Telekomunikacja, Media i Internet w Polsce

Opracowane przez DLA Piper Giziński Kycia sp. k. dla Polskiej Agencji Inwestycji i Handlu

Warszawa, 17 stycznia 2019 r.

Spis treści

1 Wstęp

1.1 Podstawowe informacje

Sektory telekomunikacji, mediów, usług elektronicznych oraz infrastruktury internetowej w Polsce charakteryzują się stosunkowo wysokim poziomem rozwoju i silną konkurencyjnością. Należy podkreślić, że wciąż jest to rynek atrakcyjny pod względem inwestycji zagranicznych i krajowych; przejęć (jak choćby kupno Netii przez Cyfrowy Polsat) i połączeń. Poszczególne sektory przenikają się i współpracują ze sobą, co w ujęciu konsumenckim przekłada się na interesujące łączone oferty.

Cennych informacji w zakresie liczb, kwot i układu sił, zarówno w zakresie infrastruktury internetowej, jak i telekomunikacji, dostarcza coroczny raport publikowany przez Urząd Komunikacji Elektronicznej (UKE). Na moment powstawania niniejszej publikacji dysponujemy raportem za rok 2017, natomiast raport za rok 2018 jest dopiero w przygotowaniu.

1.1.1 Internet

Rynek usług internetowych w Polsce charakteryzuje się dużym zróżnicowaniem jeśli chodzi o ilość operatorów, jednak układ sił jest na nim bardzo nierówny. Niemal jedna trzecia wszystkich osób, które korzystają z Internetu w Polsce, to klienci jednego operatora - Orange. Sieć ta objęła aż 31,7% użytkowników Internetu. Zaraz za Orange plasuje się Polkomtel (9,0%) oraz UPC (7,9%). Kolejni operatorzy w zestawieniu to T-Mobile i P4 (Play), którzy "zagarnęli", odpowiednio, 7,2% i 7,0%. Mniejsi operatorzy obejmują 17,4% użytkowników.

Interesujący jest również podział abonentów w zależności od form dostępu do sieci. W 2017 roku było ok. 7,1 mln użytkowników Internetu stacjonarnego. Z mobilnego dostępu do sieci korzystało ok. 7,4 mln osób. Łącznie dostęp do sieci posiada 14,5 mln użytkowników w Polsce.

1.1.2 Telefonia mobilna

Zgodnie z danymi zawartymi w raporcie UKE za 2017 rok, na krajowym rynku telefonii mobilnej na koniec 2017 r. działalność prowadziło 31 przedsiębiorców, o 2 więcej w stosunku do roku poprzedniego. Pięciu spośród nich posiadało własną infrastrukturę (tzw. operatorzy MNO), zaś 26 korzystało z sieci wybranego partnera technologicznego (tzw. operatorzy MVNO).

Co ciekawe, liczba użytkowników telefonii mobilnej od kilku lat systematycznie maleje. Na koniec 2017 r. aktywnych kart SIM było łącznie 53,3 mln, co oznaczało 4-procentowy spadek w stosunku do roku 2016. Należy zwrócić uwagę, że istotnie na ten sektor wpłynęła zmiana prawna w postaci wprowadzenia obowiązku rejestracji kart prepaid. W efekcie znacznie spadła liczba użytkowników usług przedpłaconych na korzyść klientów abonamentowych. W stosunku do roku 2016, liczba kart SIM prepaid zmniejszyła się aż o 22,3%.

1.1.3 Telefonia stacjonarna

W sektorze telekomunikacji stacjonarnej od dawna działa Orange Polska (wcześniej działający pod nazwą Telekomunikacja Polska. Drugim największym operatorem na rynku telekomunikacji stacjonarnej jest UPC (dane z raportu UKE za 2017 r.). Na dalszych miejscach plasują się Netia (obecnie część Cyfrowego Polsatu), Vectra, Telefonia Dialog i inni. Udział Orange Polska S.A. wynosił w 2017 r. jednak aż 52% rynku.

Należy zwrócić uwagę, że sektor telefonii stacjonarnej jest rynkiem kurczącym się. W 2017 r. całkowity czas trwania połączeń stacjonarnych wyniósł około 6,7 mld minut. Jest to spadek o 1,3 mld minut w porównaniu do 2016 r. Utrzymuje się zatem tendencja spadkowa, obserwowana na przestrzeni ostatnich 5 lat. Co więcej, zmniejszeniu uległa średnia miesięczna liczba minut na abonenta. W 2017 r. wyniosła 118 minut, z czego ponad 92% wszystkich minut w 2017 r. wygenerowanych zostało przez połączenia krajowe, natomiast jedynie 8% z tej liczby pochodziło z połączeń międzynarodowych

1.1.4 Usługi wiązane

Usługi wiązane są jednym z najbardziej dynamicznie rozwijających się segmentów rynku telekomunikacyjnego. W ciągu ostatnich 4 lat liczba użytkowników wzrosła znacząco - z poziomu 3,75 mln do 10,15 mln. O niezwykle szybkim rozwoju tych usług świadczy również porównanie danych w układzie rok do roku. W zestawieniu z 2016 r. nastąpił wzrost liczby użytkowników o 29%.

Usługi wiązane to oferty łączące różnego rodzaju usługi w atrakcyjne dla użytkowników pakiety. Jeśli chodzi o rok 2017, najpopularniejszym takim pakietem pozostała usługa „Telefonia ruchoma + Internet mobilny", której udział w rynku pod względem liczby użytkowników wyniósł ponad 60%. Na drugim miejscu pod względem popularności znalazła się usługa „Internet stacjonarny + Telewizja" (11%) a na trzecim „Telefonia stacjonarna + Internet stacjonarny + Telewizja" (7,2%).

1.2 Akty prawne

Najważniejszym aktem prawnym, który zawiera przepisy dotyczące działalności podmiotów na rynku telekomunikacyjnym, jak i praw abonentów, jest ustawa z dnia 16 lipca 2004 r. - Prawo Telekomunikacyjne (dalej „Prawo telekomunikacyjne"). Akt ten ma za sobą liczne nowelizacje. Ostatnie ogłoszenie tekstu jednolitego nastąpiło w drugiej połowie 2018 r. Drugim istotnym, uzupełniającym aktem prawnym dla tego sektora, jest ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, również kilkakrotnie zmieniana.

Zagadnienia dotyczące e-commerce, usług elektronicznych itd., uregulowane zostały przede wszystkim w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, z późniejszymi zmianami. W zakresie sektora dystrybucji mediów audiowizualnych znaczenie podstawowe ma ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji, z późniejszymi zmianami. Należy zwrócić

uwagę, że oprócz ww. przepisów szczególnych, do wszystkich wspomnianych sektorów mają zastosowanie przepisy ogólne o ochronie konkurencji i konsumentów, jak również o ochronie danych osobowych.

1.3 Organy rządowe i regulatorzy

Sektory telekomunikacyjny, audiowizualny oraz e-commerce pozostają obecnie w gestii głównie dwóch organów rządowych, tzn.: Ministerstwa Cyfryzacji (https://mc.gov.pl/) i Ministerstwa Kultury i Dziedzictwa Narodowego (http://www.mkidn.gov.pl). W praktyce największe znaczenie ma działalność organów regulacyjnych, którymi są: Urząd Komunikacji Elektronicznej (https://www.uke.gov.pl/) odpowiedzialny za regulację infrastruktury przedsiębiorców telekomunikacyjnych, mediów oraz nadawców, a także Krajowa Rada Radiofonii i Telewizji (http://www.krrit.gov.pl/), odpowiedzialna m. in. za udzielanie koncesji nadawcom radiowym i telewizyjnym. Z uwagi na istotną rolę, jaką w omawianych sektorach(szczególnie: telekomunikacyjnym oraz e-commerce) pełni przetwarzanie danych osobowych, należy także podkreślić ważną pozycję dwóch innych regulatorów, tzn. Urzędu Ochrony Danych Osobowych (https://uodo.gov.pl/pl) oraz Urzędu Ochrony Konkurencji i Konsumentów (https://www.uokik.gov.pl/).

2 Operatorzy telekomunikacyjni

2.1 Świadczenie usług telekomunikacyjnych - warunki

W celu świadczenia usług telekomunikacyjnych niezbędne jest uzyskanie przez operatora wpisu do rejestru prowadzonego przez Urząd Komunikacji Elektronicznej. Z kolei na eksploatację sieci telekomunikacyjnej nie są wymagane szczególne pozwolenia - oprócz pozwoleń na budowę, jak również na korzystanie ze środowiska.

Jeżeli operator chce korzystać z publicznej numeracji dla komunikacji głosowej, musi również złożyć wniosek do UKE. Przydzielenie numeracji następuje w drodze decyzji Prezesa UKE. Co do pozwoleń na częstotliwości do łączności ruchomej, pozwolenie na dane pasmo jest wydawane po przeprowadzeniu publicznego przetargu lub aukcji.

Z kolei jeśli chodzi o pozwolenia na łącza radiowe wykorzystywane do sieci dosyłowej (transmisyjnej), to wydaje się je indywidualnie dla każdego łącza. W celu nadawania sygnału telewizyjnego niezbędne jest uzyskanie dodatkowych koncesji na rozpowszechnianie lub rozprowadzanie programów radiowych i telewizyjnych udzielanych przez Krajową Radę Radiofonii i Telewizji.

2.2 Pozwolenia indywidualne: przedmiot, okres ważności, możliwość przenoszenia i obrotu

Prezes UKE wydaje różne typy pozwoleń indywidualnych. Po pierwsze, mamy pozwolenia dot. praw do częstotliwości. Przede wszystkim, podmiot może otrzymać rezerwację częstotliwości. W rezerwacji częstotliwości określa się m.in. uprawniony podmiot, na rzecz którego dokonano rezerwacji

częstotliwości, oraz jego siedzibę i adres; zakres częstotliwości lub pozycje orbitalne objęte rezerwacją; obszar, na którym mogą być wykorzystywane częstotliwości; okresy wykorzystywania częstotliwości itd. Należy nadmienić, że okres, na który przyznana zostaje rezerwacja częstotliwości, nie może przekroczyć 15 lat.

W przypadku braku dostatecznych zasobów częstotliwości podmiot, rezerwacja jest przyznawana po przeprowadzeniu konkursu (w przypadku rezerwacji częstotliwości na cele rozpowszechniania w sposób cyfrowy lub rozprowadzania programów radiofonicznych lub telewizyjnych) albo przetargu albo aukcji.

Co ważne, rezerwacja częstotliwości może być przedmiotem przeniesienia lub obrotu. Pewnym ograniczeniem w obrocie rezerwacjami jest jednak fakt, iż zbycie rezerwacji częstotliwości lub jej części wymaga zgody UKE, jednakże ww. urząd może odmówić zgody jedynie w nielicznych przypadkach określonych w Prawie telekomunikacyjnym.

Trzeci typ wspomnianych wyżej pozwoleń indywidualnych dotyczy numeracji telefonicznej w sieciach publicznych. Nazywany jest przydziałem numeracji. Podobnie jak w przypadku częstotliwości, przydział numeracji dla usług telefonii publicznej dokonywany jest przez UKE na wniosek podmiotu. Jeżeli dwa podmioty złożą wniosek w tym samym zakresie numeracji, przeprowadza się postępowanie konsultacyjne lub przetarg. Numeracja, którą przydzieli UKE, może być współużytkowana z innymi operatorami na podstawie umowy, przy czym informacja o tym fakcie musi być przekazana UKE w terminie 14 dni od dnia rozpoczęcia współużytkowania.

3 Media elektroniczne - dystrybucja gier komputerowych za pomocą platform cyfrowych w świetle obowiązującego prawa.

3.1 Rynek gier komputerowych

Polski rynek gier komputerowych według raportu Newzoo (wiodący światowy dostawca gier i analiz esportowych) w 2017 r. (raport w wersji skróconej dostępny pod adresem https://newzoo.com/solutions/standard/market-forecasts/global-games-market-report/) wart był ponad 550 mln USD i posiada silne tendencje wzrostowe. W Polsce mamy ok. 16 mln graczy. Światowy rynek gier komputerowych jest wyceniany na 121,7 mld USD, a w roku 2018 miał on wzrosnąć do 137,9 mld dolarów.

Największy wzrost notowany jest w kategorii tytułów mobilnych, tj. umożliwiających grę na urządzeniach mobilnych takich jak smartfon i tablet, oraz w dystrybucji cyfrowej. Dystrybucja cyfrowa obejmuje sprzedaż tytułów na komputery klasy PC oraz konsole stacjonarne za pośrednictwem cyfrowych platform dystrybucji. Co więcej, warto zauważyć, że tytuły oferowane w kategorii mobilnej rozpowszechniane są również za pomocą platform ekskluzywnych dla danego typu urządzeń mobilnych, związanego z producentem systemu operacyjnego właściwego dla danego urządzenia. Ponadto, platformy cyfrowe mogą być wykorzystywane także do sprzedaży zawartości dodatkowej do wydanego już tytułu tzw. DLC oraz różnego rodzaju dodatków natury „kosmetycznej" lub wpływającej na rozgrywkę. Nadmienić należy, że tego rodzaju dodatki, w przypadku niektórych tytułów, generują coraz większe zyski, porównywalne ze sprzedażą bazowego tytułu. Jako przykład można wskazać EA Sports – wydawcę popularnej serii piłkarskiej FIFA, który w 2017 r. wypracował zyski ze sprzedaży dodatków w wysokości 800 mln USD (https://www.gamesindustry.biz/articles/2017-03-01-eas-ultimate-team-now-worth-USD800-million-annually)

Na polskim rynku działa obecnie ok. 400 studiów deweloperskich (dane nieoficjalne, https://www.rp.pl/Media-i-internet/307059849-Gry-komputerowe-rosna--w-Polsce-szybciej-niz-w-UE.html&template=restricted) produkujących tytuły głównie z kategorii gier mobilnych oraz tzw. *indie*, czyli tworzonych przez niezależnych deweloperów. Rozdrobnienie rynku oraz wyżej wspomniane tendencje krajowego, jak i światowego rynku gier, przyczyniają się do znacznej atrakcyjności cyfrowych platform dystrybucyjnych dla sprzedaży swoich produktów, umożliwiając mniejszym studiom na zaistnienie na rynku. W praktyce, mniejsze podmioty mogą skorzystać z istniejących obecnie platform cyfrowych lub, w określonych wypadkach, podjąć się uruchomienia własnej platformy. W tym miejscu należy podać przykład platformy GOG operowanej przez spółkę należącą do grupy CD Projekt.

Przed skorzystaniem z ww. platform należy przeanalizować przepisy, które mogą mieć zastosowanie. W zależności od obranego modelu/obranych modeli, tzn. (i) korzystania z istniejącej platformy lub (ii) założenia własnej, zastosowanie mogą mieć odmienne regulacje. Poniżej zostanie przedstawione

krótkie podsumowanie relewantnych przepisów. Zaznaczyć należy jednak, że katalog ten nie jest wyczerpujący i zastosowanie mogą mieć inne jeszcze przepisy, m.in. w zakresie podatków, AML czy przepisy w zakresie praw własności intelektualnej. Z racji na charakter publikacji przedstawimy w sposób ogólny kwestie mogące mieć znaczenie.

3.2 Przepisy prawa

3.2.1 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2017 r. poz. 1219 z późn. zm.). wprowadza szereg wymogów w zakresie świadczenia usług drogą elektroniczną, między innymi obowiązki w zakresie poufności i bezpieczeństwa (co ma w szczególności znaczenie przy płatnościach online przy zakupie gier), konieczność spełnienia obowiązku informacyjnego wobec usługobiorców, obowiązek przedstawienia regulaminu określającego m.in. procedurę reklamacyjną, jak również obowiązki w zakresie uzyskiwania zgody na przesyłanie informacji handlowych.

3.2.2 Ustawa z dnia 30 maja 2014 r. o prawach konsumenta

Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz. U. z 2017 r. poz. 683 z późn. zm.). określa wymagania w zakresie umów zawieranych poza lokalem przedsiębiorstwa lub na odległość, w tym obowiązki informacyjne, prawo do odstąpienia od umowy oraz wyjątki od tego prawa. Warto w tym miejscu nadmienić, że czołowe platformy dystrybucyjne korzystają z tego rodzaju wyjątkó ze względu na chęć ograniczenia nadużywania tego prawa przez konsumentów. Przykładowo, jedna z platform wymaga od osób kupujących rezygnacji z ustawowego prawa do odstąpienia od umowy w ciągu 14 dni na rzecz dodatkowego ograniczenia w postaci niegrania w grę więcej niż 2 godziny w ciągu 14 dniowego terminu.

3.2.3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) w zakresie dystrybucji cyfrowej ma zastosowanie m.in. odnośnie obowiązku informacyjnego, realizacji praw podmiotów danych osobowych, retencji danych oraz wyznaczania Inspektora Ochrony Danych.

3.2.4 Ustawa z dnia 19 listopada 2009 r. o grach hazardowych

Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (t.j. Dz. U. z 2018 r. poz. 165 z późn. zm.) może mieć zastosowanie w ograniczonym zakresie, w przypadku, gdy do danego tytułu lub w ramach platformy cyfrowej oferowane są treści mieszczące się w zakresie zastosowania jej przepisów. Taka

możliwość rozważana jest w kontekście tzw. loot boxów, tj. płatnej zawartości dodatkowej do gry oferującej określone korzyści w grze o charakterze losowym, w istocie swojej mechaniki przypominające grę losową w rozumieniu ustawy. Jednakże, kwestia ta nadal jest analizowana na szczeblu krajowym jak i unijnym, i na ten moment nie jest jednoznacznie rozstrzygnięte, czy przepisy te miałyby zastosowanie. Niemniej, należy mieć na uwadze taką możliwość i konsekwencje ww. interpretacji, m.in. możliwość naruszenia państwowego monopolu na organizację tego rodzaju gier oraz generalny zakaz reklamy gier hazardowych.

3.3 Podsumowanie

Charakterystyka oraz potencjał wzrostu polskiego rynku gier, w szczególności w zakresie rynku gier mobilnych oraz dystrybucji cyfrowej, zapewnia szerokie pole działania dla podmiotów zarówno o dużej skali jak i małych i średnich przedsiębiorców. Konieczne jest jednak uprzednie zapewnienie zgodności obranego modelu dystrybucyjnego z mającymi zastosowanie normami prawa. Ze względów organizacyjnych, a także skali niezbędnych nakładów, opłacalne jest korzystanie z już istniejącej infrastruktury największych platform cyfrowych, jednakże wiąże się to z koniecznością odstąpienia od części każdorazowego zysku na rzecz operatora platformy. Przedsiębiorcy muszą dostosować obraną strategię do swoich możliwości i oczekiwań.

4 Cyberbezpieczeństwo – obowiązki i kary

4.1 Geneza regulacji

Cyfrowe technologie są wykorzystywane nie tylko dla rozwoju handlu, transportu czy usług cyfrowych, ale mogą również posłużyć przy stosowaniu praktyk nieuczciwej konkurencji czy popełnianiu przestępstw[1]. Dlatego też zapewnienie cyberbezpieczeństwa staje się coraz ważniejszym aspektem dla każdego przedsiębiorcy - tym istotniejszym, jeśli w ramach jego organizacji przeprowadzane są operacje na dużych zasobach danych. Ze względu na powyższą zależność, organy Unii Europejskiej przyjęły specjalną dyrektywę, potocznie zwaną dyrektywą NIS[2]. Z perspektywy polskiego prawa wdrożenie unijnych przepisów nastąpiło poprzez ustawę z dnia 5 lipca o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560), dalej jako („Ustawa o cyberbezpieczeństwie").

Polskie przepisy

Ustawa o cyberbezpieczeństwie jest kolejnym, po RODO, aktem prawnym dotyczącym - częściowo - podobnych aspektów działalności , który wymaga od przedsiębiorców (oraz podmiotów publicznych) dostosowania. Niniejsze opracowanie ma na celu zarówno wskazanie ogólnych założeń istotnych dla przedsiębiorców, jak i umożliwienie łatwiejszego poruszania się po tekście ustawy. Należy podkreślić, że nie wszystkie ważne kwestie zostały uregulowane w samej ustawie. Część znajduje się w rozporządzeniach unijnych lub w rozporządzeniach do ustawy, co, niestety, utrudnia sprawne poruszanie się po już i tak skomplikowanej, tematyce. Przykładem jest istotność skutku zakłócającego, która określana jest na bazie progów istotności uregulowanych w osobnym rozporządzeniu[3].

4.2 Operator usługi kluczowej i jego obowiązki

Pierwszym z istotnych pojęć wprowadzonych przez ustawę jest tzw. operator usługi kluczowej. Operatorem usługi kluczowej jest podmiot, który prowadzi działalność jednego z rodzajów wymienionych w załączniku nr 1 do Ustawy o cyberbezpieczeństwie, posiadający jednostkę

---

[1] Uzasadnienie do projektu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, druk nr 2505, str. 73 pliku dostępnego na stronie http://orka.sejm.gov.pl/Druki8ka.nsf/0/6624C41DF04E6186C1258287003D9163/%24File/2505%20cz%20I.pdf

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

[3] Rozporządzenie Rady Ministrów z dnia 11 września w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

organizacyjną na terytorium Rzeczypospolitej Polskiej. Uzyskanie statusu operatora usługi kluczowej jest możliwe wyłącznie wskutek wydania decyzji administracyjnej przez ministra właściwego do spraw informatyzacji. Ww. organ prowadzi również wykaz operatorów kluczowych.

Warto zasygnalizować, że operatorami usługi kluczowej są podmioty, które prowadzą działalność gospodarczą w sektorach energii, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję oraz infrastruktury cyfrowej[4]. W sytuacji, gdy otrzymają one decyzję o uznaniu za operatora usługi kluczowej, konieczne stanie się wypełnienie obowiązków nałożonych przez ustawodawcę, we wskazanych odstępach czasu od otrzymania decyzji, tj. kolejno, 3 miesiące, 6 miesięcy i 12 miesięcy.

Przykładowo, w ciągu 3 miesięcy należy np. powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo (lub zawrzeć umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa); wyznaczyć osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, którą należy zgłosić do odpowiedniego organu w ciągu 14 dni od wyznaczenia czy rozpocząć dokonywanie szacowania ryzyka wystąpienia incydentu. Kolejne obowiązki, które należy spełnić w ciągu 6 miesięcy to np. opracowanie dokumentacji w zakresie cyberbezpieczeństwa czy wdrożenie odpowiednich i proporcjonalnych środków technicznych i organizacyjnych zapewniających m.in. bezpieczeństwo fizyczne systemu, uwzględniając przy tym kontrolę dostępu.

Natomiast w terminie 12 miesięcy od doręczenia decyzji konieczne jest przeprowadzenie audytu bezpieczeństwa systemu i przekazanie sprawozdania z audytu wskazanym podmiotom. Należy podkreślić, że audyty będą musiały być przeprowadzane w kolejnych latach w cyklu raz na dwa lata.

4.3 Dostawca usługi kluczowej i jego obowiązki

Drugie ważne pojęcie to dostawca usługi cyfrowej. Do tej kategorii, zgodnie z Ustawą o cyberbezpieczeństwie, zostały zaliczone podmioty świadczące usługi cyfrowe, tj. internetową platformę handlową, usługę przetwarzania w chmurze lub wyszukiwarkę internetową. Koniecznym warunkiem jest posiadanie siedziby lub zarządu ma terytorium Polski lub swojego przedstawiciela w Polsce. Należy podkreślić, że dla posiadania statusu przypadku dostawcy usługi kluczowej nie jest konieczne wydanie jakiejkolwiek decyzji; dostawcą jest się, o ile spełnione są warunki przewidziane w ww. ustawie.

Dla dostawcy usługi kluczowej, w przeciwieństwie do operatora usługi kluczowej, nie ma określonych terminów na wypełnienie obowiązków, którymi są m.in. klasyfikacja incydentów. Bardzo istotnym wymogiem jest konieczność zapewnienia właściwych i proporcjonalnych środków technicznych i

[4] Załącznik nr 1 do Ustawy o cyberbezpieczeństwie.

organizacyjnych zapewniających cyberbezpieczeństwo, które określone są w unijnym rozporządzeniu wykonawczym 2018/152, poprzez - przykładowo - ustanowienie polityk w zakresie zarządzania bezpieczeństwem. Warto zaznaczyć, że podmiot świadczący usługę cyfrową będący mikroprzedsiębiorcą (zatrudniającym średniorocznie mniej niż 10 pracowników i osiągający roczny obrót poniżej 2 mln euro) lub małym przedsiębiorcą (mniej niż 50 pracowników i osiągający roczny obrót poniżej 10 mln euro) nie podlega zapisom ustawy.

4.4 Wysokość kar pieniężnych

Ustawodawca, określając wysokość kar pieniężnych, przewidział ich zakres w zależności od przewinienia, od 1.000 do 200.000 złotych. Wskazano również wyjątki - mianowicie, w przypadku operatora usługi kluczowej niewykonanie obowiązku powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub niezawarcie umowy z podmiotem świadczącym usługi z tego zakresu, zagrożone jest karą w wysokości 100.000 złotych. Najsurowsza kara, w wysokości do 1 mln zł, może zostać nałożona w sytuacji, gdy w wyniku kontroli właściwy organ stwierdzi uporczywe naruszanie przepisów ustawy, które powoduje m.in. bezpośrednie i poważne zagrożenie dla cyberbezpieczeństwa, dla obronności czy zagrożenie wystąpienia poważnej szkody majątkowej. Ze względu na niedawne wejście ustawy w życie, na moment sporządzenia niniejszej publikacji trudno jest oszacować przyszłą praktykę organu odnośnie wysokości kar.

4.5 Podsumowanie

Na koniec warte podkreślenia jest możliwe nachodzenie na siebie zakresów stosowania RODO i Ustawy o cyberbezpieczeństwie. Przykładowo, luka w bezpieczeństwie systemów informatycznych może stanowić naruszenie w rozumieniu Ustawy o cyberbezpieczeństwie, ale także doprowadzić do wycieku danych osobowych, co wiązać będzie się z odpowiedzialnością i sankcjami opisanymi w RODO, nie wspominając o konsekwencjach wizerunkowych dla podmiotu, który doświadczy takiego incydentu. Warto przytoczyć stanowisko brytyjskiego organu nadzorczego w zakresie danych osobowych (ICO), który podkreśla, że istnieje możliwość poniesienia odpowiedzialności na podstawie zarówno RODO, jak i implementowanych przepisów dyrektywy NIS, w odniesieniu do innych aspektów danego naruszenia prawa lub incydentu np. wycieku danych, mimo że są to odrębne akty prawne[5].

[5] The Guide to NIS https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/

5 Geoblokowanie

5.1 Pojęcie i skala zjawiska

Geoblokowanie (blokowanie geograficzne) rozumiane jest jako praktyka sprzedawców internetowych ograniczająca dostęp użytkowników, zarówno konsumentów jak i przedsiębiorców, do treści zawartych na stronach internetowych lub w aplikacjach mobilnych, stanowiąca formę dyskryminacji bezpośredniej lub pośredniej ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności gospodarczej.

W Unii Europejskiej, praktyka ta stosowana była nagminnie przez sklepy internetowe, które ograniczały lub całkowicie blokowały możliwość kupna towarów lub korzystania z usług klientom z innych państw członkowskich. Szacuje się, że w 2015 roku nawet 63% europejskich sklepów internetowych stosowało geoblokowanie, by uniemożliwić klientom z innego kraju nabycie oferowanych przez nie produktów, a zaledwie w przypadku 37% stron internetowych klienci z innego państwa członkowskiego mieli możliwość dojścia do ostatniego etapu poprzedzającego bezpośrednio naciśnięcie przycisku potwierdzającego złożenie zamówienia (https://ec.europa.eu/info/publications/geo-blocking-consumers-online-findings-mystery-shopping-carried-out-european-commission_en).

Przykładowo, ograniczenia wynikające z geoblokowania polegają na:

- zamieszczaniu na stronach internetowych różnych cen towarów lub usług, określonych w zależności od pochodzenia lub miejsca zamieszania lub prowadzenia działalności klienta;
- odmowie dostawy towaru lub usługi na tej samej podstawie;
- stosowania różnych warunków transakcji płatniczych w odniesieniu do klientów z różnych krajów;
- całkowitym zablokowaniu dostępu do danej strony internetowej lub aplikacji mobilnej w przypadku próby uzyskania dostępu na terytorium innego państwa członkowskiego.

Należy jednak pamiętać, że w określonych okolicznościach takie zróżnicowanie w traktowaniu klientów z innych państw UE może być obiektywnie uzasadnione (przykładowo: rozbieżne otoczenie prawne, ryzyka w odniesieniu do przepisów obowiązujących w dziedzinie ochrony konsumentów, środowiska lub etykietowania, kwestii opodatkowania i spraw fiskalnych, kosztów dostawy lub wymogów językowych), jednakże sztuczną segmentację rynku należy oceniać negatywnie i przeciwdziałać takim praktykom. Praktyka stosowania geoblokowania wpływa negatywnie na obrót

wewnątrz Unii Europejskiej, uniemożliwiając lub ograniczając klientom transakcje między państwami członkowskimi, a co za tym idzie, zmniejszając transgraniczny przepływ towarów i usług.

5.2 Rozporządzenie 2018/302 (UE) w sprawie nieuzasadnionego blokowania geograficznego

Wprowadzenie zakazu geoblokowania, jako praktyki niezgodnej ze swobodami rynku wewnętrznego, było od dłuższego czasu przedmiotem zainteresowania instytucji unijnych i stanowi jeden z elementów unijnej strategii w zakresie Jednolitego Rynku Cyfrowego. Praktyka ta uregulowana została ostatecznie w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2018/302 z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności na rynku wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE (dalej jako "Rozporządzenie"), którego przepisy obowiązują we wszystkich państwach członkowskich od dnia 3 grudnia 2018 r.

Głównym celem Rozporządzenia jest poprawienie sytuacji zarówno konsumentów, jak i przedsiębiorców będących klientami sklepów internetowych poprzez zniesienie dyskryminacyjnej praktyki geoblokowania w transgranicznej sprzedaży przez Internet. Należy zaznaczyć, że ochrona nie obejmuje przedsiębiorców, którzy nie dokonują zakupów towarów lub usług na własny użytek, ale nabywają towary lub usługi celem dalszej odsprzedaży lub dystrybucji - czyli w ramach prowadzenia własnej działalności gospodarczej.

W ograniczonym zakresie, Rozporządzenie odnosi się także do usług i towarów oferowanych *offline*, na przykład gdy konsumenci lub przedsiębiorcy są fizycznie obecni w lokalizacji danego sprzedawcy, ale albo uniemożliwia się im dostęp do produktu lub usługi, albo oferuje się im zróżnicowane warunki ze względu na ich przynależność państwową lub miejsce zamieszkania.

Usługi świadczone drogą elektroniczną, które podlegają obowiązkom wynikającym z Rozporządzenia, obejmują na przykład: usługi w chmurze, usługi hurtowni danych, hosting stron internetowych, korzystanie z wyszukiwarek i katalogów internetowych, dostarczanie serwisów www, utrzymywanie na odległość oprogramowania i sprzętu. Natomiast przepisów Rozporządzenia nie stosuje się, między innymi, do sprzedawców oferujący usługi audiowizualne, w tym usług, których zasadniczym celem jest zapewnianie dostępu do transmisji wydarzeń sportowych i które są świadczone na podstawie wyłącznych licencji terytorialnych. Inne usługi świadczone drogą elektroniczną, niebędące usługami audiowizualnymi, których główną cechą jest zapewnienie dostępu do utworów chronionych prawem autorskim (na przykład dostęp do e-booków, oprogramowania komputerowego lub transmisji strumieniowej muzyki lub korzystanie z internetowych gier wideo), podlegają przepisom Rozporządzenia z wyjątkiem zakazu stosowania zróżnicowanych warunków dostępu ze względu na

przynależność państwową, miejsce zamieszkania i miejsce prowadzenia działalności (szerzej w pkt 5.3.2 poniżej).

Należy podkreślić, że Rozporządzenie nie ma zastosowania w sytuacjach czysto wewnętrznych, to znaczy wtedy, gdy wszystkie istotne elementy transakcji następują na terytorium jednego państwa członkowskiego.

5.3 Zakaz geoblokowania

Rozporządzenie wprowadza następujące zakazy w zakresie geoblokowania, których celem jest zapobieganie tego typu praktykom w konkretnych sytuacjach, tj. gdy brak jest obiektywnego uzasadnienia dla zróżnicowanego traktowania ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności:

5.3.1 Zakaz blokowania lub ograniczania przez sprzedawców dostępu do interfejsów internetowych

Pierwszy z zakazów ma na celu zapewnienie swobodnego dostępu klientów do stron internetowych oferujących usługi oraz towary. Artykuł 3 Rozporządzenia zabrania sprzedawcom internetowym używania środków technicznych w celu blokowania lub ograniczania dostępu klienta do ich interfejsów internetowych ze względu na pochodzenie, miejsce zamieszkania lub miejsce prowadzenia działalności tego klienta.

Rozwiązania technologiczne ograniczające taki dostęp mogą obejmować w szczególności technologie wykorzystywane do określenia fizycznej lokalizacji klienta, w tym do jej monitorowania za pomocą adresu IP lub współrzędnych uzyskanych za pośrednictwem globalnego systemu nawigacji satelitarnej.

Zabronione jest także przekierowywanie użytkownika ze strony internetowej, do której starał się pierwotnie uzyskać dostęp, na stronę dostosowaną do niego ze względu na jego przynależność państwową lub obecną lokalizację, o ile nie wyraził na to wyraźnej zgody. Co więcej, nawet jeżeli użytkownik udzieli zgody na przekierowywanie, wersja oryginalna strony, którą zamierzał odwiedzić, powinna być dla niego nadal dostępna.

Powyższe zakazy nie będą mieć zastosowania w określonych okolicznościach - na przykład gdy przepis prawa konkretnego państwa członkowskiego zakazuje wyświetlania konkretnych treści lub sprzedaży konkretnych towarów i usług. W takim wypadku przedsiębiorca odmawiający sprzedaży towaru lub usługi będzie zobligowany do wyjaśnienia klientowi powodów zastosowania ograniczeń.

5.3.2 Zakaz nieuzasadnionego różnicowania ogólnych warunków dostępu do towarów lub usług

Kolejny zakaz dotyczy ograniczeń w dostępie do towarów lub usług. Zgodnie z artykułem 4 Rozporządzenia zabrania się przedsiębiorcom nieuzasadnionego różnicowania warunków dostępu do towarów lub usług w zależności od przynależności państwowej, miejsca zamieszkania lub miejsca prowadzenia działalności klienta. Takie sytuacje obejmują:

- sprzedaż towarów bez dostawy poza terytorium obsługiwane przez konkretnego sprzedawcę internetowego (przykładowo gdy klient kupuje towar, którego sprzedawca nie dostarcza do państwa członkowskiego klienta, taki klient powinien mieć możliwość otrzymania towaru w państwie członkowskim, do którego jest możliwość dostawy, na takich samych warunkach co klienci lokalni);

- sprzedaż usług świadczonych drogą elektroniczną (przykładowo: klient z innego państwa członkowskiego niż usługodawca, który chce uzyskać dostęp do usług świadczonych drogą elektroniczną, ma prawo uzyskać dostęp do takich usług na takich samych zasadach co klienci lokalni);

- sprzedaż usług świadczonych w określonej fizycznej lokalizacji, w której konkretny przedsiębiorca prowadzi działalność (przykładowo klient, który kupuje towar w sklepie znajdującym się w innym państwie członkowskim niż państwo członkowskie klienta ma prawo do traktowania w taki sam sposób, jak obywatele/rezydenci kraju handlowca)

Powyższe przypadki nie dotyczą sytuacji, w których ogólne warunki dostępu (w tym cen sprzedaży netto) oferowane przez sprzedawców internetowych różnią się w poszczególnych państwach członkowskich i kierowane są do określonych grup klientów w sposób niedyskryminujący. Przedsiębiorcy nie są również zobowiązani do dostarczania towarów do innego państwa członkowskiego, o ile nie oferują tego w ogólnych warunkach dostępu lub przepisy prawa uniemożliwiają sprzedaż konkretnych towarów lub świadczenie określonych usług.

5.3.3 Zakaz dyskryminacji w odniesieniu do płatności

Ostatni z zakazów odnosi się do niedyskryminowania w zakresie środków płatniczych, jakie akceptują sprzedawcy internetowi. Zgodnie z artykułem 5 Rozporządzenia, zakazane jest różnicowanie warunków w odniesieniu do transakcji płatniczej ze względu na przynależność państwową klienta, miejsce zamieszkania, miejsce prowadzenia działalności, lokalizację rachunku płatniczego, miejsce prowadzenia działalności dostawcy usług płatniczych lub miejsce wydania instrumentu płatniczego w UE. Muszą zostać spełnione jednak pewne warunki dotyczące samej transakcji, tzn. transakcja płatnicza musi być transakcją elektroniczną w postaci polecenia przelewu, polecenia zapłaty lub instrumentu płatniczego opartego na karcie, musi być należycie uwierzytelniona i nastąpić w walucie akceptowanej przez konkretnego sprzedawcę.

5.4 Stosowanie Rozporządzenia w Polsce i jego praktyczne konsekwencje

Zgodnie z prawem unijnym, przepisy Rozporządzenia są bezpośrednio stosowane w krajach UE, w związku z czym obywatel RP ma możliwość powołania się bezpośrednio na jego przepisy w razie napotkania przypadku nieuzasadnionego geoblokowania. Organem właściwym w sprawie egzekwowania przepisów Rozporządzenia (zgodnie z obecną wersją projektu ustawy o zmianie ustawy o ochronie konkurencji i konsumentów oraz niektórych innych ustaw) ma być Prezes Urzędu Ochrony Konkurencji i Konsumentów i to do niego klienci sklepów internetowych dotknięci nieuzasadnionymi praktykami geoblokowania będą mieli możliwość wnoszenia odpowiednich zawiadomień. Prezes Urzędu Ochrony Konkurencji i Konsumentów będzie interweniował, gdy zastosowana przez sprzedawcę internetowego praktyka stanowiąca geoblokowanie naruszy zbiorowe interesy konsumentów lub zostanie zakwalifikowana jako praktyka ograniczającą konkurencję. W związku z tym, przeciwko przedsiębiorcy, który naruszy zakaz blokowania geograficznego Prezes Urzędu Konkurencji i Konsumentów będzie mógł wydać decyzję nakazującą zaniechania bezprawnej praktyki, nakładającą obowiązek usunięcia jej skutków lub karę pieniężną do 10 proc. obrotu. W relacjach między przedsiębiorcami, naruszenie zakazu geoblokowania może narazić sprzedawcę internetowego na odpowiedzialność odszkodowawczą.

Wejście w życie przepisów wprowadzających zakaz geoblokowania oznacza dla sprzedawców internetowych konieczność weryfikacji czy funkcjonalności stosowanych przez nich stron internetowych lub aplikacji mobilnych spełniają wymogi Rozporządzenia. Weryfikacji wymagają również informacje kierowane do klientów, zamieszczane na stronach internetowych lub w aplikacjach, w szczególności regulaminy sklepów internetowych. Szczególną uwagę należy zwrócić na wszelkie blokady stron internetowych oraz automatyczne przekierowania klientów na inne wersje stron internetowych, bez uprzedniej zgody klienta i bez możliwości dostępu do wersji stron dedykowanych dla klientów innych państw członkowskich.

6 Marketing elektroniczny - kolizja trzech zgód

Prowadzenie działań marketingowych w Internecie może, w niektórych postaciach, wymagać wcześniejszego uzyskania od klientów zgody. Jednakże w przypadku Polski, taka zgoda jest wymagana, de facto na podstawie trzech różnych regulacji - prawa ochrony danych osobowych, prawa telekomunikacyjnego oraz przepisów dotyczących świadczenia usług drogą elektroniczną.

6.1 Przepisy prawa dotyczące prowadzenia marketingu elektronicznego:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 lub „RODO") (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.);

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2017 r. poz. 1219 z późn. zm.);

- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 nr 171 poz. 1800 ze zm.);

6.2 Marketing bezpośredni na gruncie RODO

Na podstawie przepisów RODO (ogólnego rozporządzenia o ochronie danych osobowych) przetwarzanie danych osobowych w celach prowadzenia marketingu bezpośredniego wymaga zidentyfikowania podstawy prawnej takiego przetwarzania - w postaci zgody podmiotu, którego dane dotyczą lub oparcia przetwarzania na przesłance prawnie uzasadnionego interesu administratora danych[6]. Zgoda będzie właściwą podstawą przetwarzania danych osobowych w przypadku, gdy dany podmiot (administrator danych) kieruje komunikację marketingową do swoich potencjalnych klientów lub, przesyłając materiały marketingowe, informuje również o produktach lub usługach innych podmiotów (np. o produktach lub usługach swoich partnerów biznesowych). Natomiast, prawnie uzasadniony interes administratora danych będzie właściwą podstawą przetwarzania danych osobowych w przypadku prowadzenia marketingu własnych towarów i usług kierowanych do aktualnych klientów.

Należy jednak pamiętać, że ograniczeniem dla przetwarzania danych osobowych na podstawie przesłanki prawnie uzasadnionego interesu administratora są interesy lub podstawowe prawa i

[6] Administrator danych to podmiot, który samodzielnie lub wspólnie z innymi podmiotami decyduje o celach i sposobach przetwarzania danych zgodnie z art. 4 pkt 7 RODO (np. administrator strony internetowej czy agencja marketingowa kierująca korespondencje zawierającą informacje marketingowe do swoich klientów)

wolności osób, których dane dotyczą. Administrator musi samodzielnie ocenić czy przetwarzanie oparte na jego prawnie uzasadnionym interesie będzie proporcjonalne w konkretnej sytuacji oraz czy nie naruszy interesów osób, które dane dotyczą, a osoba, do której kierowana jest komunikacja marketingowa, może się obiektywnie spodziewać takiej komunikacji.

Zgoda na marketing bezpośredni, zebrana zgodnie z wymogami RODO, musi spełnić określone kryteria - musi stanowić dobrowolne (w znaczeniu realnego i swobodnego wyboru), konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania, zezwala na przetwarzanie konkretnych danych osobowych w konkretnym celu. Niedopuszczalne jest zbieranie zgód blankietowych (ogólnych); należy również wyraźnie oddzielić informacje związane z uzyskaniem zgody od informacji dotyczących innych kwestii. Podmiot danych musi zostać również powiadomiony o prawie wycofania zgody w dowolnym momencie, a forma wycofania takiej zgody powinna być równie łatwa co sposób jej wyrażenia.

Brak prawidłowo pozyskanej zgody w sytuacji, w której nie istnieje żadna inna podstawa prawna do przetwarzania danych osobowych, oprócz odpowiedzialności cywilnej i karnej, zagrożony jest karą pieniężną, nakładaną w trybie administracyjnym przez Prezesa Urzędu Ochrony Danych Osobowych, w maksymalnej wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

6.3 Ustawa o świadczeniu usług drogą elektroniczną

Ustawa o świadczeniu usług drogą elektroniczną nakłada na podmioty prowadzące marketing elektroniczny obowiązek uzyskania zgody na przesyłanie informacji handlowej skierowanej do oznaczonego odbiorcy, będącego osobą fizyczną, za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Do środków komunikacji elektronicznej, obok wiadomości mailowych, zaliczamy wiadomości SMS i MMS. Niezamówioną informacją handlową mogą być również wiadomości przesyłane na konta użytkowników w portalach społecznościowych pod warunkiem, że taki portal społecznościowy służy komunikowaniu się za pomocą środków elektronicznych. Rozpowszechnianie niezamówionej informacji handlowej za pomocą środków komunikacji elektronicznej nazywany jest powszechnie *spammingiem*, a sama niezamówiona informacja handlowa – spamem. Zawartość spamu stanowią najczęściej reklamy, które mają zachęcić do zakupu towarów lub usług oferowanych przez nadawcę. Aby informację handlową uznać za zamówioną, potrzebna jest zgoda adresata na jej otrzymanie, a sposobem jej wyrażenia może być również udostępnienie w tym celu identyfikującego odbiorcę adresu mailowego.[7] Taka zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści oraz może być odwołana

[7] Art. 10 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

w każdym czasie.[8] Na gruncie ustawy o świadczeniu usług drogą elektroniczną, wymagana jest więc zgoda w modelu *opt-in. Z*goda ta powinna być wyraźna i udzielona przed otrzymaniem właściwej wiadomości reklamowej. Przykładowo, użytkownik może potwierdzić swoją chęć otrzymywania wiadomości, uprzednio aktywując link przesłany w wiadomości mailowej. System *opt-in* funkcjonuje w Polsce i zapewnia adresatom szerszą ochronę prywatności, a przedsiębiorcom ogranicza możliwości wysyłania niezamówionych informacji handlowych. Warto również podkreślić, że nie można uzależnić zawarcia umowy z użytkownikiem od wyrażenia przez konsumenta zgody na otrzymywanie informacji handlowych drogą elektroniczną.[9]

Brak prawidłowo pozyskanej zgody w sytuacji, w której doszło do wysłania niezamówionej informacji handlowej, może prowadzić do odpowiedzialności skutkującej nałożeniem grzywny w wysokości do 5.000 zł. Jednakże działanie takie może być również zakwalifikowane jako czyn nieuczciwej konkurencji, co może skutkować odpowiedzialnością wynikającą z ustawy o zwalczaniu nieuczciwej konkurencji, czyli nałożeniem przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów kary administracyjnej w wysokości do 10% obrotu osiągniętego w roku obrotowym poprzedzającym rok nałożenia kary.

6.4 Prawo telekomunikacyjne

Na podstawie ustawy prawo telekomunikacyjne, zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących (bez ludzkiej ingerencji, o masowym charakterze) dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę.[10] Do takich urządzeń i systemów zalicza się urządzenia automatycznie wytwarzające i wysyłające komunikaty głosowe, telefaksy, pocztę elektroniczną, wiadomości SMS i MMS, komunikaty internetowe, a także rozmowy telefoniczne. Prawo telekomunikacyjne wyznacza podobne standardy w zakresie wymogów zgody - nie może być ona domniemana lub dorozumiana z oświadczenia woli o innej treści; może być wyrażona drogą elektroniczną, pod warunkiem jej utrwalenia i potwierdzenia przez użytkownika; a abonent lub użytkownik końcowy musi mieć zapewnioną możliwość wycofania zgody w każdym czasie, w sposób prosty i wolny od opłat.[11] Zgoda powinna być wyrażona w modelu *opt-in* (odbiorca musi wyrazić zgodę przed przesłaniem przekazu na niezamówione komunikaty). Umieszczenie na stronie internetowej jednostki organizacyjnej adresu elektronicznego (np. adresu poczty elektronicznej) nie oznacza wyrażenia zgody na przesyłanie przekazów marketingowych z wykorzystaniem automatycznych systemów wywołujących lub telekomunikacyjnych urządzeń końcowych.

---

[8] Art. 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną

[9] wyr. SA w Warszawie z 15.2.2017 r., VI ACa 560/16, Legalis

[10] Art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

[11] Art. 174 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

Brak prawidłowo pozyskanej zgody na podstawie przepisów prawa telekomunikacyjnego może skutkować nałożeniem w drodze decyzji administracyjnej przez Prezesa Urzędu Komunikacji Elektronicznej kary w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Niezależnie od kar pieniężnych, Prezes Urzędu Komunikacji Elektronicznej może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.

6.5 Kolizja zgód

Wątpliwości interpretacyjne budzi relacja zgód z wymienionych powyżej przepisów. W szczególności relacja zgody wymaganej na gruncie prawa telekomunikacyjnego oraz ustawy o świadczeniu usług drogą elektroniczną z uwagi na fakt, że zakresy tych zgód częściowo się pokrywają. Należy zauważyć, że zgoda na gruncie ustawy o świadczeniu usług drogą elektroniczną wymagana jest jedynie w relacjach z osobami fizycznymi (konsumentami), natomiast zgoda z prawa telekomunikacyjnego obejmuje również relacje profesjonalne (między przedsiębiorcami). W związku z powyższym, wątpliwości dotyczą okoliczności czy za każdym razem, dla celów prowadzenia marketingu elektronicznego, konieczne jest zebranie trzech odrębnych zgód (w przypadku, gdy nie opieramy się na przesłane prawnie uzasadnionego interesu administratora na podstawie RODO), które muszą być pozyskane odrębnie, i niezalenie od siebie, czy też możliwe jest ich połączenie, ponieważ zakresowo istnieją między nimi relacje powiązane.

Utrwalona w Polsce linia orzeczniczej sądów administracyjnych, jak również stanowisko Generalnego Inspektora Ochrony Danych (obecnie Prezesa Urzędu Ochrony Danych)[12], wskazuje, że zasadą powinno być odrębne zbieranie zgód na przetwarzanie danych osobowych w celu marketingu bezpośredniego oraz zgód na otrzymywanie informacji handlowej na podstawie ustawy o świadczeniu usług drogą elektroniczną. Większe wątpliwości interpretacyjne budzi zestawienie zgody z ustawy o świadczeniu usług drogą elektroniczną ze zgodą na gruncie prawa telekomunikacyjnego. Również, stanowisko Prezesa Urzędu Komunikacji Elektronicznej[13] nie jest jednoznaczne w tym zakresie, wskazuje on bowiem, że mimo że zgoda z prawa telekomunikacyjnego musi być wyodrębniona z innych oświadczeń, w przypadku tego samego kanału przekazu powinna wystarczyć jedna zgoda.

6.6 Planowane zmiany w przepisach

[12] Stanowisko zamieszczone na stronie Generalnego Inspektora Ochrony Danych Osobowych (obecnie: Prezesa Urzędu Ochrony Danych Osobowych): https://giodo.gov.pl/pl/259/10003

[13] Pismo z dnia 21 października 2015 r., znak: DP.034.32.2015.L. http://www.sabi.org.pl/attachments/File/do_pobrania/UKE-2015/odpowiedz-UKE-21-10-2015.pdf

Zgodnie z projektem ustawy zmieniającej przepisy sektorowe w związku z RODO (projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679[14]), do uzyskania zgody na podstawie ustawy o świadczeniu usług drogą elektroniczną oraz zgody abonenta lub użytkownika końcowego na podstawie prawa telekomunikacyjnego mają mieć zastosowanie przepisy o ochronie danych osobowych. Oznacza to, że wymogi RODO w zakresie uzyskania zgody na przetwarzanie danych osobowych - tj. przesłanki jej uzyskania, charakter zgody, zakres, okoliczności jej udzielenia, a także zasady dokonywania oceny skuteczności oświadczenia - będą dotyczyły także pozyskiwania zgód na marketing elektroniczny. Należy podkreślić, że obecnie takie zgody nie mogą być domniemane lub dorozumiane z oświadczenia woli o innej treści, jednak RODO wprost wskazuje, że zgoda może być udzielona również w formie wyraźnego działania potwierdzającego.

6.7 Podsumowanie

W obecnym stanie prawnym, przedsiębiorca który zamierza prowadzić marketing elektroniczny musi uzyskać osobną zgodę klienta na podstawie wskazanych powyżej trzech regulacji. W praktyce można jednak zaobserwować, że niektóre podmioty łączą te zgody, co wiąże się z ryzykiem zakwestionowania prawidłowości takiego postępowania na gruncie obecnych przepisów, lub różnicują je, wskazując jedynie formę kontaktu bez powoływania się na konkretne przepisy. Nie ulega wątpliwości, że przypadku wykorzystywania do marketingu różnych kanałów komunikacji, zgoda powinna być wyodrębniona w stosunku do każdego z tych kanałów. Najprawdopodobniej przedsiębiorcy będą musieli (ponownie) zaktualizować wszelkie uzyskane dotychczas zgody, mimo że już w związku z wejściem w życie RODO większość z nich musiała przeprojektować strategię marketingową oraz dostosować się do nowych wymogów.

[14] http://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=3050