PRZEGLĄD ZACHODNI
2023, nr 3
doi.org/10.60972/PZ.2023.3.117

KATARZYNA KAMIŃSKA-KOROLCZUK
Gdańsk
ORCID 0000-0002-4895-2399

Polityka informacyjna i cyberbezpieczeństwa w Estonii i Łotwie w drugiej i na początku trzeciej dekady XXI wieku

Wstęp

Prowadzona przez Federację Rosyjską wojna przeciwko Ukrainie destabilizuje sytuację społeczno-polityczną nie tylko na terenie zaatakowanego państwa, lecz i w całym regionie. Nie pozostaje też bez wpływu na poczucie bezpieczeństwa ludzi w innych częściach świata. W wyniku procesu globalizacji, który zachodził i zachodzi w wielu obszarach, w tym politycznym i gospodarczym, państwa powiązane są na tyle silnymi więzami, że zagrożenie niepodległości jednego z nich implikuje konsekwencje dla pozostałych. Obserwując działania władz Federacji Rosyjskiej, zauważyć można dywersyfikację siły – od *soft power*, czyli miękkiej siły, którą są między innymi oddziaływania na inne państwa przy wykorzystaniu sojuszy, dyplomacji czy poprzez propagowanie kultury, na rzecz posunięć, które Joseph S. Nye określa mianem *hard power* (Nye 2004). Wojna w Ukrainie jest agresją, pokazem dominacji siły. Obok tych działań Rosja podejmuje w Europie Środkowo-Wschodniej także inne rodzaje aktywności i czyni to w zasadzie od momentu odzyskania niepodległości/pełnej suwerenności przez państwa będące wcześniej w rosyjskiej sferze wpływów (Dudzińska, Piotrowski 2017; Piotrowski, Raś 2017; Baluk 2020). Wykorzystuje rozwój technologii cyfrowych do akcji, które niejednokrotnie destabilizowały sytuację w tym regionie. Prowadzenie polityki wobec państw ościennych poprzez media, posługiwanie się w mniejszym stopniu perswazją, w większym zaś przekazywanie rosyjskiej wizji świata w materiałach propagandowych, to z kolei przykłady działań typu *smart power*. Wspomniany już Nye pojmuje *smart power* jako strategiczne łączenie instrumentów miękkiej i twardej siły w polityce zagranicznej. Jej wykorzystanie prowadzić ma między innymi do

realizacji interesów państwa stosującego siłę typu *smart* na zasadzie maksymalizacji zysków (Nye 2009). Jedną z możliwości przeciwdziałania *smart power* jest prowadzenie przez państwa narażone na ten rodzaj oddziaływania konsekwentnej i zaplanowanej polityki informacyjnej. Wzmacnia ona zaufanie do władzy, tym samym osłabiając siłę pojawiających się w przestrzeni publicznej zmanipulowanych informacji. A manipulowanie przekazem, stosowanie komunikowania intencjonalnego, jakim jest propaganda, to elementy nacisku wywieranego przez Rosję na Estonię i Łotwę. Działania skierowane są przede wszystkim do licznej ludności rosyjskojęzycznej zamieszkującej oba państwa i odnoszą różny, coraz częściej raczej niewielki, skutek (Kozłowski 2019). Odpowiedzią władz omawianych państw na prowokacje, również w sferze cyfrowej jest między innymi polityka informacyjna prowadzona poprzez media oraz wdrażanie regulacji prawnych mających zapewnić cyberbezpieczeństwo, szczególnie ze strony największego sąsiada – Rosji.

Założenia wstępne, cel artykułu i metody badawcze

Przedmiotem analizy są polityka informacyjna i ustawy oraz strategie dotyczące cyberbezpieczeństwa implementowane w Estonii i Łotwie. Założeniem uregulowań prawnych jest podwyższanie poziomu cyberbezpieczeństwa zgodnie z potrzebami polityki wewnętrznej. Regulacje odnoszą się do wytycznych Unii Europejskiej (UE) i generalnie są także kompatybilne z działaniami innych państw dostrzegających problem bezpieczeństwa cyfrowego w przestrzeni międzynarodowej (Calderaro, Craig 2020; Bechara, Schuch 2021).

W pracy przedstawione są rozwiązania wprowadzone przez Estonię i Łotwę, które mają zapewniać bardziej bezpieczne funkcjonowanie infrastruktury cyfrowej wykorzystywanej do prowadzenia polityki informacyjnej państwa oraz świadczenia usług publicznych. Celem opracowania jest analiza regulacji występujących w Estonii i Łotwie oraz ocena skuteczności podejmowanych posunięć w kontekście prowadzonej przez Rosję kampanii dezinformacyjnej mającej za zadanie destabilizowanie sytuacji w regionie. Tezą artykułu jest stwierdzenie, że działania dotyczące zapewniania cyberbezpieczeństwa są istotne dla władz Łotwy i Estonii, które dostrzegają stojące przed nimi wyzwania wynikające z niełatwego sąsiedztwa z Rosją. Podkreślić należy, że przesłanki do powstawania prawa odnoszącego się do bezpieczeństwa infrastruktury cyfrowej istniały już przed rozpoczęciem przez Rosję wojny z Ukrainą. Działania zbrojne jedynie zaostrzyły problem. Artykuł skupia uwagę na oddziaływaniach w wybranym regionie, stąd Rosja występuje jako pierwszoplanowy aktor

prowadzący kampanie dezinformacyjne. Podkreślić należy, że podobną aktywność prowadzą i inne państwa w różnych częściach świata, jak i globalnie, nie jest to jednak przedmiotem tego opracowania.

Zapewnianie cyberbezpieczeństwa narodowego to osiąganie jak najlepszej odporności na zagrożenia w cyberprzestrzeni. Z założenia cyberprzestrzeń jest miejscem powstawania, przetwarzania i wymiany informacji w systemach teleinformatycznych pomiędzy użytkownikami, tak prywatnymi, jak i realizującymi zadania państwa (Ustawa z dnia 17 lutego 2005 r.). Cyberbezpieczeństwo jest stopniowalne, odnosi się do subiektywnego poczucia braku zagrożenia lub jego występowania. We współczesnym świecie cyberbezpieczeństwo dopełnienia aspekty związane z dbaniem o zachowanie integralności terytorialnej, wpływa na zdolność do wchodzenia w sojusze oraz nawiązywania współpracy od ekonomicznej po militarną. To także jeden z gwarantów zaufania do prowadzonej polityki informacyjnej państwa. Z kolei zaufanie to podstawowy warunek skutecznego wdrażania strategii przeciwdziałania wyzwaniom wynikającym z pojawiania się dezinformacji w świecie nieskrępowanego przepływu informacji (Kamińska-Korolczuk 2021).

Polityka informacyjna państwa to komunikowanie się władzy z obywatelami, a w przypadku Estonii i Łotwy także nieobywatelami, które polega na przekazywaniu wiadomości i utrwalaniu ich treści celem informowania o przedsięwzięciach i planach władzy. Działanie służyć ma maksymalizowaniu posiadanej legitymizacji. Podkreślić należy, że polityka informacyjna może być też intencjonalnym nieinformowaniem, co prowadzić ma do osiągnięcia dokładnie tego samego rezultatu (Kamińska-Korolczuk 2021: 11). Istotną częścią polityki informacyjnej w państwach demokratycznych jest zapewnienie dostępu do rzetelnych informacji, przewidywalność procesów prowadzących do jej powstania i rozpowszechniania, a także zapewnienie bezpieczeństwa sieci przesyłu danych cyfrowych, które warunkują szybki dostęp do informacji. Presja związana z utrzymywaniem bezpiecznych łączy jest duża, szczególnie w Estonii, która jest jednym z najbardziej scyfryzowanych państw świata. Istotnym elementem w prowadzonej polityce informacyjnej jest też kondycja rynku mediów. W Estonii i Łotwie tradycje korzystania z mediów są ugruntowane, a sam rozwój prasy drukowanej i elektronicznej przebiegał dynamicznie (Kamińska-Korolczuk 2014a, 2014b), prowadząc do wykształcania społeczeństw informacyjnych, czyli takich, których cechą jest wytwarzanie informacji i czerpanie profitów z ich przetwarzania (Goban-Klas, Sienkiewicz 1999; Golka 2005).

Do zrealizowania celu pracy i potwierdzenia tezy pomocne są: 1. ustalenia poczynione na podstawie obserwacji bezpośrednich i badań terenowych; 2. analiza źródeł oraz danych zastanych wraz z systematycznym przeglądem

literatury – *systematic literature review* (Fink, 2005, s. 17) i metodą instytucjonalno-prawną polegającą na badaniu aktów normatywnych (Żebrowski 2012: 32-33), którą zastosowano do przeanalizowania zmian zachodzących w porządku prawnym Estonii i Łotwy.

Artykuł jest pracą przeglądową, a jego układ jest następujący: analiza najważniejszych kwestii związanych z kształtem polityki informacyjnej prowadzonej poprzez media przez Estonię i Łotwę, następnie przedstawienie działań dotyczących wzmacniania cyberbezpieczeństwa podejmowanych przez omawiane państwa, także tych wynikających z przynależności do UE, co pozwoli w podsumowaniu potwierdzić postawioną w artykule tezę, iż poczynania odnoszące się do zapewniania cyberbezpieczeństwa są istotne dla władz Łotwy i Estonii, a omawiane zagadnienia są postrzegane jako poważne wyzwania wynikające z sytuacji prowokowanej przez Rosję.

Prowadzone badania mają określony zasięg geograficzny – obejmują terytoria Estonii i Łotwy oraz czasowy – dotyczą okresu od wdrożenia pierwszych ustaw dotyczących cyberbezpieczeństwa po wiosnę 2023 r., czyli momentu ukończenia artykułu. Z uwagi na wieloaspektowość i obszerność zagadnienia omówiono najistotniejsze kwestie.

Estonia i Łotwa w strukturach europejskich

Od ponad trzydziestu lat Estonia i Łotwa ponownie funkcjonują w Europie jako suwerenne i demokratyczne państwa. Ze względu na położenie geograficzne Organizacja Narodów Zjednoczonych włącza je do kręgu państw Europy Północnej (ONZ), mimo iż w dyskursie publicznym, w tym i naukowym, najczęściej określa się je, wraz z Litwą, mianem „państw bałtyckich". Różnice między nimi są jednak znaczące, a odrębność opisywanych państw wynika przede wszystkim z różnie kształtującej się tożsamości kulturowej, religijnej, językowej czy narodowej. To, co niewątpliwie łączy omawiane państwa, to fakt, że zostały wcielone do Związku Socjalistycznych Republik Radzieckich (ZSRR) w 1940 r., stając się kolejnymi z piętnastu republik związkowych, a odzyskały niepodległość po okresie funkcjonowania w sferze wpływów ZSRR.

Aneksja Estonii i Łotwy do ZSRR dokonała się na mocy tajnego protokołu dodatkowego paktu Ribbentrop-Mołotow, czyli umowy międzynarodowej zawartej między III Rzeszą Niemiecką a ZSRR. W dokumencie określono strefy wpływów obu umawiających się mocarstw. Aneksja nigdy nie została uznana przez Estończyków i Łotyszy oraz część państw świata, stała się jednak faktem, a po zakończeniu II wojny światowej Estonia i Łotwa pozostały w ZSRR jako

republiki związkowe. Częścią ich historii stały się brak suwerenności, polityczne i gospodarcze funkcjonowanie w systemie państwa niedemokratycznego. Władze ZSRR podejmowały także działania, które miały prowadzić do zniwelowania poczucia odrębności narodowej Estończyków i Łotyszy (Hiden, Made, Smith 2008; Smith i in. 2002: XIX-XX).

Symbolem przeobrażeń dokonujących się w tej części Europy, które doprowadziły do upadku systemu zależnego od ZSRR i odzyskania niepodległości przez państwa regionu, stała się m.in. Śpiewająca Rewolucja, czyli kontynuacja festiwali ludowych, z których pierwszy odbył się w 1869 r. (Smith 2002: 7), pozwalająca na utrzymanie poczucia odrębności kulturowej i wiary w możliwość zmian (Vogt 2005: 20-31) oraz silnie zakorzeniona potrzeba dostępu do informacji, wypracowana jeszcze w czasie, gdy na rozwój mediów na terenie dzisiejszej Estonii i Łotwy wpływ mieli przedstawiciele inteligencji wywodzącej się z Niemców bałtyckich (Kamińska-Korolczuk 2014a, 2014b). Estonia ogłosiła niepodległość 20 sierpnia 1991 r., Łotwa dzień później. Istotną częścią procesu odbudowywania struktur państw były działania uniezależniające od niedawnego okupanta, w tym projektowanie i wdrażanie strategii prowadzących do powstania społeczeństw odpornych na dezinformację.

Od 1 maja 2004 r. Estonia i Łotwa są członkami UE. Uczestniczą w programach rozwojowych, w tym w zatytułowanym „Droga ku cyfrowej dekadzie", który Komisja Europejska UE przedstawiła na początku 2022 r. Zakłada on osiągnięcie do 2030 r. wspólnych celów państw członkowskich w zakresie wdrażania umiejętności cyfrowych. Założenie wstępne wnosi, że społeczeństwa będą miały dostęp do sprawiedliwego, bezpiecznego i chronionego środowiska internetowego (Komisja Europejska a; Komisja Europejska c). To nie pierwszy raz kiedy kwestie cyberbezpieczeństwa są poruszane na forum UE. Odnosiła się już do nich m.in. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Parlament Europejski 2016), Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie *ENISA* (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Parlament Europejski 2019). Celem uregulowań jest dążenie do wypracowania standardów reagowania na cyberataki oraz budowanie silnego systemu cyberbezpieczeństwa UE. Wdrożenie bezpiecznej i zrównoważonej infrastruktury cyfrowej oznaczać ma 100% cyfryzację usług publicznych i 80% skuteczność wdrożenia identyfikacji elektronicznej obywateli (Komisja Europejska c).

Cyfrowy rozwój państw członkowskich monitorowany jest przez Komisję Europejską UE od 2014 r. Gromadzone dane przedstawiane są w raportach Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (*The Digital Economy and Society Index, DESI*), które analizują kondycję państw w czterech obszarach Cyfrowego Kompasu na 2030 r., czyli założeniach przedstawionych w Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Wskaźniki *DESI* dotyczą następujących kwestii:

1. kapitału ludzkiego, wskazując na stopień wykwalifikowania społeczeństwa, w tym i profesjonalistów, w dziedzinie cyfrowej,
2. łączności, rozumianej m.in. jako dostęp i wykorzystanie stacjonarnych i mobilnych łączy szerokopasmowych, możliwość korzystania z bezpiecznej, wydajnej i zrównoważonej infrastruktury cyfrowej,
3. transformacji cyfrowej przedsiębiorstw polegającej m.in. na integracji technologii cyfrowych przedsiębiorstw i handlu,
4. cyfryzacji usług publicznych (Komisja Europejska d).

W raporcie *DESI* za 2022 r. Estonia zajmuje 9., a Łotwa 17. miejsce spośród wszystkich państw członkowskich UE. Na trzy z czterech wymienionych powyżej wskaźników, na które zwraca się uwagę w *DESI*, Estonia osiąga wyniki powyżej średniej UE. Wyjątkiem jest wskaźnik dotyczący łączności. Pod tym względem zajmuje 26. miejsce, tym samym znacząco odbiegając od osiągnięć na pozostałych polach cyfryzacji (Komisja Europejska 2022a: 3). Łotwa z kolei wykazuje mniejszą dynamikę wzrostu we wszystkich sferach, wykazując niższe wartości w indeksie w odniesieniu do większości państw UE. Jedynie wskaźnik czwarty – dostęp do cyfrowych usług publicznych – w 2022 r. był na poziomie powyżej średniej UE. Łotwa zajmuje 11. miejsce w UE z liczbą użytkowników e-administracji na poziomie 84%, co plasuje ją powyżej średniej unijnej, wynoszącej 65% (Komisja Europejska 2022b: 3, 4, 14).

Dwudzieste szóste miejsce Estonii pod względem nasycenia rynku infrastrukturą zapewniającą wysokiej jakości stabilną łączność to bardzo słaby rezultat jak na jedno z najbardziej scyfryzowanych w Europie państw, należących do podmiotów inwestujących w rozbudowę szerokopasmowego internetu od pierwszej dekady XXI w. (Kamińska-Korolczuk 2023). Z kolei Łotwa pod względem udostępnianej łączności zajmuje dwudzieste miejsce. Choć zasięg sieci stacjonarnej o bardzo dużej przepustowości – *very high capacity network* – *VHCN* (Berec) wynosi 91% i przekracza średnią UE o 21 punktów procentowych, to w ostatnich latach dynamika wzrostu jest niewielka, a rozwój sieci światłowodowej od 2018 r. do 2022 r. wzrósł tylko o 1%. Dla Łotwy kluczowe znaczenie ma także podnoszenie umiejętności cyfrowych ludności, co wpły-

nąć ma na poprawę wdrażania technologii cyfrowej w łotewskich przedsiębiorstwach, które w niewielkim stopniu wykorzystują możliwości cyfrowe takie jak e-faktury, praca w chmurze, sprzedaż *online* czy promocja w mediach społecznościowych (Komisja Europejska 2022b: 12-13).

Różnice w dostępie do usług cyfrowych w zależności od miejsca zamieszkania są bolączką zarówno Estonii, jak i Łotwy. W obu państwach inwestycje w infrastrukturę dotyczą głównie obszarów miejskich, na terenach wiejskich dostęp do szybkiego internetu oscyluje zaś na poziomie około 75% (Komisja Europejska 2022a; 2022b). Powodem jest gęstość zaludnienia. Nieduża liczebnie grupa użytkowników na terenach wiejskich przekłada się na niewielkie zainteresowanie operatorów sieci do rozbudowywania infrastruktury, a następnie kosztochłonnego jej utrzymania, wymagającego bardziej złożonych niż standardowe działań serwisowych i regenerowania sygnału. Plany rozwojowe obu państw zmierzać mają do poprawy tej sytuacji, co jest kluczowe dla zapewniania sprawności przesyłu danych oraz zwiększania odporności infrastruktury. Odporność infrastruktury to nie tylko korzystanie z łączy światłowodowych, które są niewrażliwe na warunki atmosferyczne czy inne czynniki zakłócające, jak np. przeszkody architektoniczne, lecz i utrzymywanie łączności kluczowych elementów infrastruktury sterowanych cyfrowo, a także zapobieganie cyberatakom.

Raporty *DESI* UE są ważne, ponieważ pozwalają na monitorowanie postępów państw, mają znaczenie prognostyczne i wpływają na planowanie wydatków związanych z rozbudowywaniem infrastruktury oraz podnoszeniem odporności systemów cyfrowych (Kamińska-Korolczuk 2023). Rozwój kompetencji cyfrowych społeczeństwa to usprawnianie jego możliwości komunikacyjnych pozwalających na prowadzenie coraz bardziej skutecznej polityki informacyjnej. Na omawianym terenie jest to kluczowe z uwagi na położenie geograficzne – sąsiedztwo z Federacją Rosyjską.

Główne założenia polityk informacyjnych i cyberbezpieczeństwa Estonii i Łotwy

Jak już wspomniano, polityka informacyjna państwa to komunikaty władzy adresowane do społeczeństwa. Skuteczna polityka informacyjna jest strategią (Cornelius 2010), działaniem, które służyć ma maksymalizowaniu zaufania do władzy, w ślad za czym podąża zwiększanie legitymizacji. W prowadzeniu polityki informacyjnej mogą być wykorzystywane bezpośrednie spotkania, jednak w dobie rozwoju mediów, w tym masowego korzystania z mediów społecz-

nościowych, komunikację publiczną prowadzi się zasadniczo poprzez media. Charakter polityki informacyjnej wynikać więc będzie nie tylko z natury władzy, lecz i ze struktury oraz wielkości rynku mediów i charakterystycznej dla danego państwa tradycji korzystania ze źródeł informacji (Kamińska-Korolczuk 2021). Z uwagi na fakt, że oba omawiane państwa położone są geograficznie w regionie szczególnie wrażliwym na prowadzone przez Rosję działania dezinformacyjne, kluczowe znaczenie ma poczucie bezpieczeństwa i zaufanie do komunikatów przekazywanych przez władzę.

W przypadku Estonii i Łotwy nasycenie rynku mediów jest duże, a tradycje prowadzenia polityki informacyjnej poprzez media ugruntowane. Społeczeństwa obu państw należą do tych zwyczajowo korzystających z mediów. Struktura środków przekazu przygotowujących materiały w językach narodowych jest rozbudowana, media adresują także znaczną ofertę do licznych mniejszości narodowych, szczególnie tych porozumiewających się w języku rosyjskim (Kamińska-Korolczuk 2014a; Kamińska-Korolczuk 2014b). Oba państwa, choć Estonia jest tu liderem, korzystają z technologii cyfrowych zarówno do komunikowania się ze społeczeństwem, jak i do prowadzenia rozbudowanych usług publicznych. Utrzymywanie odpornych łączy jest istotnym elementem polityki informacyjnej, kondycji rynku mediów, jak i zapewniania bezpieczeństwa.

Po odzyskaniu niepodległości Estonia i Łotwa zaczęły wprowadzać reformy, których celem było odbudowanie zrujnowanych gospodarek (Clemens 2001; Smith 2002). Zmiany nie pozostały bez wpływu na rynki mediów, dla których transformacja systemowa oznaczała prywatyzację i koncentrację (Vihalemm 2002). Na ich strukturę wpływa także charakterystyczny podział społeczny – występowanie licznych mniejszości narodowych, w tym najbardziej licznej rosyjskojęzycznej. Na początku 2023 r. wszystkich mieszkańców Estonii było 1 365 884, w tym Estończyków 925 892, zaś Rosjan 306 801 (Statistic Estonia). Z kolei mieszkańców Łotwy było 1 883 008, a Rosjan 445 612. Dodatkowo w Łotwie liczba osób o innej narodowości niż łotewska jest równie liczna jak ta rosyjska (Oficiālās statistikas portals).

Podziały społeczne generowały problemy w sferze publicznej obu państw (Smith, Hiden 2012: 26-46; Lagerspetz, Vogt 2013: 58-66; Kamińska-Moczyło 2014). Wpływ na taki stan rzeczy miało także uznawanie przez Rosję, iż wystarczającym powodem do prowadzenia rosyjskiej polityki informacyjnej na terenie Estonii i Łotwy jest zamieszkiwanie mniejszości rosyjskiej w obu państwach. Działania prowadzone były pod pretekstem ochrony/podtrzymywania więzi z osobami rosyjskojęzycznymi. Liczba ludności rosyjskojęzycznej rzeczywiście stanowi o sile nacisku, jaki próbuje ona wywrzeć na władzę państwa pobytu, co było widoczne podczas wydarzeń takich jak relokowanie

pomników pamięci Armii Czerwonej w Estonii czy rozpisanie referendum o uznaniu języka rosyjskiego za narodowy na Łotwie (Brüggemann, Kasekamp 2008: 425–448; Ehala 2009: 139–158; Druviete, Ozolins, 2016: 121–145). Jednak kolejne niepokoje społeczne implikowały wzrost zainteresowania władz włączeniem do krajowej komunikacji grup mniejszości narodowych – obecnie w omawianych państwach przygotowuje się dla nich treści w języku rosyjskim, które są publikowane w prasie drukowanej i elektronicznej (Kamińska-Korolczuk 2014a; Kamińska-Korolczuk 2014b). Dodatkowo na stopniowe osłabienie poczucia więzi z państwem pochodzenia – Rosją, wpływ miały i mają m.in. standard życia w Estonii i na Łotwie zasadniczo różniący się od tego w Rosji oraz wyższe poczucie bezpieczeństwa, co skłania osoby rosyjskojęzyczne do większej integracji z państwami pobytu.

Podobnie jak w większości państw, w Estonii i Łotwie maleją nakłady prasy drukowanej na rzecz prasy dostępnej na elektronicznych urządzeniach przenośnych (Vihalemm 2017; Statista). Wpływowe są, zakładane od końca lat dziewięćdziesiątych XX w., internetowe portale informacyjne, w tym istniejący od 1999 r. informacyjno-rozrywkowy *Delfi* (Balcytiene 2005: 169; Golubeva 2005: 166-168; Oster 2017: 238-241). Kluczowa rola mediów jest bezsporna w kształtowaniu opinii publicznej w każdym państwie. W Estonii i Łotwie odgrywa szczególną rolę z uwagi na tradycyjnie wysoki poziom czytelnictwa, co przekłada się na kształt rynku mediów oraz sprawność prowadzonej polityki informacyjnej poprzez media również w odniesieniu do mniejszości narodowych zamieszkujących oba państwa.

Na rynku prasy elektronicznej w obu omawianych państwach występują nadawcy publiczni i prywatni. Nadawcą publicznym w Estonii jest *Eesti Rahvusringhääling* (*ERR*, Estońskie Radio i Telewizja), w Łotwie *Latvijas Televīzija* (*LTV*, Łotewska Telewizja) oraz *Latvijas Radio* (*LR*, Radio Łotewskie). Nadawcy publiczni wypełniają misję wpisaną w ustawy o nadawaniu, w tym przygotowują audycje służące integracji narodów żyjących w Estonii i na Łotwie. Do niedawna w omawianych państwach można było odbierać audycje nadawane z terenu Federacji Rosyjskiej. Wśród rosyjskojęzycznych mniejszości popularne były stacja telewizyjna *Pirmais Baltijas Kanāls* (*PBK*, Pierwszy Kanał Bałtycki) czy *Голос Россиu* (Głos Rosji) – najstarsza stacja radiowa w Rosji, która od 2014 r. działa jako agencja prasowa i radio *Sputnik*. W 2019 r. w Estonii redakcja rosyjskiej rozgłośni i portalu internetowego *Sputnik Estonia* należących do *Rossija Sewodnia* podjęła decyzję o zakończeniu pracy. Decyzja była związana z naruszeniem sankcji UE (*International Press Institute*). Zaś 26 października 2021 r. Łotewska Narodowa Rada Mediów Elektronicznych (*NEPLP*) anulowała pozwolenie na nadawanie *PBK*,

który funkcjonował w Łotwie od 2002 r. *PBK* można było oglądać we wszystkich sieciach telewizji kablowej, przez satelitę *Viasat* w płatnym pakiecie oraz w Internecie. Jednak po kolejnych naruszeniach warunków zezwolenia na nadawanie, ustalając, że program rozpowszechnia dezinformację, w tym fałszywe informacje w szczególnym czasie pandemii *COVID-19*, koncesję uchylono (LSM.lv Ziņu redakcija 2021).

Obecnie publikacje adresowane do osób rosyjskojęzycznych przygotowywane są przez podmioty działające na terenie Estonii i Łotwy. Media publikujące w języku rosyjskim na Łotwie stanowią dużą część rynku, należą do popularnych i są opiniotwórcze, a sposób ich finansowania nie był i nadal nie jest do końca jawny (Rožukalne 2013). W porównaniu z Łotwą, w Estonii funkcjonują nieliczne media rosyjskojęzyczne, nie ma też tak wyraźnego podziału na środki masowego przekazu rodzime i obce. Publiczni nadawcy mediów elektronicznych Estonii oraz Łotwy wraz z Litwą zaproponowali uruchomienie rosyjskojęzycznego kanału telewizyjnego, którego rzetelność nie budziłaby kontrowersji, czym zasygnalizowali, że problemem nie jest dla rządów tych trzech państw nadawanie w języku innym niż rodzime, lecz przekazywanie niesprawdzonych informacji, których celem jest podsycanie niepokojów społecznych (mk, pap 2014). Estonia rzeczywiście uruchomiła rosyjskojęzyczny kanał *ETV+*, w Łotwie także funkcjonują opiniotwórcze media adresowane do mniejszości narodowych.

Sytuacja w tej części Europy, wynikająca z prowadzonych przez Rosję działań destabilizujących, mobilizuje Estonię i Łotwę do prowadzenia przewidywalnej i zwartej polityki informacyjnej w oparciu o poczucie bezpieczeństwa, w tym i tego odnoszącego się do sfery cyfrowej (Herzog 2017; Robinson, Hardy 2021). Istotną rolę w kształtowaniu polityki informacyjnej państwa pełnią strategie cyberbezpieczeństwa. Estonia jest pierwszym państwem w regionie, które taką strategię opracowało. W maju 2008 r. został ogłoszony dokument *Küberjulgeoleku strateegia 2008-2013* (Strategia cyberbezpieczeństwa 2008-2013), zawierający m.in. wnioski z cyberataków na infrastrukturę publiczną Estonii, które miały miejsce w 2007 r. (Ehala 2009). Uaktualnione założenia zawierały kolejne strategie *Küberjulgeoleku strateegia 2014-2017* (Strategia cyberbezpieczeństwa 2014-2017) i *Küberturbalisuse strateegia 2019-2022* (Strategia bezpieczeństwa cybernetycznego 2019-2022), sporządzona przez Ministerstwo Gospodarki i Komunikacji. Dokumenty są przykładem podejmowanych skoordynowanych działań ukierunkowanych na kilka pól: wypracowania w społeczeństwie umiejętności cyfrowych oraz przekonania, że jest to wartością, która gwarantuje państwu rozwój, a także, że współpraca w ramach szerszych struktur, w tym międzynarodowych, jest dobrym rozwiązaniem w dążeniu do zapewniania bezpieczeństwa w sferze cyfrowej.

Z kolei w pierwszej łotewskiej strategii cyberbezpieczeństwa *Latvijas kiberdrošības stratēģija 2014.-2018.gadam* zwracano uwagę na zależność administracji państwowej, społeczeństwa i gospodarki od usług zapewnianych przez technologie informacyjno-komunikacyjne, przy jednoczesnym podkreślaniu faktu, iż „korzystanie z narzędzi teleinformatycznych może ograniczać prawa i podstawowe wolności jednostki lub naruszać prawo do prywatności i ochrony danych osobowych" (*Latvijas kiberdrošības stratēģija*). Wyznaczono priorytety działania takie jak: 1. zarządzanie cyberbezpieczeństwem i zasobami; 2. praworządność w cyberprzestrzeni i przeciwdziałanie cyberprzestępczości; 3. świadomość społeczna, edukacja i badania; 4. gotowość i umiejętność działania w sytuacjach kryzysowych oraz 5. współpraca międzynarodowa. Podjęte działania nie były jednak zadowalające. W raportach *DESI* podkreślano, że wdrażanie celów cyfrowych w Łotwie przebiega najmniej dynamicznie spośród wszystkich państw UE (Komisja Europejska 2022b). W Nowej *Par Latvijas kiberdrošības stratēģiju 2023.-2026. gadam* czyli strategii bezpieczeństwa cybernetycznego Łotwy na lata 2023-2026 wyznaczono Ministerstwo Obrony Narodowej jako instytucję koordynującą osiągnięcie celów strategii i datę rozpoczęcia realizacji tychże celów od 1 maja 2023 r. Wizja polityki bezpieczeństwa cybernetycznego jest jasna, wykreowanie „bezpiecznej, otwartej, wolnej i niezawodnej cyberprzestrzeni, w której zagwarantowany jest bezpieczny, niezawodny i ciągły odbiór i świadczenie usług ważnych dla państwa i społeczeństwa oraz przestrzegane są prawa człowieka jednostek zarówno w środowisku fizycznym, jak i wirtualnym" (*Par Latvijas kiberdrošības*). Strategia skorelowana jest z celami UE w tej materii. Zakłada się dalsze doskonalenie zarządzania i promowania cyberbezpieczeństwa w świadomości społecznej oraz budowanie odporności sieci. Sytuacje kryzysowe zostały nazwane wprost jako zdolność do zapobiegania i zwalczania cyberprzestępczości.

Jednym z priorytetów w obu omawianych państwach jest dbanie o międzynarodową współpracę w cyberprzestrzeni. O współdziałanie w tym zakresie Estonia zabiegała już w 2015 r., tworząc w Luksemburgu cyberambasadę, czyli miejsce, w którym zabezpieczono kopie zapasowe danych na wypadek cyberataku na estońską infrastrukturę. Umowę między Estonią a Luksemburgiem sfinalizowano w 2017 r., do współpracy zaangażowano także firmy z sektora prywatnego (EAS).

Na bazie dyrektyw Parlamentu Europejskiego i Rady – dyrektywy 2002/19/WE w sprawie dostępu do sieci łączności elektronicznej oraz związanych z nimi urządzeń i ich wzajemnych połączeń (Parlament Europejski 2002a), dyrektywy 2002/20/WE w sprawie zezwoleń na udostępnianie sieci i usług łączności elektronicznej (Parlament Europejski 2002b) i dyrektywy 2009/140/WE z 25 li-

stopada 2009 r. zmieniającej dyrektywę 2002/21/WE w sprawie wspólnych przepisów regulacyjnych dotyczących sieci i usług łączności elektronicznej (Parlament Europejski 2009) oraz dyrektywy Parlamentu Europejskiego i Rady 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii parlamenty Estonii – *Riigikogu* i Łotwy – *Saeima* uchwaliły ustawy o cyberbezpieczeństwie.

Estońska ustawa z 9 maja 2018 r. *Küberturvalisuse seadus* czyli Ustawa o cyberbezpieczeństwie weszła w życie 15 sierpnia 2022 r. i „określa wymagania dotyczące utrzymania sieci i systemów informatycznych niezbędnych do funkcjonowania społeczeństwa oraz systemów sieciowych i informatycznych administracji państwowej i samorządowej, odpowiedzialność i nadzór, a także podstawy zapobiegania i rozwiązywania incydentów cybernetycznych". W ustawie zdefiniowano m.in. pojęcie „bezpieczeństwo systemów", które „oznacza zdolność systemów do przeciwstawiania się wszelkim działaniom naruszającym dostępność, autentyczność, integralność lub poufność danych przetwarzanych w systemach lub usług oferowanych przez te systemy lub dostępnych za ich pośrednictwem" oraz „incydent cybernetyczny", jako „każde zdarzenie w systemie, które zagraża bezpieczeństwu systemu lub ma na nie negatywny wpływ" (*Riigikogu*).

Z kolei łotewska Ustawa o bezpieczeństwie technologii informatycznych *Informācijas tehnoloģiju drošības likums* z 28 października 2010 r. weszła w życie 01.01.2011 r. i była kilkukrotnie zmieniana. Celem ustawy jest „poprawa bezpieczeństwa technologii informacyjnych poprzez określenie najważniejszych wymagań w celu zagwarantowania odbioru takich podstawowych usług, przy świadczeniu których wykorzystuje się te technologie". Ustawodawca zakłada, że bezpieczeństwo powinno być prognozowane, a skutkom jego naruszeń powinno się zapobiegać, co wydaje się podejściem dość życzeniowym. Ewentualne eliminowanie skutków naruszenia bezpieczeństwa spoczywa na „właściwych instytucjach" i dostawcach usług cyfrowych. Podobnie jak w ustawie estońskiej, zdefiniowano incydent związany z bezpieczeństwem technologii informatycznych, precyzując, że jest to „szkodliwe zdarzenie lub przestępstwo, w wyniku którego integralność, dostępność lub poufność technologii informatycznych jest zagrożona" (*Saeima*).

Na podstawie wdrażanych rozwiązań można zauważyć, że państwa pojmują bezpieczeństwo cyfrowe nie tylko jako dbałość o coraz lepsze systemy zabezpieczeń, lecz także edukację na rzecz świadomości użytkowników sieci oraz możliwość korzystania z internetu w każdym miejscu na ich terytorium. Dysponując rozwiniętym sektorem usług cyfrowych, dobrą edukacją społe-

czeństwa w zakresie kompetencji cyfrowych i w zasadzie powszechnym dostępem do internetu, wdrażane mogą być kolejne działania, których zadaniem jest doskonalenie pól eksploatacji nowych technologii.

Podsumowanie

Dokonany w latach dziewięćdziesiątych XX w. przełom, w wyniku którego doszło do rozpadu sojuszu państw bloku wschodniego, doprowadził do uniezależnienia się od wpływów ZSRR większości podmiotów znajdujących się w sferze jego oddziaływań od czasu II wojny światowej. Nie zakończył jednak agitacji prowadzonej przez Rosję w przestrzeni informacyjnej tych państw. Działania dezinformacyjne prowadzone są trwale, mają jednak różną siłę oddziaływania w zależności od państwa, wobec którego są stosowane (Boćkowski i in. 2022).

Estonia i Łotwa są państwami o podatnym na kryzysy położeniu geograficznym i geopolitycznym w Europie. Sąsiedztwo z Rosją wpływa na potrzebę prowadzenia odpowiedzialnej polityki informacyjnej uwzględniającej zamieszkiwanie na terenie tych państw mniejszości z mniejszością rosyjskojęzyczną na czele. Rozważne działania w obrębie rynku mediów i dbanie o cyberbezpieczeństwo wraz z rozbudowywaniem odpornej infrastruktury cyfrowej to kluczowe elementy zapewniania stabilności w sferze przekazu informacji w tym rejonie. Mimo iż działania zmierzające do realizacji tych celów wdrażane są od dawna, nie zostały w pełni wykonane. Jak wynika z przeprowadzonej analizy, funkcjonowanie obu państw w przestrzeni cyfrowej jest rozwinięte, wymaga jednak stałego monitorowania działań destabilizujących podejmowanych przez sąsiadów, ze szczególnym uwzględnieniem Federacji Rosyjskiej. Polityka informacyjna obu państw uwzględnia podtrzymywanie więzi mniejszości narodowych z państwami pobytu. Jednocześnie, poprzez regulacje eliminujące z rynku mediów te podmioty, które działały na szkodę stabilności państwa, Estonia i Łotwa wykazują aktywność na polu zabezpieczania prawa społeczeństwa do otrzymywania w środkach masowego przekazu rzetelnych informacji. Teza artykułu, stwierdzenie, że działania dotyczące zapewniania cyberbezpieczeństwa są istotne dla władz Łotwy i Estonii, które dostrzegają stojące przed nimi wyzwania wynikające z niełatwego sąsiedztwa z Rosją, jest słuszna. Działania podejmowane przez władze Estonii i Łotwy w tym zakresie podejmowane są od dawna i są strategią, której efekty znajdują dobre odzwierciedlenie w sferze mediów, a w odniesieniu do zapewniania cyberbezpieczeństwa oczekują na pełną realizację.

Bibliografia

Balcytiene A., *Media Modernisation and Journalism Cultures in the Baltic States and Norway*, Bærug R., (red.), *The Baltic Media World*, Riga, s. 169-183.

Baluk W. (2020), *Incydent czy akt agresji w rejonie Cieśniny Kerczeńskiej?*, „Wschód Europy. Studia Humanistyczno-Społeczne" nr 6 (1), s. 197-224.

Bechara F. R., Schuch S. B. (2021), *Cybersecurity and global regulatory challenges*, „Journal of Financial Crime" Vol. 28, No. 2, s. 359-374.

Berec, BEREC Guidelines on Very High Capacity Networks, https://www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-very-high-capacity-networks (dostęp: 5.04. 2023).

Boćkowski, D., Dąbrowska-Prokopowska, E., Goryń, P., Goryń, K. (2022), *Dezinformacja-Inspiracja-Społeczeństwo. Social CyberSecurity*. Białystok: Wydawnictwo Uniwersytetu w Białymstoku

Brüggemann K., A. Kasekamp A. (2008), *The Politics of History and the „War of Monu- ments" in Estonia*, „Nationalities Papers, The Journal of Nationalism and Ethnicity" Vol. 36, Nr 3, s. 425–448.

Calderaro A., Craig A. J. S. (2020), *Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building*, „Third World Quarterly" Vol. 41, No. 6, s. 917-938, DOI: 10.1080/01436597.2020.1729729 (dostęp: 29.05.2023).

Clemens Jr., W. C. (2001), *The Baltic Transformed: Complexity Theory and European Security*, Lanham: Rowman & Littlefield Publishers

Cornelius I. (2010), *Information policies and strategies*, London, Routlegde

Druviete I., Ozolins U. (2016), *The Latvian referendum on Russian as a second state language, February 2012*, „Language Problems and Language Planning" Vol. 40, Nr 2, s. 121–145.

Dudzińska K., Piotrowski M. A. (2017), *Rosyjskie zagrożenia hybrydowe dla państw bałtyckich*, 12 LIP 2017, https://pism.pl/publikacje/Rosyjskie_zagro_enia_hybrydowe_dla_pa_stw_ba_tyckich (dostęp 17.04. 2023).

Enterprise Estonia, *e-Governance,* https://e-estonia.com/solutions/e-governance/data-embassy/ (dostęp: 2.05.2023).

Ehala M. (2009), *The Bronze Soldier: Identity Threat and Maintenance in Estonia*, „Journal of Baltic Studies" Vol. 40, nr 1, s. 139–158.

Goban-Klas T., Sienkiewicz P. (1999), *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków, Wydawnictwo Fundacji Postępu Telekomunikacji

Golka M. (2005), *Czym jest społeczeństwo informacyjne?*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" r. LXVII, z. 4, s. 253-265.

Golubeva M. (2005), *EU Accession Debate on the Internet in the Baltic States: Own He- terogeneous Messages?*, Bærug R., (red.), *The Baltic Media World*, Riga:Royal Ministry of Foreign Affairs of the Kingdom of Norway, s. 166–178.

Herzog S. (2017), *Ten Years After the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity*, „Georgetown Journal of International Affairs" Vol. 18, No. 3, s. 67-78.

Hiden, J., Made, W., Smith, D.J. (red.) (2008), *The Baltic Question during the Cold War*, New York.

International Press Institute, *Four Russian and one Belarusian TV channel banned in Estonia*, 24.02.2022, https://ipi.media/alerts/four-russian-and-one-belarusian-tv-channel-banned-in-estonia/ (dostęp: 23.05.2023).

Kamińska-Korolczuk K. (2014a), *Estonia,* Matykiewicz-Włodarska A., Ślufińska M. (red.) *Systemy medialne państw Unii Europejskiej: nowe kraje członkowskie*, Toruń: Wydawnictwo A. Marszałek, s. 109–140.

Kamińska-Korolczuk K. (2014b), *Łotwa,* Matykiewicz-Włodarska A., Ślufińska M., (red.) *Systemy medialne państw Unii Europejskiej: nowe kraje członkowskie*, Toruń, Wydawnictwo A. Marszałek, s. 163–193.

Kamińska-Korolczuk K. (2021), *Polityka i media a kryzys zaufania. Polityka informacyjna mocarstw w czasie zagrożenia*, Gdańsk.

Kamińska-Korolczuk K. (2023), *Cyberbezpieczeństwo, strategie cyfrowe i agendy jako wyzwania państwa na przykładzie doświadczeń Estonii*. Kamińska-Korolczuk K., Rosłon-Żmuda J. (red.) *Modele demokracji odczytane raz jeszcze: księga jubileuszowa poświęcona Profesorowi Andrzejowi Kubce*, Toruń, Wydawnictwo A. Marszałek, s. 147–165.

Kamińska-Moczyło K. (2014), *Edukacja i imigracja w nowych i starych państwach Unii Europejskiej. Przykład RFN i Łotwy*, Boryń M., Duraj B., Mrozowska S., (red.) *Polityka młodzieżowa Unii Europejskiej*, Toruń, Wydawnictwo A. Marszałek, s. 83-101.

Kaska K., Rebane L., Vaks T., *Lessons from Estonia's National Cybersecurity Strategy: How to Succeed or Fail in Delivering Value*, https://icds.ee/wp-content/uploads/2021/05/ICDS_Report_So_Far_Yet_So_Close_chapter_II.pdf (dostęp: 19.04.2023).

Komisja Europejska a, *Cyfrowa dekada Europy: cele cyfrowe na 2030 r.*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_pl (dostęp: 17.02.2023).

Komisja Europejska b, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Cyfrowy Kompas na 2030 r.: europejska droga w cyfrowej dekadzie*, COM (2021), 118 final, 9.03.2021, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A52021DC0118 (dostęp: 17.02.2023).

Komisja Europejska c, *Kształtowanie cyfrowej przyszłości Europy*, https://digital-strategy.ec.europa.eu/pl/policies/europes-digital-decade (dostęp: 17.02.2023).

Komisja Europejska d, *Kształtowanie cyfrowej przyszłości Europy. Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI)*, https://digital-strategy.ec.europa.eu/pl/policies/desi (dostęp: 17.02.2023).

Komisja Europejska 2022a, *Digital Economy and Society Index (DESI) 2022*, Estonia, https://digital-strategy.ec.europa.eu/en/policies/desi-estonia (dostęp: 20.02.2023).

Komisja Europejska 2022b, *Digital Economy and Society Index (DESI) 2022*, Łotwa, https://digital-strategy.ec.europa.eu/en/policies/desi-latvia (dostęp: 20.02.2023).

Kozłowski G. (2019), *Polityka dezinformacyjna Rosji wobec Estonii*, „Sprawy Międzynarodowe" t. 72, nr 4, s. 107-128, http://czasopisma.isppan.waw.pl/index.php/sm/article/view/693/544 (dostęp: 23.05.2023).

Küberjulgeoleku strateegia 2008–2013, heakskiitmine. Vastu võetud 08.05.2008 nr 201, „Riigi Teataja", https://www.riigiteataja.ee/akt/12960860 (dostęp: 17.04.2023).

Küberjulgeoleku strateegia 2014–2017 rakendusplaani aastaks 2017 heakskiitmine. Vastu võetud 17.04.2017 nr 106, „Riigi Teataja", https://www.riigiteataja.ee/akt/319042017008 (dostęp: 17.04.2023).

Küberturbalisuse strateegia 2019-2022, https://www.grafilius.ee/language/et/portfolio/kuljendus-kuberturvalisuse-strateegia-2022/ (dostęp: 17.04.2023).

Latvijas kiberdrošības stratēģija 2014.–2018.gadam,

https://likumi.lv/ta/id/263912-par-pamatnostadnem-latvijas-kiberdrosibas-strategija-2014-2018-gadam (dostęp: 29.05.2023).

LSM.lv Ziņu redakcija, *Mediju uzraugs anulē PBK apraides atļauju*, 21.10.2021, https://www.lsm.lv/raksts/zinas/latvija/mediju-uzraugs-anule-pbk-apraides-atlauju.a426669/ (dostęp: 23.05.2023).

Majandus-ja Kommunikatsiooniministeerium, *Küberturbalisuse strateegia 2019-2022*, https://www.grafilius.ee/language/et/portfolio/kuljendus-kuberturvalisuse-strateegia-2022/ (09.02.2023).

mk, pap, *Litwa, Łotwa i Estonia: chcemy rzetelnej rosyjskojęzycznej telewizji*, 2.05.2014, http://wyborcza.pl/1,75477,15891597,Litwa__Lotwa_i_Estonia__chcemy_rzetelnej_rosyjskoje- zycznej.html (dostęp: 17.04.2023).

Nye J.S. (2004), *Soft Power: The Means to Success in World Politics*, New York, Harvard University

Nye J.S. (2009), *Get Smart: Combining Hard and Soft Power*, „Foreign Affairs" Vol. 88, No. 4, s. 160–63, http://www.jstor.org/stable/20699631 (dostęp: 23.05.2023).

Oficiālās statistikas portals, *Population by citizenship and ethnicity at the beginning of year – Ethnicity, Time period and Citizenship*, https://data.stat.gov.lv/pxweb/en/OSP_PUB/START__POP__IR__IRV/IRE060/table/tableViewLayout1/ (dostęp: 21.04. 2023).

ONZ, Standard country or area codes for statistical use (M49), https://unstats.un.org/unsd/methodology/m49/ (dostęp: 23.05.2023).

Oster J. (2017), *European and International Media Law,* Cambridge.

Parlament Europejski (2002a), *Dyrektywa 2002/19/WE w sprawie dostępu do sieci łączności elektronicznej oraz związanych z nimi urządzeń i ich wzajemnych połączeń*.

Parlament Europejski (2002b), *Dyrektywa 2002/20/WE w sprawie zezwoleń na udostępnianie sieci i usług łączności elektronicznej.*

Parlament Europejski 2009, *Dyrektywa Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/21/WE w sprawie wspólnych przepisów regulacyjnych dotyczących sieci i usług łączności elektronicznej*.

Parlament Europejski (2016), *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.*

Parlament Europejski (2019a), *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA*.

Par Latvijas kiberdrošības stratēģiju 2023.–2026. gadam, https://likumi.lv/ta/id/340633-par-latvijas--kiberdrosibas-strategiju-20232026-gadam (dostęp: 30.05.2023).

Piotrowski M. A., K. Raś K., (2017), *Rosyjskie zagrożenia hybrydowe dla państw bałtyckich*, „Biuletyn PISM" nr 67.

Radin A. (2017), *Hybrid Warfare in the Baltics: Threats and Potential Responses*. CA: RAND Corporation, https://www.rand.org/pubs/research_reports/RR1577.html (dostęp: 23.05. 2023).

Riigikogu, *Küberturvalisuse* seadus, *Cybersecurity Act*, „Riigi Teataja", https://www.riigiteataja.ee/en/eli/523052018003/consolide (dostęp: 13.04. 2023).

Robinson N., Hardy A. (2021), *From the „Bronze Night" to cybersecurity pioneers*, Robinson N., Hardy A., (red.), *Routledge Companion to Global Cyber-Security Strategy*, New York – London:Routlegde, s. 211-226.

Rožukalne A. (2013), *Latvia's Media Owners*, *A monograph on Latvia's media system and the most important owners thereof,* Ryga, Apgads Zinatne.

Saeima, *Informācijas tehnoloģiju drošības likums, Law on the Security of Information Technologies*, https://likumi.lv/ta/en/en/id/220962 (dostęp: 13.04.2023).

Smith D. J. (2002), *Estonia: Independence and European Integration*, London–New York: Routledge

Smith D. J. Hiden, J. (2012), *Ethnic Diversity and the Nation State: National Cultural Autonomy Revisited,* New York, Routledge

Smith D. J., Pabriks A., Purs A., Lane T. (2002), *The Baltic States. Estonia, Latvia and Lithuania,* London–New York, Routledge.

Statista.com, *Share of individuals reading online news sites, newspapers or news magazines in Latvia from 2013 to 2016*, „The Statistic Portal", https://www.statista.com/statistics/386093/online-news-consumption-in-latvia/ (dostęp: 10.04. 2023).

Statistic Estonia, https://andmed.stat.ee/en/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahva-arv-ja-rahvastiku-koosseis/RV0222U/table/tableViewLayout2) (dostęp: 21.04. 2023).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dziennik Ustaw 2023.57.

Vabariigi Valitsus, *Küberjulgeoleku strateegia 2008–2013, heakskiitmine. Vastu võetud 08.05.2008 nr 201*, „Riigi Teataja", https://www.riigiteataja.ee/akt/12960860 (10.02.2023).

Vihalemm P. (2017), *Media consumption in Estonia*, referat przedstawiony podczas 12th Conference on Baltic Studies in Europe (CBSE), Ryga.

Vihalemm P. (red.) (2002), *Baltic Media in Transition,* Tartu: University Press.

Vogt H. (2005), *Between Utopia and Disillusionment: A Narrative of the Political Transformation in Eastern Europe*, New York, Berghahn.

Żebrowski W. (2012), *Badanie polityki. Ogniwa procesu badawczego na studiach politologicznych,* Olsztyn: Wydawnictwo Uniwersytetu Warmińsko-Mazurskiego

Dr hab. Katarzyna Kamińska-Korolczuk, Uniwersytet Gdański (katarzyna.kaminska-korolczuk@ug.edu.pl)

Słowa kluczowe: cyberbezpieczeństwo w państwach bałtyckich, polityka informacyjna państw bałtyckich, polityka informacyjna wobec mniejszości narodowych, dezinformacja, cyberbezpieczeństwo Estonia, cyberbezpieczeństwo Łotwa

Keywords: cybersecurity in the Baltic States, information policy of the Baltic States, information policy towards national minorities, disinformation, cybersecurity Estonia, cybersecurity Latvia

ABSTRACT

The article presents the solutions introduced by Estonia and Latvia to make the digital infrastructure they use to carry out state information policy and deliver public services more secure. The study aims to analyze the implemented regulations and assess their efficiency. The thesis of the article is that the authorities of both countries prioritize efforts to ensure cyber security.

To achieve the aim of the study and to confirm the thesis, the following measures were helpful: 1. findings based on direct observations and field research; 2. analysis of sources and existing data along with a systematic literature review (Fink, 2005: 17) and the institutional and legal method consisting in the study of normative acts (Żebrowski 2012: 32-33) in order to analyze changes occurring in the legal order. This is a review article, and it is organized as follows: analysis of the key issues related to the shape of information policy implemented by Estonia and Latvia through the media; presentation of activities related to strengthening cyber security; conclusions.

The analysis shows that Estonia and Latvia operate effectively in the digital sphere, but it requires ongoing monitoring of the destabilizing actions performed by Russia, their largest neighbor. The information policies of both countries take into account the preservation of relations between national minorities and their countries of residence. Actions taken by the Estonian and Latvian authorities in the area of cybersecurity have been ongoing for a long time and they represent a strategy whose effects are well reflected in the media sphere. The strategy awaits full implementation to ensure an increasingly higher level of cybersecurity.

NASZE WYDAWNICTWA

INSTYTUT ZACHODNI
ul. Mostowa 27, 61-854 Poznań
tel. +61 852 28 54
fax +61 852 49 05
e-mail: wydawnictwo@iz.poznan.pl

Stanisław Sierpowski

Historia II Rzeczypospolitej

ISBN 978-83-66412-54-5
Poznań 2023, 437 ss.

Wydaniem *Historii II Rzeczypospolitej* autorstwa Stanisława Sierpowskiego Instytut Zachodni nawiązuje do ważnego nurtu w swej działalności naukowej i wydawniczej**.** Przez prawie 80 lat istnienia ukazały się tu liczne prace z zakresu dziejów Polski międzywojennej. Pracownicy naukowi Instytutu oraz badacze z nim związani koncentrowali się na dziejach polityki zagranicznej II Rzeczypospolitej, i to nie tylko w odniesieniu do stosunków polsko-niemieckich. Zajmowano się również innymi aspektami historii Polski tego okresu, zwłaszcza problematyką mniejszości narodowych.

Wieloaspektową syntezę dziejów Drugiej Niepodległości (1918-1939), będącą bilansem kilkudziesięcioletnich badań prof. Stanisława Sierpowskiego, Instytut Zachodni kieruje do szerokich kręgów czytelników. Napisana żywym językiem książka omawia wiele aspektów historii II Rzeczypospolitej, od wewnętrznych problemów politycznych i polityki zagranicznej, poprzez spory ideowe czy problematykę gospodarczą, po życie codzienne. Współczesny czytelnik znajdzie w tym nowocześnie ujętym opracowaniu próbę odpowiedzi na pytania, które nurtują kolejne już pokolenie Polaków.