Ius et Securitas 1/2026 | ISSN 3071-799X

Dorota Michalska-Sieniawska
Politechnika Koszalińska
ORCID: 0000-0003-0514-8250
dorota.michalska-sieniawska@tu.koszalin.pl

Godność człowieka jako aksjologiczna podstawa polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej

Streszczenie

Artykuł podejmuje problematykę godności człowieka jako aksjologicznej podstawy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej. Punktem wyjścia rozważań jest konstytucyjna zasada ochrony godności człowieka, wyrażona w art. 30 Konstytucji RP oraz jej znaczenie dla kształtowania praw i wolności jednostki w warunkach postępującej cyfryzacji życia społecznego. Analiza koncentruje się na ocenie, w jakim zakresie godność człowieka znajduje odzwierciedlenie w dokumentach strategicznych dotyczących cyberbezpieczeństwa, w szczególności w Strategii Cyberbezpieczeństwa RP oraz w ustawie o krajowym systemie cyberbezpieczeństwa. Analiza ta poprzedzona jest próbą zdefiniowania czym jest godność człowieka i jak ją rozumieć w zderzeniu z cyfryzacją życia. W artykule wskazano, że w polityce cyberbezpieczeństwa jej ochrona jest realizowana przede wszystkim w sposób pośredni, poprzez regulacje odnoszące się do ochrony prywatności, danych osobowych, autonomii informacyjnej oraz bezpieczeństwa prawnego jednostki. Zwrócono również uwagę na potrzebę aktualizacji i doprecyzowania ram aksjologicznych polityki cyberbezpieczeństwa w kontekście rozwoju nowych technologii, w tym sztucznej inteligencji, oraz wyzwań społeczeństwa informacyjnego.

Słowa kluczowe: godność człowieka, polityka cyberbezpieczeństwa RP, prawa człowieka w cyberprzestrzeni.

Wprowadzenie

Współczesną rzeczywistość trafnie określiła polska filozof prawa prof. M. Szyszkowska: „Żyjemy w epoce rewolucji technicznej, zwłaszcza środków łączności. Nasuwa się tu analogia z wynalezieniem druku, który w tamtej

epoce był równie rewolucyjny jak dzisiaj na przykład Internet."[1] Wskazuje dalej również, że żyjemy w czasach ruchu kulturowego zwanego New Age (Nowa Era), który głosi nowy humanizm, opierający się m.in. na przezwyciężeniu wagi scjentyzmu i racjonalizmu, aby docenić wagę uczuć i woli człowieka na równi ze sferą intelektualną[2]. W szczególności w latach dwudziestych XXI w. zaczął wyraźnie zaznaczać swoją obecność „nowy duch humanizmu", zwłaszcza w przestrzeni internetowej, powszechnie wykorzystywanej przez jego promotorki i promotorów, tworzących grupy wirtualnego wsparcia i portale szkoleniowe. Przejawia się on w negowaniu dotychczas panującego zachwytu nad osiągnięciami technicznymi nauki, postępującej cywilizacji i jednocześnie promowaniem powrotu do życia bliżej natury, najogólniej rzecz ujmując. I wydawać by się mogło, że to paradoksalne, iż wygłaszanie tych negacji odbywa się przy pomocy cyberprzestrzeni. Jest to ruch intelektualny ukierunkowany w stronę duchowości człowieka. Różne kanały internetowe i media społecznościowe zaczęły być intensywnie wykorzystywane przez osoby promujące nowe postrzeganie człowieka, w którym wyraźnie zaznacza się nowy ruch humanistyczny. Oczekiwania społeczne co do cyberbezpieczeństwa w związku z tym, są ukierunkowane na bezpieczną możliwość przeniesienia części życia duchowego jednostek w cyberprzestrzeń. Samotni ludzie, nazywani singlami, poszukujący tzw. drugiej połówki, często poznają przyszłych partnerów na portalach randkowych. Dzielenie się swoją twórczością przeniosło swój ciężar w cyberprzestrzeń. Zakupoholicy szaleją w sklepach internetowych. Hazardziści i fani gier też odnaleźli w niej swoje miejsce. Należy również zauważyć, że wirtualna przestrzeń rozciągnęła swój cień nad przestrzenią rzeczywistą. Przykładem tego jest możliwość obserwacji i dokonania pomiarów każdego zakątka kuli Ziemskiej w cyberprzestrzeni. Kolejnym przykładem są gry wirtualne, których ideą było wyciągnięcie młodych ludzi sprzed monitorów internetowych w domach, z monitorami telefonów w rękach, we wskazane w grach miejsca rzeczywiste tj. za pomocą gry Pokémon GO, która opanowała świat niczym pandemia.

Dynamiczny rozwój technologii informacyjno-komunikacyjnych oraz postępująca cyfryzacja wszystkich sfer życia społecznego powodują, że cyberprzestrzeń stała się równorzędnym obszarem realizacji praw i wolności jed-

[1] M. Szyszkowska, *Zarys europejskiej filozofii prawa,* Białystok 2004, s. 69.
[2] Ibidem, s. 71.

nostki. Proces ten generuje nowe zagrożenia dla autonomii, prywatności oraz integralności osoby ludzkiej, a tym samym stawia przed państwem wyzwanie adekwatnego ukształtowania polityki cyberbezpieczeństwa. W tym kontekście szczególnego znaczenia nabiera godność człowieka, rozumiana zarówno jako wartość konstytucyjna, jak i aksjologiczna podstawa systemu praw człowieka, ale przede wszystkim jako standard dobrej polityki i dobrego prawa.

Artykuł analizuje godność człowieka jako aksjologiczne i konstytucyjne odniesienie dla polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej. W świetle art. 30 Konstytucji RP godność stanowi podstawę wszystkich praw i wolności jednostki, a jej ochrona w warunkach cyfryzacji życia społecznego staje się coraz istotniejsza. Zgodnie z art. 30 Konstytucji RP godność człowieka ma charakter przyrodzony, niezbywalny i nienaruszalny oraz stanowi źródło wolności i praw jednostki. Chociaż akty prawne i dokumenty strategiczne dotyczące cyberbezpieczeństwa Rzeczypospolitej Polskiej nie odwołują się do niej zawsze wprost, regulują one obszary ściśle związane z jej ochroną. Polityka cyberbezpieczeństwa koncentruje się przede wszystkim na ochronie informacji, systemów i danych, zapewniając ich poufność, integralność oraz dostępność. W praktyce oznacza to, że godność człowieka jest chroniona pośrednio – poprzez ochronę danych osobowych przed wyciekiem, kradzieżą lub nadużyciem, co zapobiega naruszeniom prywatności, autonomii informacyjnej i reputacji jednostki.

Powstaje zatem pytanie o rzeczywistą rolę godności człowieka jako fundamentu aksjologicznego polityki cyberbezpieczeństwa państwa. Celem niniejszego artykułu jest analiza, w jakim stopniu i w jakiej formie godność człowieka znajduje odzwierciedlenie w polskiej polityce cyberbezpieczeństwa, w szczególności w Strategii Cyberbezpieczeństwa RP oraz ustawie o krajowym systemie cyberbezpieczeństwa, jako podstawowym akcie prawnym ściśle związanym z realizacją wytycznych polityki cyberbezpieczeństwa, a także ocena, czy klauzule dot. godności w nich zawarte są wystarczające i odpowiadają na wyzwania społeczeństwa informacyjnego.

W niniejszym artykule, rozważania dotyczące poszanowania godności w założeniach polityki dot. bezpieczeństwa w cyberprzestrzeni, obejmują założenia odnoszące się bezpośrednio do cyberprzestrzeni cywilnej RP. Tezy artykułu:1.Godność człowieka stanowi konstytucyjny i aksjologiczny fundament ochrony praw jednostki w cyberprzestrzeni, 2. Polityka cyberbezpieczeństwa RP chroni godność człowieka głównie pośrednio, poprzez regula-

cje dotyczące prywatności, danych osobowych i bezpieczeństwa prawnego. 3.Rozwój technologii i cyfryzacja życia społecznego uzasadniają potrzebę aktualizacji podejścia do ochrony godności człowieka w cyberprzestrzeni. Pytania badawcze: 1) Jaką rolę pełni godność człowieka jako wartość aksjologiczna w polskiej polityce cyberbezpieczeństwa? 2) W jaki sposób obowiązujące regulacje cyberbezpieczeństwa realizują ochronę godności jednostki? 3) Czy aktualne strategie i przepisy odpowiadają wyzwaniom ochrony praw człowieka w warunkach społeczeństwa informacyjnego?

Aby znaleźć odpowiedzi na powyższe pytania przeprowadzona została hermeneutyczna analiza dokumentów dot. strategii polityki cyberbezpieczeństwa, w pewnym zakresie również ustawy o krajowym systemie cyberbezpieczeństwa jako akcie prawnym, stanowiącym podstawę prawną realizacji polityki cyberbezpieczeństwa oraz literatury i w niewielkim zakresie publicystyki dot. niniejszego tematu.

Godność człowieka

Definiując krótko czym jest godność, można powtórzyć za M. Szyszkowską, że godność mieści się w odpowiedzi na pytanie, dotyczące tego kim jest człowiek[3]. Krótka definicja, która tak naprawdę otwiera przysłowiową „puszkę Pandory". Nie jest możliwe bowiem skonstruowanie krótkiej odpowiedzi na to pytanie. Może należy nawet stwierdzić, że w ogóle nie jest możliwe udzielenie takiej odpowiedzi, zwłaszcza satysfakcjonującej choćby większość filozofów. Konieczną jednak rzeczą jest przybliżenie znaczenia powyższych pojęć na potrzeby rozwiązań prawnych. Po pierwsze więc należy przy tym skupić się na fakcie, że człowiek jest istotą społeczną. Należy także przy każdej podejmowanej próbie definiowania, zarówno pojęcia człowiek jak i pojęcia „godność istoty ludzkiej", pamiętać że są to pojęcia transcendentalne i powinny pozostać pojęciami otwartymi, a więc ich definiowanie powinno ewoluować wraz z ewolucją cywilizacji, a w tym stosunków społecznych. Wyjątkowo wyraźnie uwidoczniły to procesy globalizacji i cyfryzacji życia.

Wracając do kwestii przedmiotowych pojęć, w odniesieniu do cyberprzestrzeni, niezbędne jest określenie zakresu uprawnień i wolności jednostki. Biorąc pod uwagę to, że każdy człowiek, nawet jeżeli nie podejmuje czynne-

[3] M. Szyszkowska, *Teoria i filozofia prawa,* Warszawa 2008, s. 56.

go uczestnictwa w wirtualnej przestrzeni, choćby udzielając się na portalach społecznościowych, a informacje go dotyczące w niej egzystują, nie można pominąć potrzeby skonstruowania na nowo ochrony prawnej godności istoty ludzkiej w związku z powszechną cyfryzacją życia. Nierzadko osoby, które nie posiadają dostępu do internetu, nie posiadają również pojęcia w jakim zakresie ich dane wrażliwe są wykorzystywane za jego pomocą. Zmiany regulacji prawnych nie nadążają za rozwojem technologii, w tym w szczególności w odniesieniu do jednostek. Pilną sprawą wydaje się więc położenie nacisku w polityce cyberbezpieczeństwa na redefinicję godności w kierunku uaktualnienia jej znaczenia w związku z pojawieniem się tzw. społeczeństwa informacyjnego. W tym celu i w celu podjęcia próby określenia ram prawnych ochrony godności istoty ludzkiej w związku z powszechną cyfryzacją życia, w pierwszej kolejności zostaje poniżej poddane analizie pojęcie „godności istoty ludzkiej".

Zgodnie z art. 30 Konstytucji, godność jest źródłem wszystkich praw i wolności człowieka. Z postanowień Konstytucji wynika, iż jest ona nienaruszalna, więc nie można nikogo jej pozbawić. Została ona również uznana „za jedną z podstawowych zasad ustroju Rzeczypospolitej"[4]. Godność jako zasada konstytucyjna oraz prawa i wolności, z niej wynikające, ujęte w Konstytucji RP, jak wskazuje W. Osiatyński, „są wyjęte spod władzy procesu politycznego i nie podlegają ograniczeniom demokratycznego ustawodawcy"[5]. Natomiast nieustanny proces tworzenia gwarancji prawnych ochrony godności, związanych z rozwojem nowych technologii, jest procesem politycznym. W tym kontekście warto przyjrzeć się znaczeniu „poszanowania godności". Jak wskazuje M. Chmaj, jej poszanowanie ma fundamentalne znaczenie dla rozwoju człowieka, gdyż godność jest rozumiana w sposób dynamiczny[6]. Dynamikę tę można rozumieć w dwojaki sposób, zarówno w sensie potrzeby jej redefinicji, zgodnej z rozwojem społecznym i technologicznym, jak i w sensie rozwoju jednostki. Zapewnienie gwarancji prawnych, umożliwiających korzystanie z praw i wolności, powinno zatem dawać jednostce pole do indywidualizmu, autonomii i samorealizacji[7]. Cyberprzestrzeń stała się w ostatnim czasie równoległą rzeczywistością, która w wielu przypadkach

[4] L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2025, s. 98-99.

[5] W. Osiatyński, *Prawa człowieka i ich granice,* Kraków 2011, s. 133.

[6] M. Chmaj, *Wolności i prawa człowieka w Konstytucji Rzeczypospolitej Polskiej,* Warszawa 2016, s. 37.

[7] Por. W. Sadurski, *Myślenie konstytucyjne,* Warszawa 1994, s. 52.

przeważa w codzienności jednostki nad fizycznym kontaktem ze społeczeństwem. Opanowała współczesną cywilizację w takim wymiarze, że znane dotąd pojęcia językowe nie pozwalają na precyzyjne werbalne opisanie czym jest, zwłaszcza że dla dużej części członków współczesnych społeczeństw jest trudna do oddzielenia od innych przestrzeni ich życia. Poszanowanie godności stało się więc bezsprzecznie tak samo istotne, jak w każdej innej, a nawet bardziej. A dlaczego bardziej? Globalizacja stała się procesem nieodwracalnym ze względu na opanowanie świata przez cyberprzestrzeń, globalizacja zaś przenosi kwestię praw i wolności człowieka w inny wymiar i przestrzeń, której twórcy idei ochrony praw człowieka nie byli w stanie przewidzieć.

Każdemu człowiekowi należy się poszanowanie jego godności jako istoty ludzkiej za sam fakt bycia człowiekiem, jak głosi doktryna praw człowieka. Od współczesnych trenerów mentalnych w pierwszej kolejności usłyszymy, że każdy ma prawo być szanowany za to, że po prostu jest. Na samym wstępie rozważań o tym, czym jest obowiązek poszanowania godności zgodnie z doktryną, należy odróżnić godność osobowościową od osobowej. Oprócz szanowania każdego jako człowieka, należy pamiętać o poszanowaniu indywidualnej, niepowtarzalnej sfery życia jednostek, ich osiągnięć i doświadczeń składających się na indywidualne imię i nazwisko. Osobowościowa godność, dotyczy więc cech indywidualnych, ukształtowanych przez każdego indywidualnie[8]. W tym miejscu warto przytoczyć myśl znanego obrońcy praw człowieka M. Nowickiego, wpisującą się w formułę godności w tym znaczeniu - ściśle odnoszącym się do każdego człowieka z osobna: „Prawa człowieka pozwalają zachować jednostce indywidualizm, przetrwać jako osoba niepowtarzalna, nigdy bowiem dotąd nie było i nigdy nie będzie już kogoś takiego jak każdy z nas, z naszym indywidualnym bagażem wspomnień, uczuć, myśli”[9]. Obecnie mamy do czynienia w szczególności z epatowaniem w cyberprzestrzeni z tą częścią godności na niebywałą skalę, z festiwalem indywidualności i niepowtarzalnych osobowości, poszukujących rzeszy fanów. Każdy, kto postanowił zaistnieć w tej przestrzeni, bezdyskusyjnie zasługuje na gwarancje ochrony jego godności, w szczególności tej osobowościowej. Ochrona ta powinna być jednak zaplanowana dla dwóch stron wspomnianego wirtu-

[8] M. Chmaj, *Wolności*..., s. 16.

[9] M. Nowicki, *Co to są prawa człowieka*?, https://hfhr.pl/upload/2022/01/co-to-sa-prawa-czlowieka-.pdf [dostęp: 12.01.2025].

alnego festiwalu osobowości, czyli dla odbiorców również, w szczególności dla młodych odbiorców, którzy są szczególnie narażeni na niewłaściwe treści, podczas gdy internet jest powszechnie dostępnym medium[10].

J. Zajadło zwrócił uwagę na to jak został użyty termin „godność" w art. 1 Powszechnej Deklaracji Praw Człowieka ONZ z 1948 roku. Jest on normatywnym wyrazem określonej koncepcji antropologicznej, która legła u podstaw Deklaracji i za jej pośrednictwem stała się ideowym podłożem dalszego rozwoju międzynarodowej ochrony praw człowieka. Przepis ten stymuluje z jednej strony przyrodzoną wolność i równość wszystkich ludzi pod względem ich praw i godności, z drugiej zaś nakaz postępowania w duchu braterstwa wynikający z takich atrybutów ludzkiej natury, jak rozum i sumienie[11]. Innymi słowy, każdy ma prawo do rozwoju własnej osobowości zgodnie z własną wolą, jako obdarzony własnym rozumem i sumieniem, w duchu równości i braterstwa.

W historii ludzkości nie było i nigdy nie będzie dwóch identycznych osób. Prawa człowieka chronią godność i niepowtarzalność każdej osoby, umożliwiając jej zachowanie własnej tożsamości i indywidualizmu. Chronią zatem nie tylko ciało i bezpieczeństwo jednostki, ale także jej wewnętrzny świat: prawo do własnych przekonań, uczuć, ekspresji i wyborów życiowych[12]. Potrzeba bezpieczeństwa należy do podstawowych i naturalnych potrzeb człowieka, wynikających z samej struktury jego bytu oraz zorientowania na samorealizację. Dopiero jej zaspokojenie stwarza warunki umożliwiające racjonalne planowanie przyszłości, realizację zamierzeń oraz osiąganie celów życiowych. Bezpieczeństwo stanowi zatem niezbędny fundament pełnego rozwoju osoby ludzkiej, pozwalając jej urzeczywistniać własne człowieczeń-

[10] J. Stelmach rozprawiając o wszechobecnej głupocie, przenikającej do każdej sfery życia, zauważa ,iż szczególne pole temu daje Internet: „(...) głupcy mają do dyspozycji cały wirtualny świat internetu oferujący niezliczoną liczbę platform i forów. A tam przecież nie ma już żadnej kontroli, więc można powiedzieć i pokazać wszystko. Fałszować fakty, bo głupiec „wie", że wszyscy je fałszują, manipulować informacjami, bo przecież inni też to robią, a nawet próbują zainteresować innych własnymi ułomnościami oraz głupotą. A wszystko po to, aby choć na chwilę zaistnieć, zwrócić na siebie uwagę innych (...)", B. Brożek, M. Heller, J. Stelmach, *Szkice z filozofii głupoty,* Kraków 2021, s. 48.

[11] J. Zajadło, *Godność jednostki w aktach międzynarodowej ochrony praw człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1989, nr 2, s. 3.

[12] Por. M. Nowicki, *Co to są prawa człowieka*?, https://www.hfhr.pl/wp-content/uploads/2016/02/Marek-Nowicki_co-to-sa-prawa-czlowieka.pdf [dostęp: 11.01.2026].

stwo i osiągać stabilne poczucie ładu. W wymiarze społecznym bezpieczeństwo nie ogranicza się wyłącznie do ochrony fizycznej czy materialnej, lecz obejmuje również zabezpieczenie osobowości człowieka, jego systemu wartości oraz godności osoby ludzkiej. Tak rozumiane bezpieczeństwo stanowi istotny fundament funkcjonowania jednostki w społeczeństwie i jej aktywnego uczestnictwa w życiu społecznym[13].

W orzecznictwie Trybunału Konstytucyjnego człowiek postrzegany jest jako autonomiczna i racjonalna jednostka, posiadająca własne plany oraz cele życiowe, do których realizacji ma prawo dążyć w warunkach bezpieczeństwa zapewnianego przez państwo prawa. Trybunał podkreśla jednocześnie, że w demokratycznym państwie prawa fundamentalne znaczenie ma zasada ochrony zaufania obywatela do państwa oraz stanowionego przez nie prawa, która wyznacza ramy relacji między jednostką a władzą publiczną[14].

Zasada zaufania do państwa i stanowionego przez nie prawa może być realizowana jedynie wtedy, gdy jednostka odczuwa bezpieczeństwo w relacjach prawnych. Odpowiedzialność za jego zapewnienie spoczywa na państwie. Zaufanie to nie ma charakteru bezwarunkowego, lecz jest efektem konkretnych działań władzy publicznej. Ujęcie bezpieczeństwa prawnego z perspektywy jednostki pozwala traktować je jako element praw człowieka, którego gwarancji obywatel może oczekiwać od państwa. Spełnienie warunków bezpieczeństwa prawnego stanowi podstawę uznania jednostki za autonomiczną i racjonalną w demokratycznym państwie prawa[15].

Wraz z rozwojem technologii ramy cyberbezpieczeństwa należy poddawać rekonstrukcjom. Autorzy książki „Prawne i społeczne aspekty cyberbezpieczeństwa", zwrócili uwagę na kilka istotnych kwestii ze względu na konieczność zapewnienia właściwej ochrony cyberprzestrzeni w dobie społeczeństwa informacyjnego. Zrobili to w formie pytań, na które należy odpowiedzieć: 1) Jakie znaczenie ma kwestia ochrony informacji (zwłaszcza prywatnych, wśród których dominującą rolę odgrywają dane osobowe)? 2) Jaka jest ochrona baz danych oraz tajemnicy przedsiębiorstwa? 3) Jaka jest ochrona oprogramowania, a także infrastruktury krytycznej państwa? 4) Jaka jest ochrona osób małoletnich oraz rodzin w cyberprzestrzeni?

[13] Por. J. Potrzeszcz, *Bezpieczeństwo prawne w orzecznictwie polskiego Trybunału Konstytucyjnego*, „Roczniki Nauk Prawnych" 2006, nr 16, s. 7-8.

[14] Ibidem, s. 8-9.

[15] Ibidem, s. 10.

5) Jaką rolę w cyberbezpieczeństwie powinny pełnić służby państwowe i administracja publiczna? 6) jak powinna wyglądać współpraca międzynarodowa w sferze cyberbezpieczeństwa?[16].

W odniesieniu do jednostek, potencjalni autorzy przedmiotowych rekonstrukcji, powinni skupić się na kwestiach bezpośrednio dotyczących ochrony dóbr osobistych czy ochrony osób małoletnich. Jednym z najbardziej pożądanych towarów w cyberprzestrzeni są dane osobowe, najczęściej zbywane między różnymi podmiotami w nie do końca legalny sposób.

Polityka cyberbezpieczeństwa

Polityka cyberbezpieczeństwa osadzona jest na założeniu, iż zapewnienie bezpieczeństwa w cyberprzestrzeni jest procesem długotrwałym, a w proces ten zaangażowane są wszystkie podmioty, zarówno prywatne, w tym obywatele, jak i publiczne. Incydenty w cyberprzestrzeni mają wpływ na życie gospodarcze i społeczne, ale także na życie poszczególnych jednostek. Zapewnienie więc bezpieczeństwa w tej kwestii, to zarówno bezpieczeństwo państwa jako całości, ale i bezpieczeństwo poszczególnych obywateli. Jak wskazuje niezależny badacz cyberbezpieczeństwa w rozmowie z serwisem „CyberDefence24.pl" dr Łukasz Olejnik, polityka państwa zatem musi obejmować zagadnienia w szerokim zakresie, od zagrożeń wewnętrznych do zagrożeń zewnętrznych, międzynarodowych. Zakres ten obejmuje również, a w istocie przede wszystkim, zagadnienia związane z obronnością państwa[17].

„Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" z 2013 roku to pierwszy strategiczny dokument, który powstał w Polsce w kwestii ochrony cyberprzestrzeni. „Jej celem strategicznym było osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa". Dokument ten obejmował swoim zakresem regulacji przedsiębiorców i osoby fizyczne. Został zastąpiony przez „Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022", dokument który jako pierwszy stanowił źródło standardów dla skoordynowanej polityki w tej kwestii, przyjęty jako uchwała nr 52/2017 Rady

[16] *Prawne i społeczne aspekty cyberbezpieczeństwa,* S. Gwoździewicz, K. Tomaszycki [red.], Warszawa 2017, s. 7.

[17] Zob. M. Fraser, *CyberMagazyn: Kto powinien kształtować politykę cyberbezpieczeństwa?*, https://cyberdefence24.pl/social-media/cybermagazyn-kto-powinien-ksztaltowac-polityke-cyberbezpieczenstwa [dostęp: 11.01.2026].

Ministrów z dnia 27 kwietnia 2017 roku[18]. „Krajowe Ramy", to dokument który stanowił podstawę kontynuacji działań podejmowanych wcześniej przez administrację rządową w celu podnoszenia poziomu cyberbezpieczeństwa. Założony główny cel, to zapewnienie wysokiego poziomu bezpieczeństwa w sektorze zarówno publicznym, jak i prywatnym oraz obywateli w zakresie świadczenia i korzystania z usług kluczowych oraz usług cyfrowych.

„Krajowe Ramy Polityki Cyberbezpieczeństwa" zostały zastąpione przez kolejny dokument, przyjęty przez Radę Ministrów jako uchwała nr 125 z dnia 22 października 2019 roku w sprawie „Strategii Cyberbezpieczeństwa RP na lata 2019-2024"[19]. Minister Cyfryzacji został wyznaczony jako koordynator jej wdrażania i jednocześnie zobowiązany do corocznego składania sprawozdania o postępach wdrażania Strategii Radzie Ministrów do 30 marca każdego roku[20]. Jak deklaruje Ministerstwo Cyfryzacji: „Polityka cyberbezpieczeństwa RP koncentruje się na ochronie systemów informacyjnych, infrastruktury krytycznej oraz zapewnieniu bezpieczeństwa narodowego w obliczu rosnących zagrożeń w cyberprzestrzeni"[21].

W uchwale tej przyjęto 5 celów szczegółowych. W ramach pierwszego celu założono rozwój systemu cyberbezpieczeństwa, oparty o ewaluację przepisów prawa – usprawnienie prawa, zarządzania i wymiany informacji w celu zwiększenia bezpieczeństwa państwa. Najważniejszym efektem realizacji tych założeń wydaje się być wdrożenie zintegrowanego systemu zarządzania cyberbezpieczeństwem oraz opracowanie krajowej metodyki szacowania ryzyka. Zawsze, kiedy chodzi o ochronę praw jednostki, ważna jest sprawność działania, a więc odpowiednie narzędzia prawne, w tym przede wszystkim procedury. Zintegrowanie działań z zasady ma prowadzić do zniwelowania luk w systemie i zwierzchniej koordynacji działań wielu odpowiedzialnych za cyberprzestrzeń podmiotów. Koordynacja działań wielu podmiotów stwarza bowiem sytuację

[18] Zob. więcej *Polityka Ochrony Cyberprzestrzeni RP*, https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/ [dostęp: 11.01.2026].

[19] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (M.P. z 2019 poz. 1037); zob. również *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022*, https://www.gov.pl/web/cyfryzacja/krajowe-ramy-polityki-cyberbezpieczenstwa [dostęp: 11.01.2026].

[20] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 26.12.2026].

[21] Ibidem.

podniesionego ryzyka wystąpienia błędów w organizacji, i co za tym idzie, rozmycia odpowiedzialności względem jednostki. Drugi z celów Strategii zakładał zwiększenie odporności systemów i zdolności reagowania na incydenty poprzez opracowanie Narodowych Standardów Cyberbezpieczeństwa i rozwój systemu certyfikacji zgodnie z Aktem o Cyberbezpieczeństwie UE[22] oraz audyty. Standaryzacja jest nieodłącznym elementem procesu wzmacniania ochrony jednostki w każdym obszarze gospodarki, spraw społecznych i publicznych, ległą więc u podstaw polityki cyberbezpieczeństwa. Trzeci cel Strategii, to wzmocnienie potencjału technologicznego państwa w cyberbezpieczeństwie, czyli rozwoju krajowych technologii i innowacji w cyberbezpieczeństwie poprzez wsparcie badań i rozwoju krajowych technologii i innowacji oraz współpracy publiczno-prywatnej z liderami rynku. Podsumowując ten cel wypada zauważyć, że uniezależnienie cyberbezpieczeństwa RP od podmiotów pozapaństwowych zwiększa bezpieczeństwo w ogóle, zmniejszając ryzyko wystąpienia niepożądanych incydentów, które są zdecydowanie trudniejsze do monitorowania i eliminacji, jeśli ich źródło znajduje się poza polską jurysdykcją. Bez wątpienia taka strategia jest jednocześnie wzmocnieniem bezpieczeństwa państwa oraz partykularnych interesów obywateli. Czwarty cel zakładał zbudowanie świadomości społecznej poprzez edukację i kampanie informacyjne oraz podnoszenie kwalifikacji kadr administracji publicznej i samorządowej oraz rozwój kompetencji specjalistycznych. Piąty cel został ukierunkowany na wzmocnienie międzynarodowej pozycji Polski w cyberbezpieczeństwie. Założono aktywny udział Polski w inicjatywach UE, ONZ i współpracy międzynarodowej, wzmacnianie eksperckiego głosu RP w pracach nad regulacjami (np. NIS certyfikacja) oraz rozwój współpracy regionalnej i dwustronnej z innymi państwami. Krótko podsumowując ten aspekt Strategii słowami zamieszczonymi na stronie informacyjnej Ministerstwa, piąty cel, to „budowa międzynarodowej pozycji Polski jako silnego i kompetentnego gracza w obszarze cyberbezpieczeństwa"[23].

[22] Akt o cyberbezpieczeństwie (Cybersecurity Act), to druga po dyrektywnie NIS ogólnoeuropejska regulacja w zakresie cyberbezpieczeństwa. Wszedł w życie 27 czerwca 2019 roku i reguluje m.in. obszar certyfikacji cyberbezpieczeństwa. Stworzył europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT, wprowadzając jednolite procedury w zakresie certyfikacji w obszarze cyberbezpieczeństwa na całym terenie UE, zob. *Akt o cyberbezpieczeństwie*, https://www.gov.pl/web/cyfryzacja/akt-o-cyberbezpieczenstwie [dostęp: 27.12.2025].

[23] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024*, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 26.12.2026].

Chociaż dokument ten nie używa dosłownie sformułowania „ochrona godności człowieka", to istotna jest część formułuje strategiczne podejście do praw i wolności jednostki w cyberprzestrzeni, w tym ochrony prywatności i wolności słowa, które są elementami szerszej ochrony godności człowieka w kontekście cyberbezpieczeństwa. Daje on gwarancje prawa do prywatności i wolnego Internetu w części opisowej dokumentu, w akapicie dotyczącym ochrony prywatności i wolności Internetu, wskazano że strategia zakłada „pełne gwarantowanie prawa do prywatności" oraz uznaje, że „wolny i otwarty Internet jest ważnym elementem funkcjonowania współczesnego społeczeństwa". Takie gwarancje wpisują się w ochronę godności człowieka w cyberprzestrzeni[24]. Odniesienie do poszanowanie praw i wolności obywateli znajduje się we fragmencie tego dokumentu, zamieszczonym w rozdziale *Wizja i cele*: „Działania rządu będą podejmowane z poszanowaniem praw i wolności obywateli oraz przez budowę zaufania między poszczególnymi sektorami rynku a administracją publiczną." Kolejna gwarancja zamieszczona w „Strategii", która wpisuje się w godność, to gwarancja ochrony informacji obywateli. Strategia w rozdziale Cel główny, choć koncentruje się na bezpieczeństwie systemów, dodaje, że główny cel obejmuje także promowanie świadomości i praktyk, które umożliwiają obywatelom lepszą ochronę ich informacji: „Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji (...) oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji"[25].

Podsumowując syntetycznie „Strategię Cyberbezpieczeństwa na lata 2019-2024", należy wskazać następujące elementy: 1) ochrona praw i wolności człowieka jako element strategii; 2) zapewnienie prawa do prywatności i wolnego Internetu; 3) gwarancja ochrony informacji obywateli. Te zapisy wskazują na ochronę godności człowieka w wymiarze wolności osobistych w cyberprzestrzeni, rozumianych jako ochrona prywatności i swobody komunikacji cyfrowej.

[24] W rozdziale dotyczącym kontekstu strategicznego cyberbezpieczeństwa w Rzeczypospolitej Polskiej znajduje się następujący akapit: „Podejmując działania mające na celu wdrożenie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, rząd będzie w pełni gwarantował prawo do prywatności oraz stał na stanowisku, że wolny i otwarty Internet jest istotnym elementem funkcjonowania współczesnego społeczeństwa." To zdanie znajduje się na stronach 6-7 tekstu pdf Strategii opublikowanego w Monitorze Polskim – Dzienniku Urzędowym Rzeczypospolitej Polskiej (załącznik do uchwały nr 125).

[25] Ibidem.

Z końcem roku 2024 upłynął okres, na jaki została uchwalona Strategia Cyberbezpieczeństwa RP na lata 2019-2024". Rada Ministrów przyjęła projekt „Strategii Cyberbezpieczeństwa RP na lata 2025-2029" dnia 8 lipca 2025 roku. „Nowa Strategia uwzględnia także zmiany w środowisku bezpieczeństwa międzynarodowego oraz kwestie związane postępem technologicznym i powszechną cyfryzacją wszystkich dziedzin życia"[26]. Ma być odpowiedzią na wzrost cyberprzestępczości zagrażającej bezpieczeństwu, prywatności i codziennemu funkcjonowaniu przedsiębiorstw, instytucji publicznych i obywateli. Dokument ten wyznacza również cele edukacyjne, informacyjne i szkoleniowe oraz plany badawczo-rozwojowe w obszarze cyberbezpieczeństwa. Uwzględnia także współpracę międzynarodową w tym zakresie[27]. Najbliższe elementy związane z ochroną praw obywateli, które można uznać za pośrednio odnoszące się do wartości związanych z godnością człowieka, są wskazywane jedynie w komentarzach i analizach organów ochrony danych (np. UODO). Prezes Urzędu Ochrony Danych Osobowych (PUODO) wskazuje, że projekt strategii ma wpływ na sferę praw i wolności człowieka, w tym ochronę danych osobowych, związanych z nimi ryzyk i przeciwdziałanie naruszeniom prywatności (np. kradzież tożsamości, cyberzagrożenia związane z AI)[28]. To odniesienie nie jest formalną wytyczną w postaci punktu „Strategii", ale oceną dokumentu pod kątem jego wpływu na prawa jednostki, co w praktyce wskazuje na zakres oddziaływania strategii na kwestie praw człowieka i godności[29]. Aktualnie nie ma jeszcze obowiązującej i oficjalnie opublikowanej „Strategii Cyberbezpieczeństwa Rzeczypo-

[26] *Projekt uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029*, https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2025-2029 [dostęp: 11.01.2026].

[27] *Rząd planuje przyjąć Strategię Cyberbezpieczeństwa na przełomie III i IV kwartału*, https://biznes.pap.pl/wiadomosci/rzad-planuje-przyjac-strategie-cyberbezpieczenstwa-na-przelomie-iii-i-iv-kwartalu [dostęp: 11.01.2026].

[28] *Prezes Urzędu Ochrony Danych Osobowych wskazał, że projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029 będzie wywierał wpływ na sferę praw i wolności człowieka, w tym na ochronę danych i informacji obywateli*, https://uodo.gov.pl/pl/138/3542 [dostęp: 11.01.2026].

[29] M. Kowalski, *Strategia Cyberbezpieczeństwa RP na lata 2025-2029 - uwagi Prezesa UODO*, https://www.poradyodo.pl/cybProjekt uchwały Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029erbezpieczenstwo/strategia-cyberbezpieczenstwa-rp-na-lata-20252029-uwagi-prezesa-uodo-13009.html [dostęp: 11.01.2026].

spolitej Polskiej na lata 2025-2029" w wersji przyjętej przez Radę Ministrów ani udostępnionej jako uchwała (np. w „Monitorze Polskim" z tekstem załącznika). Trwają prace nad projektem *Strategii*, ale dokument nie został oficjalnie opublikowany w pełnym kształcie, który można bezpośrednio cytować z numerami stron czy paragrafów. W oficjalnym projekcie Strategii brak jest bezpośredniego punktu zawierającego frazę „ochrona godności człowieka"[30]. Podsumowując, choć pełny tekst nowej „Strategii Cyberbezpieczeństwa RP na lata 2025-2029" nie jest jeszcze powszechnie dostępny w wersji oficjalnej, Prezes Urzędu Ochrony Danych Osobowych (UODO) w swoich uwagach do projektu dokumentu podkreślił: że strategia wpływa na sferę praw i wolności jednostki, oraz że rozwiązania prawne powinny być precyzyjne i chronić przed m.in. nieuprawnionym użyciem danych osobowych, ryzykiem kradzieży tożsamości, czy profilowaniem jednostek przy użyciu nowych technologii (np. narzędzi sztucznej inteligencji).

Warto podkreślić, że „Strategia" akcentując również promowanie wiedzy i dobrych praktyk wśród obywateli, pośrednio wspiera ochronę informacji osobistych i autonomii użytkowników.

Podstawowe różnice

Obszar	**Strategia 2019–2024**	**Projekt 2025–2029 (status)**
Ochrona praw człowieka	Wyraźne zapisy o prywatności i wolnym Internecie	Brak jeszcze jasnych zapisów; postulaty UODO do rozszerzenia
Nowe technologie (AI, biometryka)	Ograniczone	UODO wskazuje na konieczność rozbudowy
Podstawa prawna środków	Opiera się na KSC i istniejących regulacjach	UODO podkreśla konieczność wyraźnej podstawy prawnej
Zakres dokumentu	Kompletny dokument strategiczny	Projekt w konsultacjach
Kontynuacja działań	Określone cele i środki	Ma uwzględniać doświadczenia i zmiany środowiska cybernetycznego

[30] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029*, https://zpp.pl/storage/library/2025-07/cf7c082cf522e38345bf2df011c043a5.pdf [dostęp: 11.01.2026].

Wniosek:
Strategia 2019–2024 zawiera konkretne odniesienia do praw jednostki i ochrony prywatności w cyberprzestrzeni, stanowiąc jeden z filarów ochrony godności człowieka w kontekście cyberbezpieczeństwa. Projekt strategii 2025–2029 jest obiecujący pod względem adaptacji do nowych technologii i zagrożeń, jednak w obecnej formie wymaga doprecyzowania zapisów dotyczących ochrony praw człowieka, godności i danych osobowych, zgodnie z uwagami Prezesa UODO.

Podsumowując, „Strategia 2019-2024" zawiera jasne zapisy dotyczące ochrony prywatności i wolności w kontekście cyberbezpieczeństwa, co można traktować jako element ochrony godności człowieka. W projekcie 2025-2029 te zagadnienia nie są jeszcze w pełni ujęte w oficjalnym tekście, a postulaty UODO sugerują konieczność szerszego podejścia do ochrony danych i praw jednostki, w szczególności w kontekście nowych technologii. Choć w większości oficjalnych wersji Strategii Cyberbezpieczeństwa nie ma dosłownego odwołania do „godności człowieka" jako terminu konstytucyjnego, to ochrona tej wartości jest zawarta pośrednio. „Wytyczne Strategii Cyberbezpieczeństwa RP" dotyczące ochrony godności człowieka można ująć tak: 1) gwarancja prawa do prywatności i ochrony danych osobowych w cyberprzestrzeni – prywatność i dane osobowe – uznawane w dokumentach za kluczowe dla jednostki i wymagające ochrony; 2) wolność dostępu do informacji, wolny Internet oraz poszanowanie wolności słowa – jako element poszanowania autonomii obywatela w cyberprzestrzeni oraz jako elementu funkcjonowania społeczeństwa informacyjnego; 3) proporcjonalność środków bezpieczeństwa – tak aby prawa jednostki nie były nadmiernie ograniczane.

Także w historycznych dokumentach związanych z cyberbezpieczeństwem, takich jak doktryna BBN, podkreślano, że podejmowane działania muszą uwzględniać ochronę praw człowieka (np. wolność słowa, prywatność)[31]: 1. Bezpieczeństwo informacji jako element większych praw obywatelskich – strategia promuje działania edukacyjne i świadomościowe, które pomagają obywatelom chronić ich prawa w cyberprzestrzeni; 2. Uwzględnienie ryzyk związanych z technologiami śledzącymi, AI i identyfikacją osób w kontekście ochrony praw obywatelskich (zgodnie z uwagami Prezesa UODO).

[31] Zob. więcej *Doktryna cyberbezpieczeństwa RP*, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [dostęp: 11.01.2026].

Projekt strategii 2025–2029 ma potencjał, aby w większym zakresie uwzględnić najnowsze technologie i związane z nimi ryzyka dla praw jednostki, choć obecnie jego ujęcie tych obszarów jest krytykowane jako niewystarczające.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)

Podstawowym aktem prawnym, regulującym kwestie cyberbezpieczeństwa jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC), weszła ona w życie dnia 28 sierpnia 2018 roku[32]. Jest efektem implementacji dyrektywy 2016/1148, zwanej NIS 1, przyjętej 6 lipca 2016 r., będącej pierwszym europejskim aktem prawnym w zakresie cyberbezpieczeństwa. Została ona zastąpiona dyrektywą 2022/2555, zwaną dyrektywą NIS 2. Wprowadza szerszy zakres regulacji, jaśniejsze przepisy i silniejsze narzędzia nadzoru nad cyberbezpieczeństwem, jako odpowiedź na rosnące cyberzagrożenia dla Europy. Dyrektywa obejmuje ochronę sieci i systemów informatycznych (NIS). Nakłada ona na państwa członkowskie obowiązek przyjęcia krajowej strategii cyberbezpieczeństwa, obejmującą politykę bezpieczeństwa łańcucha dostaw, zarządzania podatnościami oraz edukację i budowanie świadomości w zakresie cyberbezpieczeństwa. Sektory objęte regulacją dyrektywy NIS 2, to energia, transport, opieka zdrowotna, finanse, gospodarka wodna i infrastruktura cyfrowa (obszary te były objęte regulacją dyrektywy NIS 1). Rozszerzono w niej zakres regulacji o regulacji o przepisy mające zastosowanie do dostawców publicznej łączności elektronicznej, takich jak media społecznościowe oraz do gospodarowania odpadami i ściekami, produkcji produktów o krytycznym znaczeniu, usług pocztowych i kurierskich oraz administracji publicznej zarówno na szczeblu centralnym, jak i regionalnym, a także sektora kosmicznego. Na podmioty duże i średnie, działające w tych sektorach krytycznych, nałożono obowiązki odpowiedniego zarządzania ryzykiem i informowania odpowiednich organów krajowych o znaczących incydentach, które mogą spowodować zakłócenia i szkody[33].

[32] Dz.U. z 2024 r. poz. 1077 (wersja od dnia 28 sierpnia 2025 r.).

[33] *Dyrektywa NIS 2: zabezpieczenie sieci i systemów informatycznych*, https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive [dostęp: 6.01.2026].

Ustawa o krajowym systemie cyberbezpieczeństwa będąca aktem powstałym w wyniku implementacji dyrektywy NIS objęła zakresem swojej regulacji administrację publiczną oraz sektor telekomunikacyjny[34]. Definiuje ona pojęcie cyberbezpieczeństwa w art. 2 pkt. 4 jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Ustawa nie zawiera klauzul o „ochronie godności jednostki" wprost, ani przepisów, które wprost odwoływałyby się do ochrony godności istoty ludzkiej w rozumieniu art. 30 Konstytucji RP. Powinna być jednak interpretowana w zgodzie z tym artykułem oraz w powiązaniu z art. 47 i 51 Konstytucji RP, odnoszących się do prywatność i ochrona danych[35]. Oznacza to, że wszelkie działania podejmowane na jej podstawie np. reagowanie na incydenty, gromadzenie informacji, muszą respektować godność jako nadrzędną wartość konstytucyjną, nawet jeśli ustawa nie wskazuje jej expressis verbis.

Ochrona godności pojawia się w tej ustawie pośrednio, poprzez regulacje służące ochronie praw i wolności jednostki w środowisku cyfrowym. Jej regulacje pośrednio korespondują z fundamentalnymi prawami człowieka (np. ochroną prywatności, integralności danych oraz dostępności usług kluczowych), które stanowią komponent godności jednostki w środowisku cyfrowym (w praktyce są częścią wdrażania standardów UE dotyczących praw obywateli).

Art. 3 ustawy o KSC, wskazujący na cele ustawy, ustanawia ramy dla zapewnienia bezpieczeństwa sieci i systemów informatycznych, które służą świadczeniu kluczowych i cyfrowych usług[36]. Realizacja tych celów ma znaczenie dla: ochrony życia prywatnego, autonomii informacyjnej jednostki, bezpieczeństwa korzystania z usług publicznych i prywatnych. Choć przepis

[34] *Ustawa o krajowym systemie cyberbezpieczeństwa*, https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa/ [dostęp: 6.01.2026].

[35] Art. 47 „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym", art. 51 ust. 1 „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby".

[36] Art. 3 [Cele Krajowego Systemu Cyberbezpieczeństwa]: „Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów".

nie używa pojęcia „godność", to ochrona podstawowych praw użytkowników usług cyfrowych stanowi jej aksjologiczne uzasadnienie. Art. 8 ust. 1 pkt 4 ustawy o KSC. Przepis nakłada obowiązek stosowania środków bezpieczeństwa z uwzględnieniem przepisów o ochronie danych osobowych. Odesłanie do RODO (oraz krajowych przepisów o ochronie danych) ma istotne znaczenie, ponieważ ochrona danych osobowych jest w prawie UE i polskim bezpośrednio wywodzona z godności człowieka, obejmuje ochronę tożsamości, autonomii decyzyjnej i integralności osoby.

Art. 8 ust. 1 ustawy o KSC wprowadza zasadę proporcjonalności środków bezpieczeństwa. Środki techniczne i organizacyjne mają być adekwatne do poziomu ryzyka, proporcjonalne, i dostosowane do skutków incydentów. Zasada ta ogranicza nadmierną ingerencję w sferę praw jednostki (np. nadzór, monitoring, przetwarzanie danych), co pośrednio chroni: wolność, prywatność, godność użytkowników systemów. W ustawie zapewniono bezpieczeństwo usług kluczowych dla funkcjonowania jednostki. Regulacje dotyczące operatorów usług kluczowych (rozdział 3 ustawy) mają znaczenie dla ochrony godności poprzez zapewnienie ciągłości usług zdrowotnych, energetycznych, transportowych czy bankowych, oraz poprzez minimalizowanie ryzyka zakłócenia świadczeń niezbędnych do godnego życia. Choć jest to ochrona pośrednia, w doktrynie przyjmuje się, że pozbawienie dostępu do podstawowych usług może naruszać godność człowieka.

Podsumowując, aksjologicznie ustawa KSC pozostaje podporządkowana konstytucyjnej zasadzie ochrony godności człowieka. Nie reguluje wprost ochrony godności istoty ludzkiej. Ochrona ta występuje pośrednio, poprzez: ochronę danych osobowych, poszanowanie prywatności, zasadę proporcjonalności, zapewnienie bezpieczeństwa usług kluczowych. Innymi słowy, ducha Strategii Cyberbezpieczeństwa RP pozwala się wpisać w konstytucyjny oraz prawnoczłowieczy porządek aksjologiczny.

Podsumowanie

Aksjologiczne podstawy polityki cyberbezpieczeństwa: godność, prywatność i bezpieczeństwo informacji. Analiza dokumentów strategicznych, w tym Strategii Cyberbezpieczeństwa RP oraz ustawy o krajowym systemie cyberbezpieczeństwa pośrednio, realizowana głównie poprzez regulacje dotyczące prywatności, ochrony danych osobowych, autonomii informacyjnej

i bezpieczeństwa prawnego jednostki. Dokumenty te łączą bezpieczeństwo państwa z bezpieczeństwem poszczególnych jednostek, wskazując, że cyberbezpieczeństwo ma wymiar zarówno systemowy, jak i indywidualny. Wnioski płynące z analizy odpowiadają na pytania badawcze: godność człowieka pełni w polityce cyberbezpieczeństwa funkcję aksjologiczną, a jej ochrona wymaga uwzględnienia praw jednostki w cyberprzestrzeni.

Obowiązujące dokumenty realizują tę ochronę pośrednio, lecz przyszłe regulacje powinny w większym stopniu integrować w wymiar aksjologiczny i konstytucyjny z konkretnymi mechanizmami ochrony w cyfrowym środowisku. Bezpośrednie zamieszczenie zasady ochrony godności, która mogłaby nadać ton szerszej koncepcji – zasady dla polityki cyberbezpieczeństwa, a co za tym idzie interpretacji regulacji prawnych dot. tego obszaru. Nadałaby ona większej elastyczności dla interpretacji zasad tej polityki i prawa w tym tak dynamicznym obszarze. Dynamicznym ze względu na rozwój technologii, więc i na rozwój zagrożeń. Jednocześnie artykuł wskazuje na potrzebę aktualizacji ram aksjologicznych polityki cyberbezpieczeństwa w kontekście nowych technologii, takich jak sztuczna inteligencja, oraz wyzwań społeczeństwa informacyjnego. Zwraca uwagę, że choć projekt Strategii Cyberbezpieczeństwa RP na lata 2025-2029 uwzględnia postęp technologiczny i rosnące zagrożenia, konieczne jest doprecyzowanie zapisów odnoszących się do ochrony praw człowieka, godności i danych osobowych.

Bibliografia

Brożek B., Heller M., Stelmach J., *Szkice z filozofii głupoty,* Kraków 2021.

Chmaj M., *Wolności i prawa człowieka w Konstytucji Rzeczypospolitej Polskiej,* Warszawa 2016.

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2025.

Osiatyński W., *Prawa człowieka i ich granice,* Kraków 2011.

Potrzeszcz J., *Bezpieczeństwo prawne w orzecznictwie polskiego Trybunału Konstytucyjnego*, „Roczniki Nauk Prawnych" 2006, nr 16.

Prawne i społeczne aspekty cyberbezpieczeństwa, S. Gwoździewicz, K. Tomaszycki [red.], Warszawa 2017.

Sadurski W., *Myślenie konstytucyjne,* Warszawa 1994.

Szyszkowska M., *Teoria i filozofia prawa,* Warszawa 2008.

Szyszkowska M., *Zarys europejskiej filozofii prawa,* Białystok 2004.

Zajadło J., *Godność jednostki w aktach międzynarodowej ochrony praw człowieka*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1989, nr 2.

* * *

Human Dignity as the Axiological Foundation of the Cybersecurity Policy of the Republic of Poland

Abstract

This article addresses the issue of human dignity as the axiological foundation of the cybersecurity policy of the Republic of Poland. The point of departure for the analysis is the constitutional principle of the protection of human dignity, as expressed in Article 30 of the Constitution of the Republic of Poland, and its significance for shaping individual rights and freedoms under conditions of the progressive digitalisation of social life. The analysis focuses on assessing the extent to which human dignity is reflected in strategic documents concerning cybersecurity, in particular the Cybersecurity Strategy of the Republic of Poland and the Act on the National Cybersecurity System. This assessment is preceded by an attempt to define human dignity and to clarify how it should be understood in the context of the digital transformation of everyday life. The article argues that, within cybersecurity policy, the protection of human dignity is implemented primarily in an indirect manner, through regulations relating to the protection of privacy, personal data, informational autonomy, and the legal security of the individual. Attention is also drawn to the need to update and further specify the axiological framework of cybersecurity policy in light of the development of new technologies, including artificial intelligence, and the challenges posed by the information society.

Keywords: human dignity; cybersecurity policy of the Republic of Poland; human rights in cyberspace.