Analiza zjawiska spamu – środki prawne ochrony przed spamem

Geneza i definicja

Etymologia pojęcia „spam" nie jest do końca znana. Przyjmuje się, że jego źródeł należy upatrywać w skeczu grupy Monthy Pythona, związanym z produktem mięsnym o skrótowej nazwie SPAM [red. Magdalena Marciniak-Piotrowska, *Analiza rynku spamu w Polsce dla Urzędu Komunikacji Elektronicznej (UKE)*, Warszawa 2014, s. 7-8.]. W latach 80. XX wieku terminem tym posługiwano się na określenie uciążliwych, długich tekstów zamieszczanych na forach dyskusyjnych, w komunikatorach społecznościowych czy w fabularnych grach komputerowych. Ostatecznie słownik New Oxford Dictionary of English w 1998 roku obok pierwszego znaczenia terminu „spam" dotyczącego wyrobu mięsnego (konserwa mięsna) opublikował drugie znaczenie jako „nieistotne lub nieodpowiednie wiadomości wysłane przez Internet do wielu grup dyskusyjnych lub użytkowników".

Współcześnie istnieje wiele definicji spamu, wśród których większość ma charakter potoczny, obiegowy zaś tylko niektóre mają cechy definicji legalnej. Pojęcie „spam" przyjęło się, zarówno w języku prawnym, jak i języku potocznym, na określenie wielokrotnie wysyłanej niechcianej korespondencji, przeważnie w celu marketingu produktów i usług o komercyjnym przeznaczeniu [https://uokik.gov.pl/konsument_w_sieci.php#faq962]. Według definicji wykorzystywanej przez portal społecznościowy Facebook, spam oznacza kontaktowanie się z innymi w celu przekazania im niechcianych treści lub próśb - obejmuje to masowe wysyłanie wiadomości, nadmiernie częste publikowanie linków lub obrazów na osiach czasu innych osób i wysyłanie zaproszeń do grona znajomych osobom, których nie zna się osobiście [https://www.facebook.com/help/217854714899185/]. Inna spotykana definicja spamu to np.: niezamówiona informacja handlowa skierowana do oznaczonego odbiorcy, będącego osobą fizyczną, za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej [art. 10 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną].

Amerykańska organizacja pozarządowa Mail Abuse Prevention System wskazuje, że pod pojęciem „spam" rozumieć należy informację (której treść i kontekst są niezależne od

tożsamości odbiorcy) przesłaną drogą elektroniczną odbiorcy, który nie wyraził uprzedniej zgody na jej otrzymanie (zgoda taka musi być wyraźna, możliwa do weryfikacji, zamierzona i zawsze odwołalna) zaś z okoliczności wynika, że wysyłający odniesie większe korzyści z faktu wysłania wiadomości w stosunku do korzyści, jakie odniesie odbiorca w związku z jej odbiorem. Spamem będzie zatem niechciana korespondencja pojawiająca się w szczególności na platformach komunikacyjnych takich jak telefon komórkowy, poczta elektroniczna, czat, strony www, portale społecznościowe typu Facebook.

W tym kontekście warto zwrócić uwagę, iż obecnie korespondencja zaliczana do spamu coraz częściej staje się narzędziem posiłkowym do działań kryminalnych w Internecie, głównie próby wyłudzeń informacji finansowych (np. hasła dostępu, numery kont bankowych), czy wysyłanie zainfekowanych wiadomości podszywając się pod zaufanych nadawców. Skala problemu urosła jednak do takiego poziomu, że w wielu krajach ustawodawcy podjęli próby stworzenie tzw. prawa anty–spamowego, przy czym warto podkreślić, iż na arenie międzynarodowej istnieje konsensus w tej kwestii tj. spam jako problem transgraniczny nie może być skutecznie zwalczany wyłącznie przy wykorzystywaniu narodowych mechanizmów prawnych co implikuje konieczność ścisłej koordynacji międzynarodowej oraz współpraca.

Regulacje ustrojowe

Problematykę prawną spamu należy rozpocząć od analizy konstytucyjnie chronionych wartości. Na gruncie ustawy zasadniczej dochodzi bowiem do pewnego rodzaju kolizji prawa do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (art. 47 Konstytucji) w opozycji, do którego można postawić wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji (art. 54 Konstytucji). W tym aspekcie szczególnego znaczenia nabiera norma konstytucyjna, zgodnie z którą władze publiczne chronią konsumentów, użytkowników i najemców przed działaniami zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu oraz przed nieuczciwymi praktykami rynkowymi. Zakres tej ochrony określa ustawa. (art. 76 Konstytucji) W sytuacji, kiedy dochodzi do kolizji dwóch dóbr, wybór tego, któremu należy przypisać wyższą wartość powinien oparty być przede wszystkim na rachunku zysków i strat [Piotr Waglowski, *Spam a prawo – próba wskazania kierunków badawczych*, Warszawa 2003, s. 3.]. Wydaje się, że dobrem szczególnie chronionym powinna być prywatność, w tym

przede wszystkim prywatność osób fizycznych (usługobiorców), co stanowi legitymizację do podejmowania działań mających na celu ochronę przed spamem.

Regulacje ustawowe

Definicje ujęte w przepisach prawa europejskiego oraz prawa polskiego ograniczają pojęcie spamu do niezamówionych informacji handlowych skierowanych do oznaczonego odbiorcy poprzez środki komunikacji elektronicznej, w szczególności pocztę elektroniczną.

Podstawowe znaczenie w zakresie ochrony przed niechcianą korespondencją elektroniczną mają przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Określa ona w szczególności obowiązki usługodawców w związku ze świadczeniem usług drogą elektroniczną, m.in. zasady ochrony danych osobowych osób fizycznych korzystających z usług świadczonych drogą elektroniczną oraz zasady wyłączania odpowiedzialności usługodawcy. Zgodnie z definicją przyjętą w art. 2 pkt 2 ustawy określenie „informacja handlowa oznacza każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi". Z kolei zgodnie z art. 10 ust 1 ustawy „zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej" a za złamanie tego zakazu ustawodawca przewidział karę grzywny (art. 24 ust. 1 ustawy). Przesyłanie niezamówionych informacji handlowych stanowiące wykroczenie, ścigane jest na wniosek osoby pokrzywdzonego, jednakże zgodnie z Kodeksem wykroczeń wykazać należ, że społeczna szkodliwość działania podmiotu jest większa niż znikoma. W przeciwnym wypadku następuje wyłączenie karalności czynu.

Ustawodawca w przedmiotowej regulacji idzie dalej, wskazując nad to, że przesyłanie niezamówionej informacji handlowej stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji ((art. 10 ust. 3 ustawy o świadczeniu usług drogą elektroniczną), który może

stanowić praktykę naruszającą zbiorowe interesy konsumentów. Warto wskazać, że w sytuacji naruszenia zbiorowych interesów konsumentów przez przedsiębiorców, stosujących bezprawne praktyki, Prezes Urzędu Ochrony Konkurencji i Konsumentów może wydać decyzję o uznaniu praktyki za naruszającą zbiorowe interesy konsumentów i nakazującą przedsiębiorcy zaniechanie stosowania owej praktyki oraz obowiązać do usunięcia jej skutków lub nałożyć na przedsiębiorcę, w drodze decyzji, karę pieniężną w wysokości nie większej niż 10% obrotu osiągniętego w roku obrotowym poprzedzającym rok nałożenia kary, jeżeli przedsiębiorca ten, choćby nieumyślnie naruszył zbiorowy interes konsumentów [art. 26-28 ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym].

Problematyka spamu została przez ustawodawcę ujęta także w innych aktach normatywnych. Tytułem przykładu można wskazać art. 172 ust. 1 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, gdzie za zakazane uważa się używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę. Z powyższego wynika, iż jakiekolwiek działania (za pośrednictwem komputera, telefonu, urządzeń mobilnych itd.), podejmowane do celów marketingu bezpośredniego, mimo nie uzyskania uprzedniej zgody osoby, do której są adresowane, są niezgodne z prawem – w konsekwencji telefony z call-center czy przesyłanie spamu drogą elektroniczną (o ile użytkownik nie wyraził wcześniej na to zgody), należy traktować jako działaniem sprzecznym z prawem [red. Magdalena Marciniak-Piotrowska, *Analiza rynku spamu w Polsce dla Urzędu Komunikacji Elektronicznej (UKE)*, Warszawa 2014, s. 30-33.]. A zatem stosownie do treści art. 209 ust 1 pkt 25 i art. 210 ustawy prawo telekomunikacyjne za nie wypełnienie obowiązku uzyskania zgody abonenta lub użytkownika końcowego, przedsiębiorcy grozi kara pieniężna nakładana przez Prezes Urzędu Komunikacji Elektronicznej, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym.

Cywilnoprawną regulację „anty-spamową" znajdziemy w ustawie z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym, w myśl której nieuczciwymi praktykami rynkowymi w każdych okolicznościach są uciążliwe i niewywołane działaniem albo zaniechaniem konsumenta nakłanianie do nabycia produktów przez telefon, faks, pocztę elektroniczną lub inne środki porozumiewania się na odległość, z wyjątkiem przypadków

egzekwowania zobowiązań umownych, w zakresie dozwolonym przez obowiązujące przepisy (art.9 pkt 3). W razie dokonania nieuczciwej praktyki rynkowej konsument, którego interes został zagrożony lub naruszony, może żądać m.in. zaniechania tej praktyki, czy usunięcia jej skutków (art. 12 ust. 1 ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym).

Innym cywilnoprawnych środków ochrony przed niezamówioną informacją handlową jest regulacja Kodeksu cywilnego w zakresie ochrony dóbr osobistych (prawo do prywatności). Nie sposób nie zgodzić się, iż przesyłanie np. drogą elektroniczną niezamówionych informacji handlowych bez uprzedniej zgody na ich otrzymanie stanowi naruszenie prawa do prywatności. Zgodnie z art. 24 § 1 k.c. „ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności, ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny."

Wysyłanie informacji handlowych wiąże się z przetwarzaniem danych osobowych. W tym względzie istotnej ochrony przed spamem należy upatrywać również w przepisach Rozporządzenia 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 (dalej RODO).

Zgodnie z art. 6 ust. 1 pkt. f RODO przetwarzanie jest zgodne z prawem, jeśli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Przepisy nie wymieniają wprost marketingu bezpośredniego jako usprawiedliwionego interesu. Jednak motyw 47 preambuły RODO wskazuje, że *Za działanie wykonywane w prawnie uzasadnionym interesie* ***można uznać*** *przetwarzanie danych osobowych do celów marketingu bezpośredniego.* **Użyte sformułowanie *można uznać* nie oznacza, że marketing zawsze będzie uzasadnionym celem.**

Jeżeli dany podmiot nie pozyskał danych osobowych konsumenta bezpośrednio od niego, to jako podmiot przetwarzający dane musi spełnić obowiązek informacyjny z art. 14 RODO. Przedsiębiorca musi przekazać skąd posiada dane konsumenta oraz przekazać szereg

innych informacji (np. czas, przez jaki dane będą przechowywane). Dodatkowo w zależności od podstawy przetwarzania danych, przedsiębiorca powinien wskazać na prawo do cofnięcia zgody (art. 13 ust. 2 lit. c i art. 7 ust. 3 RODO) lub prawo do złożenia sprzeciwu (art. 13 ust. 2 lit. b i art. 21 ust. 1 RODO).

Jeśli konsument uzna, że jego dane przetwarzane są z naruszeniem prawa, może złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych. Potwierdzenie naruszenie może skutkować nałożeniem kary administracyjnej w wysokości do nawet 10 mln euro [*https://uodo.gov.pl/pl/138/1244*].

Podsumowanie

W świeci zdominowanym przez komunikację elektroniczną kwestie związane z przesyłaniem niezamówionych informacji stają się codziennością. Co było już poruszane, materia ta jest niezmiernie istotna, gdyż spam godzi w konstytucyjne prawo do prywatności. Mimo starań ustawodawcy, zmierzających w kolejnych regulacjach normatywnych do zapewnienia jak największej ochrony przed spamem problem pozostaje nierozwiązany. Wydaje się jednak, że owa nieefektywność nie leży w prawnych środkach ochrony, które należy ocenić pozytywnie, a w braku właściwych mechanizmów pozwalających na wyszukiwaniu tzw. spamerów celem pociągnięcia ich do odpowiedzialności cywilnoprawnej, publicznoprawnej i karnoprawnej.

Warto zatem stworzyć skuteczny system umożliwiający identyfikację podmiotów, które przesyłają niezamówione informacji, co powinno przyczynić się do zmniejszenia szeroko rozumianego zjawiska „spamu". Oczywiście w dobie globalizmu skutecznie zwalczany spamu jak już podkreślano jedynie przy wykorzystywaniu krajowych mechanizmów prawnych jest nierealne co powinno skłaniać państwa do podęcia jeszcze ściślejszej współpracy międzynarodowej.

Zalążkiem takiej współpracy może być np. Zespół CERT Polska, który działa w strukturach NASK (Naukowej i Akademickiej Sieci Komputerowej) – instytutu badawczego prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w Polsce zespół reagowania na incydenty. Dzięki działalności od 1996 roku w środowisku zespołów reagujących, stał się rozpoznawalnym i doświadczonym podmiotem w dziedzinie bezpieczeństwa komputerowego. Od początku istnienia zespołu rdzeniem działalności jest

obsługa incydentów bezpieczeństwa i współpraca z podobnymi jednostkami na całym świecie, zarówno w działalności operacyjnej, jak i badawczo-wdrożeniowej. Od 1998 roku CERT Polska jest członkiem międzynarodowego forum zrzeszającego zespoły reagujące – FIRST, a od roku 2000 należy do grupy roboczej europejskich zespołów reagujących – TERENA TF-CSIRT i działającej przy niej organizacji Trusted Introducer [*https://www.cert.pl/o-nas/*].

Hubert Plichta