RAFAŁ WĄDOŁOWSKI

ORCID: 0000-0003-0601-1213
DOI: 10.4467/20801335PBW.22.049.16940

Ochrona informacji niejawnych w Bośni i Hercegowinie oraz Chorwacji. Wybrane regulacje karne i administracyjne

Abstrakt

W artykule omówiono regulacje administracyjne odnoszące się do organizacji systemu ochrony informacji niejawnych w Republice Chorwacji oraz w Bośni i Hercegowinie, a także przedstawiono przepisy karne dotyczące przestępstw przeciwko ochronie informacji niejawnych obowiązujące w tych krajach wraz z interpretacją tych przepisów. W artykule zaprezentowano również wybrane przepisy administracyjne regulujące procedurę realizacji postępowań sprawdzających w celu wydania poświadczenia bezpieczeństwa umożliwiającego dostęp do informacji niejawnych. Dodatkowo omówiono przesłanki klasyfikacji informacji i przyznania im określonej klauzuli tajności. Na podstawie analizy przepisów obowiązujących w Bośni i Hercegowinie (art. 164 § 9 Kodeksu karnego) i porównania ich z przepisami obowiązującymi z Polsce m.in. sformułowano wniosek, że polskie ustawodawstwo nie obejmuje kontratypu, który uwalniałby od odpowiedzialności karnej depozytariuszy tajemnic przekazujących informacje niejawne (bez uzyskania zgody określonych prawem organów) w celu ścigania sprawców przestępstw. Powyższe może być podstawą legislacyjnego postulatu *de lege ferenda*. Artykuł nie wyczerpuje poruszanego tematu, a jedynie wskazuje wybrane zagadnienia systemu ochrony informacji niejawnych. Zainicjowana eksploracja może zostać wykorzystana do przeprowadzenia w przyszłości pogłębionych badań przedmiotowego zagadnienia.

Słowa kluczowe

kodeks karny, ujawnienie tajemnicy, informacje niejawne, postępowanie sprawdzające, poświadczenie bezpieczeństwa, kontrwywiad.

Rozpad Związku Socjalistycznych Republik Radzieckich w 1991 r. zainicjował zmiany ustroju państw byłego bloku socjalistycznego, do którego – podobnie jak Polska – należała Jugosławia. W polskiej literaturze jest niewiele opracowań dotyczących regulacji prawnych przyjętych w państwach postsocjalistycznych, w tym utworzonych po rozpadzie byłej Socjalistycznej Federacyjnej Republiki Jugosławii[1]. Autor objął zakresem naukowego zainteresowania dwa kraje, które aktualnie należą do dwóch różnych stref wpływów politycznych: Chorwację, członka NATO i UE, oraz Bośnię i Hercegowinę, wobec której Rosja prowadzi intensywną politykę wpływu. Pokusił się również o sprawdzenie, czy regulacje przyjęte w wymienionych państwach różnią się w istotny sposób od obowiązujących w Polsce. Przybliżenie prawodawstw normujących ochronę informacji niejawnych Bośni i Hercegowiny oraz Chorwacji wydaje się uzasadnione, tym bardziej że Chorwacja jest członkiem NATO i zgromadzone wnioski dotyczące tych regulacji mogą zostać wykorzystane do budowania sojuszniczej interoperacyjności na płaszczyźnie militarnej. Niniejszy artykuł nie wyczerpuje naukowego opisu zagadnień związanych z bezpieczeństwem informacji w wymienionych państwach z uwagi na złożoność tego zagadnienia, lecz może stanowić przyczynek do dalszych pogłębionych badań tego relewantnego elementu bezpieczeństwa RP w ujęciu międzynarodowym.

Karnoprawna i administracyjna ochrona tajemnic w Bośni i Hercegowinie

W związku z brakiem polskiego piśmiennictwa dotyczącego aktów prawnych statuujących ochronę informacji niejawnych w Bośni i Hercegowinie (BiH) warto chociażby w zarysie omówić zasady przyjętego systemu ochrony tajemnic w tym kraju. Z uwagi na federacyjny charakter państwa w BiH istnieją trzy porządki prawne: ogólnokrajowy oraz oddzielne dla Federacji Bośni i Hercegowiny oraz Republiki Serbskiej. Jak trafnie zauważa Przemysław Osóbka, autonomia obu podmiotów składowych wyraża się w odrębnym podziale administracyjnym, a także posiadaniu własnych konstytucji, parlamentów i władzy wykonawczej[2]. W skład BiH wchodzi również niewielki region Brčko mający szczątkową autonomię[3].

---

[1] W literaturze przedmiotu szczegółowo opisano prawodawstwa państw Europy Zachodniej. Autorzy prezentują w nich również zagadnienia dotyczące ochrony informacji niejawnych, m.in. w opracowaniu *Jawność i jej ograniczenia*, G. Szpor (red. nauk.), t. 11: *Standardy europejskie*, C. Mik (red. tomu), Warszawa 2016. Brakuje natomiast aktualnych opracowań dotyczących krajów położonych w środkowej i wschodniej części kontynentu.

[2] P. Osóbka, *System konstytucyjny Bośni i Hercegowiny*, Warszawa 2011, s. 63 i nast.

[3] W artykule autor skupił się na porządku prawnym obowiązującym w Federacji Bośni i Hercegowiny (przyp. red.).

Aktem stanowiącym o integralności państwa jest Konstytucja BiH[4] z 14 grudnia 1995 r. Wśród 13 wolności ustanowionych w art. 2 żadna nie odnosi się do prawa uzyskiwania informacji, jest określone jedynie prawo do wolności słowa. Przykładem tego, że brak ustanowienia konstytucyjnego prawa dostępu obywateli do informacji publicznych nie uniemożliwia jego uchwalenia w innych aktach, jest system prawny obowiązujący w Stanach Zjednoczonych, ponieważ w Konstytucji USA[5] z 17 września 1787 r. również nie zawarto prawa do uzyskiwania informacji publicznoprawnych. Pierwsza poprawka do Konstytucji USA z 1791 r. ustanowiła wolność słowa[6]. Na tej podstawie Sąd Najwyższy USA wywiódł prawo uzyskiwania od władzy rzetelnych informacji w celu poszerzania wiedzy obywateli o stanie państwa[7]. Brak odrębnej regulacji konstytucyjnej w przedmiotowym zakresie nie wyłącza zatem prawa do żądania informacji od organów państwa. W związku z przyjętym zakresem regulacji, tj. neutralnością w odniesieniu do obowiązków informacyjnych administracji publicznej wobec obywatela, należy stwierdzić, że w ustawie zasadniczej BiH nie uwzględniono również przesłanek ograniczania dostępu do informacji publicznych.

Ogólnokrajowe ustawy BiH są uchwalane przez parlament składający się z Izby Reprezentantów i Izby Narodów. Parlament publikuje akty prawa w trzech językach: bośniackim, chorwackim i serbskim. Ogłasza się je w Dzienniku Urzędowym BiH (bośn. Službeni glasnik[8]). Zasadniczymi aktami prawnymi ustanawiającymi system ochrony tajemnic publicznoprawnych Bośni i Hercegowiny są ustawa z 28 lipca 2005 r. o ochronie informacji niejawnych[9] (dalej: ustawa o.i.n. BiH), która została w dużym zakresie zmieniona nowelizacją z 2009 r., oraz Kodeks karny BiH[10] (bośn. *Krivični zakon*, chor. *Kazneni zakon*, serb. *Кривични законик*), obowiązujący od 1 marca 2003 r. W terminologii aktów prawnych ustanawiających system ochrony

[4] *Ustav Bosne i Hercegovine*. Sarajevo, OHR – (Konstytucja Bośni i Hercegowiny).

[5] *Constitution of the United States of America*, House of Representatives, dok. No 110 – 50 (Konstytucja Stanów Zjednoczonych Ameryki).

[6] Zob. szerzej: R. Wądołowski, *Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 25, s. 146 i nast.

[7] Wyrok Sądu Najwyższego USA w sprawie „Hustler" v. Falwell, 485 U.S. 46, 24 II 1988 r.

[8] Tłumaczenia tekstów źródłowych oraz nazw własnych dokonała Małgorzata Uryga, tłumacz przysięgły języka chorwackiego.

[9] *Zakon o zaštiti tajnih podataka* (Službeni glasnik BiH broj 54/2005) – (ustawa o ochronie informacji niejawnych Bośni i Hercegowiny z 2005 r.). Nowelizacja została ogłoszona w Dzienniku Urzędowym w 2009 r. (Službeni glasnik BiH broj 12/2009).

[10] *Krivični zakon Bosne i Hercegovine* (Službeni glasnik BiH broj 3/2003) – (ustawa Kodeks karny Bośni i Hercegowiny z 2003 r.).

tajemnic w Bośni i Hercegowinie definicją legalną określającą informacje niejawne o najwyższej ważności ze względu na bezpieczeństwo państwa jest „tajni podatak" (serb. *тајни податак*). System ochrony tajemnicy państwowej, podobnie jak w Polsce, opiera się na dwóch filarach – karnoprawnym i administracyjnym[11].

Przestępstwa naruszające poufność informacji niejawnych prawodawstwo karne zalicza do kategorii przestępstw skierowanych przeciwko bezpieczeństwu państwa. Kodeks karny BiH w części szczególnej w rozdziale XVI pt. *Przestępstwa przeciwko integralności Bośni i Hercegowiny* w art. 164 pt. *Ujawnienie informacji niejawnych* penalizuje zachowanie polegające na ujawnieniu informacji niejawnej. Odrębną kodyfikacją prawa karnego materialnego jest Kodeks karny Federacji Bośni i Hercegowiny[12] (dalej: kk FBiH), który dotyczy tylko tego podmiotu, tj. Federacji, a nie całej Bośni i Hercegowiny. Autonomiczny prawodawca stosuje nieco odmienne nazewnictwo i zakres regulacji, stanowi bowiem o tajemnicy federacji „tajna Federacije", definiując ją w art. 2 ust. 24[13]. Czyn zabroniony jest natomiast stypizowany w art. 158 zatytułowanym *Ujawnienie tajemnicy Federacji*.

Ogólnokrajowy ustawodawca w art. 164 kk BiH penalizuje ujawnienie informacji niejawnych w typie podstawowym czynu oraz kilku kwalifikowanych, a także ustanawia kontratyp[14]. W § 1 podmiot przestępstwa został określony jako

---

[11] Czyny przeciwko informacjom niejawnym w RP spenalizowano w art. 265 oraz 266 § 2 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j. DzU z 2022 r. poz. 1138) – (dalej: kk RP). Aktem prawnym o najszerszym zakresie regulacji w odniesieniu do informacji niejawnych w RP jest *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (t.j. DzU z 2019 r. poz. 742, ze zm.).

[12] *Krivični zakon Federacije Bosne i Hercegovine* (Službene novine FBiH broj 36/2003 ispr. – 75/2017) – (ustawa Kodeks karny Federacji Bośni i Hercegowiny z 2003 r.).

[13] Tajemnicą Federacji, kantonu, miasta i gminy jest informacja lub dokument określone ustawą, innym rozporządzeniem lub aktem ogólnym właściwego organu wydanego na podstawie ustawy, których ujawnienie miałoby szkodliwe skutki dla Federacji, kantonu, miasta i gminy.

[14] Art. 164 kk FBiH: „§ 1. Osoba urzędowa lub osoba odpowiedzialna w instytucjach Bośni i Hercegowiny, lub funkcjonariusz wojskowy, upoważniony do określania tajności danych lub dostępu do informacji niejawnych, który bez upoważnienia poinformuje drugą osobę, przekaże lub w inny sposób udostępni informację niejawną bądź pozyska informację niejawną w celu podania jej do wiadomości lub przekazania osobie nieupoważnionej, podlega karze pozbawienia wolności od 6 miesięcy do lat 5. § 2. Karze z § 1 niniejszego artykułu podlega ten, kto nielegalnie pozyska informację niejawną w celu nieuprawnionego jej użycia lub kto poinformuje drugą osobę, przekaże lub w inny sposób udostępni informację niejawną bez zezwolenia, jak również kto poinformuje drugą osobę, przekaże lub w inny sposób udostępni innej osobie fakty lub środki zawierające informacje, o których wiadomo, że są informacją niejawną, a w posiadanie których wszedł nielegalnie. § 3. Karze pozbawienia wolności od roku do 10 lat podlega ten, kto popełni przestępstwo z § 1 lub 2 niniejszego artykułu: a) dla zysku; lub b) w odniesieniu do informacji, która zgodnie z ustawą została oznaczona jako »poufne« lub klauzulą »tajne«, lub jako »tajemnica państwowa«, lub klauzulą »ściśle tajne«; lub c) w celu podania do wiadomości, przekazania lub w inny sposób udostępnienia informacji niejawnej lub jej użycia poza Bośnią i Hercegowiną".

indywidualny, jest nim urzędnik, żołnierz lub osoba uprawniona do przetwarzania informacji niejawnych w instytucjach BiH. Strona podmiotowa polega na umyślności w zamiarze bezpośrednim lub ewentualnym. Dobrem chronionym jest poufność informacji niejawnych. Strona przedmiotowa polega na zachowaniu, w którego wyniku dochodzi do ujawnienia tajemnicy osobie nieuprawnionej do jej poznania. Karą za popełnienie omawianego przestępstwa jest pozbawienie wolności od 6 miesięcy do 5 lat.

W § 2 penalizacją objęto czyn polegający na pozyskaniu informacji niejawnej wbrew przepisom prawa przez jakąkolwiek osobę w celu nieuprawnionego użycia takiej informacji. Należy przyjąć, chociaż przepis o tym nie stanowi, że każde użycie nielegalnie zdobytej informacji jest nieuprawnione. Kryminalizacją objęto również ujawnienie tajemnicy innej nieuprawnionej osobie bez zezwolenia. Przyjmuje się więc, że osoba ujawniająca informację niejawną posiada ją zgodnie z prawem, lecz bezprawnie nią dysponuje. Innym sankcjonowanym zachowaniem w tym przepisie jest pośredniczenie w przekazaniu informacji niejawnej osobie nieuprawnionej, o ile osoba pośrednicząca wie, że przekazuje informację niejawną. Podmiot powyższych przestępstw został określony jako powszechny. Strona podmiotowa polega na umyślności. Odpowiedzialność karną określono w granicach kary dla przestępstwa z § 1.

W § 3 znajdują się zapisy o kwalifikowanych typach przestępstw określonych w § 1 i § 2. Ustawodawca zaostrza odpowiedzialność karną, określając ją w granicach od 1 roku do 10 lat, gdy czyn jest popełniony w celu osiągnięcia korzyści lub dotyczy informacji oznaczonych zgodnie z prawem klauzulą „poufne", „tajne" lub „ściśle tajne" albo jako tajemnica państwowa. Zaostrzonej odpowiedzialności karnej podlega również osoba, która przekazuje informację niejawną obcemu państwu albo wykorzystuje ją poza granicami BiH. Natomiast informacje stanowiące tajemnicę państwową to informacje chronione na podstawie uchylonych aktów cywilnych i wojskowych. Ustawa o.i.n. BiH w art. 86 nakazuje ich dalszą ochronę według reżimu określonego dla informacji „ściśle tajnych".

W § 4 prawodawca ustanowił reżim szczególnej odpowiedzialności osób profesjonalnie przetwarzających informacje niejawne[15]. Jeżeli podmiotem czynów

[15] Art. 164 kk FBiH: „§ 4. Jeśli przestępstwo z § 1 lub § 3 niniejszego artykułu popełniła osoba, która według ustawy o ochronie informacji niejawnych jest ustawowo upoważniona do określenia tajności informacji lub dostępu do informacji niejawnych tego stopnia, w odniesieniu do którego popełniono przestępstwo, sprawca podlega karze: a) za przestępstwo z § 1 niniejszego artykułu, karze pozbawienia wolności w wymiarze co najmniej 3 lat; b) za przestępstwo z § 3 niniejszego artykułu, karze pozbawienia wolności w wymiarze co najmniej 5 lat. § 5. Jeśli przestępstwo z § 1–3 niniejszego artykułu popełniono w czasie stanu wojennego lub bezpośredniego zagrożenia wojennego, lub stanu wyjątkowego, lub kiedy został wydany rozkaz do zaangażowania i użycia Sił Zbrojnych Bośni i Hercegowiny, sprawca podlega

stypizowanych w § 1 lub § 3 jest osoba mająca dostęp do informacji niejawnych na podstawie ustawy o.i.n. BiH albo mająca prawo do klasyfikowania informacji niejawnych, wówczas za przestępstwo z § 1 podlega ona karze pozbawienia wolności co najmniej na 3 lata, a w odniesieniu do przestępstwa z § 3 – co najmniej na 5 lat.

Zwiększenie odpowiedzialności karnej za przestępstwa z § 1–3 jest spowodowane sprawstwem podczas stanów: wyjątkowego, zagrożenia wojną lub wojny, a także podczas działań zbrojnych armii BiH. Wówczas dolna granica kary pozbawienia wolności wynosi 5 lat (zgodnie z § 5 omawianego artykułu). W następnym paragrafie zawarto przepisy dotyczące odpowiedzialności za przestępstwa określone w § 1 i § 4, które zaistniały w wyniku zaniechania. Gwarant nienastąpienia skutku, który przez zaniechanie popełnia przestępstwo z § 1, może zostać skazany na karę grzywny albo co najmniej na 3 lata pozbawienia wolności. W odniesieniu do przestępstwa z § 4 ustanowiono karę pozbawienia wolności od 3 miesięcy do 3 lat.

Jeżeli w wyniku zaniechania (opisanego w § 6) nastąpiło ujawnienie lub wykorzystanie informacji, które zgodnie z prawem zostały oznaczone jako „poufne", „tajne" lub „ściśle tajne" albo stanowiły na gruncie poprzedniej ustawy tajemnicę państwową, sprawca podlega karze pozbawienia wolności od 6 miesięcy do 5 lat (§ 7). Ważną regulacją § 8 jest zastrzeżenie, że obowiązek zachowania tajemnicy trwa również po utracie dostępu do informacji niejawnych[16]. Omawiana jednostka redakcyjna w § 9 jest zakończona kontratypem. Ustawodawca uwalnia od odpowiedzialności karnej osobę, która ujawnia lub pośredniczy w ujawnieniu informacji niejawnej, jeżeli treść upublicznionej tajemnicy narusza konstytucyjny porządek Bośni i Hercegowiny lub jest sprzeczna z umową międzynarodową. Kontratyp ma

karze pozbawienia wolności w wymiarze co najmniej 5 lat. § 6. Jeśli przestępstwo z § 1 oraz § 4 niniejszego artykułu popełniono wskutek zaniechania, sprawca podlega: a) za przestępstwo z § 1 niniejszego artykułu, grzywnie lub karze pozbawienia wolności w wymiarze co najmniej 3 lat; b) za przestępstwo z § 4 niniejszego artykułu, karze pozbawienia wolności od 3 miesięcy do lat 3. § 7. Jeśli przestępstwo z § 6 niniejszego artykułu popełniono w związku z informacją, która według ustawy została oznaczona jako »poufne« lub klauzulą »tajne«, lub jako »tajemnica państwowa«, lub klauzulą »ściśle tajne«, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 5".

[16] Art. 164 kk FBiH: „§ 8. Postanowienia z § 1, § 3–7 niniejszego artykułu mają również zastosowanie w stosunku do osoby, która bez uprawnień poinformuje drugą osobę, przekaże lub udostępni informacje niejawne po wygaśnięciu jej obowiązków jako osoby urzędowej lub osoby odpowiedzialnej w instytucjach Bośni i Hercegowiny, lub funkcjonariusza wojskowego, lub osoby upoważnionej do określania tajności informacji lub dostępu do informacji niejawnych. § 9. Nie popełnia przestępstwa ujawnienia informacji niejawnych ten, kto publikuje lub pośredniczy w publikowaniu informacji niejawnych, których treść jest sprzeczna z porządkiem konstytucyjnym Bośni i Hercegowiny, w celu podania do publicznej wiadomości nieprawidłowości związanych z organizacją, działalnością lub kierowaniem służbą lub w celu podania do publicznej wiadomości faktów stanowiących naruszenie porządku konstytucyjnego lub umowy międzynarodowej, jeśli ujawnienie nie ma poważnie negatywnych następstw dla Bośni i Hercegowiny".

zastosowanie wyłącznie wtedy, gdy publikacja tajemnicy nie powoduje poważnej szkody dla tego kraju. W polskim porządku prawnym nie ma adekwatnej regulacji, co – jak się wydaje – szkodzi transparentności realizacji funkcji władzy przez organy wykonawcze.

Artykuł 164 kk BiH jest przepisem częściowo niezupełnym, ponieważ do zdekodowania normy zakazu karnego niezbędne jest użycie kodeksowej definicji informacji niejawnych z art. 2 § 24 kk BiH[17]. Niestety, przywołana definicja nie określa przesłanek klasyfikacyjnych, wskazuje jedynie na dziedziny (działy administracji, obronności i gospodarki), z których informacje mogą stanowić tajemnicę. Bardziej szczegółowe przesłanki klasyfikacyjne, do których odsyła kodeks karny, zostały określone w ustawie o.i.n. BiH. Prawodawca wymienia w niej również dziedziny, w tym bezpieczeństwo publiczne i obronność, z których informacje podlegają ochronie jako niejawne. Jednocześnie wskazuje i wartościuje kryterium szkody dla wybranych interesów państwa. Ważnym postanowieniem jest objęcie kodeksowym terminem „informacje niejawne" tajemnic innych państw i organizacji międzynarodowych oraz regionalnych, dzięki czemu zostają one objęte ochroną karną, tj. art. 164 kk BiH, jako dobro mające podstawy aksjologiczne. Ponadto kodeks karny odnosi się nie tylko do tajemnic sklasyfikowanych na podstawie ustawy o.i.n. BiH, lecz także do tajemnic wynikających z uregulowań innych ustaw lub rozporządzeń.

Szerokie ustawowe rozumienie terminu „informacje niejawne" determinuje zatem rozległą ochronę karnoprawną tajemnic publicznoprawnych BiH oraz informacji niejawnych otrzymywanych od innych podmiotów prawa międzynarodowego i organizacji regionalnych. Ma to znaczenie dla bezpieczeństwa informacji przekazywanych również przez Polskę w ramach umowy między rządem RP a Radą Ministrów Bośni i Hercegowiny o ochronie informacji niejawnych z 2016 r.[18] Na podstawie przedmiotowej umowy strony zobowiązały się do wzajemnej ochrony

[17] Informacje niejawne – informacje z zakresu bezpieczeństwa publicznego, obronności, spraw i interesów zagranicznych, dotyczące działalności lub interesów wywiadu, bezpieczeństwa BiH, komunikacji i innych systemów istotnych dla interesów państwa, wymiaru sprawiedliwości, projektów i planów ważnych dla obronności i działalności wywiadowczej, działalności naukowej, badawczej, technologicznej, gospodarczej, finansowej, a także spraw ważnych dla bezpieczeństwa i funkcjonowania instytucji BiH, tj. struktury bezpieczeństwa na wszystkich szczeblach organizacji państwowej BiH. Są to informacje określone jako niejawne na mocy ustawy, innego rozporządzenia lub aktu ogólnego właściwego organu wydanego na podstawie prawa lub informacje określone jako niejawne zgodnie z przepisami prawa i rozporządzeniami o ochronie informacji niejawnych. Termin ten obejmuje również informacje niejawne innego państwa, podmiotów międzynarodowych i organizacji regionalnych.

[18] *Umowa między Rządem Rzeczypospolitej Polskiej a Radą Ministrów Bośni i Hercegowiny o ochronie informacji niejawnych, podpisana w Sarajewie dnia 7 czerwca 2016 r.* (DzU z 2017 r. poz. 1254).

informacji niejawnych wymienianych w trakcie współpracy. Rządy określiły wzajemne przyporządkowanie stosowanych klauzul w celu zapewniania odpowiedniej ochrony otrzymywanym informacjom. W poniższym zestawieniu zaprezentowano klauzule stosowane przez oba państwa.

Klauzula stosowana w RP	Klauzula stosowana w BiH	Odpowiednik w jęz. angielskim
Ściśle tajne	Vrlotajno	Top secret
Tajne	Tajno	Secret
Poufne	Povjerljivo	Confidential
Zastrzeżone	Interno	Restricted

W związku z kodeksowym odesłaniem zdekodowanie normy zakazu karnego i ustalenie znamion niektórych przestępstw z art. 164 kk BiH obejmujących dyspozycją klauzulowane tajemnice może nastąpić wyłącznie na podstawie przepisów ustawy o.i.n. BiH.

W art. 1 ustawy o.i.n. BiH prawodawca określił zakres wprowadzanych nią regulacji. Za priorytetowy cel legislacyjny przyjęto ujednolicenie systemu przetwarzania i ochrony informacji niejawnych BiH w dziedzinach określonych w tym przepisie, tj. m.in. bezpieczeństwa publicznego, obrony i spraw zagranicznych.

Podmioty zobowiązane do przestrzegania i stosowania ustawy zostały wymienione w art. 2 i 3. Ustawodawca nakazuje administracji publicznej oraz innym instytucjom BiH, które podczas swoich działań wynikających z ustawowych uprawnień wytwarzają informacje niejawne lub korzystają z nich, w tym organizacjom międzynarodowym i regionalnym, jeżeli tak wynika z zawartych porozumień, stosowanie przepisów tej ustawy. W omawianym akcie prawodawca ustanowił również ogólną normę zakazu ujawniania informacji niejawnych, zobowiązując każdą osobę, która legalnie albo w inny sposób weszła w ich posiadanie, do ich ochrony i zachowania w tajemnicy.

W art. 4 zawarto wiele definicji ustawowych. Z punktu widzenia odpowiedzialności karnej najistotniejsze jest rozumienie terminu „zagrożenie dla integralności Bośni i Hercegowiny". Ustawodawca określa, że jest to obiektywne zagrożenie lub atak na: porządek konstytucyjny, niepodległość, niepodzielność terytorialną, suwerenność, bezpieczeństwo, zdolność obronną i podmiotowość międzynarodową BiH.

Określenie znamion przestępstw stypizowanych w art. 164 kk BiH wydaje się niemożliwe bez ustalenia, jakiego rodzaju informacje mogą zostać sklasyfikowane jako poufne, tajne albo ściśle tajne. Klauzulowanie tajemnic na gruncie ustawy o.i.n. BiH, podobnie jak w polskim porządku prawnym, jest realizowane dwuetapowo.

Zgodnie z art. 8 przywołanej ustawy wstępny etap polega na wyselekcjonowaniu takiej informacji, której ujawnienie osobie nieuprawnionej, środkom masowego przekazu albo instytucji lub organowi innego państwa mogłoby spowodować zagrożenie dla integralności BiH, zwłaszcza w zakresie bezpieczeństwa publicznego, obrony, spraw i interesów zagranicznych, interesów wywiadu i bezpieczeństwa BiH, systemów komunikacyjnych, badań naukowych, finansów państwa, gospodarki i sądownictwa. Tak wyodrębniona informacja zyskuje status niejawnej i podlega klasyfikacji zgodnie z przesłankami określonymi w art. 19 ustawy o.i.n. BiH.

Ustawa w przywołanym artykule konstytuuje cztery stopnie tajności informacji niejawnych. Jako kryterium materialnego podziału tajemnic przyjęto interes państwa. Do poniższych klauzul ochronnych włącza się informacje niejawne, których nieuprawnione ujawnienie:

1) mogłoby zagrozić integralności BiH lub spowodowałoby nieodwracalną szkodę dla państwa – są one oznaczone klauzulą „ściśle tajne",
2) mogłoby spowodować wyjątkowo negatywne konsekwencje dla bezpieczeństwa, politycznych, ekonomicznych lub innych interesów BiH – są one oznaczone klauzulą „tajne",
3) mogłoby spowodować negatywne konsekwencje dla bezpieczeństwa lub interesów BiH – są one oznaczone klauzulą „poufne",
4) mogłoby zagrozić działalności organów państwowych albo podmiotom na pozostałych poziomach organizacji państwowej – są one oznaczone klauzulą „zastrzeżone".

Na podstawie analizy powyższych przepisów należy stwierdzić, że klasyfikowanie informacji jako niejawnych jest dokonywane na podstawie zagrożenia interesu BiH, jakie mogłoby powstać w wyniku ujawnienia ich treści, a zatem co do zasady jest zbieżne z polskimi regulacjami. Dziedziny wymienione w ustawie odpowiadają dziedzinom wskazanym w kodeksowej definicji informacji niejawnych.

W celu zachowania reguł komparatystyki prawniczej dla tego istotnego zagadnienia należy zbadać, jak przedmiotowa problematyka jest uregulowana w polskim porządku prawnym. Akt o najszerszym zakresie regulacji, w którym prawodawca ustanowił definicję informacji niejawnych, to ustawa o ochronie informacji niejawnych z 2010 r.[19] (dalej: ustawa o.i.n. RP). Prawodawca w art. 1 ust. 1[20] wskazuje kryteria, których należy użyć w procesie selekcji informacji jawnych

[19] *Ustawa o ochronie informacji niejawnych*.

[20] Tamże, art. 1. ust. 1: „Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej »informacjami niejawnymi«".

w celu wyodrębnienia tylko takich, które z uwagi na konstytucyjne[21] przesłanki ograniczenia prawa do informacji można wytworzyć jako niejawne lub następczo objąć taką ochroną. Ustanowionymi weryfikatorami są skutki, jakie mogłyby nastąpić w wyniku ujawnienia tego rodzaju informacji. Należy do nich: wystąpienie szkody dla RP, spowodowanie zagrożenia wystąpienia szkody dla RP oraz wywołanie niekorzystnego stanu interesów RP. Po przeanalizowaniu przywołanych przesłanek można zauważyć, że tworzą one materialną definicję informacji niejawnych, wskazują bowiem na treść informacji, a nie na jej formę.

W przypadku ustalenia, że ujawnienie danej informacji doprowadziłoby do zaistnienia chociażby jednego z wymienionych skutków, należy dokonać jej klasyfikacji i nadać odpowiednią klauzulę ochrony, a więc uwzględnić nakaz ustanowiony w art. 5 ustawy o.i.n. RP. Jak wskazuje Trybunał Konstytucyjny w uzasadnieniu wyroku z 2009 r.: *Obowiązek przyznawania właściwej klauzuli tajności istnieje i wynika z materialnoprawnych kryteriów klasyfikacji informacji oraz art. 7 Konstytucji*[22]. Klasyfikowanie informacji wyłącznie z zastosowaniem ww. niedookreślonych kryteriów w konsekwencji dotyczyłoby zbyt rozległej liczby informacji. W realnych działaniach osób uprawnionych do nadawania klauzul powodowałoby to dużą dyskrecjonalność oceny, które informacje należy chronić przed ujawnieniem. Z tego względu prawodawca po skonstruowaniu ogólnej definicji informacji niejawnych zawartych w art. 1, w art. 5 określa dziedziny, z jakich informacje niejawne mogą stanowić tajemnicę. Między ogólną (abstrakcyjną) definicją informacji niejawnych a przedmiotowym określeniem obszarów aktywności państwa, które należy chronić przez limitowanie informacji, zachodzi relacja nadrzędności i podrzędności. Obszary wymienione w art. 5 ustawy o.i.n. uniemożliwiają szerokie ograniczanie prawa do informacji w wyniku autonomicznego stosowania art. 1 ust. 1 tej ustawy.

Za uzasadnione należy uznać wątpliwości interpretacyjne powstające w kontekście nieostrych znaczeniowo pojęć, których ustawodawca użył do konstrukcji formalnoprawnych przesłanek służących do nadawania informacjom niejawnym wymaganego poziomu ochrony. Implikuje to pytanie, czy jakakolwiek osoba ustawowo uprawniona do nadania klauzuli dysponuje dostateczną wiedzą, aby uznać, że ujawnienie określonej informacji niejawnej spowoduje albo mogłoby spowodować np. wystąpienie wyjątkowo poważnej lub „tylko" poważnej szkody dla RP. Ustawodawca w art. 5 ust. 1–4 wymienia dziedziny, w których szkoda[23] ma wystąpić,

[21] Zobacz szczególnie: art. 61 ust. 3, art. 54 oraz art. 31 ust. 3 *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (DzU z 1997 r. nr 78 poz. 483, ze zm.).

[22] Wyrok TK z 15 X 2009 r., sygn. akt K 26/08, uzasadnienie pkt 183.

[23] Kierując się zasadą zakazu homonimiczności pojęć, należy przyjąć, że szkoda wskazana w art. 1 jest tożsama ze szkodą z art. 5.

ale nie definiuje, jak należy ją rozumieć i jakie są kryteria jej wartościowania. Ustawowe dookreślenie w tym artykule szkody pojęciami: zagrozi, pogorszy, zakłóci, utrudni, osłabi albo wywrze szkodliwy wpływ nie wyznacza jasnych ram interpretacyjnych.

Wydaje się, że ustawodawca, wskazując w art. 1 na interesy RP, odwoływał się do tych obszarów aktywności państwa, które są wymienione w art. 5 ust. 1–4. Dlatego też przywołane przepisy należy stosować łącznie, ich odrębne stosowanie bowiem prowadzi do interpretacji *ad absurdum*.

Częściowo taką sytuację potwierdza stanowisko Naczelnego Sądu Administracyjnego, który stwierdził, że (…) *informacja jest informacją niejawną, nie w następstwie jej klasyfikacji, a z uwagi na zagrożenie wynikające z jej treści lub sposobu jej uzyskania. Chroniona jest zatem jak informacja niejawna bez względu na to, czy osoba uprawniona uznała za stosowne oznaczyć ją odpowiednią klauzulą*. Naczelny Sąd Administracyjny słusznie uznał, że treść informacji jest priorytetową przesłanką objęcia jej ochroną państwa i jednocześnie pominął formalną klasyfikację (oznaczenie klauzulą) jako element przesądzający o tej ochronie[24]. Powyższa analiza stanowi podstawę, jak się wydaje – uprawnionego, wniosku, że jedynym zgodnym z prawem postępowaniem osób dokonujących wyodrębniania z szerokiego zbioru informacji tych, którym należy nadać status niejawnych, jest łączne stosowanie art. 1 i art. 5 ustawy o.i.n. RP.

Badając regulacje dotyczące klauzulowania informacji, nie można pominąć wad instytucji prawnych, które utrudniają ich ustanowienie. Kryteria wymienione w art. 5 ustawy o.i.n. RP przy uwzględnieniu niedookreśloności pojęć użytych do ich konstrukcji oraz generalnych przesłanek uznania informacji za niejawną (art. 1) utrudniają trafne nadanie klauzuli konkretnej informacji. Dodatkowo, a może przede wszystkim, tworzą warunki sprzyjające nieuzasadnionej uznaniowości przy określaniu poziomu ochrony informacji niejawnych. Urzędnicza dyskrecjonalność w nadawaniu klauzul powoduje stan niepewności, który polega na powstaniu wątpliwości co do rzeczywistej ważności danej informacji dla interesu państwa. Błędna interpretacja materialno-formalnej definicji informacji niejawnych może powodować objęcie ochroną nieistotnych informacji lub pozbawieniem takiej ochrony ważnych informacji.

Interesującym rozwiązaniem legislacyjnym zastosowanym w ustawie o.i.n. BiH jest uprawnienie depozytariusza tajemnicy do negowania istnienia informacji niejawnej, które ustanowiono w art. 26. Jeżeli istnienie tajemnicy może mieć negatywny wpływ na interes BiH, wówczas organy nie mają obowiązku potwierdzania lub zaprzeczania jej istnieniu pomimo żądań podmiotów zainteresowanych. Nie mają więc

[24] Wyrok NSA z 6 VII 2017 r., sygn. akt I OSK 932/16.

obowiązku uzasadniania odmowy udzielenia informacji, ponieważ mogą twierdzić, że nią nie dysponują. Kolejną ważną instytucją prawną wprowadzoną do systemu ochrony tajemnic BiH jest ustanowienie – jako odrębnego upoważnienia – prawa do klauzulowania materiałów niejawnych. To upoważnienie jest niezależne od prawa dostępu do informacji niejawnych, określona osoba bowiem może mieć jedynie dostęp do tajemnic bez prawa nadawania klauzuli. Ustawodawca w art. 13 wymienia osoby, które w związku z piastowanym stanowiskiem są uprawnione do nadawania klauzul „zastrzeżone", „poufne" i „tajne". Natomiast w art. 14 wskazuje wysokich urzędników państwowych, którzy mają prawo klasyfikować informacje niejawne jako „ściśle tajne", a także nadawać informacjom pozostałe klauzule ochrony.

Zgodnie z przyjętą w art. 17 procedurą klasyfikacji informacji osoba nadająca im klauzulę sporządza pisemne uzasadnienie, w którym określa potencjalną szkodę dla BiH w przypadku jej ujawnienia. Jednocześnie w art. 9 zakazuje się obejmowania informacji tajemnicą, jeśli celem jest ukrycie dokonanego przestępstwa, przekroczenia uprawnień albo jakiegokolwiek naruszenia prawa administracyjnego. Deklasyfikowanie informacji (zmiana jej klauzuli na niższą lub pozbawienie jej klauzuli) również wymaga pisemnego uzasadnienia (art. 22). Powyższe przepisy zapewne pozwalają uniknąć przypadkowego zawyżenia lub zaniżenia klauzuli albo sklasyfikowania takich informacji jako tajemnic.

Osoby wymienione w art. 2 ustawy o.i.n. BiH mogą uzyskać dostęp do informacji niejawnych po przeprowadzeniu wobec nich postępowania sprawdzającego. Postępowanie może zostać wszczęte po uzyskaniu zgody osoby, która ma być jego podmiotem. Obowiązek prowadzenia postępowania nie dotyczy informacji „zastrzeżonych", które są udostępniane pracownikom (podobnie jak w RP) w związku z zajmowanym stanowiskiem i decyzją przełożonego. Organem prowadzącym postępowania sprawdzające (bośn. *sigurnosnih provjera*) w BiH jest Agencja Wywiadu i Bezpieczeństwa (bośn. Obavještajno-sigurnosna Agencija). Osoby zajmujące stanowiska związane z dostępem do informacji o określonej klauzuli składają ankietę bezpieczeństwa osobowego (zakres merytoryczny jest zbliżony do polskiego wzoru), która wraz z wnioskiem kierownika jednostki organizacyjnej jest przekazywana wymienionej Agencji za pośrednictwem Ministerstwa Bezpieczeństwa (bośn. Ministarstvo sigurnosti). Prawodawca ustanowił trzy rodzaje postępowań sprawdzających, które są stosowane w zależności od klauzuli informacji, do których dana osoba ma uzyskać dostęp. Postępowanie o podstawowym zakresie sprawdzeń jest stosowane w odniesieniu do klauzuli „poufne", o poszerzonym – do informacji tajnych. Natomiast dostęp do materiałów ściśle tajnych jest warunkowany złożeniem poszerzonej ankiety bezpieczeństwa i dokonaniem specjalnego zakresu sprawdzeń. Jednostki organizacyjne resortu obrony narodowej oraz organy policyjne i służby

specjalne na podstawie art. 33 ustawy o.i.n. BiH realizują podstawowe postępowania sprawdzające wobec pracowników we własnym zakresie.

Procedura uzyskania poświadczenia bezpieczeństwa, podobnie jak w polskim porządku prawnym, jest autonomicznym postępowaniem administracyjnym. Od decyzji o odmowie wydania poświadczenia osoba sprawdzona może wnieść odwołanie do Komisji Parlamentarnej nadzorującej Agencję Wywiadu i Bezpieczeństwa. Jeżeli organ odwoławczy podtrzyma negatywne rozstrzygnięcie, stronie przysługuje skarga do sądu administracyjnego. Poświadczenie umożliwiające dostęp do informacji poufnych jest ważne przez 10 lat, a do wyższych klauzul – 5 lat.

Istotną regulacją chroniącą interes osoby sprawdzanej jest gwarancja zatrudnienia w danej jednostce organizacyjnej w przypadku odmowy wydania lub cofnięcia poświadczenia bezpieczeństwa, o czym mowa w art. 61 ustawy o.i.n. BiH. Pracodawca jest zobowiązany zaproponować osobie, wobec której wszczęto kontrolne postępowanie sprawdzające, jeżeli wymagają tego względy bezpieczeństwa, albo której cofnięto uprawnienia, inne stanowisko pracy, niezwiązane z dostępem do informacji niejawnych. W przypadku braku innych stanowisk pracownik zostaje zwolniony przy uwzględnieniu odszkodowania z tytułu rozwiązania stosunku pracy. Środkiem wymuszającym przestrzeganie wprowadzonych ustawą regulacji jest nie tylko odpowiedzialność karna, lecz także ustanowione ustawą kary pieniężne (art. 78 i art. 79 ustawy o.i.n. BiH). Osoby pełniące funkcje kierownicze w podmiotach zobowiązanych do przestrzegania ustawy, które nie wykonują nałożonych na nie obowiązków, mogą zostać ukarane grzywną w wysokości od 1 tys. do 5 tys. marek zamiennych[25]. Ustawodawca objął sankcjami za naruszenie przepisów pracowników, którzy wykonują obowiązki związane z ochroną informacji, np. prowadzą rejestry, wydają poświadczenia bezpieczeństwa, klasyfikują informacje albo są odpowiedzialne za stosowanie zabezpieczeń fizycznych i innych.

Uregulowanie systemu ochrony tajemnic publicznoprawnych prawem administracyjnym, a także częściowo blankietowy charakter przepisów karnych obowiązujących w BiH pozwalają na identyfikację analogicznych elementów w polskim systemie ochrony informacji niejawnych. Warto rozważyć wprowadzenie do polskiego prawodawstwa instytucji kontratypu przestępstwa ujawnienia informacji niejawnych, które popełniono w celu zawiadomienia o czynie zabronionym lub nieprawidłowościach w funkcjonowaniu administracji publicznej. Z uwagi na liczne kryteria uzyskania prawa dostępu do tajemnic oraz korzystania z niego również gwarancja zatrudnienia w razie utraty rękojmi – przynajmniej w niektórych przypadkach – wydaje się trafnym rozwiązaniem.

[25] Marka zamienna – oficjalna waluta Bośni i Hercegowiny. Jedna marka zamienna dzieli się na 100 fenigów zamiennych (przyp. red.).

Karnoprawna i administracyjna ochrona tajemnic w Republice Chorwacji

Ustawa zasadnicza Republiki Chorwacji (RCh) z 1990 r.[26] do jej nowelizacji w 2010 r., podobnie jak Konstytucja Bośni i Hercegowiny, nie zawierała wprost przepisów dotyczących prawa dostępu do informacji. Chorwacki Parlament (chorw. Hrvatski sabor[27]) 16 czerwca 2010 r. uchwalił nowelizację Konstytucji RCh, w tym m.in. art. 38, do którego dodano kolejny ustęp[28]. Wprowadzonym rozszerzeniem ustanowiono prawo dostępu do informacji, którymi dysponuje każdy organ publiczny, przy zastrzeżeniu, że ograniczenie tego prawa może nastąpić w granicach określonych prawem powszechnym proporcjonalnie do potrzeb, przy uwzględnieniu wartości wolnego i demokratycznego społeczeństwa. Arsen Bačič i Petar Bačič oceniają, że regulacja, będąca odzwierciedleniem podstawowych praw człowieka, zachowuje poziom normatywny podobnych rozwiązań prawnych obowiązujących w innych demokratycznych państwach świata. Zauważają oni, że skuteczna kontrola władzy przez społeczeństwo jest dokonywana przez wprowadzenie i przestrzeganie praw człowieka i podstawowych wolności. Prawo dostępu do informacji dotyczących sposobu sprawowania władzy ogranicza tę władzę i pozwala narodowi jako suwerenowi skutecznie nadzorować działania rządu[29]. Zbieżne co do swej istoty regulacje są zawarte w konstytucjach RP oraz Federacji Rosyjskiej[30].

Zasadniczym aktem prawnym ustanawiającym system ochrony chorwackich tajemnic publicznoprawnych jest ustawa z 13 lipca 2007 r.[31] o ochronie informacji niejawnych (dalej: ustawa o.i.n. RCh). Wymieniony akt znowelizowano ustawą

---

[26] *Ustav Republike Hrvatske* (Narodne Novine broj 56/1990) – (Konstytucja Republiki Chorwacji z 22 XII 1990 r.). Ten akt prawny był zmieniany pięć razy: ustawą z 12 XII 1997 r., ustawą z 9 XI 2000 r., ustawą z 28 III 2001 r., ustawą z 16 VI 2010 r. oraz wyrokiem Sądu Konstytucyjnego z 15 I 2014 r. Wszystkie nowelizacje są dostępne na stronie internetowej urzędowego organu publikacyjnego Republiki Chorwacji Narodne Novine (dalej: N.N.), https://narodne-novine.nn.hr/clanci/sluzbeni/1990_12_56_1092.html.

[27] Jednoizbowy parlament. Zob. szerzej: K. Składowski, *System rządów w Republice Chorwacji*, Łódź 2013, s. 98 i nast.

[28] *Odluku o proglašenju promjene Ustava Republike Hrvatske* (N.N. broj 76/2010).

[29] A. Bačič, P. Bačič, *Sloboda informiranja u sistemu ustavne podjele vlasti*, w: *Pravo na pristup informacjiam i zaštita osobnih podataka*, B.B. Vetma, M. Boban (red.), Split 2015, s. 62 i nast. (materiały z międzynarodowej konferencji naukowo-zawodowej „Prawo dostępu do informacji i ochrony danych osobowych").

[30] Zob. szerzej: R. Wądołowski, *Ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 24, s. 64 i nast.

[31] *Zakon o tajnosti podataka* (N.N. broj 79/2007) – (ustawa o ochronie informacji niejawnych, uchwalona przez Parlament Chorwacji 13 VII 2007 r.).

z 3 VII 2012 r.[32] w zakresie zwolnienia niektórych urzędników państwowych z obowiązku posiadania poświadczenia bezpieczeństwa. Drugim aktem kształtującym system ochrony jest Kodeks karny, uchwalony przez Parlament Chorwacji 21 października 2011 r.[33] (dalej: kk RCh). Alen Rajko na podstawie chorwackiego prawa kształtującego system ochrony informacji trafnie zauważa, że badanie istoty tajemnicy polega na ustaleniu granicy między obywatelskim prawem do wiedzy a publicznym interesem do zachowania pewnych informacji w tajemnicy, tj. między uzasadnionymi a nieuzasadnionymi tajemnicami[34].

Odpowiedzią ustawodawcy na zmianę Konstytucji RCh i wprowadzenie prawa do informacji było uchwalenie w 2013 r. nowej ustawy o prawie dostępu do informacji[35]. Przedmiotowy akt w znacznej mierze znowelizowano w 2015 r.[36] Prawodawca w art. 1 ust. 4 i 5 ograniczył zakres stosowania tej noweli, wskazując, że regulacja nie obejmuje informacji niejawnych – zarówno krajowych, jak i pochodzących z wymiany międzynarodowej. Istotną instytucją znowelizowanej ustawy jest zdefiniowany w art. 5 ust. 7 „test proporcjonalności i interesu publicznego", którego procedurę stosowania określa art. 16. Zgodnie z przywołanym testem w przypadku wątpliwości podczas rozstrzygania wniosku o udostępnienie informacji instytucja udostępniająca te informacje albo je chroniąca przede wszystkim jest zobowiązana zbadać, czy ich udostępnienie może skutkować naruszeniem jednego z interesów określonych w art. 15 ust. 2–4[37] i w jakim zakresie. Rozważa ona zarówno indywidualny interes strony, jak i interes publiczny w rozumieniu dobra, które zaistnieje, jeżeli informacja zostanie udostępniona.

W tekstach przepisów prawa ustanawiających chorwacki system ochrony tajemnic definicją legalną określającą informacje niejawne o najwyższym stopniu ważności ze względu na bezpieczeństwo państwa jest „tajni podatak". System ochrony, podobnie jak w Polsce oraz w BiH, jest oparty na dwóch filarach – karnoprawnym i administracyjnym.

---

[32] *Zakon o izmjeni Zakona o tajnosti podataka* (N.N. broj 86/ 2012) – (ustawa o zmianie ustawy o ochronie informacji niejawnych, uchwalona przez Parlament Chorwacji 3 VII 2012 r.).

[33] *Kazneni zakon* (N.N. broj 125/2011) – (ustawa Kodeks karny, uchwalona 21 X 2011 r.).

[34] A. Rajko, *Tajni podaci: nužnost i (ili) informativna diskriminacija?*, „Politička misao" 1997, t. 34, nr 3, s. 179 i nast.

[35] *Zakon o prawu na pristup informacijama* (N.N. broj 25/2013) – (ustawa o prawie dostępu do informacji).

[36] *Zakon o izmjenama i dopunama Zakona o pravu na pristup informacijama* (N.N. broj 85/2015) – (ustawa o zmianie ustawy o prawie dostępu do informacji).

[37] Między innymi: informacje niejawne, tajemnice handlowe i zawodowe, obszar danych osobowych i inne przypadki, np. zaistnienie podejrzeń, że ujawnienie informacji utrudni prowadzenie postępowań administracyjnych, sądowych albo wykonywanie nadzoru inspekcyjnego.

W prawodawstwie karnym przestępstwa naruszające poufność informacji niejawnych zalicza się do kategorii przestępstw skierowanych przeciw Republice Chorwacji. Kodeks karny RCh w części szczególnej w rozdziale XXXII art. 347 pt. *Ujawnienie informacji niejawnych* penalizuje w § 1 zachowanie polegające na udostępnieniu informacji niejawnej nieuprawnionej osobie. W § 2 stypizowano odrębny czyn zabroniony, który polega na pozyskaniu informacji niejawnej w celu nieuprawnionego użycia przez pozyskującego albo inną osobę. W kolejnych przepisach, tj. § 3 i § 4, prawodawca stypizował formy kwalifikowane czynów opisanych w § 1 i § 2, w § 5 natomiast sankcjonował zaniechanie skutkujące wypełnieniem znamion przestępstwa z § 1[38].

Z komentarza do art. 347 kk RCh autorstwa Zespołu Kodyfikacyjnego Ministerstwa Sprawiedliwości wynika, że sprawcą zasadniczej postaci czynu zabronionego określonego w § 1 może być wyłącznie osoba, której zgodnie z prawem powierzono informacje niejawne, czyli podmiot indywidualny[39]. Użyta w konstrukcji przepisu forma czasownikowa „udostępni" zawiera się w polskim terminie „ujawni", który zastosowano w art. 265 § 1 kk RP. Strona podmiotowa polega na umyślnym zachowaniu w zamiarze bezpośrednim lub ewentualnym. Przestępstwo popełnione w wyniku działania jest zagrożone karą pozbawienia wolności od 6 miesięcy do 5 lat. Sprawstwo na skutek zaniechania jest natomiast sankcjonowane karą pozbawienia wolności do 3 lat, o czym stanowi § 5 omawianego artykułu.

Przestępstwa stypizowanego z § 2 może dokonać osoba, która pozyska informację niejawną w celu jej nieuprawnionego użycia lub użycia przez inną osobę. Znamiona tego przestępstwa wypełni również ten, kto ujawni informację niejawną innej nieuprawnionej osobie, także wówczas, gdy pozna ona tę informację mimowolnie. Podmiot tego przestępstwa jest powszechny, ponieważ potencjalnie każdy może przypadkowo, a nawet wbrew swej woli, zapoznać się z informacją niejawną. Trudno jest bowiem uchronić się od odbioru (usłyszenia, przeczytania) informacji przekazanej przez drugą osobę, która o jej ochronie informuje dopiero po jej przekazaniu. Strona podmiotowa wymienionych przestępstw polega na umyślności

[38] Art. 347 kk RCh: „§ 1. Kto udostępni powierzone mu informacje niejawne nieupoważnionej osobie, podlega karze pozbawienia wolności od 6 miesięcy do lat 5. § 2. Kto pozyska informację niejawną w celu nieuprawnionego użycia jej przez siebie lub inną osobę lub kto udostępni innej osobie taką informację, w posiadanie której wszedł przypadkowo, podlega karze pozbawienia wolności do lat 3. § 3. Kto czyn z § 1 i 2 niniejszego artykułu uczyni dla zysku, podlega karze pozbawienia wolności od roku do lat 10. § 4. Kto przestępstwo z § 1 i 2 niniejszego artykułu popełni w czasie stanu wojennego lub bezpośredniego zagrożenia wojennego, podlega karze pozbawienia wolności od lat 3 do lat 12. § 5. Kto popełni przestępstwo z § 1 niniejszego artykułu wskutek zaniechania, podlega karze pozbawienia wolności do lat 3".

[39] K. Turkovič, *Komentar kaznenog zakona*, Zagreb 2013, s. 417.

zachowania w zamiarze bezpośrednim lub ewentualnym. Dobrem chronionym w § 1 i § 2, podobnie jak w adekwatnych przepisach RP, jest poufność informacji oraz interes państwa. Znamię czasownikowe „pozyska", zastosowane w § 2, jest niedookreślone, a więc obejmuje działania zarówno zgodne, jak i niezgodne z prawem, ważny jest cel pozyskania, tj. wykorzystanie zdobytej informacji, zadysponowanie nią bez posiadania do tego podstaw prawnych. Przepis ten stanowi o „nieuprawnionym użyciu", a zatem każdym użyciu sprzecznym z prawem, bez względu na to, czy przyniesie ono korzyści majątkowe czy osobiste. Istotną przesłanką wypełniającą znamię czynu zabronionego jest podjęcie aktywności (działania) wobec „pozyskanej" informacji, przy braku legitymacji prawnej do jej dokonywania. Samo przypadkowe zapoznanie się z tajemnicą nie jest penalizowane, staje się jednak czynem zabronionym z chwilą jej nieuprawnionego wykorzystania lub przekazania innej nieuprawnionej osobie.

W § 3 art. 347 kk RCh chorwacki prawodawca ustanowił kwalifikowany typ przestępstw określonych w § 1 i § 2. Przesłanką powodującą zaostrzenie odpowiedzialności karnej jest dokonanie wspomnianych czynów zabronionych z niskich pobudek, tj. dla zysku. Zarówno górna, jak i dolna granica kary pozbawienia wolności zostały podniesione odpowiednio – od 1 roku do 10 lat. Popełnienie przestępstw z § 1 lub § 2, gdy Chorwacja znajduje się w stanie wojny lub zagrożenia wojennego, powoduje zwiększoną odpowiedzialność karną. Zagrożenie bezpieczeństwa państwa spowodowane ujawnieniem tajemnicy albo jej nieuprawnionym użyciem w obliczu prowadzenia lub przygotowywania się do wojny jest bardziej prawdopodobne i dotkliwsze dla interesu Chorwacji[40]. Zgodnie z retrybutywnym modelem odpowiedzialności wymiar kary powinien być adekwatny do czynu, zapewne dlatego wymiar kary pozbawienia wolności zwiększono i ustanowiono na poziomie od 3 do 12 lat.

Pomimo że w art. 87 § 12 kk RCh[41] zdefiniowano termin „informacje niejawne", to redakcję omawianych przepisów karnych (art. 347 § 1 i § 2) należy uznać za niezupełną. Prawodawca przez wspomnianą definicję wprowadza dwie relewantne regulacje. Pierwszą jest odesłanie do innej ustawy (bez bliższego określania jakiej), na podstawie której danej informacji przyznano ochronę w związku z zaliczeniem jej do zbioru informacji niejawnych. A więc kryteria klasyfikacyjne nie są ustanowione kodeksem karnym, lecz inną ustawą. Druga regulacja jest normą powszechnego zakazu. Prawodawca konstruuje ją przez użycie w treści omawianej definicji

[40] Tamże.

[41] Informacja niejawna – informacja, która według odrębnej ustawy została określona jako informacja niejawna. Jako informacji niejawnej nie traktuje się informacji, której treść jest sprzeczna z porządkiem konstytucyjnym Republiki Chorwacji, lub informacji, która została oznaczona jako niejawna w celu ukrycia przestępstwa, przekroczenia lub nadużycia uprawnień oraz innych form nielegalnego postępowania w organach państwowych.

stwierdzenia: *Jako informacji niejawnej nie traktuje się informacji, której treść jest sprzeczna z porządkiem konstytucyjnym*, a zatem formułuje imperatyw zakazu utajniania informacji jawnych. Adresatem zakazu jest każdy, a więc również osoby uprawnione do uznania danej informacji za niejawną ze względu na jej znaczenie. Ustawodawca zabrania ograniczania do dostępu do takiej informacji, jeżeli stanowi ona dowód przestępstwa lub innych naruszeń prawa w organach państwowych. Przez zakaz utajniania informacji dotyczących nieprawidłowości w funkcjonowaniu władzy umożliwia zatem suwerenowi sprawowanie nad władzą nadzoru, co zapewnia utrzymanie modelu demokratycznego ustroju państwa.

Powyższe rozważania dają podstawę do stwierdzenia, że jeżeli treść informacji niejawnej jest sprzeczna z konstytucyjnym porządkiem RCh lub została objęta ochroną państwa w celu ukrycia przestępstwa albo innych naruszeń przepisów w jego organach, a zwłaszcza przekroczenia lub nadużycia uprawnień, to ujawnienie takiej informacji niejawnej nie podlega penalizacji ustanowionej w art. 347 kk RCh. Tego rodzaju informacja formalnie niejawna nie korzysta z ochrony prawa właściwej dla informacji, którą zgodnie z materialnymi przesłankami uznano za niejawną. Paralelę z powyższą regulacją stanowią przepisy Zarządzenia wykonawczego prezydenta 13526 z 2009 r.[42] Na ich podstawie prezydent USA zakazuje utrzymywania w tajemnicy informacji lub obejmowania ich klauzulą, aby ukryć naruszenie prawa przez administrację, ograniczyć konkurencję albo ukryć informacje kłopotliwe dla osoby fizycznej lub prawnej[43]. W związku z odesłaniem w art. 87 § 12 kk RCh do innej ustawy zdekodowanie normy zakazu karnego i ustalenie znamion przestępstw z art. 347 kk RCh, którego dyspozycją objęto informacje niejawne, może nastąpić wyłącznie na podstawie przepisów ustawy o ochronie informacji niejawnych z 2007 r. Jak trafnie zauważa Branko Peran, w art. 1 ustawy o.i.n. RCh prawodawca określa zakres rzeczowy normowanych nią obszarów, którymi są: pojęcie informacji niejawnych bez określonego stopnia tajności oraz dostęp do tych informacji i ich ochrona, a także stopnie tajności oraz procedura klasyfikacji i deklasyfikacji informacji niejawnych[44]. Dodatkowo chorwacki ustawodawca przez wskazanie konkretnych instytucji i stanowisk (etatów urzędniczych) precyzuje, jakie podmioty są zobligowane do jej stosowania. Są to: organy państwowe, jednostki samorządowe, osoby prawne upoważnione do wykonywania władzy publicznej,

[42] *The President Executive Order 13526* of 2009, *Classified National Security Information*, https://www.federalregister.gov/documents/2014/07/30/2014-17836/classified-national-security-information [dostęp: 18 V 2022].

[43] R. Wądołowski, *Ochrona informacji niejawnych w USA*…, s. 155.

[44] B. Peran, M. Goreta, K. Vukošić, *Pojam i vrste tajni*, „Zbornikradova. Veleučilišta u Šibeniku" 2015, nr 3–4, s. 127.

osoby prawne i fizyczne, które zgodnie z ustawą o ochronie informacji niejawnych uzyskują dostęp do informacji niejawnych lub informacji bez określenia stopnia tajności (tego rodzaju informacje są uznawane za służbowe lub tzw. wrażliwe) bądź posługują się takimi informacjami.

W art. 2 normodawca sformułował kilka definicji legalnych. Z punktu widzenia odpowiedzialności karnej najistotniejsze jest rozumienie terminu „informacja niejawna". Według ustawy jest to informacja, którą jako niejawną oznaczył uprawniony organ za pomocą określonej prawem procedury i dla której określono klauzulę niejawności, z jednoczesnym zastrzeżeniem, że informacja niejawna to również klauzulowana informacja otrzymana od innego państwa.

Dokonanie subsumpcji czynu jako wypełniającego znamiona art. 347 kk RCh zależy przede wszystkim od rozstrzygnięcia, czy ujawniona lub bezprawnie użyta informacja rzeczywiście była informacją niejawną. Chorwacki ustawodawca nie uzależnia odpowiedzialności karnej od klauzuli danej informacji niejawnej, przepis karny bowiem ma zastosowanie do wszystkich stopni informacji niejawnych. Należy przyjąć, że wymiar kary prawdopodobnie zależy od szkody, jaką spowodowało lub mogło spowodować przestępne działanie sprawcy, co jest w głównej mierze determinowane klauzulą ujawnionej informacji niejawnej. W związku z wyżej przywołaną definicją celowe jest zatem ustalenie, jakie podmioty są uprawnione do klasyfikowania informacji oraz jakie kryteria przesądzają o ich utajnianiu.

Zgodnie z art. 13 ustawy o.i.n. RCh klasyfikowania informacji jako ściśle tajnych, tajnych, poufnych i zastrzeżonych mogą dokonywać: prezydent, przewodniczący parlamentu[45], premier rządu, ministrowie, prokurator generalny, zwierzchnik Sztabu Generalnego Sił Zbrojnych, szefowie organów wywiadowczych i bezpieczeństwa RCh oraz osoby upoważnione przez wymienionych urzędników – w ramach posiadanych przez nich kompetencji. Klauzulę „poufne" oraz „zastrzeżone" mogą przyznawać szefowie pozostałych organów państwowych. Obowiązkiem osób uprawnionych do klasyfikowania informacji jest obejmowanie ochroną informacji, które są wytwarzane przez instytucje naukowe i przedsiębiorstwa w ramach realizacji projektów mających znaczenie dla bezpieczeństwa RCh.

Prawodawca w art. 3 omawianej ustawy wprowadza zakaz obejmowania klauzulą niejawności informacji w celu zatajenia przestępstwa, przekroczenia lub nadużycia uprawnień oraz innych form nielegalnego postępowania w organach państwowych. Przedmiotowa regulacja koresponduje z imperatywem art. 87 kk RCh, o którym wspomniano powyżej.

[45] Zob. szerzej: K. Krysieniel, *Ewolucja systemu politycznego w Chorwacji 1990–2010. Próba bilansu*, „Przegląd Prawa Konstytucyjnego" 2010, nr 2–3, s. 241–260.

W art. 6 ustawodawca nakłada na uprawnione osoby obowiązek klasyfikowania informacji. Jako kryterium materialnego podziału tajemnic wskazuje interes państwa. Za słuszne należy również uznać spostrzeżenie Perana, że procedura klasyfikacji informacji oznacza nadanie jednego ze stopni tajności informacji adekwatnie do zagrożenia i wartości chronionych ustawą[46]. Prawodawca stanowi, że ściśle tajnymi są informacje, których nieupoważnione ujawnienie spowodowałoby nieodwracalną szkodę dla bezpieczeństwa narodowego i żywotnych interesów RCh, a szczególnie dla: podstaw jej porządku konstytucyjnego, niezależności, integralności i bezpieczeństwa, relacji międzynarodowych, zdolności obronnej i systemu wywiadowczego, bezpieczeństwa obywateli, podstaw systemu gospodarczego i finansowego, odkryć naukowych, wynalazków i technologii ważnych dla bezpieczeństwa narodowego.

Definiowanie niższych klauzul niejawności polega na wartościowaniu szkody dla interesu państwa w odniesieniu do dóbr, które należy objąć najwyższym stopniem ochrony, tj. klauzulą „ściśle tajne". Ustawodawca w art. 7 precyzuje, że jako „tajne" należy klasyfikować informacje, których nieupoważnione ujawnienie poważnie zaszkodziłoby wartościom wymienionym w art. 6 ustawy. Jeżeli natomiast nieupoważnione ujawnienie zaszkodziłoby wyżej wymienionym wartościom bez wskazywania intensywności (wymiaru) szkody, wówczas należy stosować klauzulę „poufne".

Klauzulą „zastrzeżone" są klasyfikowane informacje, których nieuprawnione ujawnienie zaszkodziłoby działalności i wykonywaniu zadań organów państwowych przy realizacji działań wymienionych w art. 5 wspomnianej ustawy[47].

Warto wspomnieć, że na podstawie umowy z 2016 r. między rządem Rzeczpospolitej Polskiej a rządem Republiki Chorwacji w sprawie wzajemnej ochrony informacji niejawnych strony zobowiązały się do wzajemnej ochrony informacji niejawnych wymienianych w toku współpracy[48]. Rządy określiły wzajemne przyporządkowanie stosowanych klauzul w celu zapewniania odpowiedniej ochrony otrzymywanym informacjom. W zestawieniu na następnej stronie zaprezentowano klauzule stosowane przez oba państwa.

---

[46] B. Peran, M. Goreta, K. Vukošić, *Pojam i vrste tajni*…, s. 133.

[47] Art. 5. kk RCh: Ze względu na stopień zagrożenia chronionych wartości stopniami tajności (ściśle tajne, tajne, poufne, zastrzeżone – dop. aut.) z artykułu 4 niniejszej ustawy mogą być klasyfikowane informacje z obszaru działania organów państwowych w zakresie obrony, systemu wywiadowczego i bezpieczeństwa, spraw zagranicznych, bezpieczeństwa publicznego, postępowania karnego oraz nauki, technologii, finansów publicznych i gospodarki, jeśli te informacje mają znaczenie dla interesów bezpieczeństwa Republiki Chorwacji.

[48] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o wzajemnej ochronie informacji niejawnych, podpisana w Warszawie dnia 6 października 2016 r.* (DzU z 2017 r. poz. 2071).

Klauzula stosowana w RP	Klauzula stosowana w RCh	Odpowiednik w jęz. angielskim
Ściśle tajne	Vrlotajno	Top secret
Tajne	Tajno	Secret
Poufne	Povjerljivo	Confidential
Zastrzeżone	Ograničeno	Restricted

Chorwacki prawodawca precyzuje w ustawie o ochronie informacji niejawnych zakres postępowania sprawdzającego oraz kryteria uzyskiwania poświadczenia bezpieczeństwa (chorw. *certifikat*), które są zbliżone do odpowiadających im przepisów polskich. Osoby, które zajmują stanowiska związane z informacjami niejawnymi, mogą uzyskać do nich dostęp po wypełnieniu specjalnego kwestionariusza i wyrażeniu zgody na zastosowanie wobec nich procedury kontroli bezpieczeństwa osobowego (chorw. *sigurnosna provjera*). Kierownik jednostki organizacyjnej, w której zainteresowana osoba jest zatrudniona, występuje z wnioskiem do Biura Rady Bezpieczeństwa Narodowego (chorw. Ured Vijeća za nacionalnu sigurnost)[49]. Rada w celu dokonania niezbędnych sprawdzeń przekazuje kwestionariusz kandydata do Agencji Wywiadu i Bezpieczeństwa (chorw. Sigurnosno–obavještajna agencija)[50]. Ta w ramach prowadzonego postępowania kontroli bezpieczeństwa danej osoby weryfikuje informacje zawarte w kwestionariuszu oraz bada, czy występują tzw. przeszkody bezpieczeństwa wymienione w art. 18 ust. 6 ustawy o.i.n. RCh, tj.: podanie nieprawdziwych informacji w kwestionariuszu, okoliczności określone w odrębnych ustawach, które uniemożliwiają przyjęcie osoby do służby państwowej, orzeczone sankcje dyscyplinarne oraz inne fakty stanowiące podstawę podejrzeń co do poufności i rzetelności postępowania przy przetwarzaniu informacji niejawnych. Biuro Rady Bezpieczeństwa Narodowego na podstawie oceny bezpieczeństwa wykonanej przez Agencję Wywiadu i Bezpieczeństwa wydaje certyfikat lub decyzję odmowną. Od negatywnego rozstrzygnięcia stronie nie przysługuje odwołanie do organu wyższego stopnia, jednak jest ona uprawniona do złożenia skargi do sądu i prowadzenia sporu przed sądami administracyjnymi.

Reasumując, podstawą chorwackiego systemu ochrony tajemnic publicznoprawnych są ustawa o ochronie informacji niejawnych oraz częściowo blankietowe przepisy karne, podobnie jak w Bośni i Hercegowinie oraz Polsce. Aktem uszczegóławiającym chorwacką ustawę o ochronie informacji niejawnych jest ustawa z 2007 r. o bezpieczeństwie informacji, która ustanawia standardy ochrony informacji

[49] Zob. szerzej: Ured Vijeća za nacionalnu sigurnost, https://www.uvns.hr/ [dostęp: 1 X 2021].

[50] Zob. szerzej: Sigurnosno–obavještajna agencija, https://www.soa.hr/hr [dostęp: 1 X 2021].

niejawnych[51]. Adresatami tej ustawy są podmioty administracji publicznej oraz osoby prawne i fizyczne, które mają dostęp do informacji niejawnych. W przywołanym akcie zostały określone środki i zasady ochrony informacji w pięciu obszarach bezpieczeństwa, tj.: kontroli, ochrony fizycznej, zabezpieczenia danych, bezpieczeństwa systemów informatycznych i współpracy handlowej.

Ustawowe rozdzielenie prawa do nadawania klauzul informacjom niejawnym od prawa dostępu do tego rodzaju informacji, które zastosowano w prawodawstwie Bośni i Hercegowiny oraz Chorwacji, zwiększa pewność poprawnego klasyfikowania informacji, a tym samym minimalizuje niebezpieczeństwo nieuzasadnionego utajniania informacji jawnych. Wydaje się jednak, że przyjęte rozwiązanie ogranicza dynamikę obejmowania ochroną państwa informacji istotnych dla jego bezpieczeństwa. Polski ustawodawca nie wprowadził tego rodzaju regulacji, dlatego też każda osoba uprawniona do przetwarzania informacji niejawnych może dokonywać ich klasyfikacji w zakresie klauzul objętych posiadanym poświadczeniem bezpieczeństwa, o ile jest uprawniona do podpisania danego dokumentu lub oznaczenia materiału.

Jak wspomniano na wstępie, niniejszy artykuł nie wyczerpuje przedmiotu rozważań, może jednak być przyczynkiem do sformułowania problemów badawczych, a w rezultacie dać asumpt do dalszych badań naukowych. Na podstawie przedstawionego materiału należy stwierdzić, że systemy ochrony informacji niejawnych Republiki Chorwacji oraz Bośni i Hercegowiny nie są odmienne, a także nie odbiegają od polskich regulacji. Wykazują duże podobieństwa do systemu przyjętego w polskim porządku prawnym. Niektóre instytucje prawne, które nie występują w RP, mają charakter gwarancyjny w odniesieniu do praw podmiotowych danej osoby, np. zapewniają dalsze zatrudnienie w przypadku odmowy wydania poświadczenia bezpieczeństwa. Mogą również wzmacniać nadzór nad władzą wykonawczą, np. przez niesankcjonowanie ujawnienia informacji niejawnych, które objęto ochroną w celu ukrycia przestępstwa.

Bibliografia

Bačič A., Bačič B., *Sloboda informiranja u sistemu ustavne podjele vlasti*, w: P*ravo na pristup informacjiam i zaštita osobnih podataka*, B.B. Vetma, M. Boban (red.), Split 2015, s. 25–66.

Jawność i jej ograniczenia, G. Szpor (red. nauk.), t. 11: *Standardy europejskie*, C. Mik (red.), Warszawa 2016.

[51] *Zakon o informacijskoj sigurnosti* (N.N. broj 79/2007, 2484) – (ustawa o bezpieczeństwie informacji, uchwalona 13 lipca 2007 r.).

Krysieniel K., *Ewolucja systemu politycznego w Chorwacji 1990–2010. Próba bilansu*, „Przegląd Prawa Konstytucyjnego" 2010, nr 23, s. 241–260.

Osóbka P., *System konstytucyjny Bośni i Hercegowiny*, Warszawa 2011.

Peran B., Goreta M., Vukošić K., *Pojam i vrste tajni*, „Zbornikradova. Veleučilišta u Šibeniku" 2015, nr 3–4.

Rajko A., *Tajni podaci: nužnost i (ili) informativna diskriminacija?*, „Politička misao" 1997, t. 34, nr 3.

Składowski K., *System rządów w Republice Chorwacji*, Łódź 2013.

Turkovič K. i in., *Komentar kaznenog zakona*, Zagreb 2013.

Wądołowski R., *Ochrona informacji niejawnych w USA. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 25, s. 146–182.

Wądołowski R., *Ochrona tajemnicy państwowej w Federacji Rosyjskiej. Wybrane regulacje karne i administracyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, nr 24, s. 63–90.

Źródła internetowe

Sigurnosno–obavještajna agencija, https://www.soa.hr/hr [dostęp: 1 X 2021].

Ured Vijeća za nacionalnu sigurnost, https://www.uvns.hr/ [dostęp: 1 X 2021].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. DzU z 2019 r. poz. 742, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j: DzU z 2022 r. poz. 1138).

Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Chorwacji o wzajemnej ochronie informacji niejawnych, podpisana w Warszawie dnia 6 października 2016 r. (DzU z 2017 r. poz. 2071).

Umowa między Rządem Rzeczypospolitej Polskiej a Radą Ministrów Bośni i Hercegowiny o ochronie informacji niejawnych, podpisana w Sarajewie dnia 7 czerwca 2016 r. (DzU z 2017 r. poz. 1254).

Akty prawne Republiki Chorwacji

Ustav Republike Hrvatske (Narodne Novine broj 56/1990).

Zakon o izmjenama i dopunama Zakona o pravu na pristup informacijama (Narodne Novine broj 85/2015).

Zakon o prawu na pristup informacijama (Narodne Novine broj 25/2013).

Zakon o izmjeni Zakona o tajnosti podataka (Narodne Novine broj 86/2012).

Kazneni zakon (Narodne Novine broj 125/2011).

Zakon o informacijskoj sigurnosti (Narodne Novine broj 79/2007, 2484).

Zakon o tajnosti podataka (Narodne Novine broj 79/2007, 2483).

Odluku o proglašenju promjene Ustava Republike Hrvatske (Narodne Novine broj 76/2010).

Akty prawne Bośni i Hercegowiny

Ustav Bosne i Hercegovine. Sarajevo, Office of the High Representative, https://biblioteka.sejm.gov.pl/wp-content/uploads/2016/09/Bo%C5%9Bnia-i-Hercegowina_bos_010716.pdf.

Zakon o zaštiti tajnih podataka (Službeni glasnik BiH broj 54/2005).

Krivični zakon Bosne i Hercegovine (Službeni glasnik BiH broj 3/2003).

Krivični zakon Federacije Bosne i Hercegovine (Službene novine FBiH broj 36/2003 ispr. – 75/2017).

Akty prawne USA

Constitution of the United States of America, House of Representatives, dok. No 110 – 50.

Zarządzenie wykonawcze prezydenta USA

The President Executive Order 13526 of 2009, *Classified National Security Information*, https://www.federalregister.gov/documents/2014/07/30/2014-17836/classified-national-security-information [dostęp: 18 V 2022].

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z 15 X 2009 r., sygn. akt K 26/08.

Wyrok Naczelnego Sądu Administracyjnego z 6 VII 2017 r., sygn. akt I OSK 932/16.

Wyrok Sądu Najwyższego USA w sprawie „Hustler" v. Falwell, 485 U.S. 46, 24 II 1988 r.