PME

2/2020

Adres redakcji:

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl

C·H·BECK

Wydawca:

Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
fax: 22 33 77 602
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Contents

C·H·BECK

Szanowni Państwo,

zapraszam Państwa do zapoznania się z drugim numerem czasopisma Prawo Mediów Elektronicznych. W tym wydaniu znajdziecie Państwo trzy artykuły dotyczące, jak wynika z profilu merytorycznego czasopisma, wpływu nowych technologii na prawo. I tak, w publikacji *Krystyny Rogali* nt. Projektu ustawy o ochronie małoletnich przed treściami pornograficznymi – analiza proponowanych rozwiązań, zapoznamy się z zagadnieniami proponowanych rozwiązań legislacyjnych chroniących małoletnich przed treściami pornograficznymi także w sieci Internet. Kolejną wypowiedzią jest opis aktualnego zagadnienia ochrony praw i wolności obywatelskich we współczesnym świecie, w dobie tworzenia różnych systemów informatycznych służących monitorowaniu lub nawet inwigilacji. Autorem tego opracowania jest *Kamila Brylak-Hudyma*. Publikacja kończy się artykułem *Marka Leśniaka* pt. Udział w zgromadzeniu spółki kapitałowej za pomocą środków komunikacji elektronicznej po zmianach Kodeksu spółek handlowych dokonanych w ramach tzw. tarczy antykryzysowej. Ta wypowiedź odnosi się do aktualnych rozwiązań legislacyjnych wprowadzonych do polskiego prawa w czasie pandemii COVID-19.

Zachęcamy do lektury oraz do publikacji w naszym czasopiśmie.

Z poważaniem,
prof. dr hab. *Jacek Gołaczyński*

Projekt ustawy o ochronie małoletnich przed treściami pornograficznymi – analiza proponowanych rozwiązań

Krystyna Rogala[1]

Celem niniejszego opracowania jest analiza projektowanego rozwiązania w zakresie ochrony małoletnich przed treściami pornograficznymi w postaci mechanizmu blokowania stron internetowych zawierających kwalifikowane treści pornograficzne. Projekt ten stworzony został na podstawie funkcjonującego w polskim porządku prawnym mechanizm blokowania stron internetowych, niezgodnych z regulacją ustawy o grach hazardowych, który autorka przedstawia w początkowej części artykułu. Następnie omówiony zostaje tytułowy projekt ustawy o ochronie małoletnich przed treściami pornograficznymi i podjęte rozważania nad losami proponowanej regulacji po wprowadzeniu przez państwa członkowie UE przepisów wykonawczych dyrektywy Parlamentu Europejskiej i Rady (UE) 2018/1808 z 14.1.2018 r. zmieniającej dyrektywę 2010/13/UE w sprawie koordynacji niektórych przepisów wykonawczych i administracyjnych państw członkowskich dotyczących audiowizualnych usług medialnych[2].

Uwagi wstępne

Każdego dnia dostrzegalne są w naszym społeczeństwie zmiany związane z rozwojem Internetu w zakresie rozrywki, sposobu komunikowania się, budowania relacji czy prowadzenia działalności gospodarczej. W dobie Web 2.0. dostęp do Internetu stał się nie tylko podstawowym standardem, ale również nieodłącznym towarzyszem codziennych obowiązków, nie tylko osób dorosłych, ale także osób niepełnoletnich. Ze względu na brak powszechnie istniejących barier technologicznych ograniczających dzieciom dostęp do Internetu posiadają one wgląd do stron internetowych, zarówno tych z treściami odpowiednimi, jak i tymi przeznaczonymi jedynie dla osób dorosłych. W ustawodawstwach krajowych oraz międzynarodowych są podejmowane próby wypracowania odpowiednich narzędzi ograniczenia tego dostępu[3]. Nie istnieją zatem wątpliwości co do potrzeby regulacji, jednak istnieje wiele zastrzeżeń w zakresie formy i kształtu, jaką regulacja ta miałaby przyjąć – czy miałaby być to forma samoregulacji, regulacji ustawowej wspieranej przez przymus państwowy czy też próba połączenia tych dwóch alternatyw[4].

W 2014 r. nowelizacją Kodeksu karnego stypizowane zostało przestępstwo mające za przedmiot prezentowanie treści pornograficznych małoletnim lub udostępnianie im przedmiotów o tym charakterze oraz rozpowszechnianie ich w sposób umożliwiający dostęp do nich osobom niepełnoletnim[5]. Zmiany te zostały wprowadzone w celu implementacji dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej[6]. Pomimo istnienia instytucji prawnej dającej możliwość ścigania ww. przestępstw widoczna jest niechęć do wszczynania na tej podstawie postępowań karnych wśród organów ścigania, co powoduje, że przepisy te w praktyce mają znikome znaczenie[7]. Problem dostępu do treści pornograficznych wśród nieletnich pozostaje natomiast nierozwiązany, a z uwagi na postęp technologiczny staje się jeszcze bardziej powszechny. Zgodnie ze statystykami 97% dzieci codziennie korzysta z dostępu do Internetu, a ponad 80% dzieci w klasach I–III szkoły podstawowej posiada własny telefon komórkowy typu smartfon[8]. W większości przypadków nie istnieją zatem żadne bariery techniczne dla dziecka, by uzyskać dostęp do treści pornograficznych w kilkanaście sekund.

Badania przeprowadzone przez Instytut Profilaktyki Zintegrowanej w latach 2014–2017 wśród klas II i III gimnazjum ujawniły, że aż 52% chłopców miało pierwszy kontakt z pornografią przed ukończeniem 12. roku życia, z czego 27,3% ogląda treści pornograficzne od jednego do pięciu razy miesięcznie, 9,9% od sześciu do 10 razy miesięcznie, 10,9% od

[1] Autorka jest absolwentką Prawa, Studia Stacjonarne, Wydział Prawa, Administracji i Ekonomii na Uniwersytecie Wrocławskim.

[2] Dz.Urz. UE L Nr 303, s. 69; dalej jako: dyrektywa 2018/1808 lub dyrektywa zmieniająca.

[3] *M. Niedźwiedź*, Problematyka prawna ograniczenia dostępu do treści pornograficznych w Internecie ze względu na ochronę dzieci z perspektywy prawa unijnego, Problemy Współczesnego Prawa Międzynarodowego Europejskiego i Porównawczego, vol. XV, A.D. MMXVII, http://www.europeistyka.uj.edu.pl/documents/3458728/138959185/M.+Niedz%CC%81wiedz%CC%81.pdf (dostęp z 3.6.2020 r.).

[4] *Ibidem*.

[5] Ustawa z 4.4.2014 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, Dz.U. poz. 538.

[6] Dz.Urz. UE L Nr 335, s. 1.

[7] Stowarzyszenie Twoja Sprawa, Podsumowanie literatury i badań naukowych wskazujących na negatywne konsekwencje korzystania z pornografii w kontekście ochrony dzieci i młodzieży, 2019, https://www.twojasprawa.org.pl/wp-content/uploads/2019/11/RaportSTS_badania_naukowe_o_pornografii.pdf (dostęp z 10.4.2020 r.).

[8] Zob. https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/80-dzieci-w-polsce-ma-swoj-smartfon (dostęp z 10.3.2020 r.).

11 do 30 razy, a aż 11,3% czyni to ponad 30 razy w miesiącu. Dwie ostatnie grupy stanowią już formę uzależnienia (łącznie 22,2%)[9]. Wśród badanych dziewczynek kontakt z treściami pornograficznymi był znacznie rzadszy. Z uwagi na charakter publikacji należy w tym miejscu wymienić negatywne skutki kontaktu z pornografią, jako pierwszy wskazując jej uzależniający charakter i związany z nim efekt eskalacji, powodujący, że konsumenci pornografii szukają coraz bardziej drastycznych treści. Uzależnienie od pornografii w swoich skutkach porównywane jest do uzależnienia od hazardu czy środków odurzających jako powodujące zachodzenie szkodliwych procesów w mózgu. Ponadto prowadzi ono do kryzysu w relacjach społecznych współtworzonych przez konsumentów pornografii. Pornografia wpływa na odczuwanie przez jej konsumentów satysfakcji seksualnej i prowadzi do uprzedmiotowienia obrazu kobiety[10].

Reakcja ustawodawcy na patologię społeczną na przykładzie hazardu

Zjawiskiem społecznym, którego negatywny wpływ spowodował reakcję ustawodawcy, jest hazard. W literaturze uznawany jest on za formę patologii społecznej definiowanej jako „zachowania jednostek oraz grup ludzi cechujące się niezgodnością z panującym w danej społeczności systemem norm, destruktywnie i szkodliwie wpływające na funkcjonowanie danej społeczności[11]". Indywidualne skutki hazardu wpływają na powstanie somatycznych, psychicznych i fizycznych szkód gracza[12]. Jego negatywne następstwa mają jednak także swój wymiar ponadindywidualny, powodując m.in. konieczność pokrycia przez państwo kosztów zapewnienia opieki zdrowotnej, socjalnej, rehabilitacji, aparatu ścigania i wymiaru sprawiedliwości. Ponadto zjawisko to jest wyjątkowo kryminogenne i wiktymogenne[13]. W orzecznictwie UE została wypracowana jednolita linia orzecznicza w kwestii swobody państw członkowskich w przedmiocie regulacji przeciwdziałających temu negatywnemu zjawisku społecznemu[14], która została potwierdzona w rezolucji Parlamentu Europejskiego z 15.11.2011 r. w sprawie gier hazardowych oferowanych w obrębie rynku wewnętrznego[15]. Państwom członkowskim przysługuje swoboda w zakresie organizacji gier hazardowych, przy jednoczesnym poszanowaniu dla podstawowych zasad niedyskryminacji i proporcjonalności. Szkodliwość i społeczne konsekwencje, wiążące się z grami i zakładami, stanowią uzasadnienie „istnienia w tym zakresie dyskrecjonalnych uprawnień władz państwowych[16]". Trybunał Sprawiedliwości UE jako dobre rozwiązania wskazuje wprowadzenie zakazu wszelkich lub niektórych rodzajów gier hazardowych w Internecie lub o utrzymaniu monopolu państwa w tym sektorze, a także sporządzenie „czarnej listy" dostawców usług hazardowych, naruszających przepisy ustawy.

Mechanizm blokowania stron internetowych w ustawie o grach hazardowych

Sejm RP 15.12.2016 r. uchwalił ustawę o zmianie ustawy o grach hazardowych oraz niektórych innych ustaw[17] zmieniającą w sposób istotny dotychczasową regulację ustawy z 19.11.2009 r. o grach hazardowych[18]. Ustawa ta weszła w życie, z wyjątkami, 1.4.2017 r. Zgodnie z uzasadnieniem ustawy dwa podstawowe cele, które ma realizować nowa regulacja, to przeciwdziałanie szarej strefie w zakresie urządzenia gier hazardowych oraz zwiększenie poziomu ochrony graczy[19]. „Cele te przenikają się wzajemnie"[20]. Podmioty nielegalnie świadczące usługi w zakresie organizacji gier hazardowych, w swoich działaniach, co do zasady, nie wykazują bowiem dbałości o zapewnienie odpowiedniego zakresu ochrony osób grających[21]. Powyższe cele mają zostać zrealizowane przez trzy rozwiązania prawne:

1) wprowadzanie przez organizatorów gier obowiązkowego regulaminu odpowiedzialnej gry;
2) regulację monopolu państwa na gry na automatach do gier poza kasynami gry oraz na gry hazardowe w sieci Internet (poza zakładami wzajemnymi i loteriami promocyjnymi);
3) utworzenie mechanizmu blokowania dostępu do nielegalnych stron hazardowych i zakazu udostępniania usług płatniczych na tych stronach.

Gry hazardowe organizowane online są usługami transgranicznymi dostępnymi bez względu na miejsce pobytu. Ustawodawca musiał zmierzyć się z problemem oferowania przedmiotowych usług polskim odbiorcom, nie tylko przez podmioty posiadające siedzibę na terenie RP, ale także

[9] Stowarzyszenie Twoja Sprawa, *op.cit.*

[10] *Ibidem.*

[11] Zob. np. *A. Gaberle*, Patologia społeczna, Warszawa 1993, s. 18; *A. Podgórecki*, Patologia życia społecznego, Warszawa 1969, s. 24 za: *L. Wilk*, Hazard. Studium kryminologiczne i prawne, wyd. 1, Legalis/el. 2012.

[12] *L. Wilk*, *op.cit.*

[13] *Ibidem.*

[14] Zob. np. orzeczenia TSUE w sprawach: z 24.3.1994 r. Schindler (C-275/92, Legalis); z 30.11.1995 r., Gebhard C-55/94, Legalis); z 21.9.1999 r. Läärä (C-124/97, Legalis); z 21.10.1999 r. Zenatti (C-67/98, Legalis); z 11.9.2003 r. Anomar (C-6/01, Legalis) i in.

[15] Dz.Urz. UE C Nr 153E, s. 35.

[16] *A. Grzelak*, Czy rejestr domen prowadzących nielegalną działalność hazardową może naruszać prawa człowieka?, [w:] *A. Sołtys*, *M. Taborowski* (red.), Krajowe regulacje hazardu w świetle prawa Unii Europejskiej, Warszawa 2018, s. 314–318.

[17] Dz.U. z 2017 r. poz. 88; dalej jako: ustawa zmieniająca.

[18] T.j. Dz.U. z 2019 r. poz. 847 ze zm.

[19] Druk Nr 795 Rządowy projekt ustawy o zmianie ustawy o grach hazardowych z 1.8.2016 r. https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=795 (dostęp z 17.2.2020 r.).

[20] Ministerstwo Finansów, Założenia nowelizacji ustawy o grach hazardowych w świetle orzecznictwa Trybunału Sprawiedliwości, [w:] *A. Sołtys*, *M. Taborowski* (red.), Krajowe regulacje hazardu w świetle prawa Unii Europejskiej, Warszawa 2018, s. 21–23.

[21] *Ibidem.*

przez podmioty zagraniczne, w tym podmioty z pozostałych państw członkowskich UE. Polski ustawodawca zdecydował się na stworzenie narzędzia w postaci jawnego rejestru domen służących do oferowania gier hazardowych niezgodnie z ustawą, prowadzonego przez ministra właściwego do spraw finansów publicznych. Wpisowi do rejestru podlegają nazwy domen internetowych wykorzystywane do urządzania gier hazardowych bez koncesji, zezwolenia lub dokonania zgłoszenia wymaganego przez ustawę, kierowanych do usługobiorców na terytorium Polski, w szczególności gdy strony internetowe wykorzystujące nazwy takich domen są dostępne w języku polskim lub są reklamowane na terytorium Polski. „Decydujące znaczenia ma jednak sama okoliczność wykorzystywania tych domen do oferowania gier niezgodnie z ustawą"[22]. Urządzanie gier hazardowych przez Internet jest objęte monopolem państwa. Wyjątek stanowi urządzanie zakładów wzajemnych i loterii promocyjnych. Pierwsze z nich odbywa się na podstawie zezwolenia ministra właściwego do spraw finansów publicznych, a drugie na podstawie zezwolenia właściwego dyrektora izby administracji skarbowej. Wpis do rejestru dokonywany jest z urzędu, po zatwierdzeniu przez ww. ministra lub wyznaczonego podsekretarza stanu w urzędzie obsługującym ministra właściwego do spraw finansów publicznych[23]. Zgodnie z danymi zawartymi w Raporcie Najwyższej Izby Kontroli wpis jest dokonywany po weryfikacji wymogów ustawowych, w tym czy gry hazardowe są urządzane bez wymaganej koncesji, zezwolenia lub zgłoszenia. Za identyfikację domen podlegających wpisowi odpowiedzialna jest wyspecjalizowana komórka organizacyjna Opolskiego Urzędu Celnoskarbowego – od 1.9.2018 r. funkcjonująca jako Centrum Zwalczania Przestępczości Ekonomicznej w Środowisku Elektronicznym Krajowej Administracji Skarbowej tzw. Cybercentrum. „W przypadku gier losowych, badano zasady i opisy gier pod względem spełnienia definicji ustawowej, czy grającym oferowane są wygrane pieniężne lub rzeczowe, a wynik gry zależy od przypadku. W przypadku domen niepolskojęzycznych, weryfikowano, czy prezentowane treści wskazują, że oferowane gry są kierowane do graczy z Polski. Analizowano formularz rejestracyjny, regulamin serwisu, regulaminy poszczególnych gier oraz formularze kontaktowe, w szczególności pod względem możliwości założenia konta i udziału w grach, waluty gry, metod płatności[24]". Na 11.5.2020 r. w Rejestrze Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą (Rejestr) wpisanych jest 10 099 podmiotów. Wpisy ostatnich dziewięciu podmiotów zostały dokonane 11.5.2020 r.[25]. Rejestr ten jest jawny.

Mechanizm blokowania stron internetowych oparty jest na ścisłym współdziałaniu z przedsiębiorcami telekomunikacyjnymi świadczącymi usługi dostępu do sieci Internet oraz dostawcami usług płatniczych[26]. Każda zmiana dokonana w Rejestrze musi zostać przekazana do systemu teleinformatycznego przedsiębiorców telekomunikacyjnych i dostawców usług płatniczych. Ustawa wprowadza obowiązek wobec przedsiębiorców telekomunikacyjnych w zakresie trzech czynności, który aktualizuje się po uzyskaniu wiadomości o wpisie w rejestrze. W przeciągu 48 godzin od dokonania wpisu przedsiębiorcy, działając bezpłatnie, mają obowiązek uniemożliwić dostęp do strony internetowej wpisanej do rejestru. Następnie przedsiębiorca ma obowiązek przekierować wszelkie połączenia, które odwołują się do domen internetowych znajdujących się w rejestrze, na stronę internetową, prowadzoną przez ministra właściwego do spraw finansów publicznych. Na przedmiotowej stronie znajduje się komunikat zawierający w szczególności informacje o lokalizacji Rejestru, podmiotach, które legalnie oferują uczestnictwo w grach hazardowych oraz informację o grożących uczestnikom gier sankcjach. W przypadku wykreślenia danej domeny z Rejestru przedsiębiorca w ciągu 48 godzin od publikacji informacji o wykreślenie nazwy domeny internetowej ma obowiązek ponownego bezpłatnego umożliwienia dostępu do niej. Ustawa nakłada na podmiot urządzający gry hazardowe przez Internet obowiązek przeprowadzenia transakcji płatniczych, wynikających z gier, wyłącznie za pośrednictwem dostawców usług płatniczych. Obowiązek ciążący na dostawcach ma postać zakazu udostępniania usług płatniczych na stronach internetowych wykorzystujących nazwy domen internetowych wpisane do Rejestru. Ustawowy termin na zaprzestanie tych czynności wynosi 30 dni od dnia dokonania wpisu. Powyższe rozwiązanie ma na celu utrudnienie funkcjonowania na rynku krajowym podmiotów urządzających gry hazardowe za pośrednictwem Internetu niezgodnie z ustawą[27].

Ustawodawca wraz z wprowadzeniem regulacji Rejestru uregulował także środek zaskarżenia w postaci sprzeciwu od wpisu do rejestru. Podmiotami, które posiadają legitymację czynną do skierowania sprzeciwu do ministra właściwego do spraw finansów publicznych, są:

1) podmioty urządzające gry hazardowe na stronie internetowej;
2) wykorzystujące nazwę domeny wpisanej do rejestru;
3) przedsiębiorcy telekomunikacyjni;
4) posiadający tytuł prawny do domeny wpisanej do rejestru lub
5) dostawcy usług płatniczych.

[22] *Ibidem*.

[23] *S. Radowicki*, *K. Budnik*, komentarz do art. 15 (f), [w:] *S. Radowicki* (red.), Ustawa o grach hazardowych. Komentarz, Lex/el. 2019.

[24] Raport NIK, Informacja o wynikach kontroli. Nadzór nad rynkiem gier hazardowych. KBF.430.001.2019, Nr ewid. 28/2019/P/18/012/KBF, https://www.nik.gov.pl/kontrole/P/18/012/ (dostęp z 22.4.2020 r.).

[25] Zob. http://hazard.mf.gov.pl/ (dostęp z 11.5.2020 r.).

[26] *S. Radowicki*, *K. Budnik*, *op.cit*.

[27] *S. Babiarz*, *K. Aromiński*, komentarz do art. 15(g), [w:] *S. Babiarz* (red.), Ustawa o grach hazardowych. Komentarz, Lex/el. 2018.

Sprzeciw może zostać wniesiony w terminie dwóch miesięcy od dnia umieszczenia nazwy tej domeny w Rejestrze. Wniesiony sprzeciw powinien zostać rozpatrzony w terminie siedmiu dni w formie decyzji administracyjnej, która będzie podlegała kontroli sądowej. W przypadku gdy treści na stronie internetowej uległy zmianie, wykreślenie wpisu z Rejestru powinno nastąpić z urzędu. Ustawa w obecnym brzmieniu nie reguluje szczególnego trybu, w jakim wykreślenie powinno nastąpić[28].

Od czasu wejścia w życie ustawy zmieniającej pojawiły się już pierwsze zastrzeżenia w zakresie skuteczności tej regulacji[29]. W szczególności zwrócono uwagę na łatwą możliwość obejścia przepisów dotyczących Rejestru poprzez m.in. modyfikowanie nazwy domeny przez dodanie cyfry, litery, znaku interpunkcyjnego, korzystanie z sieci TOR, serwerów *proxy*, zastosowanie systemu *peer-to-peer* oraz usługi VPN[30]. Ministerstwo Finansów wskazało, że w zakresie ww. mankamentów nowej regulacji prowadzone są czynności analityczne w celu ich wyeliminowania[31]. W Raporcie NIK na jaw wyszły również nieprawidłowości związane z samym przygotowaniem do wprowadzenia regulacji m.in. w zakresie braku odpowiedniego systemu procedur zarządzania ryzykiem zewnętrznym, braku ustawowych uprawnień Krajowej Administracji Skarbowej do prowadzenia kontroli w tym zakresie, które nadano dopiero po półtora roku od wejścia przedmiotowej regulacji w życie. Udział legalnych zakładów wzajemnych online w rynku zakładów wzajemnych online ogółem wzrósł z 16,1% w 2015 r. do 49,2% w 2018 r. Wartość nielegalnego rynku przekracza zatem wartość rynku legalnego, ale dynamika wzrostu rynku legalnego jest większa niż rynku nielegalnego[32].

Projekt ustawy o ochronie małoletnich przed treściami pornograficznymi

Wskazana na wstępie skala zjawiska dostępu do treści pornograficznych wśród małoletnich staje się coraz bardziej widocznym problemem społecznym, dostrzeganym także przez ustawodawców krajowych i międzynarodowych. Ochrona dzieci przed treściami pornograficznymi znajduje swoje prawne uzasadnienie w regulacjach międzynarodowych. W Konwencji Rady Europy z 25.10.2007 r. o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych[33] uregulowany został obowiązek stron do przyjęcia koniecznych środków ustawodawczych lub innych środków w celu zapewnienia karalności umyślnego powodowania sytuacji w celach seksualnych, w której dziecko jest świadkiem obcowania seksualnego lub czynności seksualnych, nawet jeżeli nie jest zmuszone do uczestniczenia w nich. W ustawodawstwach krajowych powstały pierwsze modele regulacji mających na celu ograniczenie dostępu dzieci do treści pornograficznych, jednak dotychczas żadne z państw nie wykształciło kompleksowego rozwiązania w tym zakresie.

Państwem, które najbliżej było wprowadzenia takiej regulacji, była Wielka Brytania. Początkowo wykorzystywany był tam model samoregulacji, w którym główną rolę odgrywała organizacja *Internet Watch Foundation* (IWF), założona przez brytyjskie służby, oraz operatorów usług telekomunikacyjnych, której podstawowym zadaniem miała być kontrola treści na stronach internetowych we współpracy z Policją, Prokuraturą oraz dostawcami usług telekomunikacyjnych. Jako efekt tej współpracy powstał program *Cleanfeed Content Blocking* stanowiący rodzaj systemu umożliwiającego blokowanie treści uznanych za nieodpowiednie. W 2012 r. brytyjska organizacja podjęła współpracę z ówczesnym premierem *D. Cameronem* w celu wypracowania skuteczniejszego modelu ochrony dzieci przed treściami pornograficznym, czyniąc tym samym krok w stronę modelu współregulacyjnego. Jako centralny punkt inicjatywy przyjęto ideę automatycznego blokowania stron internetowych. Uruchomienie systemu dla danego gospodarstwa domowego miało być uzależnione od wyrażenia przez danego klienta wyraźnej zgody[34]. System ten cechował się jednak wysokim stopniem zawodności, a dodatkowo był skonstruowany w sposób umożliwiający jego łatwe obejście[35]. W 2017 r. premier Wielkiej Brytanii *T. May* zaproponowała uchwalenie ustawy – *Digital Economy Act* (DEA), mającej regulować m.in. dostęp do pornografii dla osób niepełnoletnich, wykorzystując przy tym obowiązek wprowadzenia przez domeny zawierające takie treści skutecznych metod weryfikacji wieku. Naruszenie tego obowiązku prowadzić miało do blokady strony, niedostarczanie usług płatniczych takiemu podmiotowi oraz nałożenie na niego

[28] *Ibidem*.

[29] Interpelacja poselska Nr 14249 do Ministra Cyfryzacji, Ministra Finansów w sprawie używania narzędzia VPN celem omijania zakazu wchodzenia na nielegalne strony z hazardem z 13.7.2017 r.

[30] *S. Radowicki*, *K. Budnik*, *op.cit.*, za: *S. Czubkowska*, Rejestr zakazanych domen internetowych poruszył rynek, Dziennik Gazeta Prawna, https://biznes.gazetaprawna.pl/artykuly/1060019,rejestr-zakazanych-domen-hazardowych.html (dostęp z 26.2.2020 r.); Kancelaria Prawna Skarbiec, Ustawa hazardowa łatwa do obejścia, Dziennik Gazeta Prawna, https://biznes.gazetaprawna.pl/artykuly/1064373,ustawa-hazardowa-latwa-do-obejscia.html (dostęp z 26.2.2020 r.); Raport NIK, *op.cit*.

[31] Odpowiedź Ministra Rozwoju i Finansów na interpelację Nr 14249 z 21.7.2017 r.

[32] Raport NIK, Informacja o wynikach kontroli. Nadzór nad rynkiem gier hazardowych. KBF.430.001.2019, Nr ewid. 28/2019/P/18/012/KBF, https://www.nik.gov.pl/kontrole/P/18/012/ (dostęp z 22.4.2020 r.).

[33] Dz.U. poz. 608.

[34] Biuro Analiz Sejmowych, opinia zlecona *P. Waglowskiemu* z 4.11.2013 r., Rozwiązania prawne regulujące dostęp do bezpiecznego Internetu, http://absta.pl/biuro-analiz-sejmowych-opinia-zlecona-piotr-waglowski-vagla-pl.html?page=2 (dostęp z 13.4.2020 r.).

[35] *M. Malinowska-Hirsch*, Rząd chce kontrolować porno. Jak próbowali to robić Brytyjczycy?, https://tvn24bis.pl/ze-swiata,75/blokada-pornografii-dla-dzieci-i-mlodziezy-jak-to-robila-wielka-brytania,1001647.html (dostęp z 13.4.2020 r.).

sankcji pieniężnych. Jednocześnie sposób weryfikacji wieku nie został określony ustawowo i pozostawiony został mechanizmom wolnorynkowym. Ustawa została uchwalona 27.4.2017 r.[36]. DEA przewidywał także ustanowienie organu – *the Age-Verification Regulator* (AVR), którego zadaniem miało być m.in. opublikowanie wytycznych związanych z metodami skutecznej weryfikacji wieku oraz kontrola nad wykonywaniem tego obowiązki przez podmioty prowadzące strony internetowe[37]. AVR umocowany został do nakładania kar finansowych oraz ich egzekucji i zgłaszania przypadków do usługodawców płatniczych. Przepisy te nigdy nie weszły jednak w życie. Początkowo ich wprowadzenie przełożono na 2018 r., następnie na lato 2019 r., jednak 16.10.2019 r. zrezygnowano z powyższej regulacji całkowicie, wskazując, że będą poszukiwane inne rozwiązania w tej kwestii[38].

Szef polskiego rządu 16.12.2019 r. zapowiedział wdrożenie projektu ustawy o ochronie małoletnich przed treściami pornograficznymi (Projekt)[39]. Projekt został stworzony przez Stowarzyszenie Twoja Sprawa we współpracy z Instytutem Wymiaru Sprawiedliwości, Rzecznikiem Praw Obywatelskich, Rzecznikiem Praw Dziecka, Ministerstwem Cyfryzacji, Krajową Rada Radiofonii i Telewizji („KRRiT"), Polską Izbą Informatyki i Telekomunikacji, Związkiem Pracodawców Branży Internetowej IAB Polska, Fundacją Panoptykon oraz Związkiem Dużych Rodzin 3+ w czasie rocznego projektu badawczego. Podstawowym celem proponowanej regulacji jest ograniczenie dostępu do treści pornograficznych osobom nieletnim poprzez wprowadzenie obowiązku skutecznego stosowania narzędzi weryfikacji wieku[40]. Wybór narzędzi weryfikacji również jest pozostawiony mechanizmom wolnorynkowym. Twórcy projektu wskazują przykład Wielkiej Brytanii, gdzie wraz z uchwaleniem przepisów wprowadzających obowiązki związane z weryfikacją wieku powstawać zaczęły liczne zrzeszenia branżowe wspólnie poszukujące narzędzi odpowiadających ustawowym wymogom. W tym celu konieczne będzie zapewnienie polskim przedsiębiorcom odpowiedniego *vacatio legis*, co umożliwi dostosowanie się na potrzeby nowej regulacji[41]. Projektodawcy proponują w tym zakresie 12-miesięczny okres *vacatio legis*. Skuteczność wprowadzanych przez podmioty działające na rynku narzędzi weryfikacji wieku powinna być, w ocenie projektodawców, poddana kontroli KRRiT. Ponadto przy współpracy z Ministerstwem Cyfryzacji i Prezesa Urzędu Ochrony Danych Osobowych KRRiT powinna ustalić minimalne kryteria stosowane wobec ww. narzędzi[42].

W celu zapewnienia egzekwowalności powyższej regulacji twórcy Projektu proponują rozwiązanie prawne zbliżone do tego wprowadzonego nowelizacją ustawy hazardowej[43]. Jest to uzasadnione przede wszystkim z uwagi na fakt, że treści pornograficzne są, podobnie jak usługi hazardowe, udostępniane za pomocą zagranicznych stron internetowych. Brak wprowadzenia takiego rozwiązania prowadziłby do swoistej iluzoryczności tej regulacji. Dodatkowo twórcy Projektu rozszerzają obszar regulacji nie tylko na strony internetowe, ale także „portale, na których umieszczają je (kwalifikowane treści pornograficzne[44])[45]" ich użytkownicy oraz na rozpowszechnianie ich w inny sposób – na przykład poprzez aplikacje. Jako przykład aplikacji, wobec których możliwe będzie zastosowanie przedmiotowej regulacji, można wskazać portale społecznościowe typu Instagram, Facebook czy Tumblr, które pozwalają użytkownikom na samodzielny wybór treści zamieszczanych na ich profilach. Zgodnie z art. 8 Projektu, Przewodniczący KRRiT prowadzi rejestr domen internetowych i kont, na których rozpowszechniane są kwalifikowane treści pornograficzne, bez zastosowania skutecznej weryfikacji wieku. Rejestr ten jest jawny.

Dyrektywą 2018/1808 państwa członkowskie zobowiązane zostały do zastosowania odpowiednich środków w celu zapewnienia, by audiowizualne usługi medialne, które mogłyby zaszkodzić fizycznemu, psychicznemu lub moralnemu rozwojowi małoletnich były udostępnione w taki sposób, aby małoletni nie mieli do nich dostępu. Obowiązek ten ma zastosowanie do audiowizualnych usług medialnych i do usług platformy udostępniania wideo. Dyrektywa zmieniająca wprowadza nową kategorię usług platformy udostępniania wideo. Określone zostały jako usługa, której podstawowym celem lub jej dającej się oddzielić części lub zasadniczą funkcją jest dostarczanie ogółowi odbiorców w celach informacyjnych, rozrywkowych lub edukacyjnych – poprzez sieci łączności elektronicznej – audycji, wideo stworzonych przez użytkownika lub obu tych rodzajów treści, za które dostawca platformy udostępniania wideo nie ponosi odpowiedzialności redakcyjnej, ale o sposobie zestawienia, których dostawca nie decyduje, w tym automatycznie lub za pomocą algoryt-

[36] *G. Bedloe*, The Digital Economy Act 2017 – an overview, https://drystone.com/files/3ef0c180c574c2030c35e557dfce0958.pdf (dostęp z 13.4.2020 r.).

[37] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673425/Guidance_from_the_Secretary_of_State_for_Digital__Culture__Media_and_Sport_to_the_Age-Verification_Regulator_for_Online_Pornography_-_January_2018.pdf (dostęp z 19.4.2020 r.).

[38] *M. Malinowska-Hirsch*, Rząd chce kontrolować porno. Jak próbowali to robić Brytyjczycy?, https://tvn24bis.pl/ze-swiata,75/blokada-pornografii-dla-dzieci-i-mlodziezy-jak-to-robila-wielka-brytania,1001647.html (dostęp z 13.4.2020 r.).

[39] Projekt ustawy o ochronie małoletnich przed treściami pornograficznymi https://opornografii.pl/article/stowarzyszenie-twoja-sprawa-prezentuje-projekt-przepisow-chroniacych-dzieci-przed-pornografia (dostęp z 1.3.2020 r.).

[40] Opis założeń projektu ustawy chroniącej dzieci przed pornografią. https://opornografii.pl/article/stowarzyszenie-twoja-sprawa-prezentuje-projekt-przepisow-chroniacych-dzieci-przed-pornografia (dostęp z 1.3.2020 r.).

[41] *Ibidem.*

[42] *Ibidem.*

[43] *Ibidem.*

[44] Przypis autora.

[45] *Ibidem.*

mów, w szczególności poprzez eksponowanie, flagowanie i sekwencjonowanie. W motywie 7 dyrektywy zmieniającej wskazano na potrzebę objęcia regulacją tych platform, serwisów społecznościowych, które stają coraz bardziej popularne, szczególnie wśród młodszych odbiorców, i stanowią konkurencję dla tradycyjnych dostawców audiowizualnych usług medialnych. Dyrektywa wskazuje na możliwość ograniczenia swobody świadczenia usług ze względu na nadrzędny ogólny interes publiczny, pod warunkiem że ograniczenia te będą uzasadnione, proporcjonalne i niezbędne, odwołując się do orzecznictwa TSUE w kwestii ograniczenia w zakresie reklamowania gier hazardowych. Państwa członkowskie UE do 19.9.2020 r. są zobowiązane wprowadzić regulację niezbędną do wykonania ww. przepisów.

Projekt, podobnie jak ustawa o grach hazardowych, nakłada obowiązki na przedsiębiorców telekomunikacyjnych. Polegają one na nieodpłatnym uniemożliwieniu dostępu do stron internetowych oraz kont wpisanych do Rejestru i ich usunięciu z systemów teleinformatycznych, służących do zamiany nazw domen internetowych na adresy IP oraz przekierowaniu połączeń odwołujących się do nich na stronę internetową wskazaną przez Przewodniczącego KRRiT do tego celu w Biuletynie Informacji Publicznych KRRiT. Ponadto są one zobowiązane do nieodpłatnego przywrócenia dostępu do stron internetowych oraz kont, które zostały wykreślone z Rejestru. Projekt na dokonanie czynności przez przedsiębiorcę telekomunikacyjnego przewiduje takie same terminy jak uregulowane w ustawie o grach hazardowych, przy czym z wyjątkiem terminu na ponowne umożliwienie dostępu do stron internetowych. Ponadto na przedsiębiorcę telekomunikacyjnego został nałożony obowiązek uniemożliwienia dokonywania rozliczeń usług o podwyższonej opłacie, o których mowa w art. 64 ustawy z 16.7.2004 r. – Prawo telekomunikacyjne[46], w odniesieniu do usług dostępnych za pośrednictwem domen internetowych lub kont wpisanych do rejestru w terminie 30 dni od dnia dokonania wpisu. Na wzór ustawy o grach hazardowych Projekt przewiduje zakaz udostępniania usług płatniczych na stronie internetowej wykorzystującej domenę lub konta wpisane do Rejestru. Termin dla dostawcy usług płatniczych do zaprzestania tych czynności to 30 dni od dnia dokonania wpisu domeny do Rejestru. Projekt wprowadza odmienne uregulowania w zakresie samej procedury dokonania wpisu do Rejestru, kładąc nacisk na rolę podmiotu współregulatora, w tym zakresie. „Ma on zapewnić bardziej elastyczne sposoby komunikacji z dostawcami treści z zagranicy, na co nie może sobie pozwolić organ kontroli jako organ administracyjny”[47]. Dyrektywa zmieniająca wskazuje na pozytywne aspekty współregulacji, która stanowić może pośredni element między samoregulacją a prawodawcą. Rolą współregulatora powinno być opracowanie, monitorowanie oraz egzekwowanie przestrzegania tych wytycznych. Natomiast uznanie, kontrola i finansowanie systemu współregulacji powinna pozostawać w gestii organów państwowych. Jednocześnie jednak w dyrektywie zmieniającej zaznaczono, że wybór przez dane państwo członkowskie modelu współregulacji jest jedynie opcjonalny. Zgodnie z Projektem, rolę współregulatora pełni fundacja ustanowiona na podstawie ustawy, nad którą nadzór sprawuje minister właściwy do spraw cyfryzacji. Zadaniami współregulatora jest monitoring przestrzegania obowiązku wprowadzenia skutecznych narzędzi weryfikacji wieku, inicjowanie prac badawczych w zakresie wpływu treści pornograficznych na małoletnich i inicjowanie w tym zakresie przedsięwzięć oraz działań prewencyjnych i promocyjnych, opracowywanie i publikacja zaleceń w zakresie stosowania skutecznych narzędzi weryfikacji wieku, współdziałanie z organami władzy publicznej w zakresie kontroli przestrzegania przepisów ustawy, opiniowanie projektów aktów prawnych, które mogą mieć wpływ na ochronę małoletnich przed treściami pornograficznymi. Najważniejsze z perspektywy dokonania wpisu jest jednak uprawnienie współregulatora do podjęcia, w przypadku ujawnienia okoliczności wskazujących na naruszenie obowiązku weryfikacji wieku, dalszych działań w celu ustalenia, czy doszło do naruszenia tego obowiązku. W przypadku uzasadnionego podejrzenia naruszenie to jest zgłaszane przed współregulatora Przewodniczącemu KRRiT. Przed dokonaniem zgłoszenia do organu kontroli współregulator w terminie siedmiu dni ma obowiązek podjąć próbę kontaktu z podmiotem prowadzącym daną domenę internetową za pośrednictwem poczty elektronicznej, wysyłając informację o stwierdzonym naruszeniu ustawy na adres poczty elektronicznej wskazany na stronie jako adres kontaktowy. Współregulator ma także obowiązek podjęcia próby kontaktu z usługodawcą prowadzącym domenę internetową usługodawcy, a w przypadku zamiaru zgłoszenia zasobów systemu internetowego, w ramach których udostępniono kwalifikowane treści pornograficzne z naruszeniem ustawy, powinien powiadomić podmiot zarządzający takim zasobem. Poinformowany przez współregulatora podmiot może przedstawić swoje stanowisko w sprawie sformułowane w języku polskim i spełniające określone warunki formalne. W przypadku jego uwzględnienia współregulator odstąpi od dokonania zgłoszenia do organu kontroli. W przeciwnym przypadku, dokonując zgłoszenia, współregulator poinformuje podmiot o uprawnieniach organu kontroli oraz o przysługujących środkach zaskarżenia od czynności i rozstrzygnięć organu kontroli. Powyższe zgłoszenie implikuje wiele obowiązków, które Projekt nakłada na organ kontroli. Przewodniczący KRRiT, po otrzymaniu zgłoszenia, jest obowiązany do podjęcia czynności sprawdzających, o czym informuje na stronie podmiotowej BIP urzędu KRRiT. Ponowny obowiązek in-

[46] T.j. Dz.U. z 2019 r. poz. 2460 ze zm.
[47] *Ibidem*.

formacyjny jest ograniczony do przypadku, gdy naruszenie ustawy nastąpiło w ramach konta. Organ kontroli w takim przypadku ma obowiązek poinformowania o prowadzonych czynnościach sprawdzających usługodawcę. Informacja ta powinna być sporządzona w języku polskim, a jeżeli domena internetowa nie jest prowadzona w języku polskim, co najmniej w języku angielskim.

Przewodniczący KRRiT stwierdza naruszenie, biorąc pod uwagę stanowisko współregulatora i wyjaśnienia, które zostały złożone w ramach czynności sprawdzających. Ocena treści zawartych na danej stronie internetowej lub koncie musi prowadzić w pierwszej kolejności do uznania tych treści za kwalifikowane treści pornograficzne[48], następnie oceny, czy dany podmiot zastosował narzędzie weryfikacji wieku oraz oceny jego skuteczności. Organ kontroli przed dokonaniem wpisu będzie musiał także zweryfikować, czy dane kwalifikowane treści pornograficzne nie stanowią dzieła artystycznego lub nie zostały udostępnione w ramach publikacji o charakterze wyłącznie naukowym lub edukacyjnym, a w przeciwnym wypadku zaniechać podejmowanych działań. Po stwierdzeniu naruszenia obowiązku z art. 3 ust. 1 Projektu organ kontroli niezwłocznie dokonuje wpisu do Rejestru, chyba że naruszenie w międzyczasie ustało. Podobnie jak ustawa o grach hazardowych Projekt reguluje środek zaskarżenie na dokonanie wpisu do Rejestru w postaci sprzeciwu od wpisu. Zakres legitymowanych czynnie podmiotów do jego złożenia uregulowany został analogicznie do regulacji ustawy o grach hazardowych. Obok instytucji sprzeciwu został przewidziany także osobny środek zaskarżenia, którego złożenie jest nieograniczone terminem ustawowym. Gdy dany podmiot zaprzestanie udostępniania kwalifikowanych treści pornograficznych lub wprowadzi skuteczne narzędzie weryfikacji wieku, może złożyć do organu kontroli wniosek o wykreślenie danej nazwy i adresu domeny lub konta z Rejestru. Organ kontroli jest zobowiązany do rozpatrzenia złożonego sprzeciwu i wniosku w terminie 21 dni od dnia jego otrzymania. Rozstrzygnięcie sprzeciwu zapada w formie decyzji, która podlega kontroli sądowej. Samo wniesienie sprzeciwu powoduje natomiast tymczasowe wykreślenie wpisu, chyba że naruszenie ustawy nie budzi wątpliwości.

Nowelizacja dyrektywy o audiowizualnych usługach medialnych a projekt ustawy o ochronie małoletnich przed treściami pornograficznymi

Dyrektywa o audiowizualnych usługach medialnych wprowadza zasadę swobody odbioru i zakazu ograniczania retransmisji audiowizualnych usług medialnych z innych państw członkowskich. Polska nie będzie miała zatem kompetencji do blokowania domen internetowych oraz kont podlegających jurysdykcji innego państwa członkowskiego UE. Dyrektywa zmieniająca wprowadza wyjątek od tej zasady, w przypadkach kiedy audiowizualna usługa medialna stanowi jawne, poważne oraz groźne naruszenie art. 6a ust. 1 lub szkodzi zdrowiu publicznemu bądź stwarza poważne i groźne ryzyko takiej szkody. Jest to jednak rozwiązanie ograniczone wieloma wymogami formalnymi, tj. częstotliwością ww. naruszeń, respektowaniem prawa do obrony dostawców usług medialnych, przeprowadzeniem konsultacji z państwem członkowskim, sprawującym jurysdykcję w danym przypadku. W pozostałych przypadkach kwestia naruszeń art. 6a ust. 2 przez podmiot podlegający jurysdykcji innego państwa członkowskiego będzie musiała być rozwiązana w ramach współpracy władz obu państw przy wsparciu Komitetu Kontaktowego.

Podsumowanie

Regulacje w zakresie blokowania stron internetowych budzą kontrowersje w zakresie zgodności z prawami człowieka poprzez naruszenie wolności słowa oraz dostępu do informacji[49]. Obawę powoduje w szczególności możliwość wykorzystania już powstałego mechanizmu blokowania stron internetowych do coraz innych obszarów życia społeczno-gospodarczego. Powyższe wiąże się z nieuniknioną negatywną reakcją społeczeństwa na proponowane rozwiązania, często również podsycaną przez przekazy medialne[50]. Dla znalezienia kompromisu między dwiema sprzecznymi wartościami – ochroną zdrowia a wolnością słowa i dostępem do informacji, kluczowe jest doprowadzenie, by system ten był maksymalnie hermetyczny i niewadliwy. W szczególności ważne jest, by nie prowadził do blokowania stron internetowych, na których brak jest treści niezgodnych z ustawą oraz by nie dochodziło do blokowania dostępu dla osób, które spełniają przesłankę wieku, z uwagi na wadliwie skonstruowane narzędzie weryfikacji wieku. Kształt proponowanych rozwiązań, z uwagi na konstrukcje przepisów na podstawie niejasnych sformułowań ustawowych, dających przestrzeń do ich szerokiej interpreta-

[48] Art. 2 pkt 4 Projektu „Przez kwalifikowane treści pornograficzne – rozumie się przez to treści przedstawiające rzeczywisty, udawany, wytworzony lub przetworzony a) stosunek płciowy obejmujący widoczne zespolenie narządów płciowych oraz pozycje oralno-genitalne, analno-genitalne, oralno-analne, między osobami dorosłymi tej samej lub odmiennej płci, b) zoofilię, c) masturbację oraz d) sadystyczne lub masochistyczne praktyki w kontekście seksualnym".

[49] *K. Izdebski*, Blokowanie treści internetowych. Zagrożenie dla wolności słowa i dyskryminacja, [w:] *A. Sołtys*, *M. Taborowski* (red.), Krajowe regulacje hazardu w świetle prawa Unii Europejskiej, Warszawa 2018, s. 291–305; *A. Grzelak*, Czy rejestr domen prowadzących nielegalną działalność hazardową może naruszać prawa człowieka?, [w:] *A. Sołtys*, *M. Taborowski* (red.), Krajowe…., s. 307–310.

[50] *M. Malinowska-Hirsch*, *op.cit.*

cji, uwikłanie tych zagadnień w kwestie moralne i powierzenie merytorycznej kontroli tych zagadnień organom kontroli, rodzi wiele zastrzeżeń. Najwięcej wątpliwości zdaje się budzić powierzenie oceny w zakresie uznania danych kwalifikowanych treści pornograficznych za dzieła artystyczne czy o charakterze wyłącznie edukacyjnym, co w praktyce będzie musiało odbyć się przy udziale biegłego. Projektodawcy zdają się dostrzegać podnoszone przy ustawie o grach hazardowych problemy m.in. w zakresie ochrony praw podmiotu prowadzącego domenę internetową przez wprowadzenie instytucji wniosku o wykreślenie danej nazwy z Rejestru, w przypadku zaprzestania naruszenia ustawy. Jednocześnie jednak ustawa o grach hazardowych nie wymaga od organu dokonującego wpisu przeprowadzenia tak złożonej oceny stanu faktycznego i jego subsumpcji do normy prawnej, a jedynie zweryfikowania pewnych formalnych kryteriów ustawowych. Pojawiają się także obawy w zakresie wadliwości przedmiotowej regulacji, co będzie prowadziło do jej niskiej skuteczności, spowodowanej powszechnie dostępnymi metodami jej obejścia. Twórcy Projektu wskazują, że liczą się z wystąpieniem zjawiska obchodzenia narzędzi weryfikacji wieku, które jednak nie wpłynie na brak opłacalności całego przedsięwzięcia. Szczególnie ważne jest, by polski ustawodawca przy wprowadzaniu projektowanych rozwiązań uniknął błędów, które pojawiły się przy powstawaniu Rejestru Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą i zadbał, by regulacja ta była w pełni wykonalna, wraz z zapewnieniem zaplecza technicznego i kadrowego, a także podstaw prawnych do działań podejmowanych przez odpowiednie organy kontroli.

Słowa kluczowe: blokowanie stron internetowych, ochrona małoletnich, prawo do informacji, bezpieczeństwo, rejestr, filtrowanie.

Draft law on the protection of minors from pornographic content – the analysis of proposed solutions

The article aims to analyze the proposed solution regarding the protection of minors against pornographic content as a mechanism for blocking websites containing qualified pornographic content. This project was created based on the mechanism of blocking websites, inconsistent with the Gambling Act, operating in the Polish legal order, which the author presents at the beginning of the article. Next, the article discusses a draft law on the protection of minors from pornographic content and takes into consideration the fate of the proposed regulation after the introduction of implementing provisions of the Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 by the member states of the European Union changing the Directive 2010/13/EU regarding coordination of certain executive and administrative regulations of the member states in regard to audiovisual media services.

Keywords: blocking websites, children's protection, right to information, safety, register, filtering.

Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji

Kamila Brylak-Hudyma[1]

Wszechobecny rozwój technologiczny oraz masowa komputeryzacja nieodzownie wpływają nie tylko na codzienne życie obywateli, ale również na dostępność nowych technik inwigilacji. Dynamiczny rozwój tych nowych technologii powoduje, że ustawodawstwo państw wydaje się nie nadążać z wprowadzeniem odpowiednich uregulowań prawnych, które chroniłyby podstawowe prawa i wolności obywatela przed niedozwoloną kontrolą. Według medialnych doniesień jeden z systemów inwigilacji – Pegasus miał zostać zakupiony przez Centralne Biuro Antykorupcyjne (CBA). Oprogramowanie to jest wyjątkowo trudne do wykrycia przez użytkownika, którego sprzęt został zainfekowany. Ponadto w przypadku znalezienia Pegasusa na urządzeniu przy użyciu innych programów dochodzi do jego samozniszczenia i zatarcia wszelkich śladów obecności. Oznacza to, że obywatel może być kontrolowany i o tym nie wiedzieć. Pojawiły się więc wątpliwości co do ewentualnych podstaw prawnych do używania przez władze państwa systemów szpiegujących. Niniejszy artykuł dokonuje analizy obowiązujących przepisów w kontekście hipotetycznego uprawnienia władz do kontroli obywateli przy użyciu systemów takich jak Pegasus oraz wskazuje zagrożenia, które może spowodować jego używanie. Autorka próbuje wartościować i porównać zagwarantowane w Konstytucji oraz w aktach prawa międzynarodowego prawa i wolności obywatelskie z interesem i bezpieczeństwem państwa, który miałby stanowić podstawę do przeprowadzenia tego typu kontroli.

Uwagi wstępne

Wszechobecna cyfryzacja i rozwój technologiczny odciska swoje piętno w niemal każdej dziedzinie życia ludzkiego. Gdziekolwiek się nie poruszamy, zawsze towarzyszą nam urządzenia elektroniczne z dostępem do Internetu. Nie można się oprzeć wrażeniu, że część życia jest prowadzona w tej wirtualnej przestrzeni, a rozwój technologiczny nieodzownie oddziałuje na każdą sferę funkcjonowania człowieka. Trudno wyobrazić sobie dzisiejszy świat bez ułatwień, które przyniosła ludzkości komputeryzacja oraz dostęp do Internetu. Jednakże oprócz wymieniania wszystkich ich zalet nie można nie wspomnieć o równie licznych zagrożeniach, które niesie za sobą nieustanny rozwój cyfryzacji. Przede wszystkim aby móc korzystać z niektórych dobrodziejstw Internetu czy urządzeń elektronicznych, należy w pierwszej kolejności założyć profil (konto) i podać dane osobowe. Ponadto, prowadząc portal społecznościowy czy blog, użytkownicy często udostępniają swój wizerunek oraz informacje na temat codziennych aktywności, tworząc przy tym elektroniczną bazę danych o sobie. Niektóre z aplikacji otrzymują również dostęp do aktualnej lokalizacji swoich użytkowników. Nie zawsze wiadomo, w jakich celach dane te mogą zostać użyte[2]. Pytanie, które mogłoby się w tym miejscu pojawić, to na ile świadomie użytkownicy podają o sobie informacje i czy są świadomi konsekwencji ich upublicznienia.

O ile oczywiste jest, że wszelkie ataki hakerskie, crackerskie są nielegalne i powinny zostać potępione, o tyle warto zastanowić się nad ewentualną możliwością stosowania szpiegowskich oprogramowań przez władze państwowe w celu kontroli obywateli i gromadzenia informacji o nich. Takie działania mogłyby być uzasadnione interesem i bezpieczeństwem państwa oraz wspomóc walkę z przestępczością. Jednym z takich programów, dającym szerokie spektrum inwigilacji, jest oprogramowanie Pegasus. Według medialnych doniesień z 2019 r. CBA miało je zakupić od izraelskiej firmy *NSO Group*, zajmującej się cyberbezpieczeństwem[3]. Jednakże zgodnie z oświadczeniem CBA z 4.9.2019 r. zamieszczonym na oficjalnej stronie CBA żaden: „system masowej inwigilacji Polaków" nie został zakupiony, a wszelkie spekulacje w tym temacie nie znajdują faktycznych podstaw[4]. Komunikat jest sformułowany ogólnie i nie jest w nim podana wprost informacja, że to Pegasus nie został zakupiony, co jest istotne, ponieważ program ten nie jest przeznaczony do masowej inwigilacji (kontrolowane mają być pojedyncze jednostki). Niemniej można założyć, że przy obecnej dynamice rozwoju technologicznego w przyszłości mogą powstać kolejne aplikacje czy programy szpiegujące, które będą pozwalały na tajne i masowe monitorowanie sprzętu elektronicznego jednostek.

[1] Absolwentka Prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] *A. Mednis*, Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość, Legalis/el. 2016. Niemniej należy mieć na względzie, że zgodnie z art. 13 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [Dz.Urz. UE L Nr 119, s. 1] administrator podczas pozyskiwania danych osobowych musi poinformować osobę, od której uzyskuje dane, o celach przetwarzania danych osobowych oraz wskazać podstawę prawną przetwarzania.

[3] Zob. https://businessinsider.com.pl/technologie/nowe-technologie/pegasus-opracowala-firma-nso-group-jak-wyglada-branza-w-izraelu/61b5ygx (dostęp z 10.4.2020 r.).

[4] Zob. https://cba.gov.pl/pl/aktualnosci/4207,Oswiadczenie-CBA.html (dostęp z 10.4.2020 r.).

Niniejszy artykuł ma na celu analizę przepisów prawnych w kontekście hipotetycznego uprawnienia władz do kontroli obywateli przy użyciu systemów pokroju Pegasusa oraz wskazanie zagrożenia, które może za sobą nieść tego typu aktywność poprzez potencjalne naruszenie prawa do prywatności, prawa do ochrony tajemnicy korespondencji, prawa do ochrony danych osobowych. Temat ten jest ważny, ponieważ nieustannie powstają nowe systemy inwigilacyjne, a obywatel wydaje się bezbronny w stosunku do nich. Świadomość, że państwo jest we władaniu Pegasusa czy innego szpiegującego oprogramowania, mogłaby rewolucyjnie wpłynąć na sposób użytkowania sprzętu elektronicznego i Internetu przez jednostki. Zwłaszcza biorąc pod uwagę, że niemal każdy jest posiadaczem sprzętu elektronicznego (zarówno prywatnego, jak i służbowego). Zgodnie z raportem Głównego Urzędu Statystycznego z 2019 r. pt. Polska w liczbach 2019, w 2018 r., dominującym urządzeniem, przez które Polacy łączą się z Internetem był smartfon[5].

Pegasus

Oprogramowanie Pegasus jest rozbudowanym narzędziem umożliwiającym dostęp do zainfekowanego urządzenia i zawartych w nich danych, które może bez trudu prześledzić i przechwycić. Do zainstalowania oprogramowania na telefonie komórkowym dochodzi poprzez kliknięcie w przesłany link (np. w SMS-ie). Za jego pośrednictwem dochodzi do tzw. *remote jailbreak*, który wykorzystuje istniejące luki w zabezpieczeniach urządzenia elektronicznego i powoduje osadzenie w nim Pegasusa. Użytkownik oprogramowania może od tej chwili inwigilować właściciela urządzenia, bez jego zgody i wiedzy[6]. Problematyczne jest to, że posiada on funkcję autodestrukcji, która aktywowana jest w sytuacji, gdy użytkownik szpiegowskiego oprogramowania nie komunikował się z nim dłuższy czas albo gdy prawdopodobne stało się jego wykrycie na zainfekowanym urządzeniu. Okazuje się więc, że w wielu przypadkach osoba, która była kontrolowana, nigdy nie posiądzie wiedzy na temat tego, że jej sprzęt i jego zawartość była przedmiotem inwigilacji. Twórcy Pegasusa podnoszą, że oprogramowanie tego typu są przeznaczone wyłącznie dla służb państwowych i mają służyć w walce z przestępczością oraz terroryzmem. Służby państw mają kierować działanie Pegasusa na konkretne osoby (wobec których istnieją dowody na to, że mogą być zaangażowane w działania przestępcze)[7].

Prawo do prywatności

W systemie prawa nie ma przepisu definiującego pojęcie „prywatności" czy „życie prywatne", dlatego też bliższego zrozumienia ich znaczenia należy szukać w doktrynie przedmiotu. Przedstawia ona prywatność jako pewną sferę działalności jednostki, która nie jest poddana zewnętrznej kontroli, i wskazuje, że „życie prywatne to przymioty, wewnętrzne przeżycia osobiste (jednostkowe) człowieka i ich oceny, refleksje dotyczące wydarzeń zewnętrznych i jego wrażenia zmysłowe, a także stan zdrowia oraz sytuacja majątkowa"[8]. Ze swojej istoty nie są one dedykowane na publiczne rozpowszechnienie i każdy powinien mieć zagwarantowaną możliwość dokonania dobrowolnego wyboru, czy chce, w jaki sposób, w jakim zakresie i komu udostępnić fragmenty swojej egzystencji[9]. W każdym środowisku społeczno-kulturowym obszar prywatności będzie inaczej rozumiany i gwarantowany w zależności od przystosowania osób w nim mieszkających do większej lub mniejszej potrzeby izolacji, stopnia dystansu, potrzeb nawiązywania czy też utrzymywania relacji towarzyskich[10]. Potrzeba zagwarantowania prawa do prywatności uzasadniona jest tym, że każdej osobie powinno przysługiwać prawo do „wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości innych jest swoistą *conditio sine qua* non swobodnego rozwoju jednostki"[11]. Prawo to jest gwarantowane w art. 47 Konstytucji RP i zgodnie z jego brzmieniem „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". W przepisie tym zostały zakodowane dwa rodzaje praw: pierwsze – prawo do ochrony prywatności, życia rodzinnego, czci, dobrego imienia, oraz drugie – prawo do samostanowienia[12]. Ustanowiona w art. 47 Konstytucji RP norma stanowi wskazówkę do interpretacji pozostałych praw i gwarancji konstytucyjnych, a ponadto jeśli prawo do prywatności i jego ochrona nie będzie w pełni gwarantowana przez pozostałe źródła prawa, to możliwe zawsze jest odwołanie się do gwarancji konstytucyjnej.

---

[5] Z raportu wynika również, że 96,2% przedsiębiorstw zaopatrzone jest w komputery stacjonarne lub przenośne, a 95,6% posiada dostęp do Internetu. Ponadto 66,8% z nich posiada własną stronę internetową, a 30,3% przedsiębiorców do prowadzenia działalności gospodarczej wykorzystuje także media społecznościowe, https://stat.gov.pl/obszary-tematyczne/inne-opracowania/inne-opracowania-zbiorcze/polska-w-liczbach-2019,14,12.html (dostęp z 10.4.2020 r.).

[6] Zob. https://www.komputerswiat.pl/artykuly/redakcyjne/pegasus-moze-podsluchac-kazdego-nawet-szefa-amazona-jak-dziala-system-inwigilacji/e4rkez2 (dostęp z 11.4.2020 r.).

[7] Zob. https://www.komputerswiat.pl/artykuly/redakcyjne/pegasus-moze-podsluchac-kazdego-nawet-szefa-amazona-jak-dziala-system-inwigilacji/e4rkez2; https://plblog.kaspersky.com/pegasus-spyware/6551/ (dostęp z 11.4.2020 r.).

[8] *B. Banaszak*, Konstytucja Rzeczypospolitej Polskiej. Komentarz, Legalis/el. 2012, art. 47 Nb 4, [za:] wyrok TK z 19.5.1998 r., U 5/97, OTK 1998, Nr 4, poz. 46.

[9] *Ibidem*.

[10] *J. Braciak*, Prawo do prywatności, [w:] *B. Banaszak*, *A. Preisner* (red.), Prawa i wolności obywatelskie w Konstytucji RP, Warszawa 2002, s. 278.

[11] *M. Pryciak*, Prawo do prywatności, www.bibliotekacyfrowa.pl/Content/37379/011.pdf (dostęp z 10.4.2020 r.), [za:] *M. Safjan*, Prawo do ochrony życia prywatnego, [w:] Szkoła Praw Człowieka, Helsińska Fundacja Praw Człowieka, Warszawa 2006, s. 211 i n.

[12] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Legalis/el. 2016, art. 47.

Na arenie prawa międzynarodowego i europejskiego prawo do prywatności gwarantowane jest również przez Międzynarodowy Pakt Obywatelskich i Politycznych z 19.12.1966 r.[13] oraz Kartę Praw Podstawowych UE z 26.10.2012 r.[14]. Fundamentalne znaczenie nad brzmieniem art. 47 Konstytucji RP miała regulacja zawarta w art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności z 4.11.1950 r.[15]. Przewiduje on, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji, a wszelka ingerencja władzy publicznej w korzystanie z prawa do prywatności i tajemnicy korespondencji jest niedopuszczalna. Wyjątek od tej regulacji stanowią przypadki przewidziane przez ustawę i konieczne w demokratycznym społeczeństwie z uwagi na m.in. bezpieczeństwo państwowe i publiczne, ochronę porządku, zapobieganie przestępstwom, ochronę praw i wolności innych osób.

Prawo do ochrony tajemnicy korespondencji

W art. 49 Konstytucji RP zapewniono wolność i ochronę tajemnicy komunikowania się, a ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Za komunikowanie uznaje się proces porozumiewania się, utrzymywanie relacji towarzyskich. W procesie tym muszą występować co najmniej dwie strony, które wzajemnie wymieniają się wiadomościami, z tym że dopuszcza się sytuację, w której tylko jedna z nich aktywnie przesyła komunikaty, a druga przyjmuje postawę bierną. Prawo do ochrony tajemnicy komunikowania przyznane jest wszystkim jednostkom, w tym także osobom prawnym. Sposób przekazywania informacji pozostaje w tym przypadku bez znaczenia, tzn. że osoby mogą się ze sobą komunikować osobiście albo za pomocą dostępnych środków przekazu[16]. Regulacja konstytucyjna chroni również dane osobowe osób uczestniczących w konwersacji, informacje o historii przeglądarki internetowej, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI[17]. Autonomia informacyjna obejmuje również ochronę przed niejawnym monitorowaniem osób i przeprowadzanych przez nią konwersacji[18], a także zabezpiecza przed dostępem do billingów z prowadzonych przez jednostkę rozmów telefonicznych, które zawierają dane o datach, długości trwania rozmów telefonicznych, połączeniach przychodzących i wychodzących[19]. Dzięki art. 49 Konstytucji RP osobom komunikującym się zagwarantowana jest wolność w trakcie całego procesu wymiany wiadomości i żaden inny podmiot nie powinien mieć dostępu i zapoznawać się z korespondencją, która nie była do niego adresowana.

Gwarancja autonomii informacyjnej

Kolejna gwarancja konstytucyjna, ściśle związana z prawem do prywatności, jest uregulowana w art. 51 Konstytucji RP. Regulacja ta przewiduje, że nie można nikogo zobowiązać inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Ponadto każdemu przysługuje prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a jakiekolwiek ograniczenia tego prawa mogą być przewidziane tylko przez ustawę. Każdy jest uprawniony do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą[20]. O ile postanowienia ustawy zasadniczej skierowane są w większości przypadków do organów państwa, o tyle należy rozumieć, że obowiązek przewidziany w art. 51 Konstytucji RP będzie odnosił się również do podmiotów niepublicznych. Ustawodawca przyjął zatem szeroki zakres podmiotów zobowiązanych do przestrzegania prawa zawartego w art. 51 Konstytucji RP. Warto zwrócić uwagę na redakcję przedmiotowego artykułu, użyte bowiem w ust. 1 słowo „nikt" należy interpretować jako „każdy", przez co, jak wskazuje się w doktrynie, mamy do czynienia z prawem człowieka[21]. Inaczej to wygląda w ust. 2 art. 51 Konstytucji RP. Przepis wzmiankuje już tylko o „obywatelach", co może prowadzić do konkluzji, jakoby władze publiczne mogły gromadzić, przetwarzać dane dotyczące pozostałych osób (nie obywateli) i – co ważne – informacje, które będą przetwarzane, nie muszą spełniać przesłanki niezbędności w demokratycznym państwie prawnym. Wiele trudności interpretacyjnych powoduje zawarte w ust. 2 omawianego artykułu sformułowanie: „informacje o obywatelach (...) niezbędne w demokratycznym państwie prawnym". Rozpoczynając od próby zdefiniowania zwrotu „informacja niezbędna", można przyjąć, że są to dane, które pozwolą na: „normalne funkcjonowanie jednostki w zorganizowanym w państwo społeczeństwie". Z perspektywy organów władzy publicznej niezbędne będą te dane, które są newralgiczne dla podjęcia, kontynuowania lub zakończenia podjętych działań i aktywności (pozostających oczywiście w zakresie uprawnień władzy). Doktryna nie zaprzecza możliwości istnienia i funkcjonowania baz danych czy też informatycznych systemów, które miałyby być dedykowane gromadzeniu infor-

[13] Dz.U. z 1977 r. Nr 38, poz. 167.
[14] Dz.Urz. UE C Nr 326, s. 391.
[15] Dz.U. 1993 r. Nr 61, poz. 284.
[16] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 47.
[17] Zob. wyrok TK z 30.7.2014 r., K 23/11, OTK-A 2014, Nr 7, poz. 80.
[18] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 49.
[19] M. Wild [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 49, [za:] wyrok TK z 30.7.2014 r., K 23/11, OTK-A 2014, Nr 7, poz. 80.
[20] Art. 51 ust. 1–4 Konstytucji RP.
[21] *B. Banaszak*, Konstytucja..., art. 51, Nb 4.

macji. Jednakże władza publiczna nie może posiłkować się tego typu programami tylko dla swojej wygody, ponieważ najprawdopodobniej dochodziłoby do nadużyć z jej strony[22]. Trybunał Konstytucyjny przedstawił pogląd, że co do zasady gromadzenie danych o jednostkach, nawet bez informowania ich o tym procesie, nie jest zakazane, pod warunkiem że spełnia przesłankę konieczności zgodnej ze standardami obowiązującymi w demokratycznym państwie prawnym. Chodzi więc o gromadzenie danych o jednostkach w celu ochrony wartości panujących w demokratycznym państwie prawnym, jeżeli cel ten nie może zostać osiągnięty przy użyciu innych instrumentów[23]. Przedstawione stanowisko jest niezwykle istotne w perspektywie dalszych rozważań na temat możliwości zastosowania oprogramowania Pegasus do inwigilacji społeczeństwa.

Ograniczenia praw i wolności

Przedstawione powyżej i gwarantowane przez Konstytucję RP (oraz akty międzynarodowe i europejskie) prawa nie mają charakteru absolutnego i po wystąpieniu przesłanek i spełnieniu odpowiednich warunków mogą zostać ograniczone. Wprowadzenie obostrzeń powinno spełniać konstytucyjne kryteria, tj. ograniczenie jednych praw i wolności musi być uzasadnione potrzebą zapewnienia bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób[24]. Przy wprowadzaniu jakichkolwiek ograniczeń należy kierować się zasadą proporcjonalności i dokonać porównania – wolności, która ma zostać niejako „poświęcona", oraz prawa, które ma być chronione[25]. Zgodnie z treścią zasady proporcjonalności regulacja ograniczająca wolności obywatelskie może być wprowadzona, jeżeli:

1) jest w stanie doprowadzić do zamierzonych przez nią skutków;
2) jest niezbędna do zapewnienia interesowi publicznemu, z którym jest powiązana, ochrony;
3) efekt wprowadzonych ograniczeń pozostanie w odpowiedniej relacji (proporcji) do nałożonych na jednostkę ciężarów.

Przewidziana w art. 31 ust. 3 Konstytucji RP zasada jest w inherentnym związku z zakazem nadmiernej ingerencji w sferę praw i wolności konstytucyjnych obywateli[26]. Dokonanie oceny, czy podjęta ingerencja była konieczna i proporcjonalna, jest uzależnione od analizy specyfiki poszczególnych uprawnień i wolności konstytucyjnych (np. standardy dotyczące wolności i praw ekonomicznych i socjalnych nie będą tak surowe jak te dotyczące praw osobistych i politycznych)[27]. Ograniczenie obywatelskich praw musi być wprowadzone przez ustawę.

Jedną z regulacji bezpośrednio ingerującą w sferę przedstawionych powyżej praw i wolności są przepisy dotyczące możliwości zastosowania kontroli operacyjnej. Kontrola ta jest prowadzona niejawnie i polega na monitorowaniu treści korespondencji, zawartości przesyłek oraz na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych. Oprócz treści rozmów można uzyskać jeszcze inne informacje przesyłane za pomocą sieci telekomunikacyjnych[28]. Rola przedsiębiorcy telekomunikacyjnego jest w tym kontekście bardzo ważna, ponieważ jest on zobligowany do zapewnienia, na własny koszt, warunków dostępu i utrwalania w zakresie wszystkich świadczonych usług telekomunikacyjnych[29]. Uprawnionym organem do przeprowadzenia kontroli operacyjnej jest m.in. Policja, CBA, ABW[30]. Zgodnie z art. 19 przewidziany przez ustawę z 6.4.1990 r. o Policji[31] przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw wymienionych w nim enumeratywnie, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd okręgowy może, w drodze postanowienia, zarządzić kontrolę operacyjną. Wniosek o zarządzenie kontroli składa Komendant Główny Policji, komendant wojewódzki Policji albo Komendant CBŚP po uzyskaniu zgody odpowiedniego prokuratora. Jednakże w sytuacji niecierpiącej zwłoki, która mogłaby spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, komendant może zarządzić kontrolę operacyjną, zwracając się jednocześnie do właściwego sądu z wnioskiem o wydanie postanowienia w tej sprawie. Jeżeli sąd w terminie pięciu dni od dnia zarządzenia kontroli nie wyrazi na nią zgody, to kontrola jest wstrzymywana i dokonuje się protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania[32]. Kontrola może trwać nie dłużej niż trzy miesiące, z tym że może zostać jednorazowo przedłużona o kolejne trzy miesiące[33]. Oczywiście może dojść do sytuacji, w której podczas kontroli uzyskano dowód popełnienia przestępstwa (wymienionego przez jeden z punktów

[22] *Ibidem*, art. 51, Nb 5–6.
[23] Zob. orzeczenie TK z 23.6.2009 r., K 54/07, OTK 2009, Nr 6A, poz. 86.
[24] Art. 31 ust. 3 Konstytucji RP.
[25] *B. Banaszak*, Konstytucja..., art. 47 Nb 8 [za:] wyrok TK z 21.10.1998 r., K 24/98, OTK Nr 6/1998, poz. 97.
[26] Orzeczenie TK z 23.6.2009 r., K 54/07, Legalis.
[27] *Ibidem*.
[28] *B. Opaliński*, *M. Rogalski, P. Szustakiewicz* (red.), Ustawa o Policji. Komentarz, wyd. 1, Legalis/e. 2015, art. 19, Nb 9, [za:] *J. Korycki*, Kontrola operacyjna, Prok. i Pr. Nr 7–8/2006, s. 150.
[29] Art. 179 ust. 3a ustawy z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2019 r. poz. 2460 ze zm.).
[30] Z uwagi na ramy niniejszego artykułu omówiona zostanie kontrola operacyjna przeprowadzana przez Policję oraz CBA.
[31] T.j. Dz.U. z 2020 r. poz. 360 ze zm.; dalej jako: PolU.
[32] Art. 19 ust. 3 PolU.
[33] Art. 19 ust. 8 PolU.

art. 19 PolU) i popełnionego przez osobę, wobec której była stosowana kontrola operacyjna, ale innego niż to przestępstwo, które było przedmiotem kontroli operacyjnej wobec tej osoby. Wówczas o zgodzie na wykorzystanie takiego dowodu w postępowaniu karnym będzie decydował sąd, który zarządził kontrolę operacyjną[34]. Kontrowersyjne jest jednak to, że osoba, wobec której takie działania były prowadzone, nie ma wglądu do materiałów zgromadzonych podczas ich trwania i nie może ich zweryfikować. Zgromadzone podczas kontroli materiały, które nie zawierają dowodów pozwalających na wszczęcie postępowania karnego lub dowodów mających znaczenie dla toczącego się postępowania karnego podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu[35].

Kolejną regulacją, ingerującą w sferę praw i wolności obywatelskich, jest art. 20 PolU. Zgodnie z nim Policja, z zachowaniem ograniczeń wynikających z art. 19, może uzyskiwać (niejawnie) informacje, a następnie je gromadzić, sprawdzać oraz przetwarzać. Informacjami, do których może mieć dostęp Policja, są dane osobowe, o których mowa w art. 14 ust. 1[36] ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[37]. Policja ponadto może uzyskać odciski linii papilarnych, zdjęcia, szkice i opisy wizerunku, cechy i znaki szczególne, pseudonimy oraz informacje o miejscu zamieszkania lub pobytu, wykształceniu, zawodzie, miejscu i stanowisku pracy oraz sytuacji materialnej i stanie majątku, dokumentach i przedmiotach, którymi sprawca się posługuje, sposobie działania sprawcy, jego środowisku i kontaktach[38]. Podobnie jak w przypadku prowadzenia kontroli operacyjnej, zgodę na gromadzenie i wykorzystanie danych musi wyrazić sąd. Zgromadzone dane podlegają ochronie przewidzianej w przepisach o ochronie informacji niejawnych i mogą być udostępniane jedynie policjantom prowadzącym czynności w danej sprawie i ich przełożonym. Akta zawierające te informacje i dane udostępnia się ponadto wyłącznie sądom i prokuratorom, jeżeli następuje to w celu ścigania karnego[39]. Zebrane dane osobowe przechowuje się przez okres niezbędny do realizacji ustawowych zadań Policji. Po zakończeniu sprawy (nie rzadziej niż co 10 lat od dnia uzyskania informacji) organy Policji dokonują ich weryfikacji i usuwają te dane, które okazały się zbędne[40].

Podobne uprawnienia przysługują CBA. W granicach swoich zadań[41] funkcjonariusze CBA wykonują czynności operacyjno-rozpoznawcze, czynności kontrolne czynności operacyjno-rozpoznawcze i analityczno-informacyjne, które uogólniając, mają służyć zapobieganiu popełniania przestępstw, ich wykrywaniu oraz zwalczaniu korupcji. Podczas przeprowadzania tych czynności funkcjonariusze mają obowiązek poszanowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka niezależnie od jego narodowości, pochodzenia, sytuacji społecznej, przekonań politycznych lub religijnych albo światopoglądowych[42]. Przy wykonywaniu czynności operacyjno-rozpoznawczych, które CBA podejmuje w celu wykrywania przestępstw i utrwalania dowodów ich popełnienia, może zostać zarządzona kontrola operacyjna. Wniosek o jej przeprowadzenie składa do sądu Szef CBA po uzyskaniu pisemnej zgody Prokuratora Generalnego. Kontrola operacyjna jest niejawna i może być zastosowana, jeżeli inne środki okazały się bezskuteczne albo nieprzydatne do osiągnięcia ustawowych zadań i celów CBA. Zgromadzone podczas stosowania kontroli materiały, które nie stanowią informacji potwierdzających zaistnienie przestępstwa, podlegają niezwłocznemu zniszczeniu[43]. Centralne Biuro Antykorupcyjne do realizacji ustawowych celów również może uzyskiwać niezbędne dane określone w art. 18 CenBiurAnU, a następnie je przetwarzać bez wiedzy i zgody osoby, której dotyczą. Szef CBA prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną CBA i funkcjonariusza CBA uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Kontrolę nad uzyskiwaniem przez CBA tego typu danych sprawuje Sąd Okręgowy w Warszawie[44]. Artykuł 22 CenBiurAnU daje CBA ogólne uprawnienie do tego, by w zakresie swojej właściwości uzyskiwało, gromadziło, sprawdzało i przetwarzało (w tym także niejawnie) informacje. Przepis ten był badany przez TK w przywoływanym już w niniejszym artykule wyroku z 23.6.2009 r.[45]. Trybunał stwierdził, że artykuł ten w ust. 1–3 w zakresie, w jakim dopuszcza uzyskiwanie (w tym także – niejawnie), gromadzenie, sprawdzanie i przetwarzanie informacji niezbędnych do zwalczania przestępstw, w obszarze należącym do ustawowo określonych zadań CBA jest zgodny z art. 47 w zw. z art. 31 ust. 3, art. 51 w zw. z art. 31 ust. 3 i art. 30 Konstytucji RP. Takie rozstrzygnięcie zostało uzasadnione faktem, że zwalczanie korupcji jest obowiązkiem państwa i dlatego też pod warunkiem utrzymania działań CBA ściśle w ramach ustawowo wyznaczonych – brak jest wystarczających podstaw do stwierdzenia, że postanowienia art. 22 ust. 1–3 CenBiurAnU są niezgodne z prawem do

[34] Zob. art. 19 ust. 15c PolU.
[35] Art. 19 ust. 16–17 PolU.
[36] M.in. dane osobowe ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych.
[37] Dz.U. z 2019 r. poz. 125.
[38] Art. 20 ust. 2b PolU.
[39] Art. 20 ust. 4 PolU.
[40] Art. 17–17b PolU.
[41] Art. 2 ustawy z 9.6.2006 r. o Centralnym Biurze Antykorupcyjnym, t.j. Dz.U. z 2019 r. poz. 1921 ze zm.; dalej jako: CenBiurAnU.
[42] Art. 13 CenBiurAnU.
[43] Art. 17 CenBiurAnU.
[44] Art. 18a CenBiurAnU.
[45] K 54/07, Legalis. Obecnie w art. 22 pozostał ust. 1, a pozostałe zostały uchylone.

prywatności oraz z prawem do autonomii informacyjnej. Niemniej jednak powyższe uprawnienia CBA mogą zostać użyte tylko w celu zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa. Sama możliwość kontrolowania obywateli poprzez wprowadzenie zapisów o kontroli operacyjnej budziła i wciąż budzi wiele kontrowersji. W trakcie jej trwania również można pozyskać wiele prywatnych i intymnych informacji, co oznacza, że służby państwa są już autoryzowane przez ustawodawstwo do wykorzystania mechanizmów inwigilacji względem obywateli. Niemniej następuje to tylko w przypadku enumeratywnie wymienionych przez ustawy przestępstw i jest poprzedzone ściśle określoną procedurą. Co ważne, Policja, by przejrzeć wiadomości, billing połączeń musi skontaktować się z przedsiębiorcą telekomunikacyjnym, operatorem pocztowym oraz usługodawca świadczący usługi drogą elektroniczną, czyli „zostawia po sobie ślad". Gdyby organy ścigania były we władaniu Pegasusa, nie byłyby zmuszone kontaktować się z kimkolwiek, by uzyskać potrzebne informacje. Pytanie również, czy udostępniane byłyby dane o liczbie przeprowadzonych kontroli, tak jak jest to chociażby w przypadku ustawy z 28.1.2016 r. – Prawo o prokuraturze[46]. Zgodnie z art. 11 ust. 1 PrProkU, Prokurator Generalny przedstawia Sejmowi i Senatowi roczną informację o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej. Z ostatniej przedłożonej informacji za 2018 r. wynika, że wszystkie uprawnione organy skierowały łącznie wobec 6088 osób wnioski o zarządzenie kontroli i utrwalanie rozmów lub wnioski o zarządzenie kontroli operacyjnej, przy czym: sąd zarządził kontrolę i utrwalanie rozmów lub kontrolę operacyjną wobec 5915 osób. Sąd odmówił zarządzenia kontroli i utrwalania rozmów lub kontroli operacyjnej wobec 25 osób, a wobec 148 osób wnioski o kontrolę operacyjną nie uzyskały zgody prokuratora[47]. Z przedstawionych danych wynika, że sądy w zdecydowanej większości wyrażają zgodę na przeprowadzenie kontroli operacyjnej, która powinna być traktowana jako ostateczność. Hipotetycznie więc, gdyby władze były w posiadaniu Pegasusa, to w jakiej relacji pozostawałoby jego użycie do kontroli operacyjnej? Czy w tym przypadku za ostateczność należałoby już traktować nie zastosowanie kontroli operacyjnej, a szpiegowskiego oprogramowania, czy też Pegasus byłby zastrzeżony tylko dla konkretnej służby do konkretnych działań zapewniających ochronę państwa. Niemniej w obecnym stanie: „Żaden bowiem przepis prawa nie pozwala żadnemu organowi państwowemu na przełamywanie zabezpieczeń i przechwytywanie, a także wykorzystywanie, w ten sposób treści przekazów komunikacyjnych oraz uzyskiwanie dostępu do wszelkich informacji i danych z urządzenia mobilnego"[48].

Bezpieczeństwo i interes państwa

Przedstawione uprawnienia Policji i CBA, ukierunkowane na zwalczanie przestępczości, mają za zadanie zapewnić bezpieczeństwo w państwie, które stanowi fundamentalny warunek jego rozwoju oraz społeczeństwa w nim funkcjonującego. Powszechnie przyjmowane jest, że nie jest możliwe ustanowienie stałych standardów bezpieczeństwa, ponieważ jest to proces, który zmienia się i powinien być dostosowany do zachodzących w społeczeństwie i w świecie zależności i zjawisk[49]. Dlatego ciężko jest wskazać jedną definicję bezpieczeństwa narodowego[50], co jest związane z dynamiką zmian warunków otoczenia, rozwojem cywilizacyjnym i technologicznym oraz sferą nowych potrzeb poszczególnych podmiotów. Ważne jest, by pojmować bezpieczeństwo w stosunkach narodowych jak dynamiczny proces o zmiennej intensywności[51]. W literaturze wskazuje się, że można wyróżnić cztery podstawowe wartości wchodzące w skład bezpieczeństwa narodowego – tj. przetrwanie, integralność terytorialna, niezależność polityczna, jakość życia (w wielu aspektach, np. kulturowym, rozwojowym, edukacyjnym, ekonomicznym)[52], a zagrożenie którejkolwiek z nich może stanowić niebezpieczeństwo dla szeroko pojętego interesu państwa i skutkować osłabieniem bezpieczeństwa narodowego. Zadaniem władzy jest więc troska i dbałość o zapewnienie obywatelom realnego bezpieczeństwa i ochrony, ale również powstrzymanie się od ingerowania w prywatną sferę ich życia. Wymagane jest wprowadzenie do porządku prawnego odpowiednich regulacji zapewniających instrumenty, które upoważnią władze do podejmowania adekwatnych działań pozwalających na utrzymanie porządku i bezpieczeństwa w państwie. Nieuniknione są sytuacje, w których w celu ochrony jednych wartości należy ograniczyć drugie. Wprowadzając jakiekolwiek ograniczenie wolności i praw obywatelskich, ustawodawca powinien kierować się opisaną

[46] T.j. Dz.U. z 2019 r. poz. 740 ze zm.; dalej jako: PrProkU.

[47] Jawna, roczna informacja Prokuratora Generalnego z 6.6.2019 r. o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej (druk senacki Nr 1209).

[48] Wystąpienie Rzecznika Praw Obywatelskich z 9.9.2019 r. skierowane do Prezesa Rady Ministrów w sprawie potencjalnego użycia systemu Pegasus, VII.519.2.2019.AG, s. 4, https://www.rpo.gov.pl/sites/default/files/Wystapienie_do_Premiera_ws_systemu_Pegasus_09.09.2019.pdf (dostęp z 20.4.2020 r.).

[49] *K. Olak*, *A. Olak*, Współczesne rozumienie bezpieczeństwa narodowego, ISSN 2300-1739, s. 470, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-750af56a-6af8-46ef-b41d-3a67e69d1217/c/Wspolczesne_rozumienie_467-480.pdf (dostęp 19.4.2020 r.).

[50] Pojęcie bezpieczeństwo państwa i bezpieczeństwo są ze sobą tożsame, *J. Czaputowicz*, Kryteria bezpieczeństwa międzynarodowego państwa – aspekty teoretyczne, [w:] *S. Dębski*, *B. Górki-Winter* (red.), Kryteria bezpieczeństwa międzynarodowego państwa, Warszawa 2003, s. 13.

[51] *J. Stańczyk*, Współczesne pojmowanie bezpieczeństwa, Warszawa 1996, s. 18–19.

[52] *J. Kukułka*, Bezpieczeństwo a współpraca europejska: współzależności i sprzeczności interesów, Sprawy Międzynarodowe 1982, Nr 7, s. 18.

powyżej zasadą proporcjonalności. Orzecznictwo podkreśla, że „im bardziej drastyczne (co do przedmiotu, zakresu, sposobu czy skutków) jest wkroczenie władzy w materię konstytucyjnie chronionych praw podstawowych, tym bardziej rygorystycznym przesłankom powinna podlegać procedura, stanowiąca gwarancję tego wkroczenia”[53]. Samo istnienie przepisów zezwalających na arbitralną inwigilację obywateli jest rozumiane jako naruszenie art. 8 EKPC i daje podstawę do wniesienia skargi do ETPC[54]. Nie można więc gromadzić danych o jednostkach w celu ich potencjalnego wykorzystania w przyszłości[55]. Pegasus nie mógłby więc z pewnością być używany w celach gromadzenia informacji o obywatelach, które mogłyby być w przyszłości użyte. Pomimo że prześledzenie działań obywatela z perspektywy kilku lat – gdzie był, jakie nawiązywał znajomości, czym się interesował, pozwoliłoby szybciej zweryfikować zgromadzone dowody oraz zrozumieć sposób jego działań, to takie gromadzenie danych za pomocą szpiegowskiego oprogramowania powinno zostać uznane za nielegalne. Rozwój technologiczny stanowi duże wyzwanie dla ustawodawcy, ponieważ prawo nieustannie musi być dostosowywane do pojawiających się na rynku innowacji technologicznych. Podkreśla to dynamikę zmienności pojęcia i znaczenia bezpieczeństwa państwa. Niestety, ale nie zawsze odpowiednie regulacje są wprowadzane na czas bądź nie są wystarczająco precyzyjne. Orzecznictwo podkreśla, że choć Konstytucja nie wzmiankuje o funkcjonowaniu obywateli w Internecie, to nie znaczy, że jej wolności i prawa nie będą się odnosiły analogicznie do tej wirtualnej przestrzeni i sposobu korzystania z niej. Informacje, które są przekazywane: „(...) za pomocą Internetu nie mogą być postrzegane jako funkcjonujące niejako obok, czy na marginesie konstytucyjnie chronionych form aktywności człowieka”[56].

Podsumowanie

Próbując odpowiedzieć na pytanie, czy istnieje bezpośrednia podstawa prawna pozwalająca na użycie przez władze państwowe oprogramowania typu Pegasus (tj. programu, który bez wiedzy i zgody obywatela mógłby zostać zainstalowany na jego urządzenie elektronicznym i pozyskiwał, gromadził z niego dane), należy odpowiedzieć przecząco. Nie oznacza to jednak, że oprogramowanie to nie byłoby pod pewnymi warunkami ułatwieniem dla władz państwowych w kontekście zapewnienia państwu i obywatelom bezpieczeństwa. Jednakże obywatele powinni wiedzieć, że tego typu oprogramowanie jest we władaniu władz i w przypadku uzasadnionego podejrzenia bądź współpracy przy popełnieniu przestępstwa władze mogą inwigilować ich sprzęt. Informacja, że organy ścigania są w posiadaniu takich środków, mogłaby działać prewencyjnie i zniechęcać do podejmowania działań niezgodnych z prawem. Z drugiej jednak strony przestępcy, wiedząc, że państwo dysponuje szpiegowskimi oprogramowaniami, nie pozostawialiby na swoich urządzeniach żadnych śladów, a co więcej, przy ich użyciu manipulowaliby śledztwem (fabrykowali dowody, zrzucali podejrzenia na inną osobę). Mając na uwadze, ile danych wrażliwych znajduje się w smartfonach, tego typu kontrola powinna być zastrzeżona dla najcięższych przestępstw i stanowić ostateczność – tj. zgodnie z zasadą proporcjonalności być stosowaną tylko w przypadku niemożliwości osiągnięcia celu prowadzonego postępowania przy użyciu innych dostępnych i legalnych środków. Inwigilacja przy użyciu Pegasusa pozwoliłaby, a bynajmniej mogłaby zwiększyć wiarygodność zebranych zeznań, dowodów. Procedura potencjalnego użycia systemu pokroju Pegasusa powinna zostać bardzo szczegółowo uregulowana w ustawie oraz wymieniać enumeratywnie przestępstwa i sytuacje, w których może on zostać użyty (a nawet ograniczyć się do zwalczania terroryzmu i korupcji wśród urzędników). Ustawa nie mogłaby zawierać żadnych klauzul generalnych, nie tworząc tym samym pola na rozbieżności interpretacyjne i wnioskowania prawnicze. Ponadto taki akt musiałby jasno wskazywać, czy inwigilować można całe urządzenie i jego wszystkie aplikacje, programy, galerie oraz kto miałby być odpowiedzialny za monitoring. Z pewnością taka osoba nie powinna być w żaden sposób powiązana z obywatelem, który miałby być inwigilowany oraz musiałaby zobowiązać się do zachowania w tajemnicy wszelkich informacji, które poweźmie w trakcie przeprowadzania kontroli. Ustawodawca musiałby również określić czas prowadzenia kontroli i ewentualną możliwość jej przedłużenia. Podobnie jak to jest w przywołanych powyżej regulacjach ustawy o Policji czy CBA, przepisy o ewentualnym stosowaniu programu pokroju Pegasusa musiałby wskazywać sposób niszczenia zgromadzonych danych, gdyby okazało się, że nie są one przydatne do śledztwa, oraz okres, po którym podlegałyby one usunięciu. Kolejną kwestią jest ewentualne prowadzenie rejestru gromadzącego informacje o tym, kto, kiedy, jak długo, przez kogo, w jakim celu był kontrolowany, a także na jakim urządzeniu, czy dane zostały usunięte oraz czy były przydatne i czy podlegają po upływie określonego czasu weryfikacji i usunięciu. Problematyczne jest również zajęcie stanowiska co do tego, czy kontrolowanemu obywatelowi powinno zostać wskazane, że jego prawo do prywatności zostało naruszone, do których informacji uzyskano dostęp oraz jaka była podstawa użycia szpiegowskiego oprogra-

[53] Zob. wyrok TK z 13.3.2007 r., K 8/07, Legalis.
[54] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 47, Nb 1 [za:] wyrok Europejskiego Trybunału Praw Człowieka z 4.12.2015 r. w spr. *Zakharov* przeciwko Rosji, skarga Nr 47143/06, HUDOC).
[55] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 47, Nb 1.
[56] Zob. wyrok TK z 30.7.2014 r., K 23/11, OTK-A 2014, Nr 7, poz. 80.

mowania. Jednakże taka informacja mogłaby zaszkodzić prowadzonemu postępowaniu. Pozostaje również temat nadzoru nad przeprowadzaniem inwigilacji przy użyciu Pegasusa – kto byłby za niego odpowiedzialny i jak miałby on w praktyce wyglądać. Mając na względzie dynamikę rozwoju cyberprzestępczości, z pewnością w najbliższym czasie uda się opracować odpowiednie aplikacje czy programy blokujące szpiegowskie oprogramowania bądź pozwalające na ich natychmiastowe usunięcie. Tyle że równolegle mogą powstawać kolejne programy pozwalające pozyskiwać dane z telefonów komórkowych obywateli, co doprowadziłoby do tzw. błędnego koła.

Podsumowując, organy państwa nie mogą za pomocą szpiegowskich oprogramowań gromadzić danych w celu ich potencjalnego użycia w przyszłości. Ponadto, biorąc pod uwagę już istniejące sposoby pozyskiwania i gromadzenia danych oraz kontroli obywateli (jak np. opisana powyżej kontrola operacyjna), wydaje się, że użycie szpiegowskich oprogramowań byłoby zbyt daleko ingerującym w konstytucyjne prawa i wolności obywatelskie środkiem. Niemniej temat ten wydaje się interesujący do dalszej dyskusji nad hipotetycznym użyciem systemów szpiegowskich w celu ochrony interesu i bezpieczeństwa państwa.

Słowa kluczowe: Pegasus, bezpieczeństwo państwa, prawo do prywatności, inwigilacja, cyberbezpieczeństwo.

Constitutional rights and freedoms in the face of new surveillance systems

Ubiquitous technological development and mass computerization necessarily affect not only the dailiness of the citizens but also the availability of new surveillance techniques. The dynamic development of these new technologies makes the legislation of countries seem to be lagging behind the introduction of appropriate legal regulations that would protect the fundamental rights and freedoms of citizens against unauthorized control. According to media reports, one of the surveillance systems – Pegasus was purchased by the Central Anticorruption Bureau. This software is extremely hard to detect by the user whose hardware has been infected. In addition, if Pegasus is found on the device, it is self-destructed and any traces of its presence are deleted. This means that the citizen may be controlled and does not know about it. Therefore, some doubts have arisen regarding the possible legal basis for the use of spying systems by the state authorities. The present article analyses the applicable legislation in the context of the hypothetical power of the authorities to control citizens by using systems such as Pegasus and indicates the risks that the use of Pegasus may cause. The author tries to value and compare the civil rights and freedoms guaranteed by the Constitution and international law with the interest and security of the state, which would be the basis for such control.

Keywords: Pegasus, national security, right to privacy, surveillance, cybersecurity.

Udział w zgromadzeniu spółki kapitałowej za pomocą środków komunikacji elektronicznej po zmianach Kodeksu spółek handlowych dokonanych w ramach tzw. tarczy antykryzysowej

dr hab. *Marek Leśniak*[1]

Celem niniejszego opracowania jest prezentacja wybranych skutków prawnych zmian legislacyjnych wynikających z ustawy z 31.3.2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw[2] na problematykę udziału w zgromadzeniu spółki kapitałowej za pomocą środków komunikacji elektronicznej.

Uwagi wstępne

Ostatniego dnia marca 2020 r. weszły w życie przepisy umożliwiające udział w zgromadzeniach spółek kapitałowych przy wykorzystaniu środków komunikacji elektronicznej z mocy prawa, a nie jak dotychczas z mocy umowy (statutu) spółki. Regulacje te są wynikiem reakcji ustawodawcy na nadzwyczajną sytuację spowodowaną pandemią koronawirusa (COVID-19). Warto jednak zaznaczyć, że wprowadzone zmiany mają charakter trwały, a nie czasowy przewidziany jedynie na okres pandemii. Nowe regulacje dotyczą zmian w funkcjonowaniu nie tylko organów właścicielskich, ale również menedżerskich. Niniejsze opracowanie omawia jedynie podstawowe założenia dotyczące udziału w organach właścicielskich, czyli zgromadzeniu wspólników spółki z ograniczoną odpowiedzialnością oraz walnym zgromadzeniu spółki akcyjnej[3]. Zmiany Kodeksu spółek handlowych dokonane opisywaną nowelizacją nie dotyczą walnego zgromadzenia prostej spółki akcyjnej (PSA). Przepisy obejmujące regulację prostej spółki akcyjnej, tj. art. 300^{1}–300^{134} KSH, wejdą w życie dopiero 1.3.2021 r. Jak się wydaje, przepisy te powinny również zawierać postanowienia analogiczne do regulacji dotyczącej „klasycznej" spółki akcyjnej w zakresie udziału w walnym zgromadzeniu za pomocą środków komunikacji elektronicznej.

Stan prawny dotyczący udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej przed nowelizacją

Udział w walnym zgromadzeniu spółki akcyjnej oraz zgromadzeniu wspólników spółki z o.o. przy wykorzystaniu środków komunikacji elektronicznej był możliwy na gruncie przepisów Kodeksu spółek handlowych także przed wejściem w życie ustawy zmieniającej. Regulacje dotyczące spółki akcyjnej obowiązywały od 3.8.2009 r. i były wynikiem zmian wprowadzonych przez przepisy ustawy z 5.12.2008 r. o zmianie ustawy Kodeks spółek handlowych oraz ustawy o obrocie instrumentami finansowymi[4], która stanowiła implementację do prawa polskiego art. 8 dyrektywy 2007/36/WE Parlamentu Europejskiego i Rady z 11.7.2007 r. w sprawie wykonywania niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym[5]. Regulacja ta na gruncie przepisów dyrektywy była przeznaczona wyłącznie dla spółek publicznych, natomiast polski ustawodawca umożliwił jej stosowanie w stosunku do wszystkich spółek akcyjnych. Problematyka ta była szeroko komentowana w doktrynie[6]. Z kolei przepisy

[1] Autor jest kierownikiem Zakładu Prawa Gospodarczego i Handlowego Uniwersytetu Wrocławskiego oraz notariuszem we Wrocławiu. ORCID 0000-0001-9634-9458.

[2] Dz.U. poz. 568; dalej jako: ustawa zmieniająca.

[3] Na mocy odesłania zawartego w art. 126 § 1 pkt 2 KSH regulacja znajduje zastosowanie także do walnego zgromadzenia spółki komandytowo-akcyjnej.

[4] Dz.U. z 2009 r. Nr 13, poz. 69.

[5] Dz.Urz. UE L Nr 184, s. 17; dalej jako: dyrektywa 2007/36/WE.

[6] *O. Horwath*, Elektroniczne walne zgromadzenie w świetle regulacji dyrektywy 2007/36/WE oraz prawa polskiego, Transformacje prawa prywatnego 2007, Nr 2–4, s. 54 i n.; *A. Opalski*, Reforma walnego zgromadzenia spółki akcyjnej – implementacja do prawa polskiego dyrektywy 2007/26/WE, PPH 2008, Nr 5, s. 8 in.; *R.L. Kwaśnicki*, *A. Bielecka*, „Internetowa" nowelizacja Kodeksu spółek handlowych – tabela zmian, Prawo Spółek 2009, Nr 3, s. 9 i n.; *M. Romanowski*, *A. Opalski*, Nowelizacja Kodeksu spółek handlowych w sprawie wykonywania niektórych praw akcjonariuszy spółek notowanych na rynku regulowanym, MoP 2009, Nr 7, dodatek s. 1–20; *M. Michalski*, Uwagi krytyczne do niektórych aspektów nowelizacji Kodeksu spółek handlowych z 5.12.2008 r., PPH 2010, Nr 2, s. 4 i n.; *K. Oplustil*, Dyrektywa 2007/36/WE w sprawie wykonywania praw akcjonariuszy i jej wpływ na prawo polskie (cz. I), MoP 2008, Nr 2, s. 63 i n.; *K. Oplustil*, Dyrektywa 2007/36/WE w sprawie wykonywania praw akcjonariuszy i jej wpływ na prawo polskie (cz. II), MoP 2008, Nr 3, s. 119 i n.; *J. Kołacz*, Dyrektywa 2007/36/WE w sprawie wykonywania niektórych praw akcjonariuszy, MoP 2008, Nr 9, Legalis/el. 2008; *K. Grabowski*, Dyrektywa o niektórych prawach akcjonariuszy i jej konsekwencje dla spółek publicznych, HUK – Czasopismo Kwartalne Całego Prawa Handlowego, Upadłościowego i Rynku Kapitałowego 2008, Nr 4, s. 481 i n.; *Ł. Goździaszek*, Cyberprzestrzeń spółek handlowych w kontekście prawnych problemów komunikacji elektronicznej, PPH 2009, Nr 11, s. 29 i n.; *M. Leśniak*, Kilka uwag dotyczących praktyki notarialnej w zakresie sporządzania

dotyczące spółki z o.o. umożliwiające udział w zgromadzeniu wspólników za pomocą środków komunikacji elektronicznej obowiązywały od 3.9.2019 r. na podstawie zmian wprowadzonych przez przepisy ustawy z 19.7.2019 r. o zmianie ustawy – Kodeks spółek handlowych[7].

Na gruncie poprzednio obowiązujących przepisów było wymagane udzielenie wcześniejszego upoważnienia w umowie spółki z o.o. i odpowiednio w statucie spółki akcyjnej umożliwiającego udział w zgromadzeniu przy wykorzystaniu środków komunikacji elektronicznej.

Stosownie do treści dawnych przepisów art. 234^1 § 1 pkt 1–3 KSH oraz art. 406^5 § 1 pkt 1–3 KSH umowa lub odpowiednio statut spółki mogły dopuszczać udział w walnym zgromadzeniu za pomocą – przykładowo wskazanych – sposobów wykorzystania środków komunikacji elektronicznej: 1) transmisji obrad zgromadzenia wspólników (walnego zgromadzenia) w czasie rzeczywistym; 2) dwustronnej komunikacji w czasie rzeczywistym, w ramach której wspólnicy (akcjonariusze) mogli wypowiadać się w toku obrad zgromadzenia wspólników (walnego zgromadzenia), przebywając w miejscu innym niż miejsce obrad zgromadzenia wspólników (walnego zgromadzenia); 3) wykonywania osobiście lub przez pełnomocnika prawa głosu przed lub w toku zgromadzenia. Wymienione przykładowo w powołanych przepisach[8] formy udziału w zgromadzeniu wspólników (walnym zgromadzeniu) nie były ze sobą w żaden sposób powiązane, co powodowało, że nie musiały być one stosowane łącznie. Zatem np. elektroniczne głosowanie (tzw. *e-voting*) nie musiało być połączone z możliwością udziału w dyskusji toczącej się na zgromadzeniu (tzw. dwustronna komunikacja). W doktrynie kwestionowano poprawność językową określenia mianem „udziału" w zgromadzeniu jedynie możliwości „śledzenia" transmisji jego obrad[9].

Z kolei przepisy dawnych art. 234^1 § 2 KSH i art. 406^5 § 2 KSH regulowały, że udział wspólników (akcjonariuszy) w zgromadzeniu może podlegać jedynie wymogom i ograniczeniom, które są niezbędne do identyfikacji akcjonariuszy i zapewnienia bezpieczeństwa komunikacji elektronicznej.

W przypadku spółek akcyjnych publicznych poprzednio obowiązujące przepisy regulowały również kwestie transmisji obrad walnego zgromadzenia w czasie rzeczywistym. Ponadto do spółek akcyjnych publicznych miał zastosowanie art. 406^5 § 4–5 KSH (według oznaczenia przyjętego przed wejściem w życie ustawy nowelizującej), który został uchwalony na podstawie art. 8 pkt 4 ustawy z 16.10.2019 r. o zmianie ustawy o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych oraz niektórych innych ustaw[10]. Przepisy te miały wejść w życie 3.9.2020 r.

Powyższe uwagi o charakterze wprowadzającym są niezbędne celem podkreślenia, iż aktualne regulacje zawarte w art. 234^1 KSH oraz art. 406^5 KSH nie stanowią w pełni nowego rozwiązania nieznanego wcześniej polskiemu prawu spółek.

Stan prawny dotyczący udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej po nowelizacji

1. Kodeksowy model wykorzystania środków komunikacji elektronicznej do udziału w zgromadzeniu spółki kapitałowej

Po wejściu w życie 31.3.2020 r. przepisów ustawy zmieniającej kodeksowy model wykorzystania środków komunikacji elektronicznej do udziału w zgromadzeniu wspólników spółki z o.o. oraz do udziału w walnym zgromadzeniu spółki akcyjnej przewiduje taką możliwość *ex lege*. W aktualnym stanie prawnym nie jest więc wymagane udzielenie wcześniejszego upoważnienia w umowie spółki z o.o. i odpowiednio w statucie spółki akcyjnej celem umożliwienia organizacji zgromadzenia przy wykorzystaniu środków komunikacji elektronicznej. Umowa lub statut spółki może jednak zawierać postanowienia odmienne, wyłączając możliwość udziału w zgromadzeniu za pomocą środków komunikacji elektronicznej. Jednocześnie obecna regulacja zawarta w art. 234^1 § 1 KSH oraz art. 406^5 § 1 KSH nie nakłada obowiązku zwoływania zgromadzeń spółek kapitałowych wyłącznie z użyciem środków komunikacji elektronicznej. Możliwe jest więc zwołanie zgromadzenia wspólników (walnego zgromadzenia), w którym udział będzie dopuszczalny jedynie na „tradycyjnych" zasadach, czyli przy fizycznej obecności uczestników zgromadzenia w miejscu jego obrad. Zgodnie z regulacją zawartą w art. 234^1 § 1 zd. 2 KSH oraz art. 406^5 § 1 zd. 2 KSH o udziale w zgromadzeniu wspólników (walnym zgromadzeniu) przy wykorzystaniu środków komunikacji elektronicznej decyduje zwołujący to zgromadzenie. W praktyce zwołującym będzie najczęściej zarząd.

protokołu Walnego Zgromadzenia Akcjonariuszy po wejściu w życie ustawy z 5.12.2008 r. o zmianie ustawy Kodeks spółek handlowych oraz ustawy o obrocie instrumentami finansowymi, [w:] *J. Gołaczyński*, *P. Machnikowski* (red.), Współczesne problemy prawa prywatnego. Księga pamiątkowa ku czci Profesora Edwarda Gniewka, Warszawa 2010, s. 312 i n.; *A. Herbet*, [w:] *S. Sołtysiński*, *A. Szajkowski*, *A. Szumański* i in., Kodeks spółek handlowych. Komentarz, t. 3, Legalis/el. 2013.

[7] Dz.U. poz. 1543.

[8] Na przykładowy sposób wyliczenia wskazywał użyty na końcu dawnego art. 234^1 § 1 KSH i art. 406^5 § 1 KSH zwrot „w szczególności".

[9] Por. *A. Herbet*, [w:] *S. Sołtysiński*, *A. Szajkowski*, *A. Szumański* i in., Kodeks spółek…, Nb 11 do art. 406^5.

[10] Dz.U. poz. 2217 ze zm.

2. Regulamin szczegółowych zasad udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej

Ustawodawca nałożył na spółki, które chcą zapewnić zdalny udział w zgromadzeniu wspólników (walnym zgromadzeniu), obowiązek określenia w formie regulaminu szczegółowych zasad tego udziału. W spółce z o.o. zgodnie z art. 234^1 § 3 KSH kompetencje do uchwalenia tego rodzaju regulaminu przyznano radzie nadzorczej, a gdy spółka nie posiada rady nadzorczej – wspólnikom. Warto zauważyć, że w spółkach z o.o. nieposiadających rady nadzorczej, w których decyzje w sprawie uchwalenia regulaminu powierzono wspólnikom, uchwała wspólników działających poza zgromadzeniem dotycząca regulaminu, może być przyjęta bezwzględną większością głosów (art. 234^1 § 3 zd. 3 KSH). Rozwiązanie to ma umożliwić podjęcie uchwały w sytuacji konfliktu pomiędzy wspólnikami i stanowi wyjątek od zasady określonej w przepisie art. 227 § 2 KSH wymagającej jednomyślności dla uchwał podejmowanych na piśmie poza zgromadzeniem[11]. Natomiast w spółce akcyjnej stosowny regulamin przyjmuje rada nadzorcza (art. 406^5 § 3 KSH).

Ustawodawca wprowadził ponadto zasadę, zgodnie z którą regulamin szczegółowych zasad udziału w zgromadzeniu wspólników (walnym zgromadzeniu) przy wykorzystywaniu środków komunikacji elektronicznej nie może określać wymogów i ograniczeń, które nie są niezbędne do identyfikacji wspólników i zapewnienia bezpieczeństwa komunikacji elektronicznej. Jak wskazuje *A. Szumański*, zasada ta jest wymagana przez dyrektywę 2007/36/WE jedynie dla spółek akcyjnych publicznych, jednak na gruncie Kodeksu spółek handlowych obowiązywała ona także dla spółek akcyjnych niepublicznych i spółki z o.o.[12].

Należy przyjąć, że tego typu regulamin powinien koncentrować się na normowaniu kwestii technicznych dotyczących funkcjonalności środków komunikacji elektronicznej służących zdalnemu uczestnictwu w obradach zgromadzenia oraz zawierać normy dotyczące zachowań uczestników zgromadzenia związanych z obsługą środków komunikacji elektronicznej przy wykonywaniu ich uprawnień składających się na prawo udziału w zgromadzeniu.

3. Pojęcie udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej

Nowa regulacja zawarta w art. 234^1 § 1 i 2 KSH oraz w art. 406^5 § 1 i 2 KSH inaczej określiła sposób (formę) udziału w zgromadzeniu wspólników (walnym zgromadzeniu) spółek kapitałowych przy wykorzystaniu środków komunikacji elektronicznej. W obu przepisach wskazano sposób udziału w zgromadzeniu, który polega na technicznej możliwości dwustronnej komunikacji w czasie rzeczywistym wszystkich osób uczestniczących w zgromadzeniu, w ramach której mogą one wypowiadać się w toku jego obrad, przebywając w innymi miejscu niż miejsce obrad zgromadzenia, a ponadto na zapewnieniu możliwości wykonywania osobiście przez wspólnika (akcjonariusza) lub jego pełnomocnika prawa głosu przed lub w toku zgromadzenia. Ustawodawca zdecydował, że pojęcie „udziału" w zgromadzeniu spółki kapitałowej nie może być dłużej rozumiane jedynie jako możliwość „śledzenia" transmisji obrad zgromadzenia (dawny pkt 1 art. 234^1 § 1 i art. 406^5 § 1 KSH). Ponadto poprzez użycie spójnika „i" ustawodawca połączył możliwość tzw. dwustronnej komunikacji (dawny pkt 2 art. 234^1 § 1 i art. 406^5 § 1 KSH) z możliwością wykonywania prawa głosu (dawny pkt 3 art. 234^1 § 1 i art. 406^5 § 1 KSH) w jedną formę udziału w zgromadzeniu.

Wypada zatem przyjąć, że od momentu wejścia w życie nowelizacji z 31.3.2020 r. udział w zgromadzeniu wspólników (walnym zgromadzeniu) spółki kapitałowej za pomocą środków komunikacji elektronicznej w rozumieniu art. 234^1 § 1 i 406^5 § 1 KSH oznacza konieczność zapewnienia wspólnikom (akcjonariuszom) lub ich pełnomocnikom technicznej możliwości nie tylko wzajemnej komunikacji, ale także wykonywanie prawa głosu w sytuacji, kiedy wspólnik (akcjonariusz) albo jego pełnomocnik przebywają fizycznie w innym miejscu niż miejsce obrad zgromadzenia[13]. W konsekwencji przyjętych rozwiązań wspólnik (akcjonariusz) lub jego pełnomocnik, który uczestniczy w zgromadzeniu za pomocą środków komunikacji elektronicznej, może wykonywać takie same (lub prawie takie same) uprawnienia składające się na prawo udziału w zgromadzeniu jak podczas fizycznej obecności w miejscu obrad. Obejmuje to następujące uprawnienia: do udziału w głosowaniu, a także uprawnienia wynikające z możliwości dwustronnej komunikacji w czasie rzeczywistym, czyli w szczególności: do udziału w dyskusji, do składania wniosków formalnych czy do składania projektów uchwał. Ponadto wspólnikowi (akcjonariuszowi) lub jego pełnomocnikowi będzie przysługiwać uprawnienie w postaci biernego prawa wyborczego do funkcji związanych z odbyciem zgromadzenia. To ostatnie uprawnienie, jak się wydaje, może być ograniczone jedynie możliwościami technicznymi środków komunikacji elektronicznej. Minimalny zakres wycinka praw korporacyjnych, które przysługują akcjonariuszowi (wspólnikowi) w ramach zdalnego udziału w walnym zgromadzeniu (zgromadzeniu wspólników) uległ więc poszerzeniu w stosunku do stanu istniejącego wcześniej.

[11] Tak też *A. Szumański*, Nowa regulacja udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej, PPH 2020, Nr 5, s. 11.

[12] *Ibidem*, s. 11.

[13] Tak też *A. Szumański*, Nowa regulacja udziału…, s. 10.

Ponadto obecna regulacja zawarta w art. 406^5 § 4 KSH, która nakłada na spółkę akcyjną publiczną konieczność zapewnienia transmisji obrad walnego zgromadzenia w czasie rzeczywistym, oznacza, że zapewnienie możliwości przekazywania „na żywo" obrazu i dźwięku z miejsca obrad nie jest traktowane jako jeden ze sposobów udziału w zgromadzeniu wspólników (walnym zgromadzeniu) w rozumieniu art. 234^1 § 1 i art. 406^5 § 1 KSH, a jedynie jako platforma komunikacji realizująca prawo do informacji.

Nowe rozwiązanie niewątpliwie zasługuje na aprobatę z kilku powodów. Przede wszystkim jest znacznie bardziej poprawne językowo, nie pozwala bowiem na określenie pozycji osoby jedynie obserwującej transmisję obrad mianem udziału w zgromadzeniu. Ponadto obecna regulacja powoduje, że akcjonariusze (wspólnicy) lub ich pełnomocnicy, którzy decydują się na zdalny udział w zgromadzeniu, mają zapewnioną techniczną możliwość dużej aktywności w obradach. Jednocześnie obecna regulacja nie pozostawia wątpliwości, że reprezentowana na zgromadzeniu część kapitału zakładowego wynikająca z sumy akcji (udziałów) przypadających na poszczególnych uczestników posiada zdolność do kształtowania treści uchwał będących przedmiotem zgromadzenia (kworum), akcjonariusz (wspólnik) posiada bowiem techniczną możliwość do wykonywania prawa głosu osobiście lub przez pełnomocnika.

Na zakończenie wypada jedynie dodać, że pozostawienie w art. 234^1 § 2 i art. 406^5 § 2 KSH zwrotu „w szczególności" pozwala w dalszym ciągu wnioskować, że opisana w powołanych przepisach forma udziału w zgromadzeniu wspólników (walnym zgromadzeniu) jest formą przykładową. Jak wskazuje w literaturze *A. Szumański*, zwrot ten pojawił się na dalszym etapie prac legislacyjnych, co nieco osłabia przyjętą w projekcie ustawy zmieniającej koncepcję definicji normatywnej udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej[14].

4. Miejsce odbywania się zgromadzenia spółki kapitałowej zorganizowanego przy wykorzystaniu środków komunikacji elektronicznej

Przepisy Kodeksu spółek handlowych dla spółki z o.o. (art. 234 § 1 w zw. z art. 238 § 2) podobnie jak dla spółki akcyjnej (art. 403 w zw. z art. 402 § 2) wymagają, aby zgromadzenie wspólników (walne zgromadzenie) odbywało się w siedzibie spółki[15], chyba że umowa (statut) spółki wyraźnie wskaże inne miejsce na terytorium RP[16]. Normy wynikające z powołanych przepisów Kodeksu spółek handlowych nakazują, aby zgromadzenie wspólników (walne zgromadzenie) odbywało się w miejscowości (miejscu) w przestrzeni geograficznej na terytorium RP[17]. Przy czym wykładnia celowościowa powołanych przepisów prowadzi do wniosku, że chodzi w nich o obszar geograficzny objęty granicami państwowymi oddzielającymi obszar ten od terytorium państw ościennych. Przepisy te nie obejmują polskich placówek dyplomatycznych czy polskich statków morskich i powietrznych, które nie są traktowane jak terytorium państwa polskiego. Określenie „miejsce", którym posłużył się ustawodawca w art. 234 § 1 i 2 KSH oraz w art. 403 KSH, oznacza „ograniczony wycinek przestrzeni w sensie geograficznym", ale nie obejmuje możliwości dokonania wyboru przestrzeni wirtualnej (tzw. miejsce w sieci)[18].

Konkludując, możliwość udziału w zgromadzeniu wspólników (walnym zgromadzeniu) przy wykorzystaniu środków komunikacji elektronicznej nie wpływa na zmianę istniejącej koncepcji miejsca zgromadzenia wspólników (walnego zgromadzenia), które musi być położone w określonym geograficznie punkcie na terytorium RP. Miejsce to (wraz z adresem) należy wskazać w zaproszeniu na zgromadzenie wspólników lub odpowiednio w ogłoszeniu o walnym zgromadzeniu. Regulacja dotycząca miejsca zgromadzenia wspólników w „tradycyjnej" spółce z o.o. oraz miejsca walnego zgromadzenia w spółce akcyjnej różni się zatem od regulacji zawartej w art. 240^1 § 1 i 2 KSH dotyczącej podejmowania przez wspólników uchwał w tzw. e-spółce z ograniczoną odpowiedzialnością. Te ostatnie przepisy są bowiem źródłem norm, które nie wymagają jednoznacznego określenia miejsca (miejscowości) obrad zgromadzenia wspólników tzw. e-spółki z o.o.[19].

Na zakończenie tego wątku rozważań należy jeszcze dodać, że postanowienia przepisów art. 234^1 KSH oraz art. 406^5 KSH nie odnoszą się w żaden sposób do lokalizacji (miejsca), w której znajdują się osoby uczestniczące za pośrednictwem środków komunikacji elektronicznej w zgromadzeniu wspólników (walnym zgromadzeniu). Oznacza to, że mogą one przebywać w dowolnym miejscu (miejscowości) na terenie jakiegokolwiek państwa i nie będzie to naruszać postanowień

[14] Tak też *A. Szumański*, Nowa regulacja udziału…, s. 9.

[15] W przypadku publicznej spółki akcyjnej walne zgromadzenie może odbyć się także w miejscowości będącej siedzibą spółki prowadzającej rynek regulowany, na którym akcje tej spółki są przedmiotem obrotu.

[16] Zgodnie z art. 234 § 2 KSH, jeżeli wszyscy wspólnicy wyrażą zgodę na piśmie, zgromadzenie wspólników może odbyć się również w innym miejscu na terytorium RP niż wskazane w art. 234 § 1 KSH.

[17] Por. *A. Szumański*, [w:] *S. Sołtysiński*, *A. Szajkowski*, *A. Szumański*, *J. Szwaja*, Kodeks spółek handlowych. Komentarz do art. 1–633, Nb 1 do art. 234, Legalis/el. 2005; *A. Kidyba*, Spółka z ograniczoną odpowiedzialnością. Komentarz, Nb 1 do art. 234, Legalis/el. 2005; *J.A. Strzępka*, *M. Zielińska*, [w:] *J.A. Strzępka* (red.), Kodeks spółek handlowych. Komentarz, Nb 1 do art. 234, Legalis/el. 2015.

[18] Tak też *M. Engeleit*, Wirtualne walne zgromadzenie. Wpływ Internetu na prawo spółki akcyjnej, Warszawa 2005, s. 232–236.

[19] Zob. na temat podejmowania uchwał w spółce z o.o. zawiązanej z użyciem normatywnego wzorca umowy *M. Leśniak*, „Wirtualne" zgromadzenie wspólników w e-spółce z ograniczoną odpowiedzialnością, [w:] *A. Olejniczak*, *T. Sójka* (red.), Societates et obligationes – tradycja, współczesność, przyszłość. Księga jubileuszowa Profesora Jacka Napierały, Poznań 2018, s. 311 i n.; *P. Pinior*, Podejmowanie uchwał wspólników w spółce z ograniczoną odpowiedzialnością, Warszawa 2019.

przepisów Kodeksu spółek handlowych dotyczących konieczności odbywania się zgromadzeń spółek kapitałowych na terytorium RP.

5. Dodatkowe wymogi związane ze zwołaniem zgromadzenia wspólników spółki kapitałowej zorganizowanego przy wykorzystaniu środków komunikacji elektronicznej

W przypadku spółki z o.o. poza „tradycyjnymi" wymogami związanymi ze sposobem zwołania zgromadzenia wspólników oraz treścią zaproszenia określonymi w art. 238 § 1 i 2 KSH dodano nowy § 3, zgodnie z którym „w przypadku, gdy udział w zgromadzeniu wspólników następuje przy wykorzystaniu środków komunikacji elektronicznej, w zawiadomieniu należy dodatkowo zamieścić informacje o sposobie uczestnictwa w tym zgromadzeniu, wypowiadania się w jego trakcie, wykonywania na nim prawa głosu oraz wniesienia sprzeciwu od podjętej wówczas uchwały bądź uchwał". Analogiczny przepis nakładający obowiązek zamieszczenia w zaproszeniu (ewentualnie ogłoszeniu) informacji o sposobie uczestniczenia w walnym zgromadzeniu itp. zorganizowanym przy wykorzystania środków komunikacji elektronicznej nie pojawił się natomiast w odniesieniu do niepublicznych spółek akcyjnych. Regulacja tej kwestii obejmuje jedynie spółki publiczne (art. 402^2 pkt 2 lit. d–g KSH), wydaje się jednak, że w przypadku organizacji walnego zgromadzenia w spółce niepublicznej przepis ten znajdzie zastosowanie w drodze ostrożnej analogii. Pomimo że regulacja art. 402^2 pkt 2 lit. a–g KSH nie nakazuje poinformowania o sposobie wnoszenia sprzeciwu od uchwał podjętych na zgromadzeniu odbytym przy wykorzystaniu środków komunikacji elektronicznej, nie oznacza to niemożności zawarcia takiej informacji w ogłoszeniu, art. 402^2 KSH zawiera bowiem wyliczenie przykładowe informacji objętych jego treścią[20].

Podsumowanie

Nowa regulacja ułatwia odbywanie zgromadzeń spółek kapitałowych z wykorzystaniem środków komunikacji elektronicznej, nie usuwając jednocześnie możliwości odbycia zgromadzenia w formie „tradycyjnej" w określonym miejscu. Decyzja w tym zakresie należy do zwołującego zgromadzenie.

Dokonana przez ustawodawcę próba zdefiniowania udziału w zgromadzeniu spółki kapitałowej przy wykorzystaniu środków komunikacji elektronicznej zdecydowanie szerzej określa minimalny wycinek praw korporacyjnych, które może wykonywać uczestnik zgromadzenia niż poprzednia regulacja.

Wydaje się, że nowelizacja uczyni zdalne zgromadzenia spółek kapitałowych bardziej popularnymi i bezpiecznymi, co w konsekwencji wpłynie na poprawę sytuacji gospodarczej spółek, ich udziałowców oraz otoczenia gospodarczego.

[20] Tak też *A. Szumański*, Nowa regulacja udziału…, s. 12.

Słowa kluczowe: zdalne zgromadzenia spółek kapitałowych, środki komunikacji elektronicznej.

Participation in a meeting of a private limited company by means of electronic communication after amendments to the Code of Commercial Companies made under the so-called anti-crisis shield

The purpose of this article is to present chosen legal repercussions of legislative changes resulting from the act of 31.3.2020 on the amendment of the act on special solutions connected with prevention, counteracting and fighting COVID-19, other infectious diseases and crisis situations caused by them and certain other acts regarding the issue of participation in a meeting of a private limited company by means of electronic communication.

The new regulation facilitates holding meetings of private limited companies using electronic means of communication, without removing the possibility of holding meetings in the „traditional" form in a specific place. The decision on this matter belongs to the person convening the meeting. The attempt by the legislator to define participation in the meeting of a private limited company using means of electronic communication more broadly defines the minimum segment of corporate rights that a participant in the meeting may perform than the previous regulation. It seems that the amendment will make remote assemblies of private limited companies more popular and secure, which in turn will improve the economic situation of companies, their shareholders and the economic environment.

Keywords: remote meetings of private limited companies, electronic means of communication.