i obywateli
    c. Poprawa wizerunku jednostki
    d. Inne (proszę określić): _____

SEKCJA 5: WPŁYW NA CODZIENNĄ PRACĘ

10. **W jakim stopniu RODO wpłynęło na Państwa codzienne obowiązki w pracy?**
    a. W żadnym stopniu
    b. W niewielkim stopniu
    c. W umiarkowanym stopniu
    d. W znacznym stopniu
    e. W bardzo dużym stopniu

11. **Czy zauważyli Państwo wzrost biurokracji i obciążeń administracyjnych po wprowadzeniu RODO?**
    a. Tak, znaczny wzrost
    b. Tak, niewielki wzrost
    c. Nie zauważyłem/am zmian
    d. Nie, obciążenia się zmniejszyły
12. **Jak oceniają Państwo dostępność narzędzi i zasobów niezbędnych do zapewnienia zgodności z RODO w Państwa jednostce?**
    a. Bardzo dobra
    b. Dobra
    c. Średnia
    d. Zła
    e. Bardzo zła
13. **Czy wprowadzenie RODO wpłynęło na sposób komunikacji z mieszkańcami /obywatelami?**
    a. Tak, stała się bardziej formalna
    b. Tak, jest teraz bardziej ograniczona
    c. Nie zauważyłem/am zmian
    d. Tak, jest teraz bardziej otwarta i przejrzysta

SEKCJA 6: PRZESTRZEGANIE I KONTROLA

14. **Jak oceniają Państwo skuteczność kontroli wewnętrznych dotyczących przestrzegania RODO w Państwa jednostce?**
    a. Bardzo skuteczne
    b. Skuteczne
    c. Średnio skuteczne
    d. Nieskuteczne
    e. Bardzo nieskuteczne
15. **Czy mieli Państwo do czynienia z przypadkami naruszeń danych osobowych? Jeśli tak, jak zostały one rozwiązane?**
    a. Tak, zostały szybko i skutecznie rozwiązane
    b. Tak, ale ich rozwiązanie było trudne i czasochłonne
    c. Nie mieliśmy do czynienia z naruszeniami
    d. Nie wiem

16. **Jakie są Państwa propozycje na poprawę postrzegania RODO w jednostkach samorządu terytorialnego w Polsce?**
    a. Wzmocnienie szkoleń i podnoszenie świadomości pracowników
    b. Poprawa systemów informatycznych i bezpieczeństwa danych
    c. Lepsza współpraca z inspektorem ochrony danych
17. **Jak w Państwa jednostce jest monitorowana i dokumentowana zgodność z RODO?**
    a. Przez regularne audyty wewnętrzne
    b. Przez zewnętrzne audyty i oceny zgodności
    c. Za pomocą systemów zarządzania dokumentacją
    d. Nie jest to monitorowane
18. **Czy w Państwa jednostce stosuje się procedury oceny skutków dla ochrony danych (DPIA) przy wprowadzaniu nowych projektów lub systemów przetwarzających dane osobowe?**
    a. Tak, zawsze
    b. Tylko przy większych projektach
    c. Rzadko
    d. Nie wiem, co to jest
19. **Jak często Państwa jednostka aktualizuje polityki i procedury związane z ochroną danych osobowych?**
    a. Regularnie, przynajmniej raz w roku
    b. Tylko gdy zmieniają się przepisy
    c. Sporadycznie
    d. Nie aktualizujemy takich dokumentów
20. **Jak jest realizowane prawo dostępu do danych, ich sprostowania, usunięcia czy przenoszenia przez mieszkańców/obywateli w Państwa jednostce?**
    a. Proces jest szybki i zautomatyzowany
    b. Proces jest realizowany ręcznie, ale jest efektywny
    c. Realizacja praw jest trudna i czasochłonna
    d. Mamy problemy z realizacją tych praw
21. **Czy Państwa jednostka doświadczyła kontroli przez Urząd Ochrony Danych Osobowych? Jeśli tak, jakie były wyniki?**
    a. Tak, wyniki były pozytywne
    b. Tak, wyniki były negatywne i są wdrażane korekty

c. Tak, były pewne nieprawidłowości, ale zostały poprawione
d. Nie było kontroli

22. W jaki sposób pracownicy są informowani o konieczności podpisywania klauzul RODO przy przekazywaniu danych osobowych?

a. Poprzez szkolenia i instrukcje
b. Za pomocą systemów elektronicznych (np. pop-upy przy wprowadzaniu danych)
c. Przez bezpośrednie polecenia od przełożonych
d. Nie jesteśmy informowani o tej konieczności

23. Jakie kroki są podejmowane w przypadku stwierdzenia naruszenia przepisów RODO w Państwa jednostce?

a. Natychmiastowe zgłoszenie do UODO i podjęcie działań naprawczych
b. Wewnętrzne dochodzenie i rozwiązanie problemu bez zgłaszania
c. Nie jesteśmy pewni procedur
d. Nie mieliśmy do czynienia z naruszeniami

WYKAZ JEDNOSTEK SAMORZĄDU TERYTORIALNEGO, W KTÓRYCH PRZEPROWADZONO BADANIA ANKIETOWE

Województwa:

1. Województwo Kujawsko-Pomorskie
2. Województwo Pomorskie

Powiaty:

1. Powiat Aleksandrowski
2. Powiat Brodnicki
3. Powiat Nowomiejski
4. Powiat Toruński
5. Powiat Wejherowski

Gminy:

1. Gmina Aleksandrów Kujawski
2. Gmina Bobrowo
3. Gmina Cekcyn
4. Gmina Chełmża
5. Gmina Choczewo
6. Gmina Ciechocinek
7. Gmina Czernikowo
8. Gmina Dąbrowa Chełmińska
9. Gmina Dobrcz
10. Gmina Dobrzyń nad Wisłą
11. Gmina Gniewino
12. Gmina Gniewkowo
13. Gmina Gostycyn
14. Gmina Inowrocław
15. Gmina Krokowa
16. Gmina Kurzętnik
17. Gmina Lisewo
18. Gmina Lubawa
19. Gmina Lubicz

20. Gmina Łubianka
21. Gmina Łysomice
22. Gmina Nowe Miasto Lubawskie
23. Gmina Obrowo
24. Gmina Pabianice
25. Gmina Papowo Biskupie
26. Gmina Płużnica
27. Gmina Pruszcz
28. Gmina Radomin
29. Gmina Radziejów
30. Gmina Skała
31. Gmina Świedziebnia
32. Gmina Świekatowo
33. Gmina Waganiec
34. Gmina Warlubie
35. Gmina Wejherowo
36. Gmina Wielka Nieszawka
37. Gmina Zławieś Wielka
38. Miasto i Gmina Brześć Kujawski
39. Miasto i Gmina Chodecz
40. Miasto i Gmina Izbica Kujawska
41. Miasto i Gmina Jabłonowo Pomorskie
42. Miasto i Gmina Kowalewo Pomorskie
43. Miasto Aleksandrów Kujawski
44. Miasto Chełmża
45. Miasto Inowrocław
46. Miasto Kraków
47. Miasto Legionowo
48. Miasto Nowe Miasto Lubawskie
49. Miasto Radziejów
50. Miasto Toruń