Wprowadzenie

Bezpieczeństwo, tożsamość, prywatność – aspekty prawne

Wprowadzenie

Przedmiotem naszych rozważań jest wskazanie obszarów, gdzie występują zagrożenia dla prywatności jednostki w warunkach rozwoju nowych technologii i określenie niezbędnych kierunków regulacyjnych. W tym zakresie badań niezbędne jest ustalenie statusu jednostki w warunkach regulacji zapewniających ochronę bezpieczeństwa personalnego, ale także publicznego – w aktualnym stanie prawnym – oraz wskazanie nowych zasad działania administracji publicznej oraz dookreślenie granic ingerencji władz publicznych. Problem ten odnosi się do kilku podstawowych obszarów regulacji. Są nimi: ochrona konstytucyjnych praw i wolności jednostki, ograniczenia tych praw i wolności w warunkach koniecznego działania administracji publicznej, ustalenie instrumentów realizacji tej ochrony.

Wobec takich założeń badawczych, nie tylko problematyka ustalenia nowych rozwiązań regulacyjnych jest podstawą rozważań. Pytaniem zasadniczym i priorytetowym wydaje się być kwestia definiowania celów ochrony bezpieczeństwa publicznego w kontekście praw jednostki, bowiem bezpieczeństwo konstytucyjnie stanowi uzasadnienie wszelkich ograniczeń, ale także jest podstawą działania administracji publicznej i stosowania określonych instrumentów przez władzę publiczną. Odnosić się to będzie do pytań badawczych o poziom definiowania celów bezpieczeństwa narodowego (bezpieczeństwo państwowe, bezpieczeństwo wewnętrzne, bezpieczeństwo indywidualne – personalne), zakresu definiowania i kompetencji w zakresie realizacji tych celów (rozwiązania instytucjonalne, normy prawne, procedury). Zagadnienie to będzie dotyczyło roli państwa, treści zadań publicznych, wyznaczanych przez cele interesu publicznego, odpowiedzialności organów administracji publicznej i uprawnień, ale także obowiązków samej jednostki – obywatela. Granice wyznaczać muszą prawa podstawowe wyrażone w umowach międzynarodowych i Konstytucji RP.

W tym obszarze istotna jest potrzeba dookreślenia celów regulacyjnych, wyrażonych w strategiach i założeniach stanowiących podstawę polityki regulacyjnej, w oparciu o tendencje rozwojowe związane z ideologią wolności jednostki w pełnym obszarze jej aktywności.

W konsekwencji obszar naszych rozważań należy podzielić na cztery sfery:

1. Prawa indywidualne, podstawowe z uwzględnieniem aspektów aksjologicznych, których podstaw należy upatrywać w filozoficznych i socjologicznych koncepcjach godności człowieka.
2. Tożsamość, jako zjawisko i stały element związany z bezpieczeństwem personalnym i narodowym a wyzwania świata cyfrowego.

3. Rozwiązania systemowe dotyczące prywatności i tożsamości zaprezentowane na wybranych przykładach, ze szczególnym uwzględnieniem obowiązującego systemu prawa konstytucyjnego i administracyjnego w warunkach cyfrowych.
4. Bezpieczeństwo jako przesłanka ograniczeń ochrony prywatności i tożsamości.

Podstawowym problemem badawczym jest określenie współczesnego statusu jednostki – jako części narodu – obywatela w obszarze regulacyjnym, w kontekście ochrony bezpieczeństwa narodowego. Na sytuację prawną jednostki – obywatela składa się określony zespół praw i obowiązków wyznaczonych przez normy prawne oraz decyzje organów administracyjnych. W tym obszarze badań należy wydzielić sferę praw i obowiązków konstytucyjnych człowieka od uprawnień i obowiązków obywatela w sferze wykonawczej państwa, czyli administracji publicznej. Jest to szczególnie istotna kwestia dla analizy przedmiotowego zagadnienia w kontekście zmian społecznych związanych z rozwojem tzw. demokracji cyfrowej i potrzeby zapewnienia cyberbezpieczeństwa.

W tym aspekcie możemy mówić o władzy publicznej, która staje przed nowym zadaniem – ponownej legitymizacji w ramach trójpodziału władzy, gdzie granice tego podziału zacierają się na skutek powszechnie występującej konwergencji administracyjnej, prawnej jako konsekwencji konwergencji technologicznej. Sytuacja jednostki – obywatela wymaga nowego podejścia regulacyjnego. Po erze działań *ex post* coraz częściej wymagana jest koncepcja regulacji *ex ante*. Warunki cyfrowe i postęp technologiczny niosą ryzyko utraty kontroli, monitorowania przez władze publiczne warunków bezpieczeństwa – począwszy od bezpieczeństwa publicznego, a kończąc na partykularnych interesach jednostkowych zawartych w ogólnie pojętym bezpieczeństwie personalnym. Dochodzi tu do głosu jeszcze czynnik międzynarodowy, wymagający współpracy międzypaństwowej w warunkach zatarcia granic państwowych i podążającego pozbawiania różnic tożsamościowych. Wydaje się, że w tych warunkach niezbędne jest ustalenie priorytetów i dookreślenie obszarów prymatu instytucji publicznych nad światem koncernów gospodarczych, wykorzystujących nowe technologie w osiąganiu zysku kosztem m.in. prywatności konsumenta[1].

Sytuacja prywatności jednostki zagwarantowana normami prawa międzynarodowego oraz normami konstytucyjnymi stanowi podstawę ustaleń warunków funkcjonowania państwa prawa. Należy tu odnieść się także do ochrony praw podstawowych gwarantowanych przez przepisy prawa europejskiego[2]. W skali globalnej regulacje dotyczące prawa do prywatności wymagają aktualizacji. Wynika to z faktu, iż wielkie koncerny działające w skali międzynarodowej nadzorują i monitorują zachowania konsumenckie użytkowników sieci – najczęściej za bardziej lub mniej świadomą zgodą. Glokalizacja to standard w warunkach gospodarki napędzanej *big data*. Optymalizacja kampanii marketingowych to pozycjonowanie danych, profilowanie i tworzenie systemów sprzedaży opartych na wiedzy o jednostce. Jak podnoszą *J-H. Lorenzi*,

[1] *J.-H.Lorenzi*, *M. Berrebi*, Przyszłość naszej wolności, s. 236–237.

[2] Karta Praw Podstawowych Unii Europejskiej, Dz.Urz. UE C 83 z 2010 r., s. 389.

M. Berrebi „ (...) przerażającą granicę przekroczono w dziedzinie kontroli naszej własnej woli. Znajomość danego człowieka jest i będzie tak duża, że ostatecznie będzie miała wpływ na jego zachowanie. W tym przypadku bez wahania można mówić o mechanizmie samospełniającego się proroctwa, to znaczy o niemal trwałej utracie naszej wolności wyboru jako jednostek"[3]. Prawa podstawowe są traktowane jako jedna z zasad europejskiego porządku prawnego, i w taki też sposób ich ochrona podlega analizie w orzecznictwie Trybunału Sprawiedliwości UE. Pojawia się jednak problem styku dwóch koncepcji prawa do prywatności. Koncepcji kontynentalnej, w ramach której istotnym elementem ochrony jest godność, z której wynika ochrona uczuć i potrzeba zachowania intymności od tradycji wywodzącej się z amerykańskiego poczucia wolności, wyrażanej jako wartości związanej z zapewnieniem ochrony miejsca, nienaruszalności miru domowego. Ta różnica w pojmowaniu prawa do prywatności przekłada się automatycznie na koncepcję regulacji sfery prawa do prywatności[4]. Jednocześnie należy podkreślić, iż inna jeszcze bardziej zróżnicowana może być relacja pomiędzy uprawnieniami i obowiązkami w sferze prawa administracyjnego i działań administracyjnych na poziomie krajowym. Dlatego analizie należy poddać przede wszystkim sytuację prawną jednostki – obywatela w warunkach działania administracji publicznej na poziomie krajowym[5]. W rzeczywistości kwestia ta dotyka priorytetu funkcji państwa nad regułami wolności gospodarczej. Sama definicja administracji publicznej może być sformułowana w oparciu o jej cele, czyli m.in. ochronę bezpieczeństwa narodowego. Ostatecznie potrzeby jednostek wypełniają treść potrzeb państwa. Jedną z takich potrzeb jest poczucie bezpieczeństwa. Wynika to z faktu, iż organ administracyjny nie jest odbiorcą zachowania się obywatela, lecz jedynie podmiotem weryfikującym to zachowanie. Często ta weryfikacja jest związana z ograniczeniami wolności i praw podstawowych, podyktowanymi ochroną interesu publicznego, a jednym z jego głównych celów jest zapewnienie bezpieczeństwa. Zjawisko to jest szczególnie widoczne w sferze opozycji ochrony danych osobowych wobec obowiązków tzw. retencji danych. Dlatego w tej relacji należy poddać analizie także kwestię obowiązków obywatelskich, które stanowią oczywistą konsekwencję organizacji i funkcjonowania państwa jako suwerena.

Kolejnym istotnym dla naszych rozważań pojęciem będzie zagadnienie publicznych praw podmiotowych. Publiczne prawo podmiotowe to pojęcie ściśle związane z uprawnieniami i kompetencjami, jakie nabywa podmiot w ramach określonego stosunku prawnego, związanego z sytuacją tego podmiotu w przestrzeni prawa publicznego. W przypadku badań związanych ze statusem jednostki – obywatela w przestrzeni ochrony prawa do prywatności, w ramach organizatorskiej i zarządczej funkcji państwa. Celem tych badań jest postawienie diagnozy w zakresie kondycji państwa pol-

[3] *J.-H. Lorenzi*, *M. Berrebi*, Przyszłość naszej wolności, s. 226.

[4] Zob. *S. Stalla-Bourdillon*, *J. Phillips*, *M.D. Ryan*, Privacy vs. Security, s. 7.

[5] Zagadnienie ochrony praw i wolności na poziomie europejskim zostało omówione w pracy *M. Dybowskiego*, Prawa fundamentalne, w której autor omawia funkcje jakie pełnią prawa fundamentalne we wspólnotowym porządku prawnym poprzez odwołania do orzecznictwa TSUE.

skiego w obszarze zapewnienia bezpieczeństwa narodowego i bezpieczeństwa personalnego w warunkach rozwoju cyberprzestrzeni.

Analiza powyższego zagadnienia pozwoli na dokonanie podziału sytuacji jednostki – obywatela na działania związane z gwarancjami konstytucyjnymi, które będą zawsze stanowić podstawę oceny w stosunku do ustaleń statusu jednostki – obywatela w ramach funkcjonowania państwa, w szczególności w sferze realizacji jego funkcji organizatorskiej. Istotne znaczenie mają rozwiązania systemowe dotyczące praw i wolności obywatelskich związanych z prawem do prywatności w obszarze działań organizatorskich państwa. Pojawiają się tu dwa problemy. Jeden dotyczy kwestii nadzorowania i jego różnych instrumentów, które służą władzy publicznej w realizacji zadań związanych z ograniczeniami wolności jednostki – obywatela. Ta sfera zagadnień obejmuje kwestie związane z sytuacją prawną w świetle ustaleń konwencyjnych, związanych np. z nietykalnością cielesną i integralnością moralną. Kluczowym elementem tej analizy będzie zakaz wykorzystywania wobec jednostki inwazyjnych systemów informacyjnych.

Drugi problem dotyczy przejmowania kontroli przez rozwinięte przedsiębiorstwa technologiczne, które wykorzystują wiedzę o jednostce w skali globalnej, a unikanie kontaktu z nimi będzie miało charakter wykluczenia społecznego. Modele biznesowe Facebooka, Google'a czy Amazona polegają na identyfikacji użytkownika, zbieraniu informacji na jego temat, a następnie ich sprzedaży. W środowisku technologicznym wolność wyboru według własnej woli staje się problematyczna. Obszar ten dotyczy także wykorzystywania mechanizmów rynkowych, opartych na przetwarzaniu wiedzy o użytkownikach i manipulowaniu tą wiedzą w walce politycznej. Walka informacyjna wkraczająca w obszar prywatny w konsekwencji może także doprowadzić do kryzysu tożsamości narodowej. Wydaje się, że sytuacja ta powoduje naturalny protest i wzmacnia potrzebę konsolidacji przede wszystkim na poziomie narodowym, krajowym, uwzględniającym te elementy bliskie danej społeczności, które ją identyfikują. Jednak wykorzystywanie tego typu słabości to kolejny poziom zagrożeń, które dotykają suwerenności narodu i państwa.

Zauważony przez Autorki konflikt pomiędzy potrzebą zapewnienia cyberbezpieczeństwa a prawem do prywatności jednostki – obywatela, wymaga także rozważenia z punktu widzenia zjawiska cyberterroryzmu. Wydaje się, że wybór między wolnością a bezpieczeństwem jest wyborem bardzo trudnym. Zagrożenie cyberterroryzmem nosi bowiem dwojaki charakter. Z jednej strony mogą to być zamachy, starty materialne, strach w społeczeństwie. Z drugiej jednak, za zagrożenie można także uznać nadmierną reakcję państwa. Ważne jest, aby społeczeństwa demokratyczne zdołały pokonać terroryzm, zachowując swoje zasady wolności, na których zostały zbudowane. Zamknięcie przez państwo obywatela w dobrze strzeżonej twierdzy, coraz to nowsze systemy monitoringu, inwigilacji i kontroli, nie stanowią rozwiązania problemu. Oznaczałoby to utratę wartości, w tym prawa do prywatności, których w walce z cyberterroryzmem trzeba bronić. Dla zapewnienia cyberbezpieczeństwa należy przyjąć podejście akceptowalnego ryzyka i myśleć o nim w sposób innowacyjny, postrzegając je jako proces

o wielu ogniwach, w tym rozwiązań prawnych i rozwiązań organizacyjnych. Ważna jest świadomość, że walka z cyberterroryzmem to nie tylko technika i organizacja, lecz także wyzwania o charakterze moralnym. Uwzględniając kwestie moralne, należy mieć na uwadze podstawowe wartości, takie jak prywatność jednostki – obywatela. Nie można bowiem łamać zasad, których się broni. Jeżeli walcząc z cyberterroryzmem i broniąc wartości demokratycznych zaczniemy ze strachu przed zagrożeniem je łamać, terroryści będą mogli uznać, że wygrali[6].

Ten tak ważny obszar badawczy należało podzielić na kilka szczegółowych zagadnień, uporządkowanych tematycznie, stanowiących jednocześnie zakres rekomendacji w obszarze przyszłych regulacji, również ograniczeń w obszarze prawa do prywatności, jako nieuniknionego etapu w ochronie człowieczeństwa i przyszłości ludzkości.

[6] *T.R. Aleksandrowicz*, Terroryzm międzynarodowy, s. 157–158.