

Warszawa, dnia 7 czerwca 2010
PIIT/583/2010

Pani Magdalena Gaj
Podsekretarz Stanu

Ministerstwo Infrastruktury
ul. Chałubińskiego 4/6
00-928 Warszawa

Szanowna Pani Minister,

W imieniu Polskiej Izby Informatyki i Telekomunikacji przedstawiam rezultaty prac członków PIIT w zakresie **Grupy Roboczej ds. bezpieczeństwa, integralności sieci i spamu**.

Osoby akredytowane przez PIIT do Grupy Roboczej przeprowadziły obszerną wewnętrzną dyskusję, w wyniku której powstał dokument przedstawiający wady obecnego projektu przepisów antyspamowych (**memorandum w załączeniu**).

Równolegle do prac nad memorandum traktującego o dotychczasowej propozycji przepisów antyspamowych, powstaje dokument z konkretnymi propozycjami przepisów antyspamowych, który w zamierzeniu ma zawierać przepisy wolne od wad dostrzeżonych przez PIIT. Ponieważ redagowanie przepisów w zakresie tejże niezwykle złożonej materii jest zadaniem trudnym, PIIT skończy prace nad przedmiotowym dokumentem najprawdopodobniej w drugiej połowie czerwca 2010 r.

Z kolei w przedmiocie bezpieczeństwa i integralności sieci, PIIT prowadzi prace nad ustaleniem efektywnego modelu regulacji pozwalającej na utrzymanie przez przedsiębiorców telekomunikacyjnych bezpieczeństwa i integralności sieci przy zachowaniu praw i ochrony użytkowników końcowych. Zagadnienie to zostanie przedstawione wspólnie z dokumentem opisującym temat regulacji anty-spamowych.

Z poważaniem

Dr inż. Wacław Iszkowski

Prezes PIIT

Załączniki:
- memorandum w sprawie obecnego projektu przepisów antyspamowych

Memorandum w sprawie obecnego projektu przepisów antyspamowych umieszczonych w projekcie przedstawionym w maju 2010

Zasadność wprowadzenia mechanizmów prawnych umożliwiających skuteczną walkę ze spamem jest oczywista, jednak na etapie legislacji tak skomplikowanej materii należy dołożyć szczególnych starań, aby zapisy były jak najbardziej klarowne i jasno precyzowały uprawnienia i obowiązki operatorów/ dostawców usług, jak również prawa użytkowników końcowych. Regulacja tego zagadnienia powinna również wyważyć koszty ponoszone przez operatorów w stosunku do uzyskiwanych potencjalnych korzyści.

Obecny projekt stanowi znakomity materiał wyjściowy dla merytorycznych dyskusji nad kształtem norm prawnych opisujących efektywnego modelu regulacji występujących w sieci telekomunikacyjnej nadużyć.

Punktem wyjścia dla prowadzonej dyskusji w ramach grupy roboczej jest zdefiniowane możliwych nadużyć występujących w sieci telekomunikacyjnej. Na tym etapie dyskusji identyfikujemy następujące nadużycia:

1. **spam** – czyli przesyłanie niezamówionych przez użytkownika komunikatów, które mają na celu uzyskanie korzyści ekonomicznej przez podmiot wysyłający (choć nie zawsze korzyść ekonomiczna jest identyfikowana);
2. wysyłanie przez zainfekowany komputer użytkownika wiadomości/komunikatów, w celu uniemożliwienia normalnego funkcjonowania sieci telekomunikacyjnej - **botnet**.
3. **pozostałe nadużycia**¹, m.in.:
 - o obraźliwa i nielegalna treść;
 - o złośliwe oprogramowanie (wirusy, robaki sieciowe, konie trojańskie, dialery itp.);
 - o gromadzenie informacji (skanowanie, podsłuchy, inżyniera społeczna);
 - o próby włamania (wykorzystanie luk systemowych, próby nieuprawnionego logowania);
 - o włamania (włamania na konto, do aplikacji);
 - o atak na dostępność zasobów (atak blokujący serwis (Dos), rozproszony atak blokujący serwis (DDoS), sabotaż komputerowy);
 - o atak na bezpieczeństwo informacji (nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji);
 - o oszustwa komputerowe (nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, kradzież tożsamości, podszycie się).

¹ Szerzej: Raport CERT Polska http://www.cert.pl/PDF/Raport_CP_2009.pdf
oraz Raport CERT.GOV.PL <http://www.cert.gov.pl/download.php?s=3&id=105>

Wszystkie wyżej zdefiniowane nadużycia wpływają w sposób niekorzystny na:

- funkcjonowanie sieci telekomunikacyjnej - obniżenie parametrów jakościowych i uniemożliwienie świadczenie usług telekomunikacyjnych, w tym ponoszenie strat finansowych;
- użytkowników końcowych - brak możliwości skorzystania z usług telekomunikacyjnych, w tym ponoszenie strat finansowych.

Ograniczanie zjawisk nadużyć w sieci telekomunikacyjnej sprowadzać powinno się do:

- niezwłocznego blokowania przez operatora ruchu sterującego sieciami komputerów w sieci botnet (wysyłające nieświadomie spam lub uczestniczące w innych nadużyciach);
- analizowania ruchu przychodzącego i wychodzącego od klienta na poziomie szczegółowości umożliwiającym prawidłowe sklasyfikowanie wiadomości spam / nie-spam (tym samym zezwalające na częściowe odczytywanie przesyłanych komunikatów dokonywane przez autonomiczne urządzenia przeciwsпамowe);
- analizowania ruchu przychodzącego do klienta pozwalającego wykryć i reagować na nadużycia bez konieczności uzyskania zgody klienta;
- usuwania wiadomości z poczty elektronicznej użytkowników zaklasyfikowanych jako stwarzające zagrożenie dla funkcjonowania sieci, bez konieczności uzyskania zgody klienta, a w wypadkach uciążliwego przesyłania spamu nawet wbrew woli klienta;
- uświadamiania użytkownika końcowego o istniejącym zagrożeniu;
- dbania przez użytkownika końcowego o stan ochrony własnego komputera poprzez używanie programów antywirusowych;
- współpracy między operatorami w zakresie wykrywania nadużyć w sieci telekomunikacyjnej – przykładowo wykorzystując kontakty pomiędzy zespołami CERT;
- edukacji użytkowników końcowych w zakresie występujących w sieci nadużyć – zadanie skierowane do organów administracji państwowej.

Mając tak zdefiniowany obszar nadużyć występujących w sieci telekomunikacyjnej wdrożenie nowych rozwiązań prawnych wymaga przeprowadzenie następującego procesu analitycznego:



Regulacja antyspamowa

Problematyka prawna zwalczania tzw. niezamówionych komunikatów (wiadomości) uregulowana jest w dwóch unijnych aktach prawnych:

- dyrektywie 2000/31/WE o niektórych prawnych aspektach usług społeczeństwa informacyjnego (art.7) oraz
- dyrektywie 2002/58/WE zmienionej dyrektywą 2009/136/WE (art.13) w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej.

W art.7 ust.1 dyrektywy 2000/31/WE ustanowiono zakaz przesyłania niezamówionej informacji handlowych za pomocą poczty elektronicznej, a w art.13 dyrektywy 2002/58/WE – zakaz wykorzystywania automatycznych systemów wywołujących, faksów lub poczty elektronicznej dla celów marketingu bezpośredniego, bez uprzedniej zgody abonentów.

Dotychczasowa implementacja zapisów prawa Unii Europejskiej w ustawodawstwie polskim w zakresie regulacji spamu została wdrożona do Ustawy o świadczeniu usług drogą elektroniczną oraz Ustawy Prawo telekomunikacyjne.

Odpowiednie przepisy zostały zidentyfikowane przez Ministerstwo Infrastruktury w ramach prac nad projektem ustawy Prawo telekomunikacyjne.

W dyrektywach rozróżnia się wyraźnie regulację dotyczącą treści i regulację dotyczącą transmisji. Projekt regulacji antyspamowych przygotowany przez Ministerstwo - szczególnie w zakresie kompetencji Prezesa UKE - jako wyrażnie dotyczący kwestii treściowych, jest niezgodny z dyrektywą 2002/21/WE. Wskazać należy, iż intencją regulacji antyspamowych jest ochrona prywatności, a kompetencje w zakresie ochrony praw konsumentów związanych z zagadnieniami związanymi z przesyłaną treścią oraz reklamą posiada Prezes UOKiK.

Już na tym etapie prac PIIT jest w stanie negatywnie ocenić niekonsekwencję polegającą na „przeniesieniu” części regulacji z ustawy o świadczeniu usług drogą elektroniczną (u.ś.u.d.e.), a pozostawieniu pozostałych przepisów. Nie dostrzegamy bowiem zalet płynących z dualizmu uregulowań tej samej kwestii w dwóch różnych ustawach (tu trzeba wskazać np. na fakt, iż definicja oraz wymogi związane z przesłaniem informacji handlowej miałyby pozostać uregulowane w u.ś.u.d.e., zaś konsekwencje naruszenia wymogów w tym zakresie byłyby określone w Pt; ponadto część niezbędnych informacji, które miałyby być obligatoryjnie przesyłane wraz z informacją handlową określoną w u.ś.u.d.e., byłaby wymieniona w Pt).

PIIT postuluje o uregulowanie kwestii związanych z treścią niezamówionych komunikatów (tj. spamu) w ustawie, która wydaje się bardziej właściwą, tj. w u.ś.u.d.e.

Regulacja nadużyć w sieci telekomunikacyjnej wpływające na integralności sieci

W przypadku nadużyć w sieci telekomunikacyjnych wpływających na stan bezpieczeństwa i integralności sieci przepisy ustawy Prawo telekomunikacyjne jedynie identyfikują zagadnienie bez ustalenia jakichkolwiek regulacji określających relacje podmiotów funkcjonujących na rynku telekomunikacyjnym (przedsiębiorcy telekomunikacyjni, użytkownicy końcowi, organy administracji państwowej).

Poniżej przedstawiamy szczegółowe uwagi do propozycji przedstawionej przez Ministerstwo Infrastruktury

1) w art. 60 dodaje się pkt 8 w brzmieniu:

- 8) *szczegółowe warunki podejmowania przez dostawcę usług telekomunikacyjnych działań, o których mowa w art. 175g ust. 1 – 5.”;*

UWAGI PIIT:

Rozwiązania techniczne wspierające walkę ze spamem oraz zagrożeniami integralności sieci telekomunikacyjnych ewoluują w sposób dynamiczny, w sposób adekwatny do rozwoju zagrożeń oraz powstających technologii. Z tego względu niecelowym jest umieszczanie w regulaminach bądź umowach szczegółowych warunków określających działania podejmowane przez dostawcę – każda bowiem zmiana sposobu działań dostawcy (nawet niewpływająca bezpośrednio na prawa abonentów) wymagałaby przeprowadzenia kosztownego procesu dokonania zmian umów ze wszystkimi abonentami. Koszty tego procesu mogłyby zniechęcać dostawców do nieustannego implementowania nowych proklienckich rozwiązań.

Wydaje się, iż do realizacji art. 20 ust. 1 lit. h dyrektywy 2002/22/WE (w brzmieniu nadanym dyrektywą 2009/136/WE) wystarczy wskazanie w umowie lub regulaminie rodzaju działań, które przedsiębiorca może podjąć w związku zagrożeniami bezpieczeństwa lub integralności (dyrektywa nie wymaga wskazywania szczegółowych warunków).

W tym miejscu warto również wskazać, iż podejmowane działania ograniczenia zjawiska spamu nie dotyczą tylko przedsiębiorcy

telekomunikacyjnego ale również użytkownika końcowego. W związku z tym, regulamin świadczenia usług (w zakresie spam) może również zawierać zapisy odnoszące się do użytkownika końcowego.

2) uchyla się art. 172;

UWAGI PIIT:

Poddajemy pod rozważenie przeniesienie art. 172 Pt do ustawy o świadczeniu usług drogą elektroniczną (ustawa ta bowiem reguluje obowiązki usługodawcy związane ze świadczeniem usług drogą elektroniczną, do których należy zaliczyć również wykorzystywanie automatycznych systemów wywołujących dla celów marketingu).

3) w art. 175 ust. 1 otrzymuje brzmienie:

„1. Przedsiębiorca telekomunikacyjny, z uwzględnieniem art. 160 ust. 2, jest obowiązany podjąć środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa przekazu komunikatów w związku ze świadczonymi usługami, w szczególności w przypadku ujawnienia przekazu komunikatów:

- 1) które zawierają zidentyfikowane treści, załączniki, kody lub skrypty mające na celu naruszenie prywatności lub bezpieczeństwa odbiorcy;*
- 2) w których nadawca ukrywa lub fałszuje swoją tożsamość;*
- 3) które ze względu na swój rodzaj, częstotliwość lub ilość stanowią zagrożenie dla integralności lub bezpieczeństwa sieci lub świadczenia usług telekomunikacyjnych.”;*

UWAGI PIIT:

Jakkolwiek cel przepisu jest jak najbardziej słuszny, brzmienie jednostki jest obciążone niedoskonałościami. Dyspozycja przepisu uzależniająca podjęcie działań dostawcy od ujawnienia przekazu wskazanych komunikatów nie może znaleźć zastosowania ze względu na istnienie obowiązku zachowania tajemnicy telekomunikacyjnej (w polskiej ustawie przewidzianej m.in. w art. 159 Pt).

Zwracamy też uwagę, iż przepis nakazuje dostawcy jednoczesne podjęcie środków technicznych oraz organizacyjnych, mimo tego iż często wystarczającym będzie jeden typ środków.

Nie jest też wiadomy zakres podmiotowy właściwy dla czynności ujawnienia przekazu (tzn. bezosobowe odwołanie się do „ujawnienia przekazu” powoduje, iż nie jest jasne kto byłby władny do skutecznego pod względem prawnym stwierdzenia, iż dany komunikat należy uważać za „ujawniony”, a przy tym za zawierający niedozwoloną treść) – w szczególności czy nakaz podejmowania działań przez dostawcę realizuje się w przypadku otrzymania jakiegokolwiek (nawet nieprawdziwej) informacji o przekazie *niedozwolonych* komunikatów. Nie jest też możliwym ustalenie przez dostawców, czy nadawca fałszuje swoją tożsamość lub ją ukrywa, zatem przepis 175 ust. 1 pkt 2 należy uznać za niewykonalny.

Pkt 3 omawianego przepisu jest niezwykle istotny dla bezpieczeństwa sieci operatorów (a w konsekwencji jest istotny dla klientów korzystających z sieci), jednakże zdaniem PIIT dyspozycja tego przepisu powinna stanowić dla dostawców uprawnienie do podjęcia określonych działań, a tym samym nie powinna być obligatoryjnym obowiązkiem jak proponuje się w projekcie

(szczególnie ze względu na pojemność oraz ocenny charakter określeń takich jak natężenie częstotliwości oraz ilość komunikatów).

4) po dziale VII dodaje się dział VIIa w brzmieniu:

„DZIAŁ VIIa

Zwalczanie wysyłania spamu

UWAGI PIIT:

Naszym zdaniem regulacje dotyczące treści wysyłanej za pośrednictwem sieci telekomunikacyjnych (do takiej treści zalicza się również spam) powinny konsekwentnie pozostać przedmiotem u.ś.u.d.e.

5) **Art. 175a. 1. Zakazane jest wysyłanie:**

- 1) komunikatów, których treść i kontekst są niezależne od tożsamości odbiorcy,
- 2) komunikatów z wykorzystaniem automatycznych systemów wywołujących, dla celów marketingu bezpośredniego,
- 3) komunikatów, których zadaniem jest tworzenie baz danych teleadresowych odbiorców, w szczególności dla celów marketingowych,
- 4) informacji handlowej w rozumieniu art. 2 pkt 2 ustawy z dnia 18 lipca 2002 r.
o świadczeniu usług drogą elektroniczną
- jeżeli odbiorca nie wyraził na ich przesłanie uprzedniej zgody.

Art. 175a. 2. Komunikaty i informacje, o których mowa w ust. 1, stanowią spam.

UWAGI PIIT:

Powyższa propozycja definicji spamu wykracza poza definicję przewidzianą w dyrektywie (por. motywy 68 oraz 70 dyrektywy 2009/136/WE, w których pod pojęciem „spam” rozumie się niezamówione komunikaty o charakterze komercyjnym; por. również art. 13 dyrektywy 2002/58/WE traktujący w zasadzie jedynie o marketingu bezpośrednim).

Proponowana definicja nie zawiera również istotnego elementu, jaki istnieje w art. 10 u.ś.u.d.e., tj. określenia, iż przepis dotyczy informacji przesyłanych „za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej” (brak takiego zawężenia może powodować rozciągnięcie zakresu przepisu na formy „nie-elektroniczne”, jak np. masowa wysyłka listów papierowych).

Zwracamy także uwagę na fakt, iż wykładnia językowa powyższego przepisu prowadzi do wniosku, że zakazane ma być przesyłanie również komunikatów technicznych wytwarzanych przez urządzenia, a służących poprawnej komunikacji (komunikaty te mogą być uznane za niezależne od tożsamości odbiorcy).

Pkt 1 (szczególnie z uwagi na wyłączenie zawarte w ust. 6) jest praktycznie normą o pustym zakresie – wszelkiego typu wiadomości noszące znamiona spamu mieszczą się bowiem w zakresie pojęcia informacji handlowej.

W pkt 3 użyto niepoprawnego złożenia językowego. Nie sposób bowiem stwierdzić, że komunikat może tworzyć bazę danych lub że stoi przed nim takie zadanie - komunikat może być co najwyżej środkiem do realizacji danego celu.

Pkt 4 odwołuje się do art. 2 ust. 2 u.ś.u.d.e. W obliczu zamiaru wykreślenia całego art. 10 u.ś.u.d.e (art. 10 bowiem ma być wykreślony na mocy pkt 9 projektu nowelizującego) u.ś.u.d.e. stanie się w tym zakresie aktem ograniczonym praktycznie do „przechowywania” definicji służącej wykładni przepisu z innego aktu, tj. art. 175a ust. 1 ustawy prawo telekomunikacyjne. Zdaniem PIIT jest to zabieg co najmniej niewskazany pod względem poprawności legislacyjnej.

Ust. 2 statuujący, iż dane zjawisko stanowi spam, nie mieści się w logicznym układzie ustawy Prawo telekomunikacyjne, które definicje ustawowe zawiera w tzw. słowniczku znajdującym się w art. 2 Pt.

Konstrukcja art. 175a jest również sprzeczna z pozostałymi przepisami ustawy, które wręcz nakazują dostawcy wysłać klientom komunikaty, które stanowią spam w rozumieniu art. 175a (por. np. przepisy nakazujące doręczania informacji o zmianach cennika lub regulaminu, mimo braku wyrażenia przez abonenta uprzedniej zgody).

6) Art. 175a. 3. *Ciężar udowodnienia posiadania zgody odbiorcy na przesłanie komunikatów i informacji, o których mowa w ust. 1, spoczywa na nadawcy komunikatu.*

Art. 175a. 4. *Wysyłanie spamu stanowi czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503, z późn. zm.).*

Art. 175a. 5. *W przypadku, gdy przedsiębiorca, w związku ze sprzedażą produktu lub usługi otrzymuje od swoich klientów dane teled adresowe, w tym adresy elektroniczne, może wykorzystywać te adresy dla potrzeb marketingu bezpośredniego swoich produktów lub usług, pod warunkiem, że klienci zostali jednoznacznie, w sposób łatwy i zrozumiały poinformowani, w chwili zbierania danych i przy każdej okazji otrzymania takich informacji w przypadku klientów, którzy początkowo wyrazili zgodę, o możliwości sprzeciwienia się takiemu wykorzystaniu ich danych i odwołania zgody, w sposób prosty i wolny od opłat.*

UWAGI PIIT:

Redakcja ust. 5 jest sprzeczna z art. 13 ust. 2 dyrektywy 2002/58/WE. Dyrektywa nakazuje bowiem jednorazowo poinformować klientów, iż klient może wyrazić swój sprzeciw względem wykorzystywania jego danych teled adresowych (sprzeciw może być złożony bezpośrednio przy zbieraniu danych teled adresowych, a także w dowolnej chwili w przyszłości – w tym po otrzymaniu poszczególnych wiadomości). Tymczasem projektowane przepisy miałyby - wbrew dyrektywie - wymagać od dostawców informowania klientów przy okazji wysyłania do nich każdej kolejnej wiadomości. Byłoby to wymogiem pozbawionym uzasadnienia, a przy tym dla wielu środków komunikacji wręcz niewykonalnym (np. ze względów technicznych wiadomość SMS może zawierać w sumie jedynie 160 znaków²).

Nie jest też zasadnym kopiowanie użytego w dyrektywie sformułowania (*notabene* być może poprawnego dla języków obcych, ale nie odpowiadającego stylistyce stosowanej w języku polskim) „w przypadku klientów, którzy początkowo wyrazili zgodę”, gdyż bezcelowe jest wskazywanie się na klientów, którzy początkowo wyrazili zgodę, skoro tylko

² Tu należy podkreślić, że łączenie kilku wiadomości w dłuższy ciąg jest obciążone trudnościami takimi jak brak możliwości zagwarantowania jednoczesnego otrzymania przez klienta wszystkich elementów składowych (klient, ze względu na natężenie ruchu w sieci lub ze względu na przepełnienie pamięci własnego telefonu może otrzymać tylko część takiej wiadomości). Nie sposób pominąć też faktu, iż klient wyrażający wolę otrzymywania informacji typu SMS, na skutek otrzymywania kilkakrotnie większej ilości SMSów (zwiększona ilość wynikałaby z wymagań ustawy nakazującej wysyłania obszernego tekstu niebędącego w obszarze praktycznych zainteresowań klienta), nabrałby przekonania, iż to dostawca wysłała mu niechciane informacje (niepożądany negatywny wizerunek danego przedsiębiorcy).

do takich można wysłać informację. Wystanie informacji do innych klientów – tych, którzy zgody nie wyrazili – oznacza bowiem wysłanie spamu.

Wprowadzenie przepisu ust. 5 (mającego implementować art. 13 ust. 2 dyrektywy 2002/58/WE), bez odpowiedniej modyfikacji ustawy o ochronie danych osobowych, spowoduje, iż przepis ten wejdzie w kolizję z art. 23 ust. 4 pkt 1 ustawy o ochronie danych osobowych. Wydaje się, że jeśli ustawodawca zamierza wprowadzić dodatkowe obostrzenia dla uprawnień podmiotu przetwarzającego dane wskazanych w art. 23 ust. 4 pkt 1 ustawy o ochronie danych osobowych, należałoby wyraźnie rozgraniczyć obydwa przepisy poprzez ustalenie normy kolizyjnej.

Niezależnie od powyższych uwag do niniejszego przepisu należy wskazać, iż ze względu na zakres tejże jednostki daleko wykraczający poza działalność strictly telekomunikacyjną (np. rozsyłanie informacji przez sklepy AGD) należałoby ją umieścić w akcie, który jest odpowiedni dla tego typu regulacji – tj. w ustawie o świadczeniu usług drogą elektroniczną.

7) Art. 175a. 6. *Przepisu ust. 1 nie stosuje się w przypadku używania poczty elektronicznej lub podobnego środka bezpośredniego porozumiewania się na odległość między osobami fizycznymi, w celach osobistych niezwiązanych z prowadzoną przez te osoby, chociażby ubocznie, działalnością zarobkową, wykonywanym przez nie zawodem lub pełnioną funkcją.*

UWAGI PIIT:

Komunikacja werbalna (głosowa) w telefonii stacjonarnej lub ruchomej nie jest środkiem podobnym do poczty elektronicznej. Zatem z przepisu ust. 6 wynika, że ust. 1 stosuje się do komunikacji telefonicznej dokonywanej w celach osobistych między osobami fizycznymi. Z pewnością nie jest to intencją ustawodawcy, jednakże umieszczenie w tym rozdziale przepisu o takim brzmieniu prowadzi do przedstawionych wniosków.

8) Art. 175b. *Komunikat i informacja, o których mowa w art. 175a ust. 1, wysłane po uprzednim uzyskaniu zgody odbiorcy powinny zawierać oznaczenie wysyłającego, jego adres korespondencyjny lub wskazanie gdzie można te dane uzyskać oraz informacje o możliwości i sposobie odwołania zgody. Przepis art. 174 stosuje się odpowiednio.*

UWAGI PIIT:

W przypadku informacji typu SMS nie posiadają wystarczającej przestrzeni, aby wpisywać do nich miejsce ze szczegółowymi danymi, a także informacje o sposobie odwołania zgody (por. uwagi do 170a ust. 5). Przepis ten jest zatem sprzeczny z międzynarodowymi normami ETSI standaryzującymi systemy telefonii komórkowej.

9) Art. 175c. *Prezes UKE wszczyna z urzędu postępowanie w sprawach o nałożenie kary pieniężnej za wysyłanie spamu, które ze względu na swój charakter, częstotliwość lub ilość stanowią zagrożenie dla integralności lub bezpieczeństwa sieci lub świadczenia usług telekomunikacyjnych.*

UWAGI PIIT:

Przepis, mimo dokonanych zmian jest wciąż nieprecyzyjny i w praktyce będzie oznaczał daleko idącą dowolność organu przy podejmowaniu decyzji o wszczęciu postępowania.

Mając na uwadze, iż przedmiotem tego postępowania będzie nałożenie kary administracyjnej, precyzyjne określenie podstaw wszczęcia i wydania decyzji nakładającej karę jest konieczne. Brakuje określenia, kto będzie adresatem takiego postępowania oraz brak jest wskazania trybu, w jakim postępowanie miałyby się toczyć.

Pozostawienie wskazanych uchybień spowoduje naruszenie Konstytucji RP.

Niezależnie od powyższych uwag trzeba wspomnieć, iż art. 175c wydaje się być sprzeczny z projektowanym art. 209a. Bowiem przesłanki w art. 175c (tj. przesłanki wszczęcia postępowania) są różne od przesłanek wymienionych w art. 209 ust. 1 pkt 25 oraz 209a (przesłanki nałożenia kary). Powstaje zatem wątpliwość, czy Prezes UKE może nałożyć karę w przypadkach, w których nie jest uprawniony do wszczęcia postępowania na podstawie art. 175c (np. w sytuacji, gdy wysyłany jest spam, który nie powoduje zagrożenia integralności lub bezpieczeństwa sieci, ale jest masowy i charakteryzuje się wysoką uciążliwością).

Wprowadzenie art. 175c w proponowanym brzmieniu poskutkowałoby również tym, że mogłyby pojawić się argumenty, iż w sprawach o nałożenie kary w przypadkach innych niż art. 175c (np. nałożenie kary na operatora za nieprzestrzeganie obowiązków regulacyjnych), wszczęcie nie będzie mogło nastąpić z urzędu (wymagany będzie wniosek). Wynika to z faktu, że skoro w jednym przepisie racjonalny ustawodawca stosuje pojęcie „wszczyna z urzędu”, to a contrario w przypadku braku takiego sformułowania wśród innych przepisów karnych, wszczęcie z urzędu nie może nastąpić (będzie konieczny wniosek zgodnie z k.p.a., do którego odsyła art. 206 ust. 1 Pt).

Przepis pomija ponadto fakt, iż w praktyce spam jest rozsyłany przez osoby fizyczne, które nie prowadzą działalności telekomunikacyjnej. Jeśli osoby te prowadzą jakąkolwiek działalność, jest mało prawdopodobnym, aby kara w wysokości 3% rocznego (zaksięgowanego) przychodu była dla osoby fizycznej karą posiadającą walory odstrasżające. Warto zaznaczyć, iż w wielu przypadkach użytkownicy końcowi, których terminale wysyłają spam nie są tego świadomi. W związku z tym przepis ten jest praktycznie niewykonalny w praktyce.

10) Art. 175d. *Przy Prezesie UKE tworzy się ogólnopolski punkt przyjmowania zgłoszeń o wysłaniu spamu w celu:*

- 1) *gromadzenia i przetwarzania informacji na potrzeby prowadzonych postępowań;*
- 2) *wykrywania i eliminowania przypadków wysyłania spamu;*
- 3) *wykonywania zadań określonych w art. 192 ust. 1 pkt 21, w szczególności w zakresie współpracy międzynarodowej z jednostkami odpowiedzialnymi za zwalczanie wysyłania spamu.*

UWAGI PIIT:

Wydaje się, iż przy tworzeniu przepisu pominięto fakt, iż od lat z powodzeniem funkcjonują następujące polskie centra (tzw. CERT - *Computer Emergency Response Team*) zaangażowane w walkę z incydentami bezpieczeństwa sieci, incydentami dotyczącymi spamu oraz podnoszenie świadomości w zakresie bezpieczeństwa wśród użytkowników sieci Internet:

- CERT Polska działający w strukturach Naukowej i Akademickiej Sieci Komputerowej (www.cert.pl);

- CERT TP działający przy Telekomunikacji Polskiej S.A. (www.tp.pl/prt/tpcert);

- Rządowy Zespół Reagowania na Incydenty Komputerowe będący jednostką w strukturach Agencji Bezpieczeństwa Wewnętrznego (www.cert.gov.pl);
- Zespół CERT przy Ministrze Obrony Narodowej.

PIIT sugeruje rozważyć, czy model regulacji oparty na przekazywaniu informacji do Prezesa UKE będzie efektywny, jak również możliwy do zrealizowania, zważywszy na brak stosownego zaplecza teleinformatycznego oraz ze względu na znaczną skalę zjawisk, których wykrycie wymaga bezpośredniego nadzorowania ruchu poszczególnych operatorów, jak również w świetle funkcjonowania ośrodków CERT wskazanych powyżej.

Niezależnie od praktycznych uwag przedstawionych powyżej, art. 175d należy uznać za przepis zbyt ogólny – wskazane jest co najmniej ustalenie trybu oraz przesłanek działalności Prezesa UKE w tym zakresie.

- 11) Art. 175e.** *Prezes UKE w toku prowadzonego postępowania dotyczącego wysyłania spamu może żądać od dostawców usług telekomunikacyjnych i operatorów dostarczenia w wyznaczonym terminie informacji niezbędnych dla wypełnienia jego zadań, w tym danych osobowych abonentów.*

UWAGI PIIT:

Przepis stanowi zagrożenie dla ochrony prywatności, gdyż ustalenie, czy odbiorca wyraził zgodę na przestanie komunikatu wymagałoby zapoznania się z treścią komunikatu oraz dokonywanie wykładni oświadczeń woli.

Zdaniem PIIT bez określenia trybu i sposobu przekazywania danych, przepis pozostawiłby Prezesowi UKE nieograniczoną swobodę, co z kolei byłoby sprzeczne z konstytucyjnym porządkiem prawnym (art. 49 Konstytucji).

Należy też stwierdzić, iż projektowana norma godzi w zasady zawarte w art. 218 k.p.k. oraz art. 241 k.p.k.

Jeżeli jednak ustawodawca miałby zamiar wyposażyć Prezesa UKE w kompetencje organów ścigania – wówczas należałoby rozważyć nowelizację k.p.k. oraz ustawy o Policji, a także ustawy o prokuraturze (pojawiłby się wątpliwość czy prokurator może nadzorować postępowania prowadzone przez Prezesa UKE tak jak czyni to względem Policji). Tym niemniej rozważania te byłyby bezprzedmiotowe z uwagi na sprzeczność takiej konstrukcji z Ustawą Zasadniczą.

- 12) Art. 175f.** *Dostawcy usług telekomunikacyjnych obowiązani są, w ramach oferowanych przez nich usług, do utworzenia i prowadzenia punktów przyjęć skarg dotyczących naruszenia bezpieczeństwa telekomunikacyjnego, w tym incydentów wysyłania bądź otrzymywania spamu, w celu:*

- 1) *badania przypadków wysyłania spamu;*
- 2) *umożliwienia swoim abonentom zgłaszania przypadków naruszeń bezpieczeństwa telekomunikacyjnego;*
- 3) *współpracy z punktami przyjęć skarg innych dostawców usług telekomunikacyjnych na terenie kraju.*

UWAGI PIIT:

Nie jest wiadomym, w jakim celu dostawcy mają tworzyć punkty przyjęć skarg, skoro w art. 175d przewiduje się, iż ogólnopolski punkt przyjmowania zgłoszeń ma prowadzić Prezes UKE, jak również istnieją już inne punkty wymiany informacji między operatorami. Warto zwrócić uwagę, iż przedsiębiorcy

telekomunikacyjni są zainteresowani współpracą z istniejącymi punktami wymiany informacji nt. nadużyć w sieci i nie potrzeba w tym zakresie dodatkowych regulacji wymuszających na nich taką współpracą (każda informacja pozyskana z CERT pozwala operatorowi obniżyć ryzyko wystąpienia strat związanych z nadużyciem w sieci).

Przepis z punktu 3 należałoby sformułować w ten sposób, aby dostawcy zyskali wyraźne uprawnienie do wymiany z innymi dostawcami informacji służących walce ze spamem oraz naruszeniami bezpieczeństwa teleinformatycznego (wyłączenie tajemnicy telekomunikacyjnej w tym zakresie musi być wyraźne, a nie dorozumiane).

13) Art. 175g. 1. *Dostawca usług telekomunikacyjnych w przypadku ujawnienia wysyłania spamu w ramach dostarczanych usług, który ze względu na swój charakter, rodzaj, częstotliwość lub ilość stanowi zagrożenie dla integralności lub bezpieczeństwa sieci, świadczenia usług telekomunikacyjnych i użytkowników, podejmuje działania mające na celu ustalenie zakończenia sieci, z którego spam został wysłany oraz metodę jego dystrybucji.*

UWAGI PIIT:

Brzmienie przepisu może skutkować dowolnością interpretacyjną wynikającą z braku precyzyjnego określenia, w jakich sytuacjach dostawca usług telekomunikacyjnych będzie podejmował działania przeciwdziałające przesyłaniu spamu. „Ocena” decyzja przedsiębiorcy co do podjęcia działań antyspamowych może skutkować roszczeniami ze strony klientów, stąd istotne jest ustawowe wyłączenie odpowiedzialności przedsiębiorcy względem klientów za podejmowane działania związane ze zwalczaniem spamu.

Ustalenie, czy przesyłane wiadomości stanowią spam, wymaga zapoznania się z treścią komunikatu (z uwagi na obowiązek tajemnicy telekomunikacyjnej może to być problematyczne) oraz ewentualnego kontaktu z odbiorcą (ze względów praktycznych zdarza się, iż jest to niemożliwe), co powoduje, iż obowiązek ten można uznać za niewykonalny.

Przepis nie precyzuje (co też należy uznać za błąd), kto miałby ujawnić przesyłanie spamu: prokurator, sąd, czy może anonimowy donos. Nie jest też jasne, czy ujawnienie miałoby być udowodnione, czy też wystarczyłoby jego uprawdopodobnienie.

Z punktu widzenia przedsiębiorcy telekomunikacyjnego istotne jest, aby przepisy prawa koncentrowały się na możliwości umożliwienie podjęcie odpowiednich działań w celu ochrony bezpieczeństwa sieci, a w tym pozostałych użytkowników końcowych.

14) 2. *W przypadku zlokalizowania zakończenia sieci, z którego wysłany został spam, dostawca usług telekomunikacyjnych jest obowiązany do poinformowania, drogą elektroniczną lub za pomocą podobnego środka bezpośredniego porozumiewania się na odległość, o tym fakcie abonenta oraz do udostępnienia jasnej i przejrzystej instrukcji umożliwiającej usunięcie stwierdzonych nieprawidłowości, wraz z odpowiednim bezpłatnym oprogramowaniem, o ile to technicznie możliwe. Abonent powinien zostać także poinformowany o konsekwencjach, o których mowa w ust. 4, nieusunięcia stwierdzonych nieprawidłowości w terminie, o którym mowa w ust. 3.*

UWAGI PIIT:

Przepis wskazuje na dwa środki komunikacji: 1) droga elektroniczna; 2) środek bezpośredniego porozumiewania się na odległość podobny do drogi

elektronicznej, ale nie będący drogą elektroniczną. PIIT nie jest w stanie podać ani jednego przykładu środka, który mógłby zaliczyć się drugiej grupy.

Przepis nakazuje poinformować abonenta, ale nie wiadomo, czy chodzi o abonenta „spamującego”, czy o abonenta „poszkodowanego spamem”. Z ust. 3 oraz z ogólnej wiedzy w zakresie informatyki o występującym zjawisku infekowania komputerów oraz rozsyłania spamu z zainfekowanych komputerów można wywodzić, że w tym miejscu chodzi o abonenta „spamującego”, jednakże dopracowanie niniejszego sformułowania jest niezbędne. Podobna wątpliwość zachodzi w odniesieniu do instrukcji, którą należy udostępnić abonentowi.

Z przepisu wynika, że dostawca po zlokalizowaniu zakończenia sieci (np. nr IP w sieci Internet), nawet jeśli to zakończenie znajduje się w sieci innego dostawcy, powinien wzywać tego (obcego mu) abonenta do zaniechania naruszeń oraz udostępnić mu oprogramowanie i instrukcje. Przepis nie ogranicza bowiem katalogu podmiotowego do abonentów tego dostawcy, co należy uznać za błąd legislacyjny.

Zwracamy uwagę, iż jeśli „stwierdzonymi nieprawidłowościami” jest np. jednorazowe wysłanie 40 milionów sztuk spamu w postaci poczty e-mail, nie ma obiektywnych możliwości usunięcia tego typu nieprawidłowości (spam z danego komputera lub telefonu komórkowego został wysłany i nie ma możliwości cofnięcia tejże wysyłki).

Aby oprogramowanie było „odpowiednie”, dostawca musiałby poznać problem wywołwany spamem. Sprowadzałoby się to do obsługi serwisowej, która jest technicznie możliwa, ale nieproporcjonalnie kosztowna.

W odniesieniu do telefonów komórkowych oraz rzadszych systemów operacyjnych komputerów, dostawcy będą zmuszeni do zakupu oprogramowania oraz bezpłatnego jego udostępniania swoim użytkownikom.

Zważywszy na wielość i zmieniające się dynamicznie typy zagrożeń (wirusy, konie trojańskie, spyware) nie jest możliwe dostarczenie użytkownikowi oprogramowania, ani też instrukcji postępowania, z wykorzystaniem których będzie możliwe pełne wyeliminowanie nieprawidłowości w konkretnym przypadku.

O ile nałożenie na operatora obowiązku informacyjnego o zagrożeniach, jakie wiążą się z korzystaniem z sieci oraz wskazywanie możliwych metod ich ograniczenia należy uznać za w pełni uzasadnione, o tyle przerzucenie odpowiedzialności na operatora/dostawcę usług za należyte zabezpieczenie urządzeń, z których korzystają abonenci ich usług, należy odczytać za nadmierne obciążenie.

Z proponowanego przepisu wynika ciążący na dostawcy obowiązek skutecznego poinformowania abonenta. Tymczasem z doświadczeń obecnie istniejących centrów CERT (por. uwagi do art. 175d) wynika, iż niejednokrotnie abonent świadomie i celowo unika kontaktu z operatorem (dotyczy to w szczególności tych abonentów, którzy z premedytacją łamią regulamin korzystania z danej usługi).

Nie jest jasne, czy wtrącenie „o ile to [jest] technicznie możliwe” dotyczy pierwszego, drugiego, trzeciego członu zdania, czy też dotyczy całego przepisu.

15) 3. Abonent jest obowiązany do usunięcia stwierdzonych nieprawidłowości w terminie 2 dni od dnia otrzymania informacji, o których mowa w ust. 2.

UWAGI PIIT:

Przepis w proponowanym brzmieniu stanowi wręcz zachętę do wysyłania spamu. Bowiern podmiot „spamujący” na kontynuowanie procedury będzie miał dodatkowe 2 dni, a w przypadku nieodbierania od operatora korespondencji, będzie władny do „spamowania” w nieskończoność (długi 2-dniowy termin miałby się liczyć od momentu otrzymania przez abonenta informacji). Wskazujemy, iż ograniczenie zjawiska spamu wymaga natychmiastowej reakcji przedsiębiorcy telekomunikacyjnego, który zidentyfikował nadużycie (w tym spam). Operator nie jest w stanie akceptować ograniczenia funkcjonalności własnej sieci telekomunikacyjnej (z powodu wysłanego spamu) przez tak długi okres czas jak 2 dni.

16) 4. W przypadku uchybienia terminowi wskazanemu w ust. 3 dostawca usług telekomunikacyjnych ogranicza funkcjonalność świadczonych usług, w szczególności ogranicza przepływność łącza do 32 kbit/s do abonenta i 16 kbit/s od abonenta do czasu usunięcia stwierdzonych nieprawidłowości.

UWAGI PIIT:

Przepis pomija fakt, iż dostawca często nie ma możliwości ustalenia, czy oraz kiedy abonent otrzymał informację.

Nie wiadomo w jaki sposób dostawca miałby badać, czy nieprawidłowości zostały usunięte (np. usunięcie nieprawidłowości może polegać na uzyskaniu zgody odbiorców na otrzymanie jak dotąd niechcianych komunikatów, zatem należałoby w takim przypadku badać czy nadawca otrzymał zgodę odbiorcy). Nie wiadomo, czy jeśli nadawca wystosuje oficjalną deklarację, iż „nie będzie już wysyłać niezamówionych komunikatów”, to czy będzie to środkiem wystarczającym do uznania, iż usunął nieprawidłowości.

Ograniczenie przepływności dostępu do sieci Internet (bo o taką usługę zapewne chodzi ustawodawcy) do konkretnych wartości wyrażonych w ustawie jest dla niektórych dostawców zabiegiem dość kosztownym – tylko część przedsiębiorców posiada obecnie możliwość wprowadzenia limitów przepustowości o wskazanych wartościach.

Jeśli nieprawidłowości dotyczą spamu typu SMS, nie ma możliwości ograniczenia przepływności. Zatem przepis, bez odpowiednich wyłączeń, jest nieprecyzyjny, a dla pewnych segmentów wręcz martwy.

Zmuszenie dostawców do obligatoryjnego ograniczania przepływności w każdym kanale spowoduje, iż to dostawcy mogą być głównymi ofiarami osób spamujących – bowiem to dostawcy będą musieli podjąć środki techniczne, które niekiedy są kosztowne.

Nie jest wiadomym, w jaki sposób dostawca, nie posiadając dostępu do urządzeń abonenta, miałby ustalić, czy w każdym przypadku nieprawidłowości zostały usunięte. Nie jest jasne, przy pomocy jakiej służby dostawca miałby to badać i jakie dowody byłyby wystarczające do uznania, że nieprawidłowości usunięto.

17) 5. Przywrócenie pełnej funkcjonalności usług do wartości określonych w umowie o świadczenie publicznie dostępnych usług telekomunikacyjnych po usunięciu nieprawidłowości przez abonenta w terminie 7 dni od dnia otrzymania informacji, o których mowa w ust. 2, jest wolne od opłat.

UWAGI PIIT:

Nie wydaje się celowym przerzucenie na operatorów/dostawców usług wszelkich kosztów związanych z wystąpieniem spam, w tym kosztów powiadamiania abonenta, ograniczania przepływności i jej odblokowywania w sytuacji, gdy czynności te są *de facto* wywoływane jego działaniem lub zaniechaniem (często wynikającym z niedbalstwa). Zdaniem PIIT, brak obowiązku abonenta w partycypowaniu w takich kosztach (brak chociażby opłaty za wznowienie właściwej przepływności usługi), z uwagi na brak prewencyjnego i motywującego charakteru opłaty, ograniczy skuteczność przepisów - abonent nie będzie odczuwał potrzeby zabezpieczenia używanego sprzętu w sposób ograniczający prawdopodobieństwo wystąpienia nieprawidłowości w przyszłości.

18) *6. Dostawca usług telekomunikacyjnych przesyła niezwłocznie do jednostki organizacyjnej, o której mowa w art. 175d, wszelkie informacje dotyczące zlokalizowanego w ramach świadczonych usług zakończenia sieci, z którego został wysłany spam, w tym dane osobowe abonenta, oraz informacje dotyczące podjętych przez dostawcę działań.*

UWAGI PIIT:

Imperatywny charakter przepisu nakazuje dostawcy przekazywać również te dane, których nie posiada lub których nie jest w stanie pozyskać. Przepis należałoby ograniczyć do informacji posiadanych.

19) *7. Dostawca usług telekomunikacyjnych przesyła niezwłocznie do jednostki organizacyjnej, o której mowa w art. 175d, informacje o przypadkach wysyłania do swoich abonentów spamu spoza terytorium Rzeczypospolitej Polskiej;*

UWAGI PIIT:

Jak wynika ze wstępnych analiz PIIT, operatorzy nie posiadają narzędzi, które odpowiadałyby wymogom przepisu. Z tego względu niezbędne jest dokonanie stosownej analizy Oceny Skutków Regulacji.

Przedsiębiorcy telekomunikacyjni powinni mieć możliwość swobodnej wymiany informacji nt. nadużyć występujących w sieci z operatorami, którzy również znajdują się poza granicą RP.

20) *8. Przepisów ust. 3 - 4 nie stosuje się do podmiotów publicznych w rozumieniu art. 2 ust 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r., Nr 64, poz. 565 oraz z 2006 r. Nr 12, poz. 65 i Nr 73, poz. 501 oraz z 2008 r., Nr 127, poz. 817).*

21) *w art. 192 w ust. 1 dodaje się pkt 21 w brzmieniu:*

„21) prowadzenie postępowań i wykonywanie innych zadań związanych ze zwalczaniem wysyłania spamu.”,

22) *w art. 209 w ust 1 pkt 25 otrzymuje brzmienie:*

„25) nie wypełnia obowiązków uzyskania zgody, o których mowa w art. 161, 166, 169, 173-174 oraz 175a,”,

23) *po art. 209 dodaje się art. 209a w brzmieniu:*

„Art. 209a. 1. Kto wysłał spam, zleca jego wysyłanie lub odnosi korzyści z jego wysyłania podlega karze pieniężnej w wysokości od 100 złotych do 100 000 złotych

2. Podmiot, który w wyznaczonym terminie nie udzieli Prezesowi UKE informacji, o których mowa w art. 175e oraz w art. 175g ust. 7, bądź nie podejmie działania określonego w art. 175g ust. 4, podlega karze pieniężnej w wysokości od 100 złotych do 5000 złotych.

UWAGI PIIT:

Przepis art. 209a ust. 2 jest niezależny od prawnokarnego pojęcia winy oraz nakazuje podejmować działania określone w art. 175g ust. 4 niezależnie od możliwości technicznych. Prowadzi to do sytuacji, w której podmiot nie ograniczający przepływności np. z powodu braku możliwości technicznych (np. nie ma możliwości ograniczyć przepływności wysyłania komunikatów SMS) będzie wg ustawy naruszał art. 209a ust.2, zaś Prezes UKE będzie zobligowany do nałożenia kary pieniężnej.

24) 3. Dostawca usługi telekomunikacyjnej, który nie wypełnia obowiązku utworzenia i prowadzenia punktu przyjmowania skarg, o którym mowa w art. 175f, podlega karze pieniężnej w wysokości od 100 złotych do 5000 złotych.”;

25) w art. 210 ust. 1 otrzymuje brzmienie:

„1. Kary pieniężne, o których mowa w art. 209 ust. 1 oraz w art. 209a, nakłada Prezes UKE w drodze decyzji, przy czym karę pieniężną, o której mowa w art. 209 ust. 1, wymierza się w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym.”;

26) W ustawie z dnia 18 lipca 2002 r. – o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204, z późn. zm.) wprowadza się następujące zmiany:

1) uchyla się art. 10;

2) art. 23 otrzymuje brzmienie:

„Art. 23. Kto wbrew obowiązkowi nie podaje danych, o których mowa w art. 5 ust. 2, 3 lub 5, albo podaje dane nieprawdziwe lub niepełne, podlega karze pieniężnej w wysokości od 100 do 5000 złotych, nakładanej przez Prezesa Urzędu Komunikacji Elektronicznej w drodze decyzji administracyjnej.”;

3) po art. 23 dodaje się art. 23a w brzmieniu:

„Art. 23a. Kto nie wypełnia obowiązków określonych w art. 9, podlega karze pieniężnej w wysokości od 100 do 5000 złotych, nakładanej przez Prezesa Urzędu Komunikacji Elektronicznej w drodze decyzji administracyjnej.”;

4) uchyla się art. 24 i 25.

27) [przepis przejściowy] Do spraw wszczętych na podstawie art. 10 ustawy z dnia 18 lipca 2002 r. – o świadczeniu usług drogą elektroniczną i niezakończonych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.