PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE
ISSN 1733-2486

TOM XV, ZESZYT 9, cz. 1

http://piz.san.edu.pl

E-BIZNES
I OCHRONA DANYCH OSOBOWYCH

Redakcja
Andrzej Jackiewicz
Łukasz Sułkowski

Brodnica, Łódź, Warszawa 2014

Koszt wydania Zeszytu 9, cz. 1
sfinansowany ze środków: Społecznej Akademii Nauk, Burmistrza Brodnicy,
Starosty Brodnickiego oraz ZPC „Vobro" i firmy M. Hildebrandt

Zeszyt recenzowany

Redakcja naukowa: Andrzej Jackiewicz, Łukasz Sułkowski

Komputerowy skład tekstu, redakcja i korekta techniczna: Jadwiga Poczyczyńska

Projekt okładki: Marcin Szadkowski

ISSN 1733-2486

Wydawnictwo
Społecznej Akademii Nauk
e-mail: **wydawnictwo@spoleczna.pl**
tel. 42 632 50 23, 42 632 50 26 w. 339

Wersja papierowa wydania jest wersją podstawową

Druk i oprawa: Mazowieckie Centrum Poligrafii, ul. Słoneczna 3C,
05-260 Marki, www.c-p.com.pl; biuro@c-p.com.pl

Spis treści

Wstęp

Rozwój technologii informatycznych oraz Internetu sprawiły, że współczesne przedsiębiorstwo to dynamiczny w swej formie e-biznes, stojący przed licznymi wyzwaniami natury prawnej, księgowej, podatkowej, itp.

Świat e-biznesu to m.in.:

- bankowość elektroniczna, w tym internetowa oraz zastosowanie tabletów czy telefonów komórkowych do regulowania płatności pieniężnych i monitoringu rachunków bankowych a także zapłata transakcji w wyniku wprowadzenia technologii zbliżeniowej;
- rozliczanie transakcji z kontrahentami i publiczno-prawnych z Zakładem Ubezpieczeń Społecznych (ZUS), Urzędem Skarbowym (US), Urzędem Celnym (UC) za pomocą programów finansowo-księgowych, a także konieczność systematycznej aktualizacji programów finansowo-księgowych do zmieniających się przepisów podatkowych (VAT, PDOP, PDOF) i niepodatkowych (np. ZUS);
- rozwój e-handlu;
- polityka bezpieczeństwa w firmie skutecznie chroniąca przed atakami hakerów;
- niezwykle wrażliwy prawnie proces gromadzenia i ochrony danych osobowych zgodzie z ustawą o ochronie danych osobowych, która wręcz rygorystycznie nakazuje chronić te dane.

Firmy stają więc przed koniecznością ponoszenia większych nakładów na działalność IT (aktualizacje oprogramowania, szkolenie personelu), a jednocześnie muszą robić zakupy i zabezpieczyć potencjalnych klientów przed cyberprzestępcami i wyciekiem poufnych danych.

Oddajemy do rąk Czytelników kolejny Zeszyt nr 9 cz. 1 w czasopiśmie „Przedsiębiorczość i Zarządzanie" (tom XV) zatytułowany *E-biznes i ochrona danych osobowych*, który stanowi wyraz najnowszych badań pracowników naukowych Społecznej Akademii Nauk i wielu praktyków z sektora IT, prawa i rachunkowości w przedmiocie dociekań naukowych i analiz badawczych.

W publikacji wyodrębniono trzy segmenty badań obejmujące obszary tematyczne:

1. Rachunkowość w rzeczywistości wirtualnej.
2. Ochrona danych osobowych w zasobach informatycznych.
3. Prawne aspekty ochrony przedsiębiorstw w przestrzeni wirtualnej.

Rzetelna analiza naukowa treści publikacji w powyższych obszarach pozwala wzbogacić dyskurs intelektualny i uzyskać odpowiedź na pytania:

– Jakie są korzyści i zagrożenia w prowadzeniu e-biznesu?
– Czym jest polityka bezpieczeństwa w firmie?
– Na ile programy finansowo-księgowe (programy komputerowe) przystają do zmieniającej się rzeczywistości księgowo-podatkowej i do ograniczenia ryzyka nierzetelnego prowadzenia ksiąg?
– Na czym polega instytucja identyfikacji praw autorskich w obszarze e-biznesu?

Wyrażamy przekonanie, że publikacja przyczyni się do pogłębienia wiedzy o korzyściach i zagrożeniach wynikających z posługiwania się w biznesie i codziennym życiu Internetem, a także będzie stanowić płaszczyznę do ciągłego edukowania się społeczeństwa w nowoczesnych technologiach informatycznych. Będzie to także niewątpliwie przyczynek do dyskusji odnośnie permanentnego dbania o bezpieczeństwo w sieci, ochronę danych osobowych i kreację nowych konkurencyjnych technologii. Będzie również refleksją nad miejscem i rolą firmy w świecie e-biznesu. Reasumując, to także istotny element wzmocnienia pozycji firmy w warunkach rywalizacji rynkowej zarówno na poziomie krajowym jak i zagranicznym.

Podziękowania pragniemy skierować do przedstawicieli samorządu terytorialnego i lokalnego biznesu z Brodnicy, z którymi współpraca naukowo-dydaktyczna Wydziału Zamiejscowego SAN w Brodnicy ma już wieloletnią tradycję, owocującą wydaniem kolejnego już Zeszytu Naukowego. Cieszy nas, że do twórczej współpracy włączył się Urząd Skarbowy w Brodnicy, którego uwagi odnośnie rozliczeń VAT, rzetelności w przygotowaniu kadr w zakresie rozliczeń publiczno-prawnych są wyjątkowo cenne i budujące poprawne i partnerskie relacje biznesu z organami podatkowymi.

Za pomoc w organizacji i współfinansowaniu projektu badawczego serdecznie pragniemy podziękować: władzom samorządu reprezentowanym przez Burmistrza Brodnicy Pana Jarosława Radacza i Starostę Brodnickiego Pana Piotra Boińskiego, Naczelnikowi Urzędu Skarbowego w Brodnicy Panu Markowi Kryś, przedstawicielom lokalnego biznesu – Panu Wojciechowi

Wojenkowskiemu – właścicielowi firmy VOBRO, oraz Panu Markowi Hildebrandt – Przewodniczącemu Rady Miasta Brodnica i właścicielowi sieci sklepów.

Dziękujemy Pani Hannie Szeląg – biegłemu rewidentowi, Prezesowi Kancelarii Biegłych Rewidentów Josef Welt Sp. z o.o. w Łodzi oraz Wójtowi Gminy Ozorków Panu Władysławowi Sobolewskiemu, którzy łącząc praktykę z teorią podatkowo-rachunkową przyczyniają się do rozwoju wspólnych badań i osiągnięć naukowych Społecznej Akademii Nauk.

Słowa podziękowania kierujemy również pod adresem recenzentów, których cenne uwagi przyczyniły się do nadania ostatecznego kształtu tej publikacji.

W imieniu autorów
Dr Andrzej Jackiewicz
Prof. dr hab. Łukasz Sułkowski

Rachunkowość w rzeczywistości wirtualnej

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 11-22

Andrzej Jackiewicz
Społeczna Akademia Nauk

Wirtualna księgowość – problemy identyfikacji dokumentów i rozliczeń podatkowych z tytułu VAT w programach komputerowych

Virtual accounting – problems with documents identification and VAT tax settlements in computer programs

Abstract: Fair goods and services tax settlement requires the identification of documents (invoices) in respect to the object and subject. Thus, it is necessary to recognize the subject of taxation and the object who has the right to issue invoices in domestic and international trade. In the light of changes in the regulations the turnover of e-invoices is important but it is essential as well to ensure that they are genuine and integral in trade.

Key words: identification of documents, e-invoices, e-controll, tax calculations.

Wstęp

Prowadzenie ksiąg rachunkowych (podatkowych) w podmiotach gospodarczych w warunkach zmieniających się przepisów prawa bilansowego i podatkowego stanowi znaczące wyzwanie w zakresie wiedzy i kompetencji służb finansowo-księgowych. Jednocześnie należy podkreślić, że współczesna księgowość to w dużej mierze księgowość elektroniczna, oparta na określonych zasobach informatycznych dotycząca programów finansowo-księgowych takich jak kadry, płace, gospodarka magazynowa, podatki, itp. Dość często jest to jeden program przystosowany do elektronicznego prowadzenia ksiąg, który zawiera wiele opcji niezbędnych do ewidencji dokumentów i rozliczeń podatkowych i niepodatkowych. Na tym tle istotnego znaczenia nabiera problem rzetelnej identyfikacji dokumentów stanowiących o rzetelności ksiąg, a także rozwój form elektronicznych w postaci e-faktur obniżających koszty transakcji, oraz problemy e-kontroli jak również brak pobrania danych z systemu informatycznego. To istotne wyzwania badawcze a zarazem podatkowe, bowiem dane z programu F-k (finansowo-księgowego

– w dalszej części zwanego F-k) służą do rozliczeń podatkowych i są weryfikowane w czasie e-kontroli.

Celem artykułu jest wskazanie roli i znaczenia rzetelnej identyfikacji dokumentów w podatku VAT w układzie podmiotowo-przedmiotowym, uwarunkowań e-fakturowania i konsekwencji e-kontroli w rozliczeniach podatkowych.

Prowadzenie ksiąg rachunkowych przy użyciu komputera w ustawie o rachunkowości

W art. 13 ust 2, 3, 4 i 5 ustawy o rachunkowości ustawodawca uregulował podstawowe zasady prowadzenia ksiąg rachunkowych przy zastosowaniu komputera. Do istotnych uwarunkowań prawnych w tym zakresie należy:

- posiadanie przez jednostkę oprogramowania umożliwiającego uzyskiwanie czytelnych informacji zapisów w księgach rachunkowych, ich wydrukowanie i przeniesienie na informatyczny nośnik danych;
- wskazanie nazwy programu przetworzenia danych;
- zapewnienie automatycznej kontroli ciągłości zapisów (danych);
- zapewnienie automatycznej numeracji stron, oznaczenie pierwszej i ostatniej oraz numerowanie kolejnych stron;
- wydrukowanie księgi nie później niż na koniec roku obrotowego;
- archiwizacja księgi poprzez przeniesienie na informatyczny nośnik danych.

W prowadzeniu ksiąg przy użyciu komputera podatnik powinien posiadać „Instrukcję użytkowania programu finansowo-księgowego", która zawiera co najmniej elementy opisane w art. 10 ust. 1 pkt 3 „c" ustawy o rachunkowości.

Identyfikacja podmiotowo-przedmiotowa dokumentów (faktur) a problem rzetelnych rozliczeń VAT

Zmiana zasad fakturowania i momentu powstania obowiązku podatkowego w podatku od towarów i usług w latach 2013–2014 spowodowała „rewolucję" w rozliczaniu podatku VAT. Rozpoznanie obowiązku podatkowego na podstawie art. 19a ustawy, tj. z chwilą dokonania dostawy (z wyjątkami), a nie z chwilą wystawienia faktury, spowodowało, że podatnicy (przedsiębiorcy) mogą przywiązywać mniejszą uwagę do treści faktury, jako dokumentu, który powinien odzwierciedlać faktyczny przebieg operacji gospodarczej. W tym zakresie w literaturze przedmiotu, a także interpretacjach

podatkowych i orzecznictwie WSA, NSA pojawia się postulat rozpoznania rzetelności faktur (jako dokumentu) w aspekcie podmiotowo-przedmiotowym. Na tym tle istotne jest m.in. orzecznictwo WSA dotyczące prawa do odliczenia podatku naliczonego bowiem podatnik poza fakturami nie posiadał żadnych innych dokumentów potwierdzających wykonanie usług udokumentowanych fakturami. WSA stwierdził, co następuje: „źródłem prawa do odliczenia podatku naliczonego nie jest sama faktura, lecz nabycie towaru lub usługi i wykorzystanie do wykonania czynności opodatkowanych. Tylko faktura rzetelna od strony podmiotowej i przedmiotowej, tzn. dokumentująca rzeczywistą czynność opodatkowaną podatnika, przez niego wykonaną i udokumentowaną tą fakturą daje jej odbiorcy uprawnienie do odliczenia wykazanego w niej podatku" [Wyrok I SA/Bk 165/14 WSA w Białymstoku z 10.07.2014].

Jak wynika z powyższego wyroku, WSA wskazał trzy segmenty „faktury rzetelnej" w aspekcie podmiotowo-przedmiotowym, tj.:

- faktura powinna dokumentować rzeczywistą czynność opodatkowaną,
- czynność wykonaną,
- czynność udokumentowaną fakturą.

Znacznie szerzej interpretację „podmiotowo-przedmiotową" przedstawił Dyrektor Izby skarbowej w Łodzi z dnia 23 sierpnia 2013 r. na podstawie pytania podatnika o stawkę VAT za drewno opałowe – czy zostawić 8% czy też 23%? Dyrektor wyjaśnił, co następuje:

- to podatnik jest zobowiązany do prawidłowego określenia przedmiotu opodatkowania;
- podatnik powinien prawidłowo zdefiniować i zaklasyfikować wykonanie czynności;
- to podmiot (podatnik) sam klasyfikuje prowadzoną działalność, swoje produkty, towary itp. wg PKWiU [Interpretacja indywidualna Dyrektora…, 2013, s. 16].

Jak łatwo dostrzec poprawna klasyfikacja przedmiotowa (przedmiotu opodatkowania) jest wyłącznie w gestii podatnika i stanowi zarazem wyzwanie dla służb finansowo-księgowych, a jednocześnie ryzyko podatkowe, jeżeli podatnik niewłaściwie rozpozna PKWiU i stawkę VAT, o czym przekonała się jedna z firm po kilku latach.

Przykład 1. Podmiot podatku – Spółka zastosowała preferencyjną 8% stawkę VAT. W toku kontroli podatkowej organ podatkowy badając rzetelność prowadzenia ksiąg podatkowych i rozliczeń z tytułu VAT nie dopatrzył

się uchybień. Nie zakwestionowano podstaw opodatkowania, terminów rozliczeń, zasadności zwrotu, obowiązku podatkowego. Jednak po dwóch latach fiskus zakwestionował obniżoną stawkę VAT i wydał decyzję określającą zobowiązanie w podatku VAT wraz z odsetkami. Izba Skarbowa utrzymała w mocy stanowisko pierwszej instancji. Spółka odwołała się do WSA, który przyznał rację organom podatkowym. Spółka złożyła kasację do NSA, który również podtrzymał stanowisko WSA na niekorzyść spółki. Z tej sprawy należy wyciągnąć poważne wnioski, sprowadzające się do tego, że to zadaniem podatnika (podmiotu gospodarczego) jest rzetelne rozpoznanie przedmiotu opodatkowania i stawki VAT, a w przypadku wątpliwości ograniczenie ryzyka podatkowego poprzez wystąpienie o interpretację podatkową, którą podatnik może zaskarżyć. Oznacza to również, że zastosowanie preferencyjnej stawki VAT na fakturze jest zawsze obarczone ryzykiem [opracowanie własne].

Podobnie sytuacja przedstawia się w przypadku wystawienia faktur, w których podatnik wykaże zwolnienie z podatku VAT. W tym przypadku, zgodnie z art. 106e ust 1, pkt 39 ustawy o VAT, gdy dostawa towarów lub świadczenie usług zwolnionych z podatku na podstawie art. 43 ust. 1 art. 113 ust. 1 i 9 ustawy lub przepisów wydanych w oparciu o art. 82 ust 3 ustawy, obowiązkiem podatnika jest wskazanie na fakturze podstawy prawnej zwolnienia, tj.:

1) przepisu ustawy o VAT lub przepisu wykonawczego;
2) przepisów dyrektywy 2006/112/WE, lub
3) innej podstawy prawnej, przykładowo w oparciu o PKWiU, PKOB.

Jeżeli podatnik zastosuje błędną stawkę lub zwolnienie – może złożyć korektę, prawnie skuteczną tylko w ściśle określonych warunkach, zgodnie z ordynacją podatkową.

Należy jednak zauważyć, że powołując się na przepis art. 43 ust. 1 ustawy, przykładowo w zakresie świadczeń medycznych zwolnionych z podatku – jest wiele wątpliwości i podatnik powinien dochować należytej staranności w rozpoznaniu podstawy prawnej zwolnienia. Przykładowo SP ZOZ „Alfa" świadczył usługi badania kierowców, na pozwolenia na broń, jako ratujące zdrowie i zastosował zwolnienie z VAT, podając podstawę prawną art. 43, ust 1, pkt 18 ustawy o VAT. Po dwóch latach w wyniku kontroli podatkowej, podatnik zobowiązany był zapłacić 186.383 zł tytułem korekty stawki na 23% i doliczenia odsetek. Gdyby główna księgowa rzetelnie rozpoznała przedmiot opodatkowania nie byłoby ryzyka podatkowego i utraty płynności [Korekta błędnej podstawy prawnej…2014, s. 66].

Problem rozpoznania podmiotu VAT dotyczy zarówno podmiotów krajowych, jak i podmiotów UE w przypadku transakcji wewnątrzwspólnotowych, eksportowych i w tej materii należy zweryfikować czy nie zachodzi wykluczenie, jako podmiotu **nieistniejącego** na podstawie art. 88 ust 3a ustawy o VAT. To bardzo poważne wyzwanie. Na podstawie rozważań, zarys koncepcji analizy podmiotowo-przedmiotowej faktur przedstawia tabela 1.

Tabela 1. Podmiotowo-przedmiotowy zakres analizy faktur

Zakres podmiotowy	Zakres przedmiotowy
- identyfikacja źródła kontrahenta; - od kogo, czy istnieje; - status podatnika: a) podatnik VAT UE (w systemie VIES); b) podatnik VAT krajowy; c) podatnik zwolniony podmiotowo; - adresy e-mail; - adresy doręczeń.	- przedmiot opodatkowania w tym prawidłowa klasyfikacja czynności; - rodzaj operacji gospodarczej i na podstawie jakiego dokumentu, np.: faktury, e-faktury, dowodu obrotu materiałowego, towarowego; - kontrola dowodów księgowych (merytoryczna i formalno-rachunkowa).

Źródło: opracowanie własne.

Na tle licznych oszustw w podatku VAT szczególnego znaczenia nabiera „dochowanie należytej staranności" służb finansowo-księgowych w rozpoznaniu podmiotu (kontrahenta) jak też od strony przedmiotowej, co wyraźnie zaznaczył Trybunał Sprawiedliwości UE [Wyrok Trybunału (trzecia izba) z dn. 21.06.2012] oraz silnie akcentuje Ministerstwo Finansów.

Faktury w formie elektronicznej (e-faktury) – problemy prawne obrotu

E-faktura to dokument zdematerializowany – wirtualny, ale ma zawierać wszystkie elementy faktury zawarte w art. 160e ustawy o VAT. Na tym tle pojawiły się wątpliwości czy brak przykładowo numeru podatnika VAT-UE w transakcjach wewnątrzwspólnotowych powoduje, że dokument ten nie będzie uznawany za fakturę w rozumieniu przepisów ustawy o VAT. W tym przypadku faktura zawierająca pewne braki, formalne błędy uprawnia podatnika do wprowadzenia jej do obrotu prawnego i daje prawo do odliczenia podatku naliczonego, pod warunkiem, że nie będzie wykluczona na podstawie art. 88 ust. 3a ustawy (pusta faktura) [Problemy interpretacyjne związane…, 2014, s. 11].

Zgodnie z treścią art. 106 m (autentyczność pochodzenia faktury) ustawy, podatnik określa sposób zapewnienia, tj.:

a) autentyczność pochodzenia;
b) integralność treści i czytelność faktury.

Przez autentyczność pochodzenia należy rozumieć pewność, co do tożsamości dostawy, usługodawcy lub wystawcy faktury.

Integralność treści i czytelność faktury należy określić, jako brak zmian w zakresie danych. Są to istotne kryteria dla rzetelności obrotu w aspekcie prawnym. Dokonując liberalizacji przepisów ustawy o VAT oraz pełnej implementacji Dyrektywy 2006/112/WE ustawodawca przyjął stanowisko, że integralność i czytelność mogą być spełnione przy zachowaniu „dowolnych kontroli biznesowych, które ustalają wiarygodną ścieżkę audytu między fakturą a dostawą towarów lub świadczeniem usług" (art. 106 m ust 4). Oznacza to, że podatnik sam zapewnia integralność treści i autentyczność pochodzenia e-faktury. Udostępnianie e-faktur podlega zatem akceptacji ich odbiorcy i może to być zgoda ustna, jak ma to miejsce obecnie w przypadku wielu firm. Zdarza się, że podatnik obawia się oszustw, „pustych faktur". W tej sytuacji, jeżeli będzie to umowa dorozumiana pomiędzy kontrahentami (stronami transakcji) to przykładowo ze wskazaniem adresów mailowych, osoby odpowiedzialnej za wystawienie faktury, co powoduje, że strony uważają, że dokumenty z tych stron są autentyczne i nie wymagają potwierdzenia.

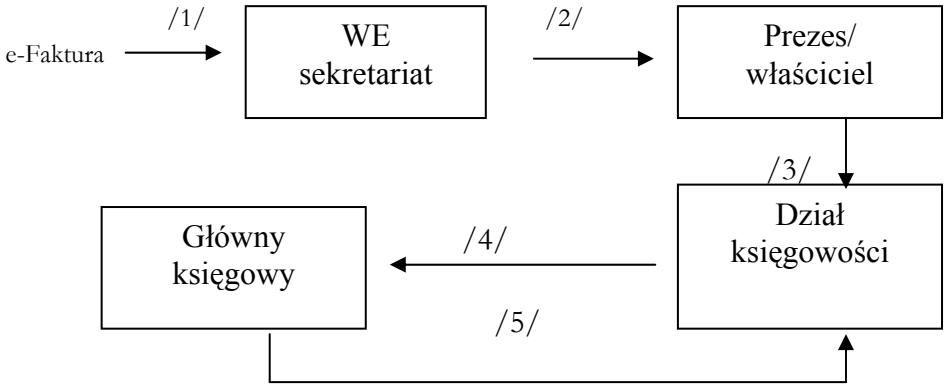
Autor tego artykułu doświadczył stanowiska, że dostawca nie zgodził się na takie warunki (z jakiej poczty e-mail wysyłane będą e-faktury, kto jest upoważniony do ich wystawiania), pozostały więc faktury papierowe. Rzetelność obrotu gospodarczego podatnik powinien zatem odpowiednio zabezpieczyć, rozpoznać kto jest dostawcą, czy firma znana, czy nowa na rynku, bowiem w świetle prawa akceptacja ustna stanowi zawarcie umowy. Istotne jest również stanowisko prezentowane w Leksykonie VAT [Sokołowska-Strug (red.), 2014, s. 354], zgodnie z którym zapewnienie autentyczności pochodzenia i integralności treści faktury należy realizować w sposób następujący:

a) zarówno sprzedawca jak i nabywca zobowiązani są do powiązania otrzymanych e-faktur z konkretnymi dostawcami towarów lub usług;
b) strony powinny precyzyjnie określić wystawcę faktury i sprzedawcę;
c) te zalecenia mają być realizowane poprzez wprowadzenie specjalnych zasad, które będą regulowały ścieżkę tworzenia, przesyłu, poboru e-faktury (np.: z jakiego adresu e-mail na jaki adres e-mali e-faktura ma zostać wysłana);
d) e-faktury w tym obrocie muszą być w formacie nieedytowalnym.

Te istotne wskazówki autora Leksykonu potwierdzają, że obrót e-fakturami wymaga dużej rozwagi i odpowiedzialności, co uchroni podatnika przed nierzetelnością w dokumentowaniu transakcji.

W praktyce zdarza się również, że mogą pojawić się przeszkody formalne, czy techniczne, które uniemożliwiają wystawienie i przesłanie e-faktury (np.: awaria systemu komputerowego, brak zasilania, itp.). Organy podatkowe wyrażają pogląd, że można w tym przypadku wystawić fakturę papierową pod warunkiem otrzymania powiadomienia od odbiorcy o wycofaniu akceptacji dotyczącej wystawienia e-faktury [Tamże, s. 355].

Rysunek 1. Przykładowy obieg e-faktur w firmie (po ich wcześniejszej akceptacji)



Opracowanie własne: na podstawie badań.

Opis schematu:

1. e-faktura wchodzi na pocztę sekretariatu;
2. pracownik sekretariatu, zgodnie z „Instrukcją kancelaryjną" rejestruje dokument, nadaje nr wchodzący i przesyła e-fakturę do Prezesa/właściciela firmy celem sprawdzenia pod względem merytorycznym (czy taka transakcja była, cena, itp.);
3. Prezes/właściciel firmy po sprawdzeniu pod względem merytorycznym przesyła do działu księgowości w celu sprawdzenia pod względem formalnym i rachunkowym oraz dokonanie dekretacji faktury;
4. dział księgowości przesyła e-fakturę do głównego księgowego, który sprawdza poprawność dekretacji, treści faktury, itp. Po akceptacji głównego księgowego e-faktura powraca do pkt.5;
5. e-faktura powraca do działu księgowości celem jej ujęcia w księgach.

Do omówienia pozostaje jeszcze jedna zasadnicza kwestia – czy akceptacja nabywcy oznacza, że dotyczy to wszystkich e-faktur od kontrahenta? W celu odpowiedzi należy przytoczyć stanowisko Dyrektora Izby Skarbowej w Poznaniu z 25.02.2011 r., które jest następujące: „przepisy nie nakładają obowiązku stosowania formy elektronicznej dla wszystkich faktur przesyłanych do danego kontrahenta, a tylko do faktur za konkretnie wskazane usługi, dla których kontrahent wyraził zgodę (akceptację)" [Faktury w formie elektronicznej i papierowej – sposób.., 2014, s. 66].

Z analizy treści wyjaśnień Dyrektora IS wynika, że zanim podatnik powie „tak" dla akceptacji e-faktur powinien przemyśleć swoje relacje biznesowe i problemy prawne dotyczące wymogów zapewnienia autentyczności i integralności e-faktury.

Z rozważań wynika również postulat aktualizacji w firmie „Instrukcji obiegu i kontroli dokumentów i dowodów księgowych" niezbędnej w poprawnej autoryzacji obrotu gospodarczego. Istotne jest również przyjęcie określonej formuły obrotu e-fakturami w firmie, co autor prezentuje na rysunku 1.

Jest to przykładowy schemat obiegu e-faktury, który w zależności od specyfiki może być modyfikoany celem dostosowania do struktury organizacyjnej podmiotu. Należy jednak wskazać, aby e-faktura wprowadzona do obiegu w danej firmie nie mogła być „skasowana" w obiegu, co powinno być odpowiednio zaprogramowane w systemie elektronicznego obiegu dokumentów oraz programie F-k.

E-kontrola jako forma weryfikacji rozliczeń podatkowych

Rozwój księgowości (rachunkowości) komputerowej stał się faktem. Firmy mają do dyspozycji różne programy dostępne na rynku, które mogą użytkować na podstawie:

a) przeniesienia prawa własności na nabywcę, co występuje w praktyce i poprawnie skonstruowanej umowy, ale może też być w formie;
b) licencji na użytkowanie programu F-k (licencja jako uprawnienie z patentu) z prawem do aktualizacji programu lub też nie. Należy rzetelnie przygotować odpowiednią umowę z licencjodawcą (na jaki okres, jakie warunki, itp.);
c) nabycia programu F-k nieodpłatnie, jako dodatku do czasopism, w ramach promocji firm.

Udokumentowanie nabycia programu należy do podatnika. Organy podatkowe czy skarbowe powołując się na art. 286 §1 pkt 4 mogą „pobierać

dane w formie elektronicznej" z programu komputerowego firmy (elektronicznego systemu finansowo-księgowego). W tej sytuacji organy kontrolne (US, UKS) mogą zażądać m.in.:

– przekazania pisemnej informacji o rodzaju używanego oprogramowania w tym:
  a) nazwy producenta;
  b) wersji oprogramowania;
  c) daty rozpoczęcia użytkowania w księgowości;
  d) tworzenia i obsługiwania przez ten program rodzajów formatów plików (w tym także, z których i do których można konwertować i eksportować dane) [Żujewska, 2012, s. 14].

Jednym z istotnych warunków rzetelnego prowadzenia ksiąg podatkowych (rachunkowych) jest posiadanie przez podmiot „Instrukcji użytkowania programu F-k".

W toku wszczęcia kontroli podatkowej kontrolujący sprawdzają m.in.:

1) czy operacje gospodarcze dokumentowane i rejestrowane są ręcznie czy w programie F-k;
2) czy program posiada licencję;
3) czy dokumenty mogą być przesyłane drogą mailową (pliki tekstowe, czy PDF, Excel), każda forma jest przyjęta;
4) podatnicy mogą przekazać dane z programu, w tym również drogą mailową;
5) organy kontrolne weryfikują:
   a) NIP podatnika;
   b) sprawdzają kontrahentów;
   c) czy kontrolowany program rzetelnie rozlicza VAT;
   d) gdy zostaną stwierdzone nieprawidłowości, podatnik zostaje zobowiązany do okazania dokumentów (czy są rzetelne, czy sprawdzono podatnika w systemie VIES);
   e) kolejność wystawiania faktur, rachunków (czy zachowana czy też nie, podatnik może anulować fakturę, która nie może być w obiegu, obrocie prawnym, czy obrót fakturami papierowymi czy e-fakturami, czy poprawny termin powstawania obowiązku podatkowego, co ma wpływ na rzetelność rozliczeń VAT i kwotę zobowiązania lub nadwyżki podatku naliczonego nad należnym, są różne terminy powstania obowiązku podatkowego, np. w turystyce, robotach budowlanych, itp. – w zależności od stanu prawnego VAT) czy faktury zakupu przykładowo dwie takie same, ten sam numer (fv nr …) – więc należy sprawdzić kontrahentów;

f) sprawdzenie, weryfikacja czy nie występują podmioty wrażliwe (które dokonują oszustw w podatku VAT[1]);
g) kontrola podatkowa obejmuje ściśle podany okres (rok, 2 lata, półrocze, itp.).

Należy podkreślić, że organy kontrolne (US, UKS) posiadają odpowiednie narzędzia analityczne (programy) do weryfikacji rozliczeń podatkowych w ściśle określonych programach F-k. W tej sytuacji istotne jest:

a) znać program F-k (jakie opcje rozliczeń VAT, kosztów, korekty kosztów, korekty VAT, sporządzanie deklaracji i ich korekt);
b) czy program jest aktualizowany na bieżąco;
c) jakie rozliczenia podatkowe należy generować ręcznie.

To tylko niektóre wskazówki jakże niezbędne w rzetelnych rozliczeniach podatkowych i weryfikowane w e-kontroli.

Problemy rozliczeń podatku VAT w programach F-k

Kluczowy problem – jakim jest rzetelność prowadzenia ksiąg rachunkowych – jest ściśle uwarunkowany elektronicznym przetwarzaniem danych w programie F-k. Panuje przekonanie (nie u wszystkich głównych księgowych), że program „załatwi" wszystko, wystarczy wprowadzić odpowiednie dokumenty, zadekretować operację itp. Nic bardziej mylnego, bowiem zmiany podatkowe, w tym podatku od towarów i usług, pdof, pdop sprawiają, że niezbędna jest stała ingerencja bezpośrednia i monitoring głównego księgowego w system rozliczeń podatkowych w zakresie jego dostosowania do dynamiki rozwoju firmy i zmienności wymogów przepisów podatkowych. Na podstawie przeprowadzonych badań w biurach rachunkowych z regionu Łodzi autor dokonał specyfikacji problemów rozliczeń podatku VAT wg stanu na lipiec-sierpień 2014 r.

Ograniczenia opcjonalne (programistyczne) programów w zakresie ewidencji i prawidłowego deklarowania podstawy opodatkowania VAT są następujące:

– „złe długi" brak powiązań pomiędzy terminami płatności (rozrachunkami) a rejestrami VAT. Ewidencja i deklarowanie korekty VAT w związku z brakiem zapłaty (zarówno dostawcy jak i odbiorcy) wymaga ręcznego tworzenia dodatkowych rejestrów w programach i późniejszego ich korygowania w przypadku zapłaty;

[1] Przedstawiony zakres czynności e-kontroli wynika z doświadczeń autora w pracy na stanowisku kontrolera wewnętrznego i biegłego w sprawach sądowych.

- VAT od samochodów – dopiero teraz, po pół roku obowiązywania ustawy zaczynają pojawiać się aktualizacje programów dostosowujące je do wyliczania 50% VAT od wydatków z wiązanych z samochodami osobowymi w działalności mieszanej. Opcji takich nie było również przy wcześniejszych limitach 50 i 60% odliczania VAT od leasingu czy najmu. Wyliczenie kwoty odbywało się ręcznie na fakturze, w osobnych ewidencjach poza programami i należało również pilnować przekroczenia granicy limitu odliczenia (5.000,00 i 6.000,00 zł);
- transakcje nabyć wewnątrzwspólnotowych – konieczność wystawiania poza programem faktur wewnętrznych (bądź ich ekwiwalentów w dobie obecnego braku obowiązku ich wystawiania) oraz konieczność ich oddzielnego księgowania;
- nietransakcyjne przemieszczanie towarów – brak mechanizmów ewidencyjnych powiązanych z występowaniem obowiązku podatkowego w pdof/pdop a VAT, mimo zaksięgowanego wcześniej dokumentu, istnieje konieczność ręcznego przeliczania faktur wg ustawy, czyli po kursie z 15-dnia następującego po miesiącu dostawy;
- niektóre programy nie przewidują korekty VAT-UE, dochodzi więc do sytuacji, w których deklaracje wysyłane są elektronicznie, a ich korekty pocztą z wyjaśnieniem;
- niektóre programy (bardzo zresztą dobre merytorycznie i technicznie) nie mają aplikacji do podpisu elektronicznego;
- system nie rozpoznaje obowiązku podatkowego (tj. z chwilą wydania towaru, wykonania usługi, a nie z chwilą wystawienia faktury);
- zmiana zasad odliczenia podatku naliczonego (warunkiem nie tylko dokonanie dostawy, wykonanie usługi, ale koniecznym jest posiadanie faktury. Zatem podatek należny powstaje z chwilą dokonania dostawy, ale odliczenie podatku naliczonego u nabywcy pod warunkiem posiadania faktury);
- rozliczanie VAT strukturą zakupów, programy nie wyodrębniają czynności sporadycznych, nie podlegających opodatkowaniu, ponadto na tle niejednorodnych interpretacji podatkowych powstaje problem określenia w mianowniku przychodów nie podlegających opodatkowaniu.

To tylko niektóre problemy. Odnosząc się przykładowo do „ulgi na złe długi" [Kiedy dłużnik musi skorygować… 2014, s. 51–53] programy nie są skorelowane pomiędzy nieterminowo opłaconą fakturą, ujętą już w księgach i upływem terminu zapłaty w ciągu 150 dni od upływu terminu płatności wykazanego na fakturze lub zawartego w umowie pomiędzy stronami.

Należy zatem przypomnieć, że w deklaracji VAT-7, wpisuje się osobę która sporządziła deklarację i ponosi odpowiedzialność z tego tytułu.

Podsumowanie

1. Identyfikacja dokumentów w ujęciu podmiotowo-przedmiotowym (kontrahenta, strony transakcji, przedmiot opodatkowania – czynność) jest warunkiem rzetelnego prowadzenia ksiąg podatkowych i rozliczania VAT.
2. Wiele operacji gospodarczych w podatku VAT program F-k nie jest w stanie wygenerować. Niezbędna jest ingerencja głównego księgowego, pod warunkiem bardzo dobrej znajomości przepisów i zmian prawa podatkowego oraz parametrów użytkowych programu F-k.
3. Księgi prowadzone komputerowo (elektroniczne zasoby informatyczne) stanowią dowód w postępowaniu podatkowym. Forma e-kontroli sprawia, że użytkownik programu (podatnik) powinien być w każdej chwili gotowy do przekazywania danych o programie i przesyłania elektronicznego (on-line) wybranych rozliczeń ustalonych w przedmiocie kontroli.

Bibliografia

Faktury w formie elektronicznej i papierowej – sposób dokumentowania transakcji sprzedaży, (2014), Poradnik VAT, nr 8 (368) z 20.04.2014, wyd. Gofin, Gorzów Wlkp.

Interpretacja indywidualna Dyrektora Izby Skarbowej w Łodzi z dnia 23.08.2013 r., nr IPTPP4/443-448/13-2/MK, [w:] Stawka VAT przy sprzedaży drewna opałowego, Gazeta Podatkowa, nr 80 z 07.10.2013.

Kiedy dłużnik musi skorygować VAT naliczony, (2014), Poradnik VAT, nr 9 (369) z 10.05.2014, wyd. Gofin, Gorzów Wlkp.

Korekta błędnej podstawy prawnej na fakturze, (2014), Poradnik VAT, nr 10 (370) z 20.05.2014 r., wyd. Gofin, Gorzów Wlkp.

Problemy interpretacyjne związane z określoną w ustawie definicją faktury, (2014), Poradnik VAT nr 5 (365) z dn. 10.03.2014, wyd. Gofin, Gorzów Wlkp.

Sokołowska-Strug E. (red.) (2014), *Inne metody zapewniające przesłanie e-faktur*, [w:] Leksykon VAT, 2 wydanie CH Beck, Warszawa.

Ustawa z dn. 11.03.2014 r. o podatku od towarów i usług (Dz. U. z 2011 r., nr 177, poz. 1054 z późn. zm.)

Ustawa z dn. 29.09.1994 r. o rachunkowości (stan prawny styczeń 2014).

Wyrok Trybunału (trzecia izba) z dn. 21.06.2012 r, http://eur-lux.europa.eu, 07.11.2012, godz. 18.05.

Wyrok WSA w Białymstoku z 10.07.2014 r. – I SA/Bk 165/14.

Żujewska M. (2012), *Jak fiskus e-kontroluje podatników*?, Gazeta podatkowa, nr 93 z 19.11.2012.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 23-36

Monika Podolska, Beata Pesta
Dariusz Szczepański
Szpital Brodnicki

Zintegrowany system informatyczny SP ZOZ w Brodnicy jako źródło informacji o kosztach i podstawa efektywnego zarządzania

Integrated information system in Health Care Center in Brodnica

Abstract: The authors present the problems related to the takeover of the Health Care Center in Brodnica and implementation of information system, including processing and protection of personal data. They present the list of modules, the principles of making copies of databases and giving access to the third party to the bases or their parts. In this light it is important to point out a cost account and a precise calculation of the expenses which are necessary for effective hospital management.

Key words: implementing information systems, financial plan, structure of revenues, description of information systems, data processing and protection.

Problemy związane z etapem przejęcia Zespołu Opieki Zdrowotnej w Brodnicy

Na mocy umowy zawartego porozumienia z dnia 22.03.2013 r. pomiędzy Powiatem Brodnickim a Gmina-Miasto Grudziądz Szpital Brodnicki od 1 kwietnia 2013 r. stał się jednostką samodzielną, a podmiotem tworzącym został Powiat Brodnicki. Wpis ten jest podstawą do funkcjonowania szpitala, jako samodzielnej jednostki, która świadczy usługi medyczne.

W procesie rozłączania szpitali brodnickiego i grudziądzkiego Kujawsko-Pomorski Oddział NFZ udzielił zgody na cesję kontraktów, kontrakty z NFZ zostały przejęte przez ZOZ w Brodnicy w proporcji 9/12. Kontrakt na 9 miesięcy roku 2013 r. wyniósł 15 841 179,00 zł. Wartość tegoż kontraktu, który jest bardzo niski, nie odzwierciedlała potrzeb prawie 80 tysięcznej liczby mieszkańców powiatu, ani tym bardziej wskaźników epidemiologicznych. Zgodnie z porozumieniem Regionalny Szpital Specjalistyczny w Grudziądzu dokonał zwrotu mienia nieruchomego i ruchomego, w tym wyposa-

żenia oraz sprzętu niezbędnego do prowadzenia dzielności medycznej. Regionalny Szpital Specjalistyczny dokonał również przekazania umów cywilno-prawnych oraz zwrotnego przekazania pracowników przejętych od ZOZ w Brodnicy zgodnie z art. 23^1 Kodeksu Pracy. Szpital został przejęty bez zadłużenia.

Od rozpoczęcia samodzielnej działalności szpitala trzeba go dokapitalizować, przeznaczając środki pieniądze, na zakup i wdrożenie zintegrowanego systemu informatycznego, który warunkuje m.in. samodzielne rozliczanie się z NFZ. Koszt zakupu i wdrożenia zintegrowanego systemu informatycznego w ZOZ w Brodnicy wyniósł 429 270 zł. Dzięki zaangażowaniu pracowników udało się wdrożyć system informatyczny przed planowanym terminem. Od 01.08.2013 r. szpital uzyskał możliwość samodzielnego rozliczania z NFZ, bez pośrednictwa Szpitala w Grudziądzu.

Na rozpoczęcie samodzielnego funkcjonowania szpital otrzymał od Powiatu Brodnickiego pożyczkę w wysokości 1.000.000,00 zł oraz zaciągnął kredyt w rachunku bieżącym w Banku Spółdzielczym w wysokości 1.500.000,00 zł. Ponadto ZOZ w Brodnicy otrzymał z Powiatu Brodnickiego, Urzędu Miasta, Stowarzyszenia „Nasz Szpital" oraz Fundacji, w ramach podpisanych umów nieodpłatnego użytkowania sprzęt medyczny i wyposażenie na kwotę ogółem 729.779,90 zł. Zespół Opieki Zdrowotnej w Brodnicy pomimo niedoszacowanego kontraktu kupił w 2013 roku z środków własnych sprzęt i urządzenia medyczne na kwotę 311.443,79 zł. W planach na lata 2014–2016 jest pełne odtworzenie urządzeń i sprzętu medycznego wymaganego zawartymi kontraktami z NFZ, np.: tomografu, RTG, USG i inne. Powyższe zakupy finansowane będą ze środków własnych i obcych.

Trudne początki funkcjonowania Szpitala – wdrażanie systemów informatycznych

Szpital brodnicki zmagał się z wieloma trudnościami okresu przejściowego, min.: niedoszacowanym kontraktem i nieprawidłową strukturą organizacyjną, której efektem był 105% wskaźnik wynagrodzeń osobowych w stosunku do przychodów z NFZ.

Również ważnym jak i nieodzownym element w rozpoczęciu dzielności szpitala był koszt zakupu i wdrożenia zintegrowanego systemu informatycznego, który warunkował między innymi:

- samodzielne rozliczanie się z NFZ,
- wdrożenie systemu kadrowo- płacowego,
- uruchomienie apteki szpitalnej,

- sporządzaniu struktury kosztów bezpośrednich,
- sporządzaniu struktury ośrodków kosztów,
- stworzenie gospodarki kasowej,
- stworzenie gospodarki magazynowej,
- stworzenie odpowiednich aplikacji do analizy i sprawozdawczości finansowej,
- modernizacja systemu ESKULAP,

Koszt zakupu i wdrożenia systemu były bardzo wysoki kształtował się na poziomie 429 270,00 zł, które pokrył Powiat Brodnicki. W maju 2013 roku z powodzeniem ukończono starania szpitala o ponowne uruchomienie Podstawowej Opieki Zdrowotnej Nocnej i Świątecznej finansowanej z NFZ, którą utracił grudziądzki zarządca szpitala. Szpital brodnicki zgłosił Kujawko-Pomorskiemu Oddziałowi NFZ w Bydgoszczy gotowość uruchomienia SOR-u. Spełnione zostały wszystkie wymagania dla tego oddziału i od 06.06.2013 r. SOR zaczęto przyjmować pierwszych pacjentów.

Skutecznie przeprowadzone postępowanie przetargowe na wyłonienie dostawców usług sterylizacji, wyżywienia, leków, materiałów opatrunkowych i sprzętu jednorazowego użytku oraz systemu informatycznego umożliwiły od 01.08.2013 r. usamodzielnienie i niezależność od RSS w Grudziądzu.

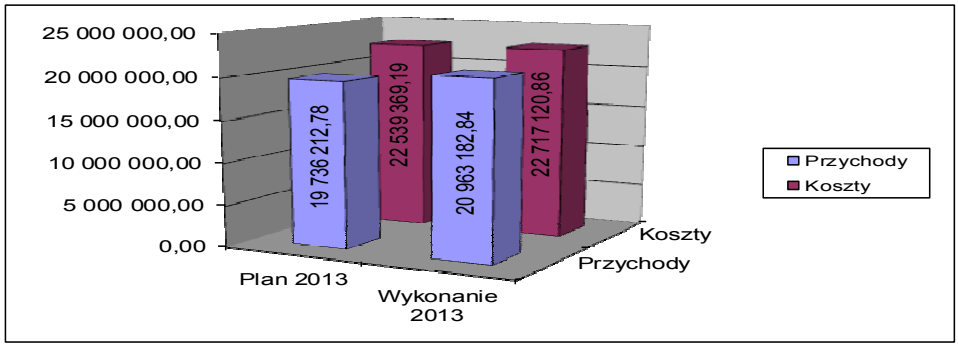
Na koniec września 2013 r. dyrektor szpitala Dariusz Szczepański poinformował, że już po 5 miesiącach od usamodzielnienia szpital uzyskał po raz pierwszy dodatki miesięczny wynik finansowy.

Realizacja rocznego planu finansowego Zespołu Opieki Zdrowotnej w Brodnicy

Roczny plan finansowy (od 01.04.2013–31.12.2013) Zespołu Opieki Zdrowotnej w Brodnicy po wprowadzonej korekcie zakładał uzyskanie przychodów w wysokości 19.736.212,78 zł, zaś planowane koszty wynosiły kwotę 22.539.369,19 zł, a więc planowana strata na koniec 2013 roku miała wynieść 2. 803.156,41 zł (po dodaniu kosztów amortyzacji 2.157.755,76 zł).

Na dzień 31.12.2013 roku uzyskano przychody ogółem w wysokości 20.963.182,84 zł, tj. o ponad 6% więcej niż zakładano, zaś koszty wyniosły 22.717.120,86 zł. Tym samym uzyskano stratę w wysokości 1.753.938,02 zł (po uwzględnieniu amortyzacji – 1.144.748,34 zł). Plan i wykonanie przychodów i kosztów za 2013 rok przedstawia rysunek 1.

Rysunek 1. Plan i wykonanie przychodów i kosztów ZOZ w Brodnicy w 2013 roku



Źródło: opracowano na podstawie zapisów księgowych Szpitala w programie FK „Simple".

Należy stwierdzić, iż osiągnięty ujemny wynik finansowy za 2013 rok w stosunku do planowanego jest o 47% niższy niż zakładano (po uwzględnieniu amortyzacji). Przeprowadzone prace związane z wdrożeniem w IV kwartale 2013 r. Programu Optymalizującego w ujęciu przychodowo – kosztowym, miały wpływ na ograniczenie ujemnego wyniku. Do najważniejszych uzyskanych efektów realizacji w/w programu można zaliczyć:

- Wygenerowanie po 5 miesiącach samodzielnej działalności dodatniego wyniku finansowego;
- Zwiększenie zakresu wykonywanych badań laboratoryjnych, co przyczyniło się do podwyższenia, jakości otrzymywanych wyników jak również do wzrostu przychodów od prywatnych odbiorców usług medycznych i Niepublicznych Zakładów Opieki Zdrowotnej oraz zmniejszenie kosztów usług zewnętrznych;
- Podjęcie współpracy z Komendą Powiatową oraz Prokuraturą Okręgową na wykonywanie badań medycznych i prosektoryjnych;
- Wdrożenie programu kontroli zużycia leków, materiałów i sprzętu jednorazowego użycia;
- Przeprowadzenie programu restrukturyzacji kosztów;
- przeprowadzenie programu restrukturyzacji przychodów z NFZ poprzez zwiększenie o ponad 3,5 mln złotych kontraktu w stosunku do przejętego na dzień 01.04.2013 roku;
- utrzymywanie względnej płynności finansowej (regulowanie w terminie wynagrodzeń oraz zobowiązań publicznoprawnych) pomimo niedoszacowanego kontraktu;
- rozstrzygnięcie 12 postępowań w ramach UZP na kwotę ponad 3 mln zł.;

- stałe doskonalenie funkcjonowania ZOZ w oparciu o autorski program „Optymalizacji funkcjonowania SP ZOZ w Brodnicy", który prowadzony był w zakresie restrukturyzacji, optymalizacji zatrudnienia, korzystania z usług zewnętrznych, zarządzania jakością.

Przychody i struktura

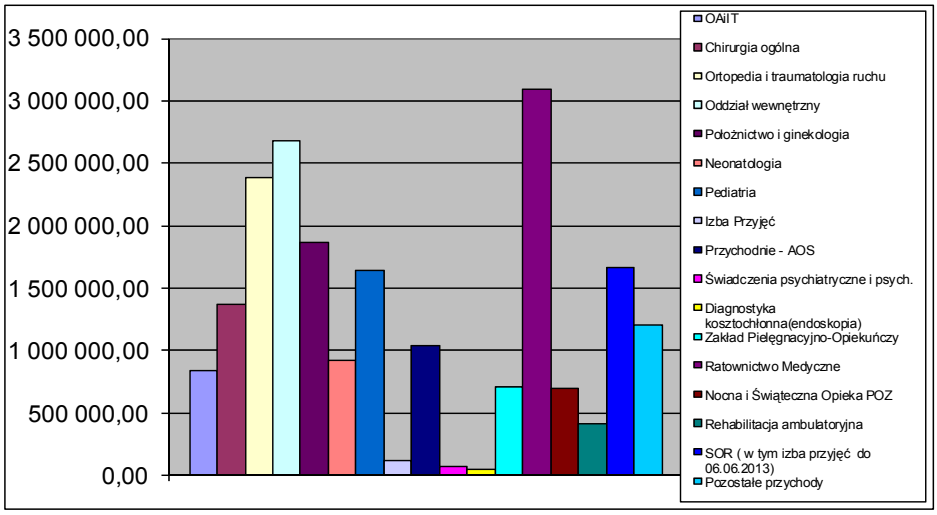
W okresie od 01.04.2013 r. do 31.12.2013 r. Zespół Opieki Zdrowotnej uzyskał przychody w wysokości **20.963.182,84 zł**. W strukturze uzyskanych przychodów największy udział stanowią przychody z NFZ – 93,4% (19.579.957,66 zł), kolejno pozostałe przychody operacyjne – 3,4% (717.232,91 zł) i pozostałe przychody medyczne 2,9% (610.762,70 zł).

Na prowadzanie działalności statutowej Zespół Opieki Zdrowotnej w Brodnicy uzyskał w 2013 roku fundusze, które pochodzą ze sprzedaży usług medycznych Narodowemu Funduszowi Zdrowia, sprzedaży badań diagnostycznych oraz usług medycznych podmiotom nieuprawnionym do bezpłatnego leczenia – płatne, pozyskał również fundusze z innej działalności gospodarczej (dzierżawienie powierzchni, wynajęcie sali w prosektorium, itp.). Na rysunku 2 pokazano przychody uzyskane przez poszczególne oddziały w okresie od 01.04.2013 r. do 31.12.2013 r.

W udziale procentowym przychodów w przychodach całkowitych w działalności ZOZ-u zachowana jest następująca proporcja: największy udział stanowią przychody z NFZ, następnie pozostałe przychody medyczne. Najwyższe przychody generuje „Ratownictwo Medyczne", „Oddział Wewnętrzny", Oddział Ortopedyczny". Najmniejszy udział w przychodach stanowią „Świadczenia psychiatryczne" i „Diagnostyka kosztochłonna".

Oceniając dynamikę przychodów planowanych do zrealizowanych należy zwrócić uwagę, iż szpital w 100% zrealizował w okresie od IV do XII 2013 roku przyznany limit z NFZ. Nie mniej jednak ZOZ wykonując zapisy Ustawy o Działalności Leczniczej z dnia 15.04.2011 r., art. 15 nie był uprawniony do odmowy udzielenia świadczenia zdrowotnego osobie potrzebującej natychmiastowej pomocy ze względu na zagrożenie życia lub zdrowia. W związku z powyższym pomimo restrykcyjnego przestrzegania limitu kontraktowego zawartego z NFZ, wystąpiły niezapłacone nadwykonania w kwocie 421.202,64 zł. Przedłożono do Dyrektora NFZ wniosek o zapłatę w/w kwoty za wykonane świadczenia w Zespole Opieki Zdrowotnej w Brodnicy.

Rysunek 2. Przychody uzyskane przez poszczególne oddziały w okresie od 01.04.2013 r. do 31.12.2013 r.



Źródło: opracowano na podstawie zapisów księgowych Szpitala w programie FK „Simple".

Komputeryzacja – przetwarzanie i ochrona danych osobowych – (koszty wprowadzenia)

Opis systemu informatycznego wykorzystywanego do obsługi części administracyjnej SIMPLE.ERP

Do obsługi informatycznej części administracyjnej ZOZ w Brodnicy wykorzystywany jest program SIMPLE.ERP firmy SIMPLE S.A. ul. Bronisława Czecha 49/51, 04-555 Warszawa SIMPLE.ERP. Jest Zintegrowanym Systemem Informatycznym zapewniającym spójną i kompleksową obsługę procesów gospodarczych w całym zakresie działalności zgodnie z obowiązującymi przepisami prawa. Aplikacja SIMPLE.ERP działa w architekturze klient-serwer. Serwer aplikacji jest zlokalizowany w pomieszczeniu serwerowni. Oprogramowanie działa w środowisku Windows; na serwerze zainstalowany jest system operacyjny Microsoft Windows Serwer 2008 R2, stanowiska kliencie posiadają systemy operacyjne z rodziny Microsoft Windows. Na serwerze dedykowanym dla aplikacji SIMPLE.EPR zainstalowana jest relacyjna baza danych wraz z instalacją klienta aplikacji. Dostęp do danych aplikacji realizowany jest poprzez połączenie aplikacji klienckiej zainstalowanej na komputerze danego pracownika z serwerem bazy danych. Silnikiem bazy danych dla SIMPLE.ERP jest Microsoft SQL Serwer 2008 R2.

Wykaz modułów

ZOZ w Brodnicy wykorzystuje następujące moduły programu SIMPLE.ERP: Finanse, Info, Majątek Trwały, Obrót towarowy, Personel.

Finanse – Opis producenta: „Obszar funkcjonalny FINANSE I KSIĘGOWOŚĆ SIMPLE.ERP stanowi doskonałe narzędzie zarządzania finansami jednostki, integrujące wszystkie dane finansowe oraz informacje dotyczące efektywności realizowanych procesów biznesowych. Wspiera prowadzenie rachunkowości firmy zgodnie z wymogami najnowszych przepisów prawa oraz obsługę ewidencji księgowej, zwiększając wydajność pracy działów księgowości".

Info – Opis producenta: „INFO jest biblioteką dodatkowych funkcji do popularnego arkusza kalkulacyjnego MS EXCEL i stanowi rozszerzenie funkcjonalności części FINANSE i KSIĘGOWOŚĆ SIMPLE.ERP. Moduł pozwala na tworzenie szeregu różnego rodzaju raportów, zestawień i analiz finansowych w czasie rzeczywistym".

Majątek Trwały – Opis producenta: „Obszar funkcjonalny MAJĄTEK TRWAŁY SIMPLE.ERP to system umożliwiający skuteczne wsparcie procesu zarządzania majątkiem trwałym jednostki poprzez pełną kontrolę nad rejestracją wszelkich zmian związanych ze składnikami majątku oraz ich historią. Wykorzystanie narzędzi informatycznych w prowadzeniu ewidencji ilościowo-wartościowej składników majątku trwałego, pozwala na znacznie efektywniejsze zarządzanie tymi składnikami".

Obrót towarowy – Opis producenta: „Obszar funkcjonalny SIMPLE.ERP OBRÓT TOWAROWY to skuteczne narzędzie pozwalające w pełni kontrolować procesy obrotu towarowego i w efektywny sposób zarządzać logistyką i dystrybucją w firmie, wpływając na poprawę jej rentowności i konkurencyjności. Wspomaga procesy zakupu i sprzedaży: zarówno krajowe, eksportowe jak i wewnątrzunijne oraz zarządzanie magazynami: własnymi i obcymi. Jego elastyczność pozwala na odzwierciedlenie w systemie SIMPLE.ERP wszystkich procesów biznesowych firm produkcyjnych, usługowo-handlowych jak i przedsiębiorstw sfery budżetowej".

Personel – Opis producenta: „Obszar funkcjonalny PERSONEL SIMPLE.ERP jest nowoczesnym narzędziem do zarządzania jednym z podstawowych zasobów każdej firmy – pracownikami. Przeznaczony jest do wspierania procesów zarządzania zasobami ludzkimi, zapewniając realizację wszystkich zadań związanych z obsługą personalną oraz płacową. Jest także narzędziem dostarczającym kadrze zarządzającej informacji, pozwalających w wygodny sposób analizować dane o pracownikach. Spełnia wszystkie wy-

mogi prawne dotyczące zatrudnienia w Polsce. Opis algorytmów i parametrów poszczególnych modułów programu SIMPLE.ERP został zamieszczony w dokumentacji systemu.

Przetwarzanie i ochrona danych

Serwer bazy danych i aplikacji Simple. ERP zlokalizowany jest w pomieszczeniu serwerowi, do którego dostęp jest chroniony poprzez system elektronicznej ewidencji dostępu – dostęp poprzez kod pin lub zaprogramowaną kartę magnetyczną. Dostęp do pomieszczenia serwerowni posiadają pracownicy Sekcji Informatycznej. Serwer zapisuje dane na dyskach twardych połączonych w macierz dyskową typu RAID 1 (mirroring) zabezpieczającą przed utratą danych z powodu awarii pojedynczego dysku. Raz na dobę w godzinach nocnych wykonywana jest kopia bazy danych, która jest powielana na inny zasób dyskowy oraz archiwizowana na taśmę magnetyczną. Udostępnienie osobie trzeciej zbiorów lub ich części:

1. Do wglądu na terenie jednostki – wymaga zgody kierownika jednostki lub osoby przez niego upoważnionej.
2. Poza siedzibą zarządu jednostki – wymaga pisemnej zgody kierownika jednostki oraz pozostawienia w jednostce potwierdzonego spisu przejętych dokumentów, chyba że odrębne przepisy stanowią inaczej.

Zasady archiwizacji pozostałych zbiorów określone są w instrukcji kancelaryjnej. Pozostałe zbiory przechowuje się zgodnie z ustawą.

System Eskulap

Kolejnym systemem komputerowym wykorzystywanym w Zespole Opieki Zdrowotnej w Brodnicy jest System Eskulap, który ma charakter modułowy zależący od potrzeb naszego szpitala. W ZOZ Brodnica wykorzystywane są następujące moduły: POZ, Blok Porodowy, Laboratorium, Bakteriologia, Pracownia Diagnostyczna, Zakład Histopatologii, Apteka, Ambulatoryjna Dokumentacja Medyczna, Rozliczenia z Płatnikami, Kalkulacja Kosztów Procedur, Rachunek Kosztów Leczenia, Blok Operacyjny, Poradnia, Gabinet, Dokumentacja Medyczna, Zlecenia Medyczne, Hierarchiczna Dokumentacja Medyczna, Ruch Chorych (Oddział + Izba Przyjęć + Statystyka), Archiwum, Gruper, Kolejki Oczekujących, Rejestracja Poradni, Apteczka Oddziałowa, Zakażenia Szpitalne, Pogotowie Ratunkowe, Żywienie, Poczta, HL7, Sterowniki do maszyn laboratoryjnych, Symulator JGP, Rehabilitacja.

Za pomocą modułu Kalkulacja Kosztów Procedur, Rachunek Kosztów Leczenia zostaje wdrażany system całkowitej weryfikacji kosztów procedur

szpitalnych. Wyliczanie procedur rozpoczęte zostało w Szpitalnym Oddziale Ratunkowym i Pracowni Endoskopii. Dzięki integracji systemu Eskulap z systemem SIMPLE jest możliwe pobieranie dekretów na koniec miesiąca z Działa Farmacji w celu zaksięgowania zużycia leków i materiałów opatrunkowych na poszczególnych ośrodkach kosztów. Wszelkiego rodzaju informacje związane ze zużyciem materiałów na poszczególnych ośrodkach kosztów otrzymać można na bieżąco dzięki odpowiednim zestawieniom uzyskanym z programu, są one istotne przy budżetowaniu, ponieważ można skontrolować stan zużycia poszczególnych materiałów w wyznaczonym dniu.

Struktura organizacyjna ośrodków kosztów Zespołu Opieki Zdrowotnej

Struktura organizacyjna w Zespole Opieki Zdrowotnej jest bardzo rozbudowana. Wiąże się przede wszystkim z zakresem działalności jednostki. Poziom analityki kosztów na poszczególnych ośrodkach została oparty na czterech poziomach (rysunek 3).

Rachunek kosztów w Zespole Opieki Zdrowotnej w Brodnicy

Rachunek kosztów ZOZ Brodnica składa się z trzech elementów:

1. Informacji medycznej o każdym pacjencie.
2. Systemu finansowo-księgowego.
3. Kontrolingu i zarządzania.

Istotnym elementem kalkulacji kosztów jest ich analiza na podstawie kosztów bezpośrednich i pośrednich. Lecząc pacjenta każdy szpital zadaje sobie następujące pytania: Ile kosztuje koszt hotelowy utrzymania pacjenta? Czy został efektywnie liczony i rozliczany? Czy określona procedura nie jest wyliczona w dobry sposób zgodny z normami? Czy szpital jest gotowy sprzedawać swoje usługi na zewnątrz?

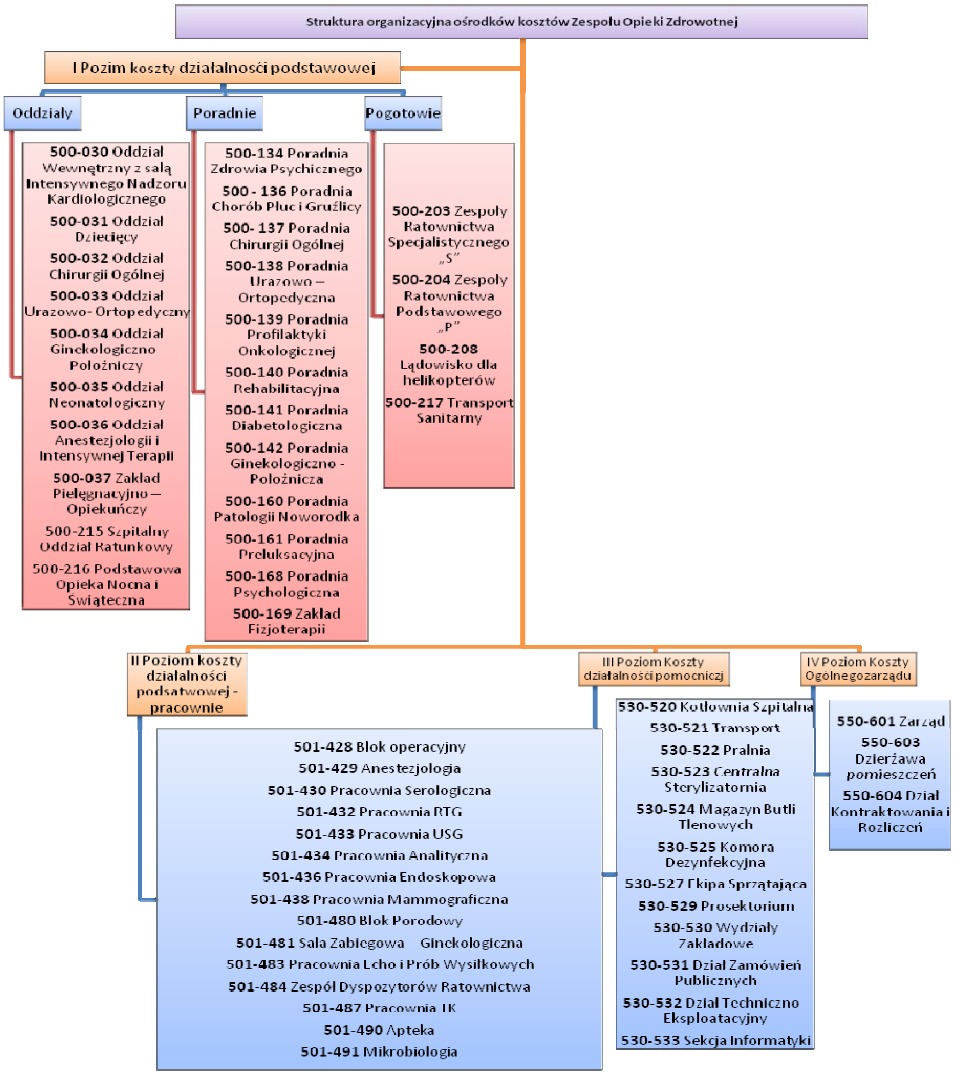
Wprowadzenie precyzyjnych wyliczeń kosztów jest elementem niezbędnym do prawidłowego zarządzania szpitalem. Dlatego tak istotne jest wyliczanie procedur za pomocą kart technologicznych, które obrazują m.in.:

- rzeczywiste zużycie określonych materiałów,
- rzeczywisty czas pracy określonych pracowników,
- rzeczywisty czas pracy określonych urządzeń,
- badania wykonywane wewnątrz i na zewnątrz szpital.

Precyzyjne wyliczenie kosztów określonych procedur jest podstawa zaradzania. Efektywny wyliczenie zapewnia informacje czy wykonywanie danej procedury jest opłacalne dla szpitala. Precyzja w wyliczaniu kosztów wiąże się również z księgowanie kosztów odpowiednio do ich miejsca wygenero-

wania, czyli na poszczególny ośrodek kosztów (załącznik 1) oraz za pocą analizy określonego kosztu (tabela 1).

Rysunek 3. Schemat struktury organizacyjnej ośrodków powstania kosztu Zespołu Opieki Zdrowotnej w Brodnicy



Źródło: opracowanie własne na podstawie Rozdzielnika Kosztów ZOZ Brodnica.

Koszty bezpośrednie księgowane są na poszczególnych ośrodkach kosztów po uprzednim opisaniu faktur, rachunków oraz zestawień przez osoby zobligowane do ich wykonania. Koszty pośrednie rozksięgowywane są na podstawie rozdzielników odpowiednio dopasowanych do ośrodka kosztów.

Tabela 1. Klucze podziałowe kosztów bezpośrednich

MIEJSCE POWSTANIA KOSZTU	KLUCZ
Bloku Operacyjny/Anestezjologia	Ilość punktów określonych za daną operację/zabieg
Pracownia: Serologiczna, Analityczna, Mikrobiologii, RTG, TK, USG, Mammografii	Wartość wykonywanych badań na ośrodkach kosztów.
Dyspozytornia Ratownictwa	Ilości wyjazdów Zespołów Ratownictwa
Apteka Szpitalna	Wartości zużytych leków
Transport	Przejechane kilometry
Centralna Sterylizatornia	Kosztu wykonanej sterylizacji
Magazyny Butli Tlenowych	Ilość wydanych butli
Komora Dezynfekcyjna	Ilość zdezynfekowanych materacy
Ekipa Sprzątająca	Czas sprzątania
Pralnia	Kilogramy prania
Prosektorium	Ilość zgonów
Wydziały Zakładowe: Dział Zamówień Publicznych, Sekcja Informatyki	Wskaźnik płac (wynagrodzenia + kontrakty) Zespołu Opieki Zdrowotnej
Zarząd	Wskaźnik płac (wynagrodzenia + kontrakty) Zespołu Opieki Zdrowotnej
Dział Kontraktowania i Rozliczeń	wskaźnik wartości kontraktu

Źródło: opracowanie własne na podstawie Rozdzielnika Kosztów ZOZ Brodnica.

Rozwiązywanie problemów kosztowych i decyzyjnych

Istotnym elementem związanym z kontrola i analizą poszczególnych kosztów stało się budżetowanie, które zostało wprowadzone z dniem 01.4.2014 roku. Limity wprowadzane zostały na te ośrodki kosztów, których zużycie było duże i bardzo zróżnicowanie w stosunku do jednostki czasu. Dlatego limity wprowadzono na: 401-01 Leki, 401-07 – Materiały opatrunkowe, 401-11 Tkaniny i bieliznę, 401-15 Artykuły biurowe. Zostały one przydzielone na podstawie analizy kosztów z okres I kwartału 2014 roku i obłożenia pacjentów. Budżetowanie wprowadzone zostało m.in. na:

- **500-030** Oddziale Wewnętrzny z salą Intensywnego Nadzoru Kardiologicznego
- **500-031** Oddziale Dziecięcy
- **500-032** Oddziale Chirurgii Ogólnej
- **500-033** Oddziale Urazowo-Ortopedycznym
- **500-034** Oddziale Ginekologiczno-Położniczym
- **500-035** Oddziale Neonatologicznym
- **500-036** Oddziale Anestezjologii i Intensywnej Terapii
- **500-037** Zakładzie Pielęgnacyjno-Opiekuńczym
- **500-215** Szpitalny Oddział Ratunkowym

Kontrola budżetowania przeprowadzana jest dwa razy dziennie za pomocą podglądu do zestawień programu SIMPLE (401-11 Tkaniny i bielizna, 401-15 Artykuły biurowe), Eskulap (401-01 Leki, 401-07 – Materiały opatrunkowe). Ważnym elementem kontroli kosztów było również wprowadzanie wydawania materiałów opatrunkowych przez Aptekę Szpitalną dniem 01.04.2014 r.

Duże znaczenie, jeżeli chodzi o kontrolę kosztów ma rozliczanie procedur za pomocą kart technologicznych, dzięki, którym znany jest rzeczywisty koszt wykonania danej usługi. Rozliczanie tych kosztów wprowadzane jest stopniowo za pomocą weryfikacji procedury sporządzanej przez pracownika danego oddziału, poradni czy pracowni i rozliczania przez pracownika księgowości. Koszty te rozliczane są za pomocą cenników zewnętrznych i wewnętrznych. Takie rozliczanie procedur medycznych pozwoli na kontrolę kosztów określonych zabiegów i procedur. Taki rodzaj kontroli pozwala stwierdzić czy dana usługa jest kosztochłonna i czy wykonanie jej na zewnątrz nie będzie tańszym kosztem.

Ponadto analiza wszystkich kosztów przeprowadzana jest na podstawie comiesięcznych zestawień. Dzięki nim możliwie jest stwierdzenie czy koszt na przykład na danym oddziale wzrósł czy spadł i czym było to spowodowane. Tak bardzo rozwinięta analiza jest możliwa dzięki możliwością, jakim dało wdrożenie program SIMPLE. Każda analiza jest oparta na podstawie faktur i rachunków wprowadzanych do systemu i rozksięgowywanych zgodnie z opisem.

Efekty działań po analizie kosztów

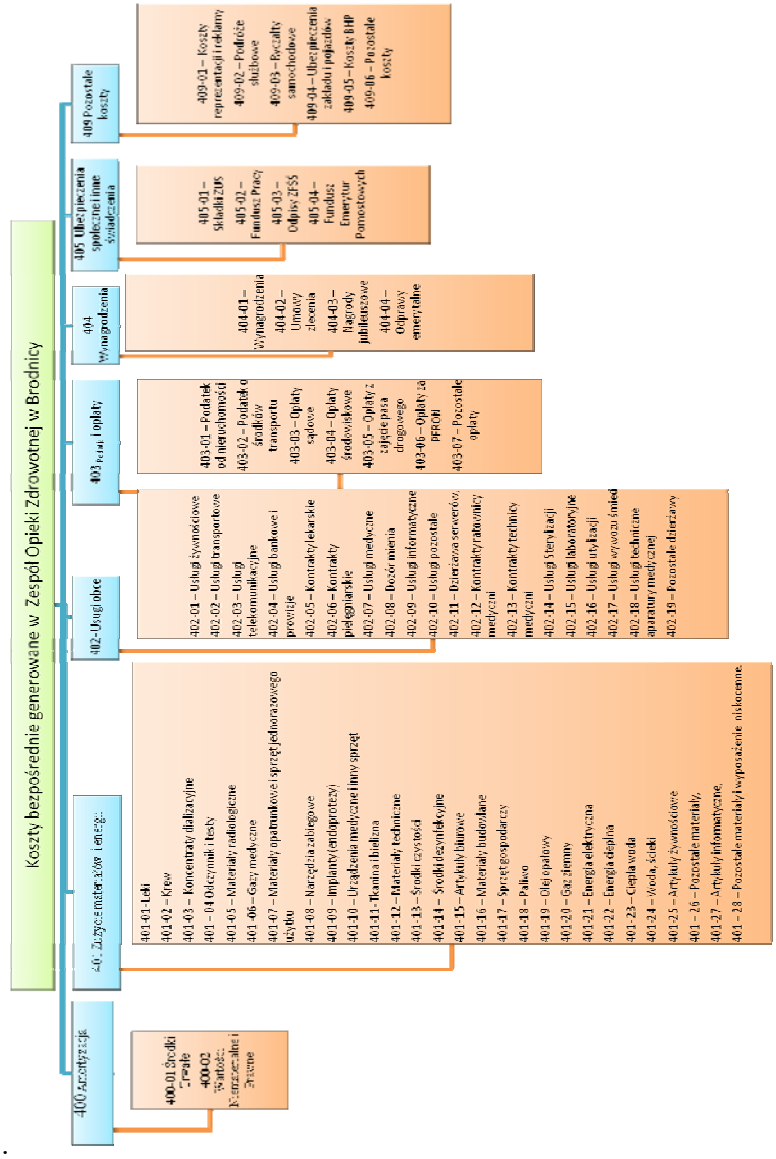
Efektem analizy kosztów poszczególnych jednostek jest wdrożenie etapami działań naprawczych. Po zapoznaniu się z poszczególnym kosztami na określonych ośrodkach kosztów rozpoczęto m.in.:

1. Optymalizacja zatrudnienia Zakładu Pielęgnacyjno-Opiekuńczego (6 etatów pielęgniarskich i 1 etat pracownika gospodarczego).
2. Redukcje zatrudnienia w Dziale Techniczno-Eksploatacyjnym (4 etaty pracowników gospodarczych).
3. Redukcje zatrudnienia Ekipy Sprzątającej (1 etat kierowniczy).
4. Redukcja zatrudnienia w Dziale Kontraktowania i Rozliczeń – połączenie tego działu z Sekcją Informatyki ze względu na wysoka informatyzacje rozliczeń NFZ (1 etat specjalisty ds. rozliczeń).
5. Reorganizacja i restrukturyzacja zatrudnienia pielęgniarek w zakresie Bloku Operacyjnego – przejścia na kontrakty.
6. Reorganizacja i restrukturyzacja etatów w Oddziale Chirurgii Ogólnej i Oddziale Urazowo-Ortopedycznym (2 pielęgniarki i 1 opiekun pacjenta).
7. Połączenie koordynacji Ratownictwa Medycznego ze Szpitalnym Oddziałem Ratunkowym (zamiast 2 – 1 koordynator).
8. Reorganizacja zatrudnienia w Zakładzie Radiologii (zmniejszenie ilości godzin, zmiana koordynatora).
9. W planach outsourcing pralni (likwidacja pralni szpitalnej i przejście na usługi zewnętrzne).

Najważniejszym elementem zarządzania Zespołem Opieki Zdrowotnej jest analiza i nadzór nad kosztami generowanymi na poszczególnych ośrodkach kosztów. Istotny wpływ na wszelkiego rodzaju cięcie kosztów ma ich kontrola w oparciu o dane finansowo-księgowe uzyskane z Systemu SIMPE i ESKULAP.

Modernizacja poszczególnych oddziałów, poradni, pracowni, opiera się na analizie kosztów bezpośrednich i pośrednich. Odpowiednio dobrane współczynniki wyliczania kosztów są kluczowe w księgowaniu. Analiza kosztów na poszczególnych ośrodkach kosztów jest podstawą do wprowadzania, których skutkiem będzie osiągniecie dodatniego wyniku finansowego. Wysoka informatyzacja i integracja systemów informatycznych daje możliwość efektywnego gospodarowania na każdym szczeblu Zespołu Opieki Zdrowotnej.

Znacznik 1. Schemat kosztów bezpośrednio generowanych



Źródło opracowanie własne na podstawie Rozdzielnika Kosztów ZOZ Brodnica.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 37-48

Ryszard Thiel
Urząd Skarbowy w Brodnicy

Zjawisko „pustych faktur" jako zagrożenie dla finansów publicznych i przedsiębiorców na wybranych przykładach oszustw podatkowych

The phenomenon of "empty invoices" in the light of revealed tax frauds and jurisdiction – legal and criminal aspects

Abstract: The phenomenon of "empty invoices", the so called fictitious invoices, leads to tax frauds, real tax fraud or dishonest cost documentation. The task of tax organs is to reveal such objects and to protect the public finance. The author presents selected examples of fictitious invoices based on the jurisdiction of the Provincial Administrative Court, Supreme Administrative Court and negative effects of such practice on economic objects.

Key words: empty invoices, ready-made companies, legal and criminal liability, tax fraud.

Wprowadzenie

Ze zjawiskiem pustych faktur i związanymi z nimi przestępstwami problem ma nie tylko Polska, ale również inne kraje Unii Europejskiej. Zjawisko to dotyczy różnych branż gospodarczych, bowiem w tym przypadku towarem jest głównie podatek, a nie rzeczywisty produkt. Przyczynami narastania tego problemu jest zarówno liberalizacja regulacji związanych z zakładaniem działalności gospodarczej i jej prowadzenie, jak również jednolitość unijnego rynku oraz swobodny przepływ towarów i usług.

Niniejszy artykuł ma na celu zobrazowanie jak nagannym zjawiskiem jest wprowadzenie do obrotu gospodarczego pustych faktur i jakie niesie zagrożenie dla Budżetu Państwa oraz jak w sposób bezpośredni dotyka uczciwych przedsiębiorców.

Definicja i mechanizm

Celem sprecyzowania, jakie zagadnienie podatkowe jest przedmiotem niniejszego opracowania należy na wstępie zdefiniować, co to są „puste faktury". Wypracowane przez organy podatkowe i orzecznictwo stanowisko pozwala na stwierdzenie, że za „puste faktury", które możemy także określić, jako faktury fikcyjne, uznamy taką dokumentację podatkową, która nie dokumentuje żadnej rzeczywistej transakcji, a jedynie została wytworzona wyłącznie w celu wyłudzenia podatku od towarów i usług, tj. prawa do odliczenia podatku naliczonego, jak również zaliczenia wykazanego w nich wydatku do kosztów uzyskania przychodów celem zmniejszenia zobowiązania podatkowego w podatku od towarów i usług oraz podatku dochodowym.

Analizując obszary występowania pustych faktur należy stwierdzić, że to zjawisko, występuje w prawie każdej branży działalności gospodarczej, niezależnie od rozmiaru prowadzonej działalności gospodarczej. Ponadto można stwierdzić, że puste faktury dokumentują zakup różnego rodzaju usług niematerialnych, jak również usług transportowych, budowlanych, szkoleniowych, informacyjnych, reklamowych, pośrednictwa, a także takich towarów jak: złom, artykuły elektroniczne, paliwa, złoto, części samochodowe.

Wprowadzenie do obrotu fikcyjnych faktur odbywa się przy okazji zupełnie legalnego obrotu gospodarczego, a polega to na wprowadzeniu przez przedsiębiorcę do obrotu gospodarczego kilku fikcyjnych faktur miesięcznie celem wygenerowania braku obowiązku zapłaty części podatku i wyprowadzenia pieniędzy z firmy, a bywa czasami także tak, że przedsiębiorca, który zatrudnia pracowników na „czarno", nie mogąc wypłacanych wynagrodzeń zaliczyć w koszty uzyskania przychodu, kupuje fikcyjne faktury. Są to jednak zjawiska, które w wyniku przeprowadzonej analizy możliwości technicznoosobowych badanego podmiotu gospodarczego i przeprowadzonych czynności sprawdzających można w miarę „łatwo" ujawnić. Jednakże organy podatkowe mają do czynienia z o wiele bardziej skomplikowanymi mechanizmami, które opierają się na rozbudowanych mechanizmach oszustw podatkowych i tworzeniu zorganizowanych grup przestępczych, które głównie mają na celu wyłudzenie podatku od towarów i usług.

Zjawisko fikcyjnych faktur znalazło także swoje odzwierciedlenie w opracowywanych przez Ministerstwo Finansów Krajowych Planach Dyscypliny Podatkowej, zgodnie z którymi w obszarze „Podmioty niezgłaszające działalności gospodarczej, znikające, zaprzestające składania deklaracji lub zawieszające działalność gospodarczą" podjęto próbę wskazania elementów charakterystycznych dla zjawiska fikcyjnych faktur i stwierdzono, że „szcze-

gólną odmianą przestępstw karuzelowych są przestępstwa typu łańcuchowego. Charakteryzują się one tym, że zazwyczaj ograniczają się do działalności w ramach jednego państwa, a obieg dokumentów nie posiada cech koła. Przykładem tego ostatniego jest tworzenie tzw. łańcucha podmiotów powiązanych z udziałem podmiotów nieprowadzących faktycznie działalności gospodarczej, tzw. słupy lub pełniących rolę „znikającego podatnika". W ramach łańcucha można wyróżnić wszystkie kategorie podmiotów występujące w klasycznej karuzeli z tym, że liczba podmiotów nieistniejących jest znaczna. Ostatnim ogniwem takiego łańcucha jest często podmiot dokonujący eksportu głównie do krajów, z którymi ograniczona jest wymiana informacji podatkowych (np. Rosja, Ukraina). Ma to na celu utrudnienie ujawnienia przestępczego charakteru transakcji i dotarcia do faktycznych inicjatorów przestępstwa wyłudzenia zwrotu VAT. W szczególności dotyczy to branży paliwowej oraz towarów o dużej wartości, lecz małych gabarytach, np. telefony komórkowe. Powyższy mechanizm przestępczy w zasadzie pozostaje cały czas niezmieniony (może ulegać jedynie modyfikacjom), zmieniają się natomiast towary wykorzystywane w procederze wyłudzania zwrotu podatku VAT z tytułu eksportu, którymi są np.: tekstylia, płyty CD z programem do interaktywnej nauki języka obcego, telefony komórkowe, drobna elektronika, itp.

Jednymi z cech charakteryzujących tę grupę podatników jest:

- brak możliwości technicznych wykonywania działalności gospodarczej w określonym zakresie np. obrotu paliwami;
- wskazywanie adresu siedziby i miejsca wykonywania czynności w miejscu zamieszkania, np. w mieszkaniu usytuowanym w budynku wielorodzinnym;
- niezgłaszanie wszystkich posiadanych rachunków bankowych związanych prowadzoną działalnością.

Celem podmiotów wprowadzających do obrotu fikcyjne faktury jest przede wszystkim zmniejszenie zobowiązań podatkowych w podatku od towarów i usług poprzez odliczenie podatku naliczonego z tych faktur, zmierzające często do wyłudzenia zwrotu podatku od towarów i usług z urzędu skarbowego. Analogiczna sytuacja dotyczy podatku dochodowego od osób prawnych/fizycznych, gdzie wprowadzenie ww. faktur w ciężar kosztów uzyskania przychodów prowadzi do zaniżenia zobowiązania podatkowego za dany okres rozliczeniowy.

Przestępstwa związane z wprowadzeniem do obrotu fikcyjnych faktur przybierają różne formy, począwszy od tych mniej skomplikowanych polegających na zakupie przez przedsiębiorcę jednej lub kilku fikcyjnych faktur w celu zmniejszenia obciążeń podatkowych, a skończywszy na tworzeniu

zorganizowanych struktur przestępczych, których celem jest w głównej mierze wyłudzanie nienależnych zwrotów podatku VAT.

Celem wyeliminowania tego zjawiska organy podatkowe winny wykorzystywać wszelkie informacje sygnalizujące o podejrzeniu występowania ww. przestępstwa podatkowego, a w szczególności od policji i prokuratury, urzędów kontroli skarbowej oraz z przeprowadzonych kontroli podatkowych.

Przy analizie zjawiska fikcyjnych faktur należy również zwrócić uwagę na mechanizm, w którym wykorzystywane są tzw. „ready-made spółki" (są to spółki sprzedawane, zarejestrowane z tzw. czystym kontem, tj. nigdy wcześniej nie prowadziły żadnych operacji gospodarczych i które są gotowe do podjęcia działalności w dniu ich nabycia). Są to spółki zarejestrowane pod jednym adresem przez osobę oferującą je do sprzedaży. Po sprzedaży, spółki te rozpoczynając swoją działalność wykazują bardzo wysokie obroty przy znikomych wpłatach podatku VAT, lub od razu wnioskują o zwroty podatku VAT. Przeprowadzane przez właściwy urząd skarbowy czynności kontrolne, dotyczące zasadności zwrotów kończą się wynikami niedającymi podstaw do wstrzymania zwrotów, gdyż dla udowodnienia popełnianych przestępstw konieczna jest wymiana informacji na poziomie administracji podatkowych krajów UE i przeprowadzenie czynności kontrolnych wobec kontrahentów polskiego podmiotu. Po pewnym, zwykle dość krótkim czasie, podmiot zmienia siedzibę i w innym województwie pod właściwością innego urzędu skarbowego kontynuuje wyłudzanie zwrotu VAT. Istotne jest także to, że pomimo wczesnego wykrycia procederu nie udaje go skutecznie zablokować. Dodatkowo spółki dokonują zgłoszeń rejestracyjnych VAT-R, w których deklarują składanie deklaracji kwartalnych natomiast faktycznie składają te deklaracje miesięcznie" [Krajowy Plan Dyscypliny Podatkowej Ministerstwa Finansów na 2012 r.].

Jak z powyższego wynika zjawisko pustych – fikcyjnych faktur może przybierać różne formy i sposoby ich wprowadzania do obrotu gospodarczego, ale charakteryzują się one jednym celem, zmniejszeniem wpływu danin podatkowych do Skarbu Państwa.

Celem zobrazowania jak naganne jest to zjawisko i jaka jest jego skala, dokonano w ujęciu tabelarycznym (tab. 1) wskazania wartości brutto ujawnionych faktur przez urzędy kontroli skarbowej w okresach półrocznych [Pokojska 2014].

Odnośnie wielkości ujawnionych, pustych – fikcyjnych faktur przez urzędy skarbowe nie pozyskano danych, ale należy zakładać, że skala tych wielkości jest również znaczna.

Tabela 1. Wartości brutto ujawnionych faktur przez urzędy kontroli skarbowej w okresach półrocznych

Urząd Kontroli Skarbowej	II półrocze 2012r.	I półrocze 2013r.	II półrocze 2013r.
Białystok	88 130 562,00	292 519 524,00	386 246 642,00
Bydgoszcz	1 012 584 395,94	1 548 817 367,21	972 343 620,79
Gdańsk	1 177 727 887,00	585 414 578,00	959 297 033,00
Katowice	**1 686 856 666,00**	**1 821 437 140,00**	990 566 195,00
Kielce	93 628 588,00	25 632 821,00	168 968 658,00
Kraków	287 856 630,00	945 947 824,00	1 095 541 826,00
Lublin	82 955 684,00	43 490 112,00	572 301 839,00
Łódź	119 300 000,00	405 000 000,00	815 000 000,00
Olsztyn	187 979 044,00	172 947 715,00	885 646 066,00
Opole	*24 786 842,00*	*4 151 817,00*	73 128 320,00
Poznań	228 096 326,00	1 288 321 128,00	996 947 788,00
Rzeszów	202 264 205,00	84 523 780,00	245 496 082,00
Szczecin	230 674 235,00	40 301 700,00	135 125 305,00
Warszawa	1 282 584 683,00	749 843 603,00	**1 308 108 825,00**
Wrocław	920 967 923,00	1 035 851 861,00	982 858 840,00
Zielona Góra	40 827 061,00	71 258 466,00	*9 957 959,00*
Ogółem	**7 667 220 731,94**	**9 115 459 436,21**	**10 597 534 998,79**

najwyższe wartości ujawnione

najniższe wartości ujawnione

Źródło: Pokojska 2014.

Celem wskazania, o jakiej wielkości należnego podatku od towarów i usług oraz wartości netto generowanej w koszty działalności gospodarczej mówimy, dokonałem wyliczenia tych wielkości i tak w:

- II półroczu 2012 r.: kwota podatku VAT wyniosła 1.433.707.941,75 zł, wartość netto wyniosła 6.233.512.790,19 zł;
- I półroczu 2013 r. kwota podatku VAT wyniosła 1.704.516.805,15 zł, wartość netto wyniosła 7.410.942.631,06 zł;

- II półroczu 2013 r. kwota podatku VAT wyniosła 1.981.652.885,96 zł, wartość netto wyniosła 8.615.882.112,83 zł;

Dopiero tak dokonana analiza obrazuje, z jaką skalą i wielkością oszustw podatkowych mamy do czynienia.

Odpowiedzialność wystawcy i nabywcy „pustych" faktur w świetle wybranego orzecznictwa oraz kodeksu karnego i kodeksu karnego skarbowego

W sytuacji, kiedy wprowadzimy faktury do obiegu, czyli przekażemy oryginały faktur innemu podmiotowi gospodarczemu, jesteśmy zobowiązani do zapłaty kwoty podatku VAT w wysokości, jaka została wykazana na tych fakturach. Stan taki określają przepisy art. 108 ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2011 r. nr 177, poz. 1054 z późn. zm.) zgodnie, z którym w przypadku, gdy osoba prawna, jednostka organizacyjna niemająca osobowości prawnej lub osoba fizyczna wystawi fakturę, w której wykaże kwotę podatku, jest obowiązana do jego zapłaty. Przepis ten stosuje się odpowiednio w przypadku, gdy podatnik wystawi fakturę, w której wykaże kwotę podatku wyższą od kwoty podatku należnego. Taka regulacja prawna oznacza, że bez względu na to, czy faktura rzeczywiście odzwierciedla stan faktyczny, jesteśmy zobowiązani do zapłaty podatku VAT w niej wykazanego, a podatek z „pustej faktury" nie podlega rozliczeniu w deklaracji. Winien on być odrębnie odprowadzony do urzędu skarbowego w terminie do 25 dnia miesiąca następującego po miesiącu, w którym została wystawiona faktura VAT lub w terminie do 25 dnia miesiąca następującego po kwartale, jeżeli wybraliśmy rozliczenie kwartalne.

W prawie wspólnotowym, odzwierciedleniem przepisu art. 108 ustawy o podatku od towarów i usług jest art. 203 Dyrektywy nr 2006/112/WE Rady Unii Europejskiej z dnia 28 listopada 2006 r. w sprawie wspólnego systemu podatku od wartości dodanej [Dz. Urz. UE L 347 z 11.12.2006, s. 1]. Stanowi on bowiem, że już samo wykazanie na fakturze określonej kwoty jako kwoty podatku VAT zobowiązuje podatnika do jej zapłaty.

Podkreślenia wymaga również fakt, iż art. 108 ustawy o podatku od towarów i usług podobnie jak ww. art. 203 Dyrektywy 2006/112/WE, ma charakter sanacyjno-prewencyjny i ma zapobiegać nadużyciom w systemie VAT. Należy stosować go z uwzględnieniem analizy, czy zaistniała sytuacja wytworzona faktem wystawienia faktury, niesie za sobą ryzyko jakiegokol-

wiek obniżenia wpływów z tytułu podatków, zgodnie z zasadą neutralności podatku od towarów i usług.

Takie uregulowanie jest wynikiem szczególnej roli faktury w prawie podatkowym, a w szczególności w zakresie podatku od towarów i usług, bowiem dla podatnika, który otrzymał fakturę wartość wykazanego w niej podatku naliczonego staje się podstawą do obniżenia podatku należnego, czyli zobowiązania podatkowego, lub też może prowadzić do żądania zwrotu podatku. Możemy więc stwierdzić, że w przypadku wystawienia faktury zawierającej wykazaną kwotę podatku, nawet jeżeli faktura taka nie odzwierciedla stanu faktycznego, adresat takiej faktury potraktuje wykazany w niej podatek jako podatek naliczony podlegający odliczeniu, a organy podatkowe nie ujawnią tej nieprawidłowości i dlatego zobowiązanie wystawcy faktury do zapłaty podatku bez względu na jego związek z czynnością opodatkowaną stanowi swego rodzaju ograniczenie możliwości dokonywania nadużyć prawa do odliczenia podatku [Fornalik 2003, s. 519].

Powyższe okoliczności prowadzą do stwierdzenia, że przepis art. 108 ust. 1 ustawy o podatku od towarów i usług przewiduje szczególny przypadek samoistnego powstania obowiązku podatkowego wskutek samego wystawienia faktury wykazującej kwotę podatku od towarów i usług. Obowiązek ten przyjmuje postać swoistej sankcji, która polega na tym, że niezależnie od tego, czy w sprawie zaistniał obrót będący podstawą opodatkowania podatkiem od towarów i usług oraz niezależnie od rozmiarów i konsekwencji podatkowych tego obrotu, każdy wystawca tzw. pustej faktury liczyć się musi z koniecznością zapłaty wykazanego w niej podatku.

Należy jednak pamiętać, że takie postępowanie jest również objęte sankcjami z Kodeksu Karnego lub Kodeksu Karnego Skarbowego zgodnie z art. 286 §1 kodeksu karnego kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. W kodeksie karnym skarbowym przewidziano natomiast szczególną regulację na mocy, której kto przez podanie danych niezgodnych ze stanem rzeczywistym lub zatajenie rzeczywistego stanu rzeczy wprowadza w błąd właściwy organ narażając na nienależny zwrot podatkowej należności publicznoprawnej, w szczególności podatku naliczonego w rozumieniu przepisów o podatku od towarów i usług, podatku akcyzowym, zwrot nadpłaty lub jej zaliczenie na poczet zaległości podatkowej lub bieżących albo przyszłych zobowiązań podatkowych, podlega karze grzywny do 720 stawek dziennych (do 16.128.000 zł. od

01.01.2014 r.) albo karze pozbawienia wolności, albo obu tym karom łącznie (art. 76 §1 k.k.s.).

W sytuacji, kiedy pomiędzy przedsiębiorcami dojdzie do porozumienia w celu wystawiania fałszywych faktur, nieodzwierciedlających prawdziwych transakcji, tylko po to, aby zmniejszyć kwotę należnego podatku od towarów i usług u kontrahenta podatnika to taka „pusta faktura" nie daje nabywcy prawa do odliczenia wykazanego w niej podatku, a reguluje to art. 88 ust. 3a pkt 4 lit. a ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2011 r. nr 177, poz. 1054 z późn. zm.).

Należy bowiem wskazać, że faktura musi odzwierciedlać rzeczywistość i tylko, wówczas uprawnia ona do odliczenia podatku od towarów i usług jak również zaliczenia poniesionego wydatku w koszty prowadzonej działalności gospodarczej. W przypadku, gdy faktura odzwierciedla rzeczywistość to na wystawcy faktury ciąży obowiązek podatkowy w podatku od towarów i usług, a tym samym realnie istnieje podatek naliczony, który został wykazany na fakturze jako podatek należny z tytułu transakcji i tylko taki podatek może zostać odliczony na kolejnym etapie obrotu gospodarczego przez drugą stronę transakcji.

Ustawodawca w ramach walki ze zjawiskiem pustych faktur w dokonanych zmianach w przepisach regulujących zasady odliczania podatku od towarów i usług od 1 stycznia 2014 r., jako jeden z warunków odliczenia wskazał powstanie obowiązku podatkowego po stronie dostawcy towarów lub usług. Taka regulacja prawna pozwala na stwierdzenie, że w przypadku pustych faktur obowiązek podatkowy nigdy nie powstanie, a jedynym skutkiem wygenerowania pustej faktury będzie obowiązek zapłaty podatku wykazanego na tej fakturze.

Na koniec niniejszego opracowania chciałbym wskazać wybrane przypadki ujawnionych w toku kontroli podatkowych i skarbowych okoliczności związanych z wprowadzeniem do obrotu gospodarczego faktur, którym można przypisać znamiona faktur pustych, a które były przedmiotem sądowego badania z jednoczesnym przywołaniem fragmentów treści orzeczeń Naczelnego Sądu Administracyjnego gdzie dokonano szczegółowej analizy stanu prawnego i faktycznego.

Przykład 1. W sytuacji nawet gdy przedsiębiorca nie wiedział, że jego pracownik wystawiał fałszywe faktury, to ma obowiązek odprowadzić należny podatek od towarów i usług z tych dokumentów i z tego obowiązku nie zwalnia go nawet zawiadomienie policji o popełnieniu przestępstwa – wyrok Naczelnego Sądu Administracyjnego o sygn. akt I FSK 359/12 do I FSK

371/12. W powołanym wyroku NSA – odrzucił argumentację w myśl, której wystawione bez wiedzy pracodawcy, niezaewidencjonowane dokumenty – jako dokumenty fałszywe nie powinny być traktowane jako „puste faktury", od których należy zapłacić VAT.

Stan faktyczny: Naczelnik urzędu skarbowego nakazał podatnikowi zapłatę podatku od towarów i usług wynikającego z wystawionych faktur. W wyniku czynności sprawdzających przeprowadzonych u kontrahentów podatnika ustalono, że posiadają oni faktury VAT, wystawione przez firmę podatnika, które nie zostały zaewidencjonowane w rejestrach sprzedaży podatnika i nie zostały rozliczone przez niego w deklaracjach VAT-7. W trakcie kontroli podatkowej podatnik złożył pisemne wyjaśnienie, z którego wynika, że znalazł kopie niezaewidencjonowanych faktur z lat 2008–2010 do preparowania, których przyznał się jego pracownik. Za te faktury pracownik otrzymywał od klientów połowę wartości VAT. Po usłyszeniu takich wyjaśnień podatnik zgłosił sprawę na policję, jednakże organy podatkowe ustaliły należne zobowiązanie wynikające z wystawionych faktur. Podatnik z takim rozstrzygnięciem się nie zgodził i złożył skargę do Wojewódzkiego Sądu Administracyjnego w Łodzi, który wyrokiem z 15 listopada 2011 r. (sygn. akt ISA/Łd 969/11) uchylił decyzję organu podatkowego. Sąd stwierdził, że w tej sprawie nie mieliśmy do czynienia z tzw. pustymi fakturami, ale z dokumentami podrobionymi, ponieważ nie tylko nie odzwierciedlały one okoliczności w nich wskazanych, ale przede wszystkim były sfałszowane. Taki sfałszowany, podrobiony dokument nie może zostać uznany za fakturę w rozumieniu ustawy o podatku od towarów i usług. Z uwagi na takie orzeczenie organ podatkowy złożył skargę kasacyjną do Naczelnego Sądu Administracyjnego. Naczelny Sąd Administracyjny uznał, że sporne faktury zawierały wszystkie elementy, które powinna zawierać faktura w myśl przepisów o podatku od towarów i usług. Ponadto dokumentowały sprzedaż tych towarów i usług, które są przedmiotem działalności firmy skarżącego. Są to więc puste faktury wystawione przez podatnika. To podatnik, jako pracodawca ponosi odpowiedzialność za dobór pracowników. Podatnik przyznał temu pracownikowi prawo i kompetencje do wystawiania faktur i pomimo, iż podatnik nie brał udziału w tym działaniu, to jednak podatek wykazany w wystawionych fakturach powinien zapłacić. Sąd ponadto stwierdził, że brak uznania odpowiedzialności pracodawcy z tego tytułu skutkowałoby przeniesieniem odpowiedzialności za prowadzenie działalności gospodarczej na Państwo, ponieważ Pracodawca sam wybiera i zatrudnia pracowników i powinien brać odpowiedzialność za ich działania, także za te, które są niezgodne z prawem i zdaniem sądu jest to element ryzyka gospodarczego. Na-

czelny Sąd Administracyjny powołał się w rozstrzygnięciu na orzecznictwo Trybunału Sprawiedliwości UE (np. sprawy o sygn. akt: C-35/05, C-342/87, C-643/11), zgodnie z którym każdy kto wystawia faktury VAT ma obowiązek zapłaty podatku. Z art. 203 Dyrektywy 112 wynika, że VAT należy odprowadzić bez względu na zaistnienie czynności podlegającej opodatkowaniu. W przypadku, gdy osoba prawna, jednostka organizacyjna niemająca osobowości prawnej lub osoba fizyczna wystawi fakturę, w której wykaże kwotę podatku, jest zobowiązana do jego zapłaty. W tej sprawie wystawcą faktury jest formalnie podatnik, ponieważ to jego dane były na fakturze, a dane te wpisywał jego pracownik.

Mając na uwadze powyższe okoliczności należy stwierdzić, że przypadku gdy ujawniona zostanie taka faktura w firmie to możemy dokonać jej anulowania w sytuacji gdy kontrahent otrzymał ją i odesłał oraz nie zaksięgował jej, kiedy jednak dokonał już zaksięgowania to należy dokonać korekty przedmiotowej faktury.

Przykład 2. Nawet w sytuacji, gdy przedsiębiorca w sposób niewłaściwy udokumentuje poniesiony koszt tj. faktura zostanie wystawiona przez inny podmiot niż faktyczny sprzedawca to tak udokumentowany koszt nie daje prawa do odliczenia realnego kosztu i nie ma przy tym znaczenia, że podatnik odliczał koszty w dobrej wierze, przekonany, że faktury są wystawione prawidłowo – wyrok Naczelnego Sądu Administracyjnego o sygn. akt II FSK 1834/11.

Stan faktyczny: Przedsiębiorca kupił olej napędowy za prawie 30 tys. zł. i jak w toku kontroli wyjaśnił, płacił dostawcom paliwa gotówką, a część faktur przychodziła do niego pocztą. W toku kontroli okazało się, że wystawiły je inne podmioty niż faktyczny sprzedawca. Naczelnik Urzędu skarbowego, a potem Dyrektor Izby Skarbowej, uznali, że jeśli wystawcy faktur nie byli właścicielami paliwa, to nie mogli udokumentować jego sprzedaży. A to oznacza, że przedsiębiorca nie powinien wykazywać takich zakupów w księdze podatkowej ani zaliczać ich do kosztów uzyskania przychodu. Z takim stanowiskiem organu podatkowego podtrzymanym przez Dyrektora Izby Skarbowej nie zgodził się podatnik i wniósł odwołanie do Wojewódzkiego Sądu Administracyjnego. W sądzie I instancji podatnik wygrał spór o prawo do odliczenia wydatków. Wojewódzki Sąd Administracyjny w Łodzi orzekł, że nie wystarczy samo uznanie przez organy, iż faktury, które mają stanowić dowód zakupu, są puste. Podatnik może dowieść w inny sposób, że poniósł wydatki, na które te dokumenty wskazują. W ocenie Sądu Wojewódzkiego należy je wyrzucić z kosztów dopiero wtedy, gdy nie będzie dowodu, że przedsiębiorca faktycznie zapłacił za paliwo. Z takim stanowiskiem nie zgo-

dził się organ podatkowy II instancji i złożył skargę kasacyjną do Naczelnego Sądu Administracyjnego.

Naczelny Sąd Administracyjny przyznał jednak rację organom podatkowym. Podkreślił, że obowiązkiem podatnika jest prowadzić księgi w sposób rzetelny. Oznacza to, że aby odliczyć dany wydatek, nie wystarczy tylko faktyczna zapłata za jakiś towar czy usługę. Ważne jest także, aby transakcja była potwierdzona przez prawidłowo sporządzony dokument księgowy – w tym przypadku fakturę wystawioną przez faktycznego właściciela sprzedawanego towaru. W sytuacji, gdy dokumenty sporządził ktoś inny, a kupujący na podstawie tych faktur odpisał wydatki w podatkowej księdze przychodów i rozchodów, to zapisy te są nieskuteczne. Nie mogą więc wywrzeć żadnych skutków podatkowych. Wynika to z tego, że w rzeczywistości sporne paliwa nie zostały kupione od wystawców faktur. Naczelny Sąd Administracyjny wskazał, że przy potrącaniu kosztów nie można pomijać zasad ich dokumentowania. Zaznaczył on także, że „dla pozbawiania podatnika prawa do kosztów nie ma znaczenia, czy podatnik działał w dobrej czy złej wierze".

Zakończenie

Mając na uwadze skalę zjawiska pustych – fikcyjnych faktur należy stwierdzić, że wyłudzenia w podatku od towarów i usług to nie tylko straty dla budżetu, ale także uderzenie w uczciwe firmy. Trudno jest bowiem konkurować na rynku z podmiotem, który ma z góry zagwarantowaną 23-procentową marżę. Dlatego zwalczanie tego typu przestępstw jest priorytetem służb podatkowych i skarbowych. Największe osiągnięcia w walce z tym zjawiskiem mają służby skarbowe, które posiadają bardziej wyspecjalizowany charakter z uwagi na posiadane uprawnienia prawne oraz korzystające z różnych programów informatycznych pozwalających na trafniejsze typowanie podmiotów do kontroli. Należy także wskazać, że działania służb kontrolnych nie mają za główny cel zwiększenie ściągalności podatków, ale walkę z przestępstwami skarbowymi. Rozbicie grupy przestępczej nie oznacza, że taka grupa zacznie płacić podatki, ale jej wyeliminowanie zapobiegnie kolejnym wyłudzeniom. Ponadto w Ministerstwie Finansów w sposób ciągły, trwają prace, których głównym celem jest eliminacja negatywnych zjawisk bezpośrednio związanych z wpływami do budżetu. Jednym z takich rozwiązań mogłaby być koncepcja tzw. modelu podzielonej płatności [www.polskieradio.pl/…] (*split payment*) w podatku od towarów i usług. Zgodnie z tą zasadą firma, która kupuje towar, płaci na rachunek bankowy sprzedawcy tylko kwotę netto, a VAT naliczony na fakturze wpłaca na spe-

cjalne konto tej firmy założone przy urzędzie skarbowym i dedykowane tylko rozliczeniu tego podatku, jednakże takie rozwiązanie mogłoby ograniczyć płynność sprzedawców.

W ramach walki ze zjawiskiem „pustych faktur" celem ochrony uczciwych podatników, należałoby stworzyć bazę podmiotów gospodarczych, w której w przypadku stwierdzenia oszustwa podatkowego służby kontrolne dokonywałyby stosownej adnotacji, ale mając na uwadze fakt, że dopiero prawomocne rozstrzygnięcie winno stanowić przesłankę takiego zapisu, to taki mechanizm byłby mało skuteczny i dlatego podmioty gospodarcze w sposób staranny winny analizować, z kim prowadzą działalność gospodarczą.

Bibliografia

Krajowy Plan Dyscypliny Podatkowej Ministerstwa Finansów na 2012 r.

Pokojska A. (2014), *Nie ma branży wolnej od oszustw podatkowych*, Dziennik Gazeta Prawna z 3 kwietnia 2014 r. nr 65 (3706).

Fornalik J. (2003), [w:] *VI Dyrektywa VAT*, (red.) K. Sachs, C.H. Beck, Warszawa.

http://www.polskieradio.pl/42/273/Artykul/1110610,Sciganie-wyludzen-VAT-nowe-metody-i-priorytety-skarbowki.

Wyrok WSA w Łodzi z 15.11.2011 Sygn. Akt. I SA/Łd 966/11 (dotyczy przykładu 1).

Wyrok NSA z 08.15.2013 Sygn. Akt. II FSK 1834/11 (dotyczy przykładu 2).

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 49–60

Aleksy Banasiak
Społeczna Akademia Nauk

Uwarunkowania bezpiecznego prowadzenia małego przedsiębiorstwa w wirtualnej przestrzeni

Conditions for safe-keeping small businesses in the virtual space

Abstract: Despite the increasing globalization of business is growing role of small and medium-sized enterprises. In their functioning, however, face a number of obstacles and dangers. Many of the dangers associated with an increasing use of the Internet in their business. This is especially true of small businesses, which, due to their characteristics, are not able to put yourself adequate security.
The aim of the study is to identify selected, the most common, threats to the safe operation of small businesses and attempt to indicate the ability to counter these threats.
Keywords: A small business, small business security company.

Wstęp

Małe przedsiębiorstwa stanowią podstawową grupę firm sektora MŚP. Mimo postępującej globalizacji odgrywają decydującą rolę w rozwoju gospodarczym kraju. W swojej działalności napotykają jednak na szereg barier i niebezpieczeństw. Często nie zdają sobie nawet sprawy z czyhających w otoczeniu zagrożeń. Pokonywanie barier i likwidacja niebezpieczeństw jest w małych firmach szczególnie trudna ze względu na ich specyfikę. Mogą bowiem do tego celu wykorzystywać jedynie bardzo ograniczone środki, w porównaniu z dużymi, czy nawet średnimi przedsiębiorstwami.

Coraz więcej barier i niebezpieczeństw wynika z faktu, że następuje szybka wirtualizacja otoczenia, w którym funkcjonują przedsiębiorstwa. Przynosi to wiele korzyści, ale powstają także nowe, nieznane dotąd zagrożenia. Właściciele małych przedsiębiorstw uważają często, że tego typu podmioty nie są narażone na niebezpieczeństwa związane z wirtualizacją działalności, bądź nie znajdują się w sferze zainteresowania np. cyberprzestępców. Wydaje im się, że takie problemy dotyczą tylko dużych organizacji.

W praktyce jest jednak często odwrotnie. Łatwiej jest bowiem uderzyć w biznesowych „maluchów", bo – inaczej niż korporacje są łatwym celem ataku.

Małe firmy także w przyszłości będą najpopularniejszą, a zarazem najbardziej dynamicznie rozwijającą się formą działalności gospodarczej. Bezspornym staje się więc fakt, że należy monitorować i wspierać procesy rozwoju i kształtowania konkurencyjności tej grupy przedsiębiorstw, zwracając szczególną uwagę na stojące przed nimi zagrożenia. Bezpieczeństwo funkcjonowania, inaczej bezpieczeństwo biznesowe, jest bowiem jednym z podstawowych czynników warunkujących ich rozwój.

Celem opracowania jest identyfikacja wybranych, najczęściej występujących, zagrożeń dla bezpiecznego funkcjonowania małych przedsiębiorstw oraz próba wskazania na możliwości przeciwdziałania tym zagrożeniom. Szczególna uwaga została zwrócona na zagrożenia związane z wirtualizacją otoczenia, w którym przedsiębiorstwa te funkcjonują.

Specyfika funkcjonowania i zarządzania małym przedsiębiorstwem

Za małe przedsiębiorstwo uznaje się przedsiębiorstwo zatrudniające mniej niż 50 pracowników i którego roczny obrót lub całkowity bilans roczny nie przekracza 10 milionów euro [Dominiak 2005 , s. 33]. Dodatkowo powinno spełniać tzw. kryterium niezależności, zgodnie z którym inne podmioty nie partycypują w więcej niż 25% wkładów, udziałów lub akcji, więcej niż 25% udziału w zysku lub więcej niż 25% głosów na zgromadzeniu wspólników, walnym zgromadzeniu akcjonariuszy, walnym zgromadzeniu spółdzielców.

Rolę sektora MSP, w którym małe przedsiębiorstwa odgrywają główną rolę, z punktu widzenia efektów w gospodarce, analizuje K. Safin. Wymienia on [Safin 2008, s. 50]:

1) Efekt postępu technicznego (innowacyjność) – przewaga MSP nad dużymi przedsiębiorstwami polega tu m. in. na efektywności badań i tempie ich wdrażania. Wynika to z konieczności efektywnego wykorzystania ograniczonych zasobów i nacisku konkurencji.
2) Efekt zatrudnienia – MSP wnoszą duży wkład w powstawanie nowych miejsc pracy i jednocześnie dają większą pewność ich utrzymania niż duże.
3) Efekt ekologiczny – wpływ MSP na środowisko ma charakter mniej agresywny i zdecentralizowany a ogólna szkodliwość oddziaływania jest mniejsza w stosunku do dużych przedsiębiorstw.

4) Efekt makroekonomiczny – MSP wpływają na wzrost gospodarczy w sposób pośredni poprzez tworzenie nowych miejsc pracy czy np. tworzenie sieci współpracy kooperacyjnej.
5) Efekt stabilizacyjny – małe i średnie firmy skuteczniej radzą sobie z kryzysem, recesją czy wahaniami koniunktury. Wynika to z większej zdolności adaptacyjnej i elastyczności działania.
6) Efekt regionalnej decentralizacji – MSP dla swojego funkcjonowania mają mniejsze wymagania infrastrukturalne. Mogą powstać w miejscach, w których duże przedsiębiorstwa nie byłyby w stanie funkcjonować.
7) Efekt mobilizacji kapitałów – MSP wykorzystują najczęściej własne zasoby właściciela, które w innym przypadku zostałyby skonsumowane bądź złożone np. w banku.
8) Efekt transformacyjny – MSP wspierają procesy transformacji rynkowej tworząc pozytywny obraz przedsiębiorczości.

Dlatego też problematyka zarządzania małymi przedsiębiorstwami jest coraz częściej poruszana w opracowaniach naukowych. Należy w tym miejscu podkreślić, że wszystkie ogólne, uniwersalne zasady zarządzania przedsiębiorstwem dotyczą również małych przedsiębiorstw. Konieczne jest jednak zwrócenie uwagi w procesach zarządzania na pewne specyficzne problemy dotyczące tylko tych przedsiębiorstw. Skuteczne zarządzanie w tej grupie przedsiębiorstw staje się powoli podstawowym kanonem działania ich właścicieli. R. W. Griffin uważa, że „pod pewnymi względami skuteczne zarządzanie jest nawet ważniejsze w przedsiębiorstwach małych niż dużych" [Griffin 1997, s. 59]. Duża firma może bowiem bez trudu powetować nawet wielką stratę związaną z nieudaną realizacja jakiegoś projektu, podczas gdy małe przedsiębiorstwo często nie jest w stanie udźwignąć nawet niewielkiej straty z tego tytułu.

Podstawowym problemem związanym z zarządzaniem w małych firmach jest brak profesjonalizacji zarządzania. Właściciele zazwyczaj nie mają zarówno odpowiedniego wykształcenia jak i doświadczenia w tym zakresie. Zarządzanie najczęściej odbywa się na zasadzie intuicji a także metodą prób i błędów. Rzadko są stosowane nowoczesne metody i narzędzia zarządzania, oparte na systemach komputerowych. Wszystko to powoduje to, że działania nie zawsze są w pełni efektywne.

W większości przypadków nie występuje w małych firmach zarządzanie strategiczne. Przedsiębiorstwa te najczęściej posługują się strategiami rodzącymi się w bieżącym działaniu, w sposób nieuporządkowany i przypadkowy. Działają w sposób intuicyjny, nie tworząc sformalizowanej misji, wizji czy

planu strategicznego. Jeśli już są tworzone strategie tych firm, to najczęściej nie zawierają elementów związanych z bezpieczeństwem funkcjonowania.

W zarządzaniu w małych firmach występują tendencje zachowawcze i duży opór przed zmianami. Właściciel boi się ponoszenia ryzyka związanego z nowymi przedsięwzięciami. Firmy te działają w bardzo konkurencyjnym otoczeniu, powodującym konieczność nieustannego wprowadzania innowacji, szukania nowych rozwiązań, wprowadzania nowych technologii. Dla wielu z nich stanowi to duże wyzwanie, ponieważ najczęściej zostały założone w oparciu o koncepcję przedsiębiorcy – pomysłodawcy a nie w oparciu posiadane umiejętności i wiedzę.

Działania małych firm z reguły nastawione są krótkookresowo. Nie występuje planowanie długookresowe a firmy dążą do osiągnięcia maksymalizacji zysku w krótkim okresie czasu. Nie sprzyja to tworzeniu projektów decydujących o rozwoju tych firm w dłuższym horyzoncie czasowym. Działalność bieżąca polega często na szukaniu tzw. „okazji". Brak odpowiedniego przygotowania działań powoduje duże ryzyko.

Istotnym problem rzutującym na zarządzanie jest tutaj problem finansowania rozwoju. Swoją działalność opierają najczęściej na kapitale właścicieli. Podstawowe źródło finansowania jakim jest kredyt bankowy, z reguły jest niedostępne. Firmy te nie są bowiem w stanie zagwarantować odpowiednich zabezpieczeń. Nie mają też odpowiedniej historii dla oceny wiarygodności kredytowej.

Cechą małych przedsiębiorstw są mało złożone struktury organizacyjne. Przedsiębiorstwa te są mało sformalizowane. Z jednej strony jest to cecha pozytywna, ponieważ układ decyzyjny jest przejrzysty a przepływ informacji szybki. Z drugiej strony prowadzi to często do rozmycia kompetencji i odpowiedzialności oraz do skupienia wszystkich decyzji w rękach właściciela.

Problemem oddziałującym na zarządzanie małymi firmami jest brak możliwości pozyskiwania pracowników o wysokich kwalifikacjach, ze względu na ograniczone możliwości finansowe. A właśnie tacy pracownicy są tutaj najbardziej pożądani. Powinni oni mieć szerokie kwalifikacje do pełnienia różnych funkcji, w przeciwieństwie do dużych przedsiębiorstw, gdzie w tym zakresie występuje duża specjalizacja. Małe firmy nadal w zbyt w małym stopniu korzystają z możliwości jakie daje e-komunikacja. Wynika to z jednej strony z zachowawczych postaw przedsiębiorcy, z drugiej zaś braku odpowiednich kwalifikacji i umiejętności.

Zagrożenia dla bezpiecznego funkcjonowania małych przedsiębiorstw w wirtualnej przestrzeni – wybrane obszary

Nowoczesne technologie informatyczne zmieniają oblicze współczesnej gospodarki. Internet staje się nowym narzędziem prowadzenia biznesu. Jest to narzędzie, które posiada takie cechy, jak:

- globalny zasięg,
- powszechny, praktycznie nieograniczony dostęp,
- interaktywność – możliwość prowadzenia komunikacji w czasie rzeczywistym,
- szybkość – komunikacja w każdej chwili i bardzo szybko,
- nieograniczona dostępność w czasie,
- taniość.

Wszystkie te cechy powodują, że Internet jest w coraz większym stopniu wykorzystywany przez małe przedsiębiorstwa. Zachodzi jednak pytanie, czy jest to w pełni bezpieczne dla tego typu przedsiębiorstw? Bezpieczeństwo funkcjonowania małego przedsiębiorstwa, inaczej bezpieczeństwo biznesowe, powinno być częścią zintegrowanego systemu zarządzania tym przedsiębiorstwem. W małej firmie, z ograniczonymi zasobami materialnymi i niematerialnymi, nie zawsze jest to realizowane.

Bezpieczeństwo biznesowe można podzielić na obszary, których dotyczy. Do najważniejszych należą: bezpieczeństwo internetowe, bezpieczeństwo prawne, bezpieczeństwo e-sprzedaży, bezpieczeństwo finansowe i kapitałowe, bezpieczeństwo podatkowe, bezpieczeństwo na rynku, bezpieczeństwo działania w okresie spowolnienia gospodarczego. Wiele z tych problemów związanych jest z koniecznością działania w wirtualnym otoczeniu, które z jednej strony przynosi małym przedsiębiorstwom wiele korzyści, z drugiej jednak może narażać w pewnych przypadkach na różnego rodzaju niebezpieczeństwa.

Bezpieczeństwo internetowe

W nowoczesnej gospodarce Internet stanowi przydatne narzędzie wsparcia dla prowadzenia działalności gospodarczej, gdyż m. in:

- stanowi źródło informacji,
- zwiększa możliwości w obszarze zarządzania,
- otwiera dostęp do szerokiego rynku,
- umożliwia nawiązywanie kontaktów,
- ułatwia przeprowadzanie transakcji.

Mimo swoich korzystnych właściwości Internet może w niektórych sytuacjach stanowić zagrożenie dla przedsiębiorstw, szczególnie tych małych. Szacuje się, że celem 77 proc. cyberataków na świecie są małe i średnie przedsiębiorstwa. Tymczasem 64 proc. podmiotów z tego sektora nie wdraża polityki bezpieczeństwa danych. [www.e.pb.pl]. Niewątpliwie wskaźniki dla małych przedsiębiorstw, które zdecydowanie przeważają liczbowo w tym sektorze, będą jeszcze gorsze.

Małe firmy nie doceniają znaczenia ochrony swoich danych. Może to dotyczyć w szczególności firm prowadzonych przez starsze pokolenie przedsiębiorców, którzy zaczęli szerzej korzystać z możliwości, jakie daje Internet w prowadzeniu biznesu. Z reguły nie przeszli odpowiednich szkoleń w tym zakresie. Ponadto wydaje im się, że problem ich nie dotyczy, ponieważ ataki są skierowane na wielkie korporacje. Ale korporacje są w tym zakresie względnie zabezpieczone. Posiadają specjalistów, którzy zajmują się wyłącznie tym problemem. Są ponadto w stanie przeznaczyć na ten cel odpowiednie środki finansowe. Ataki internetowe o różnym charakterze są więc przede wszystkim skierowane na sektor małych i średnich przedsiębiorstw.

Jeśli mali przedsiębiorcy już decydują się na stosowanie zabezpieczeń, są to najczęściej zwykłe programy antywirusowe, które nie chronią danych w dostatecznym stopniu. Są one bezbronne wobec ukierunkowanych ataków cyberprzestępców. Straty z tego tytułu mogą być bardzo dotkliwe. Mogą dotyczyć m. in.: utraty danych, kradzieży pomysłów, kradzieży danych dotyczących rynku i odbiorców, realizacji fałszywych przelewów itp.

Małe firmy, ze względu na swoja specyfikę, nie są więc w większości przypadków samodzielnie chronić swoich danych. Wyjściem z tej trudnej sytuacji może być zastosowanie outsourcingu i skorzystanie z pomocy zewnętrznych partnerów w zakresie zarządzania systemami informatycznymi. Outsourcing uznawany jest za jedną najpopularniejszych koncepcji zarządzania współczesnymi organizacjami. W roku 2011 w Polsce około 20% procesów biznesowych przekazywano na zewnątrz [Zieniewicz 2014, s. 78]. Jest jednak stosowany głównie przez większe firmy i korporacje. Koncepcję wykorzystania outsourcingu należy więc w większym stopniu propagować i wykorzystywać w małych przedsiębiorstwach.

Bezpieczeństwo prawne

Właściciele małych przedsiębiorstw działają w dużym stopniu w oparciu o własną intuicję. Szczególnym zagrożeniem może być brak dostatecznej znajomości aktualnych przepisów prawa oraz jego interpretacji. System

prawny dotyczący prowadzenia działalności gospodarczej jest skomplikowany. Odpowiednie przepisy znajdują się ponadto w wielu aktach prawnych, często o charakterze rozporządzeń. Przedsiębiorca musi poświęcić wiele czasu na ich odnalezienie. Nie ma jednak gwarancji, że właściwie zastosuje przepisy prawa. W większości przypadków nie jest możliwe skorzystanie z pomocy prawnej wyspecjalizowanych fachowców. Usługi prawne są w Polsce relatywnie drogie i małe firmy korzystają z nich w ograniczonym stopniu. Ponadto występuje coraz większa specjalizacja prawników.

Na pogorszenie ich sytuacji prawnej wpływa także fakt, że najczęściej są to firmy nieposiadające osobowości prawnej. Występują jako osoby fizyczne bądź spółki osobowe. Przyjęte formy organizacyjno-prawne, takie jak jednoosobowa działalność gospodarcza, spółka cywilna czy spółka jawna powodują, że właściciel bądź wspólnik odpowiada za zobowiązania firmy całym swoim majątkiem. Bezpieczniejsze może być prowadzenie działalności w formie spółki kapitałowej. Przy małej skali działalności dobrym rozwiązaniem jest spółka z ograniczoną odpowiedzialnością. Rozwiązaniem w zakresie bezpieczeństwa prawnego może być podpisywanie umów ryczałtowych na doradztwo prawne z kancelariami prawnymi, zatrudniającymi specjalistów w wielu dziedzinach. Można tutaj wykorzystać przesyłanie danych i informacji z wykorzystaniem Internetu przy zapewnieniu odpowiedniej ochrony.

Konieczne jest również włączenie w rozwiązanie tego problemu instytucji publicznych, takich jak np. urzędy gmin, urzędy skarbowe itp. Zatrudnieni tam urzędnicy powinni w większym służyć przedsiębiorcom pomocą merytoryczną w zakresie interpretacji przepisów prawa.

Bezpieczeństwo w zakresie e-sprzedaży

Sprzedaż z wykorzystaniem Internetu staje się coraz popularniejsza. Jest realizowana również w dużym stopniu przez małe firmy. Sprzedaż internetowa pozwala obniżyć koszty działalności poprzez np. ograniczenie punktów sprzedaży detalicznej, ograniczenie powierzchni magazynowej, powierzchni biurowej, rezygnację z marż pośredników, tańszą promocję i reklamę, itp.

Stosowanie tej formy sprzedaży może jednak w niektórych przypadkach narażać przedsiębiorstwa na pewne niebezpieczeństwo. Sprzedaż internetowa jest bowiem obwarowana szeregiem wymogów prawnych. Każdy sklep internetowy powinien mieć swój regulamin. Regulaminy te w małych firmach zawierają często błędy, które można podzielić na dwie grupy. Do pierwszej zalicza się tzw. niedozwolone klauzule umowne, czyli zamieszczanie w regulaminie postanowień, które kształtują prawa i obowiązki klientów w sposób sprzeczny z dobrymi obyczajami, rażąco naruszając ich interesy.

Do drugiej grupy należą błędy polegające na pominięciu w regulaminie postanowień, które obowiązkowo powinny się w nim znaleźć. Błędy te wynikają z reguły z małej wiedzy przedsiębiorców w tym zakresie i braku konsultacji z prawnikami. Mała firma może być w tym przypadku zostać pozwana do Sądu Ochrony Konkurencji i Konsumentów. W przypadku przegrania sprawy wiąże się to z koniecznością poniesienia kosztów nawet do kilkunastu tysięcy złotych. Na rynku pojawiło się wiele podmiotów, które wykorzystują niewiedzę przedsiębiorców i masowo składają pozwy. Następnie proponują ugodę i wycofanie pozwu w zamian za zapłacenie na ich rzecz określonej kwoty pieniędzy.

Przedsiębiorcy powinni śledzić rejestr klauzul niedozwolonych prowadzony w formie elektronicznej. Można go znaleźć na stronie www.uokik.gov.pl.. W miarę możliwości powinni także konsultować regulaminy przed ich opublikowaniem z prawnikami.

Bezpieczeństwo finansowe i kapitałowe

Współczesne małe przedsiębiorstwa działają w bardzo konkurencyjnym otoczeniu. Aby utrzymać swoja pozycję, muszą zabezpieczyć określone środki, zarówno na finansowanie bieżącej działalności operacyjnej jak i na inwestowanie w majątek rzeczowy, wartości niematerialne i prawne a także w kapitał ludzki.

Podstawową kwestią pozostaje pytanie, w jakim stopniu przedsiębiorstwo zamierza korzystać z własnych, a w jakim stopniu z obcych źródeł finansowania? Drugą kwestią jest odpowiedź na pytanie, jaka część tych środków zostanie zaangażowana w działalności bieżącej a jaka część zostanie przeznaczona na działalność rozwojową?

Właściciele i kadra zarządzająca małych firm starają się działać bardzo ostrożnie w sferze gospodarki finansowej. Przejawia się to w unikaniu przedsięwzięć kapitałochłonnych i o długim okresie zwrotu. Przedsiębiorstwa te są z reguły nastawione na osiąganie efektów w krótkim okresie czasu. Właściciel stara się prowadzić firmę tak, aby nie stracić nad nią kontroli. W wielu przypadkach nie stara się o jej stały wzrost i rozwój a wystarcza mu satysfakcja z jej posiadania i kierowania nią.

Małe i średnie przedsiębiorstwa, w znacznie większym stopniu aniżeli firmy duże, są narażone na wahania koniunktury. Mają bowiem mniejsze możliwości dywersyfikacji ryzyka. To z kolei wpływa na konieczność posiadania pewnych dodatkowych rezerw zasobów finansowych. Przedsiębiorstwa te mają utrudniony dostęp do finansowania zewnętrznego. Wynika to przede wszystkich z braku możliwości zabezpieczenia kredytu czy pożyczki.

Problemem jest też często krótki okres funkcjonowania i związany z tym brak historii świadczącej o wiarygodności takiej firmy. Rozwiązaniem może być w tym przypadku skorzystanie z funduszy poręczeń kredytowych, których głównym zadaniem jest ułatwienie przedsiębiorcom oraz osobom rozpoczynającym działalność gospodarczą dostępu do zewnętrznego finansowania w postaci kredytów bankowych oraz pożyczek na prowadzenie działalności gospodarczej. Fundusze poręczeń kredytowych, są instytucjami o charakterze non profit.

Fundusze poręczają zobowiązania finansowe przedsiębiorcom, którzy posiadają zdolność kredytową, nie posiadają natomiast wymaganych przez instytucję finansującą zabezpieczeń. Poręczenie udzielane przedsiębiorcy stanowi od 50% do 80% kwoty kredytu/pożyczki. W niektórych przypadkach maksymalna wartość poręczenia jest ograniczona kwotowo. W zależności od funduszu, poręczeniem mogą być objęte kredyty lub pożyczki przeznaczone między innymi na rozpoczęcie lub rozszerzenie działalności, finansowanie inwestycji, finansowanie działalności gospodarczej, wdrażanie nowych rozwiązań technicznych lub technologicznych, tworzenie nowych miejsc pracy, itp. [www.parp.gov.pl (1)].

Inną formą wykorzystywania długoterminowych źródeł finansowania przedsiębiorstw jest *franchising*. W dużym stopniu przyczynia się do rozwoju małych i średnich przedsiębiorstw, pobudza ich aktywność gospodarczą, uczy samodzielności [Żurek 2007, s. 623]. Istotą franchisingu jest to, że przedsiębiorstwo o ugruntowanej na rynku pozycji przekazuje inicjatywę działalności mniejszym przedsiębiorstwom (franchisingobiorcom), udostępniając im możliwość korzystania z nazwy firmy, znaku towarowego, wiedzy i doświadczeń a także określonych środków trwałych. Dzięki temu małe i średnie przedsiębiorstwa powiększają swój majątek rzeczowy oraz majątek niematerialny. Do zalet franchisingu dla małych i średnich przedsiębiorstw można zaliczyć [Skowronek-Mielczarek 2007, s. 91]:

- zmniejszone ryzyko podjęcia działalności gospodarczej wynikające z reputacji i marki franchisingodawcy;
- pomoc w wyborze miejsca prowadzenia działalności gospodarczej, szkoleniu załogi, zakupie wyposażenia, decyzjach inwestycyjnych;
- korzyści skali wynikające z działań reklamowych i marketingowych dawcy;
- korzyści techniczne i technologiczne z tytułu prowadzonych przez dawcę badań;
- pewność i stałość zaopatrzenia w surowce i półprodukty;
- ochrona przed konkurencją.

Dla aktywnych i dynamicznych firm z sektora MSP franchising może zatem stanowić określoną strategię rozwoju. Internet może być źródłem informacji o możliwościach pozyskiwania kapitału. Jest to szczególnie ważne dla małych przedsiębiorstw zlokalizowanych w terenie, które mają ograniczone kontakty biznesowe w tym zakresie.

Bezpieczeństwo podatkowe

Prowadzeniu działalności gospodarczej towarzyszy ryzyko podatkowe. Wynika ono ze skomplikowanego systemu podatkowego. Ponadto przepisy podatkowe ulegają częstym zmianom. Jednocześnie praktyka pokazuje, że są różnie interpretowane w zależności od konkretnego urzędu skarbowego. Podstawowe problemy, przed którymi stają przedsiębiorcy to rozwiązywanie problemów podatkowych oraz optymalizacja zobowiązań podatkowych.

Internet jest już powszechnie wykorzystywany przede wszystkim do składania e-deklaracji podatkowych. Upraszcza to procedury, zabezpieczając jednocześnie przed pomyłkami. Następnym krokiem powinna być szersza możliwość kontaktów z urzędem skarbowym, np. w zakresie interpretacji przepisów czy uzyskania koniecznego zaświadczenia, np. o niezaleganiu z płatnościami podatków.

Bezpieczeństwo na rynku

Małe przedsiębiorstwa działają w zdecydowanej większości przypadków na rynkach lokalnych. Są w dużym stopniu uzależnione od stopnia rozwoju społecznego, a przede wszystkim ekonomicznego, lokalnych społeczności. Potencjał ekonomiczny danego obszaru będzie wpływał na możliwości rozwojowe tych przedsiębiorstw. Dużym zagrożeniem jest także dla nich konkurencja ze strony korporacji. Przykładem jest upadek małych sklepów w związku z ekspansją dużych sieci handlowych, konkurujących przede wszystkim cenowo.

Należy pamiętać, że w związku z przystąpieniem Polski do Unii Europejskiej w 2004 roku nastąpiła istotna zmiana uwarunkowań funkcjonowania tego sektora. Wiąże się to z szerokim otwarciem krajowego rynku dla produktów i towarów z innych krajów Unii Europejskiej, jak również z pojawieniem się w otoczeniu polskiego sektora MSP większej niż poprzednio zagranicznej liczby konkurentów.

Przeciwdziałać tego typu zagrożeniom małe firmy mogą poprzez tworzenie różnego rodzaju form współpracy. Jednym z rozwiązań są coraz powszechniej występujące w gospodarce klastry oraz powiązania sieciowe. Pozwalają one małym firmom łączyć zasoby, poprawiać innowacyjność, konku-

rencyjność i produktywność. Mikro i małe przedsiębiorstwa stanowią aktualnie 71% wszystkich członków istniejących klastrów [www.parp.gov.pl (2)].

Szczególnie ważna staje się tutaj informacja o działalności małych lokalnych podmiotów gospodarczych. Powinna to być z jednej strony informacja o produktach dla klientów, z drugiej zaś informacja dla innych podmiotów o możliwości nawiązywania współpracy. Internet może być podstawowym narzędziem do realizacji tego celu.

Bezpieczeństwo działania małych przedsiębiorstw w okresie spowolnienia gospodarczego

Zapoczątkowany w 2008 roku kryzys oraz spowolnienie gospodarcze wpłynęły w dużym stopniu na funkcjonowanie małych przedsiębiorstw. Wynika to głównie z braku monitorowania sytuacji i odpowiednio wczesnego zidentyfikowania zagrożeń oraz ostrzegania przed nimi. Współczesne przedsiębiorstwa, funkcjonujące w turbulentnym otoczeniu, narażone są bardzo często na konieczność działania w warunkach kryzysu. Z badań przeprowadzonych przez M. Poradę-Rochoń [2009, s. 154] wynika, że aż 69 proc. polskich przedsiębiorstw zetknęło się z kryzysem. Nawet najlepiej zorganizowane i rynkowo przystosowane przedsiębiorstwo nie jest odporne na ryzyko w prowadzeniu działalności gospodarczej. Dotyczy to w szczególności małych przedsiębiorstw, gdzie do powstawania sytuacji kryzysowych mogą się m.in. przyczyniać: zakłócenia w przepływie informacji, samozadowolenie z osiągniętej pozycji, brak programu rozwoju przedsiębiorstwa, brak kontroli finansowej, złe gospodarowanie majątkiem czy błędne inwestycje.

Kryzys najczęściej nie pojawia się nagle (poza niektórymi przypadkami, np. klęska żywiołowa, katastrofa, awaria, pożar itp.) i rozwija się w dłuższym okresie. Przede wszystkim jednak najtrudniejsze jest zaobserwowanie wchodzenia przedsiębiorstwa w fazę kryzysu, ponieważ w fazie początkowej jego symptomy są najczęściej trudno zauważalne. Poza tym często występuje zjawisko negacji kryzysu, gdyż wszyscy widzą to, co chcą widzieć.

Tylko wczesne rozpoznanie kryzysu może pozwolić na podjęcie w odpowiednim czasie działań zapobiegających jego skutkom. Ważne jest aby powołane do tego instytucje ostrzegały przedsiębiorstwa o możliwościach pojawienia się sytuacji kryzysowych. Wiele z takich sytuacji można prognozować, jak np.: przewidywane zmiany kursów walut, przewidywane kierunki zmian cen nośników energii itp. Właściciele małych firm nie posiadają takiej wiedzy a jest ona nieodzowna w podejmowaniu decyzji biznesowych.

Podsumowanie

Powstanie firmy i rozpoczęcie działalności nie gwarantuje, że osiągnie ona sukces. Otoczenie, w którym przyjdzie jej funkcjonować, jest bardzo burzliwe. Niezależnie od fazy rozwoju, w której znajduje się mała firma, narażona jest na wiele zróżnicowanych niebezpieczeństw. W tego typu firmach są one bardzo często bagatelizowane, co kończy się w wielu wypadkach ich upadłością. Wiele z tych niebezpieczeństw związanych jest z wirtualizacją otoczenia, w którym małe przedsiębiorstwa funkcjonują. Przy tym otoczenie wirtualne ulega bardzo szybkim i jednocześnie rewolucyjnym zmianom. Konieczne jest więc stałe uświadamianie przedsiębiorcom zarówno możliwości wykorzystania nowoczesnych technologii informatycznych i Internetu w prowadzeniu biznesu jak i zagrożeń płynących z otoczenia, w szczególności z otoczenia wirtualnego. Pozwoli to im na ograniczenie ryzyka prowadzenia działalności.

Bibliografia

Dominiak P. (2005), *Sektor MSP we współczesnej gospodarce,* Wydawnictwo Naukowe PWN, Warszawa.

Griffin R. W. (1997), *Podstawy zarządzania organizacjami,* PWN, Warszawa.

http://www.e.pb.pl/ineks.php?act=popups&sub=article_print&id=164322&mode=html (w dniu 5.05.2014 r.)

http://www.parp.gov.pl/index/index/2305 [2] (w dniu 12.05.2014 r.)

http://www.parp.gov.pl/index/index/364 [1] (w dniu 12.05.2014 r.)

Porada-Rochoń M., *Restrukturyzacja przedsiębiorstw w procesie adaptacji do współczesnego otoczenia. Perspektywa międzynarodowa,* Difin, Warszawa 2009.

Safin K. (red), (2008), *Zarządzanie małym i średnim przedsiębiorstwem,* Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław.

Skowronek-Mielczarek A. (2007), *Małe i średnie przedsiębiorstwa. Źródła finansowania,* C.H. Beck, Warszawa.

Zimniewicz K. (2014), *Teoria i praktyka zarządzania. Analiza krytyczna,* PWE, Warszawa.

Żurek J. (red.) (2007), *Przedsiębiorstwo, zasady działania, funkcjonowanie, rozwój,* Fundacja rozwoju Uniwersytetu Gdańskiego, Gdańsk.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 61-82

Hanna Szeląg
Prezes Kancelarii Biegłych Rewidentów „Josef Welf" Sp. z.o.o.

Bariery natury podatkowej i rachunkowej w rozliczeniach transakcji towarowych przez Internet

Tax and accounting barriers associated with the sale of goods over the internet

Abstract: Article is devoted to discussing the formal and legal conditions related to the activity of selling goods on the Internet. The article indicates the legal provisions that determine trade on the internet and difficulties in their application – due both to the volatility and uncertainties regulations and technical barriers in the implementation of solutions that would have to meet regulatory requirements.

Key words: e-commerce, tax liability, issuing of goods, mail order, value limits of mail orders, place of goods issueing.

E-commerce – trwała rewolucja czy chwilowa moda

Tak jak rewolucją w handlu na początku XX wieku było pojawienie się pierwszych ogólnodostępnych domów handlowych, tak na początku XXI wieku rewolucją w handlu jest pojawienie się „globalnego domu handlowego" jakim jest internet. Handel internetowy zyskał swoją definicję w elektronicznej encyklopedii WIKIPEDII: „Handel elektroniczny (e-handel, ang. e-commerce) – procedury wykorzystujące środki i urządzenia elektroniczne (telefon stacjonarny i komórkowy, faks, Internet, telewizję) w celu zawarcia transakcji handlowej. Najbardziej popularną metodą handlu elektronicznego jest handel internetowy, gdzie występują transakcje handlowe pomiędzy sprzedającymi a kupującymi. Najbardziej powszechną formą handlu elektronicznego są sklepy internetowe" [Wikipedia].

Jak widać nawet w internetowej encyklopedii definicja handlu internetowego jest dość archaiczna. Chociaż z początkiem XXI wieku e-commerce weszło pod strzechy to jego początki były jeszcze w ubiegłym stuleciu. Jak czytamy w WIKIPEDII: „Handel elektroniczny oznaczał pierwotnie ula-

twienia transakcji handlowych drogą elektroniczną. Zakupy on-line zostały wynalezione w roku 1979 w Wielkiej Brytanii przez Michaela Aldricha. W roku 1980 były szeroko stosowane przez takich producentów jak Ford, Peugeot-Talbot, General Motors i Nissan. Od 1990 roku zawierał dodatkowo systemy planowania zasobów przedsiębiorstwa (ERP) eksploracji danych i hurtowni danych. Od 2000 roku większość amerykańskich i europejskich przedsiębiorstw oferuje swoje usługi w Internecie. W Polsce pierwszy sklep internetowy powstał w 1997 roku" [Wikipedia].

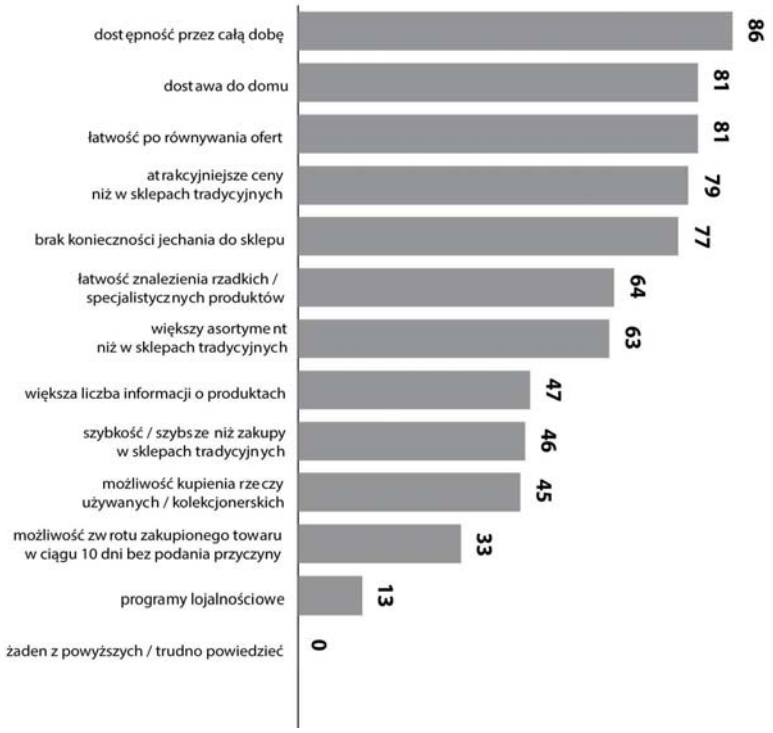
Jak widać początkowo handel internetowy rozwijał się w sektorze świadczeń dla przedsiębiorstw. Odbiorców detalicznych traktowano głównie jako odbiorów usług świadczonych przez Internet. Jednak upowszechnienie dostępu do sieci spowodowało, że internet stał się poważnym narzędziem komunikacji z klientami również w zakresie dostawy towarów.

Aktualne badania oraz prognozy na najbliższe lata powszechności dostępu do internetu wskazują, że „w 2016 roku na świecie będzie 3 mld internautów. Oznacza, to że blisko połowa ludzi na ziemi będzie korzystać z sieci" [Raport „The Internet Economy in G-20"]. Jak przewidywał laureat nagrody Pulitzera Thomas Friedman internet sprawił, że „Świat jest płaski". Klienci z każdego zakątka świata oczekują atrakcyjnych ofert usług i towarów z miasta, kraju, a nawet kontynentu. Jak twierdzą autorzy raportu „The Internet Economy in G-20" The Boston Consulting Group – wartość gospodarki internetowej w 20 najpotężniejszych ekonomicznie krajach świata przekroczy 4,3 bln USD. To oznacza, że Internet będzie piątą największą gospodarką świata – mniejszą od amerykańskiej, chińskiej, japońskiej i indyjskiej, ale większą od niemieckiej. Największa gospodarka europejska jest mniejsza od swobodnej wymiany towarów i usług w globalnym Internecie.

Co doceniają konsumenci

Badania przeprowadzone przez Izbę Gospodarki Elektronicznej dowodzą, że głównym motywem korzystania z handlu internetowego jest wygoda i oszczędność takich zakupów. Rysunek 1 przedstawia szczegóły motywów dokonywania zakupów on-line.

Rysunek 1. Motywy dokonywania zakupów on-line



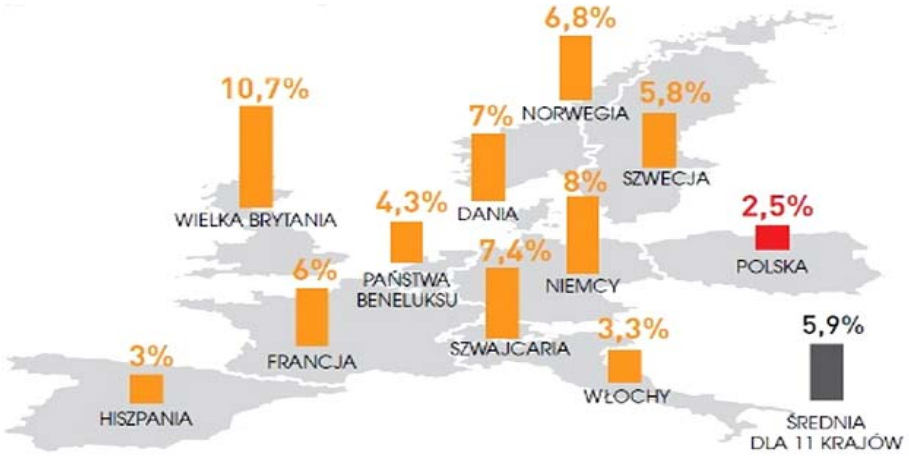
Źródło: Raport *E-commerce w Polsce 2014; Geminus dla e-Commerce Polska,* s. 41.

Jak na tym tle wygląda polski e-handel

Polscy przedsiębiorcy nie pozostają w tyle. Co więcej, przegląd rynku e-commerce wskazuje, że w dużej mierze są to firmy z polskim kapitałem. Firma doradcza Deloitte informuje, że „wielkość gospodarki internetowej w Polsce w ciągu ostatnich sześciu lat podwoiła się i odpowiada ona już za 5,8% PKB wypracowanego w 2012 roku. Całkowita wartość dodana polskiego e-commerce wynosiła w 2012 roku 7,3 mld zł" [*Wpływ E-commerce na gospodarkę*]. Wnioski Deloitte potwierdza Ministerstwo Skarbu Państwa publikując w marcu 2013 roku na swojej stronie internetowej przewidywania odnośnie handlu internetowego w roku 2012 i szacunki na rok 2013 i 2014. „W roku 2012 prawdopodobnie wzrósł o blisko 23% rok do roku, do wartości 21,5 mld zł – wynika z szacunków SMB, Kelkoo i Forrester Research prezentowanych w raporcie e-commerce portalu Interaktywnie.com. By uzmysłowić sobie skalę wzrostu tego rynku w ostatnich latach, warto przypomnieć, że dziesięć lat temu handel inter-

netowy w Polsce miał wartość 330 mln zł, czyli 1,5% wartości z 2012 roku, a pięć lat temu był wart 5 mld zł, czyli około 23% wartości z zeszłego roku. Rok 2013 ma być kolejnym okresem dwucyfrowej dynamiki wzrostu rynku e-commerce w Polsce: może ona wynieść 21,4%, w wyniku czego rynek będzie wart 26,1 mld zł, wynika ze średniej oczekiwań ekspertów ankietowanych przez portal Interaktywnie.com" [*Polski rynek e-commerce rośnie w szybkim…*]. E-handel zmienia wygląd rynku. Jak wynika z raportu e-commerce powołującym się na szacunki SMB, Kelkoo oraz Forrester sprzedaż za pośrednictwem internetu staje się coraz ważniejszą gałęzią polskiego handlu detalicznego. O ile w 2010 roku udział e-commerce w całkowitej wartości rynku detalicznego wynosił 2,5% to w roku 2012, prawdopodobnie wyniósł 3,8%, po wzroście z 3,1% rok wcześniej. Oczekuje się również, że wartość rynku e-commerce w Polsce w roku 2014 przekroczy 4% wartości całkowitej sprzedaży detalicznej. Jednak jak widać na poniższym schemacie jest to poziom, jaki większość państw starej Europy osiągnęła już w 2010 roku.

Rysunek 2. Udział wartości zakupów online w ogólnej wartości sprzedaży detalicznej w Polsce oraz innych wybranych krajach Europy w 2010 roku



Źródło: na podstawie danych Center for Retail Research na zlecenie Kelkoo.

Czynników, które leżą u podstaw tego opóźnienia zapewne jest wiele. Jednak jedną z ważnych barier jest złożoność przepisów prawa. Uciążliwości tej nie zmniejsza również praktyka organów podatkowych, z Ministerstwem Finansów na czele, tworząc częstokroć sprzeczne interpretacje tych przepisów.

Poniżej prezentuję wybrane bariery związane ze stosowaniem przepisów prawa podatkowego, na które napotykają przedsiębiorcy.

Problemy w ustaleniu daty obowiązku podatkowego

Podatnicy prowadzący działalność handlową z wykorzystaniem Internetu napotkają bariery już na samym początku ustalania swoich obowiązków w podatku VAT. Pierwsze pytanie, jakie zadaje sobie podatnik to pytanie kiedy podatek VAT jest wymagany. To jest pytanie o datę powstania obowiązku podatkowego. W tym zakresie ustawodawca dokonał począwszy od 01 kwietnia 2014 roku zmian ustawy o VAT. Do końca 2013 roku obowiązek podatkowy w praktyce gospodarczej powstawał w dacie wystawienia faktury, co musiało nastąpić w terminie 7 dni od wydania towarów.

Począwszy od 2014 toku nowy art. 19a ust.1 ustawy o VAT określa generalną regułę stanowiącą, że obowiązek podatkowy powstaje w z chwilą wydania towaru. Obowiązujący od 1 stycznia 2014 roku przepis jest spójny z art. 63 Dyrektywy 2006/112/WE Rady Unii Europejskiej z dnia 28 listopada 2006 roku w sprawie wspólnego systemu podatku od wartości dodanej. Dyrektywa stanowi, że zdarzenie powodujące powstanie obowiązku podatkowego ma miejsce, a VAT staje się wymagalny w momencie dostarczenia towarów lub wykonania usług.

Jak słusznie wskazano w komentarzu do 112 Dyrektywy pod redakcją Krzysztofa Sachsa i Romana Namysłowskiego „w związku z faktem, że pojęcie zdarzenia powodującego powstanie obowiązku podatkowego jest definiowane na podstawie terminu dostarczenia towaru lub wykonania usługi, w określonych przypadkach konieczne jest również zdefiniowanie tych pojęć" [Sachs, Namysłowski 2008, s. 423]. Wysiłek przybliżenia pojęcia dostawy towarów podjął polski ustawodawca. W myśl art. 7 ust. 1 ustawy o VAT przez dostawę towarów rozumie się przekazanie prawa do rozporządzania towarami jak właściciel. Tu pojawiają się pierwsze dylematy podatników: czy obowiązek podatkowy powstaje w dacie fizycznego wydania towaru czy też przekazania prawa własności. Ustawodawca nie wyjaśnia, co należy rozumieć pod pojęciem „przekazanie prawa do dysponowania towarem jak właściciel". Należy się zgodzić z oceną Adama Bartosiewicza wyrażoną w komentarzu do ustawy o VAT, że „chodzi przede wszystkim o możliwość faktycznego dysponowania rzeczą, a nie rozporządzania nią w sensie prawnym. Istotą dostawy towarów nie jest przeniesienie własności. Zwrotu: „prawo do rozporządzania jak właściciel" nie można interpretować jako „prawa własności" [Bartosiewicz, Kubacki, VAT-7 2013, s. 125]. Z drugiej jednak strony „należy podkreślić, że pojęcie dostawy towarów na gruncie przepisów o VAT należy rozumieć bardzo szeroko i nie można go ograniczać jedynie do fizycznego wydania towarów" [*Nowe zasady powstawania obowiązku podatkowego w VAT*…].

Podobne stanowisko zajął Europejski Trybunał Sprawiedliwości. W orzeczeniu C-320/88 (Shipping and Forwarding Safe B.V v. Staatecretaris van Financiën) ETS posłużył się w tym kontekście terminem „własności ekonomicznej".

Tym samym określenie daty wymagalności podatku VAT nie jest możliwe w oparciu o polskie przepisy, lecz wymaga odwołania się do dorobku ETS. Mimo przybliżenia rozwiązania problemu, podatnik rozwijający handel przez Internet w dalszym ciągu nie potrafi odpowiedzieć na pytanie – kiedy powstaje obowiązek podatkowy.

Z czego wynika złożoność zagadnienia w przypadku e-comerce? E-commerce to styk rzeczywistości elektronicznej ze światem realnym. Świat wirtualny to szybka komunikacja: przepływ zamówienia, umowy a nawet płatności. Świat analogowy to fizyczne przekazanie zamówionego towaru. Zaletą handlu internetowego jest możliwość obsługi klienta na odległość. Jednak wiąże się to z wysyłką towaru do odbiorcy do miejsca odległego częstokroć o dziesiątki, setki lub nawet tysiące kilometrów. Kiedy zatem dochodzi do wydania towarów i przekazania do rozporządzania nimi jak właściciel: z chwilą wydania towarów poczcie, kurierowi, profesjonalnemu przewoźnikowi, czy też z chwilą, kiedy podmioty te przekażą towar odbiorcy?

Analizując publikacje dotyczące powyższego zagadnienia można stwierdzić, że na tak postawione pytania odpowiedzi nie zna nawet Minister Finansów. Do wniosków takich w prowadzi rozbieżność w zakresie określenia daty powstania obowiązku podatkowego „w sprzedaży na odległość" jaka objawia się między informacjami publikowanymi na stornie internetowej Ministerstwa Finansów.

W celu ułatwienia wdrożenia zmian w ustawie o VAT daty ustalenia obowiązku podatkowego Ministerstwo Finansów opublikowało na stronie internetowej specjalną broszurę, w której dwukrotnie poruszyło między innymi kwestię daty powstania obowiązku podatkowego „w sprzedaży na odległość". Ministerstwo Finansów wyjaśniło podatnikom, że w przypadku, gdy „towar jest wysyłany przez dostawcę nabywcy za pośrednictwem przewoźnika, kuriera, poczty itp. (ryzyko utraty towaru ponosi nabywca) – dokonanie dostawy towaru następuje z chwilą wydania towaru podmiotowi, który jest zobowiązany do jego dostarczenia, z tym bowiem momentem dostawca przenosi prawo do rozporządzania jak właściciel" [*Zmiany w zakresie określania momentu powstania obowiązku*..]. Jednocześnie w tym samym dokumencie uzależniło datę powstania obowiązku podatkowego w przypadku sprzedaży na odległość na rzecz konsumenta na odległość od sposobu zapłaty za to-

war. W broszurze Ministerstwa Finansów problem ten zilustrowano następującym przykładem: „Firma dokonuje dostaw towarów wyłącznie wysyłkowo. W tym celu korzysta z usług pocztowych oraz firm kurierskich. Nabywca wybiera sposób dostarczenia (pocztą lub kurierem) i dokonuje zapłaty w chwili odbioru towaru (ryzyko utraty towarów ponosi dostawca). W takich przypadkach obowiązek podatkowy będzie powstawał z chwilą wydania towaru jego nabywcy" [*Zmiany w zakresie określania momentu powstania obowiązku*…].

Należy ze zdziwieniem przyjąć stanowisko Ministerstwa Finansów, w którym datę dostawy towarów tj. przekazania prawa do rozporządzania towarem jak właściciel wiąże ze sposobem zapłaty. Określenie innego momentu powstania obowiązku dla transakcji opłacanych przez nabywców „za zaliczeniem" nie znajduje umocowania zarówno w zaktualizowanej ustawie o VAT jak i w 112 Dyrektywie oraz dorobku ETS. Tak więc broszura, która miała ułatwić wdrożenie przez podatników znowelizowanej ustawy o VAT stworzyła u nich nowe bariery.

Niestety to niefortunne stanowisko nie doczekało się dotychczas sprostowania i podatnicy, którzy rozwijają swój e-handel w dalszym ciągu nie dość, że nie mają wsparcia, to napotykają bariery wynikające z niejasnych przepisów i niejednoznacznych stanowisk Ministerstwa Finansów.

Jednocześnie Minister Finansów „po cichu" wycofuje się z kuriozalnej informacji w wydanej broszurze w drodze indywidualnych interpretacji wydawanych na wnioski podatników. W interpretacji indywidualnej (wydanej w imieniu Ministra Finansów) z 22 kwietnia 2014 roku nr ILPP5/443-11/14-5/KG dyrektor Izby Skarbowej w Poznaniu wyjaśnia spółce, która nie reguluje w umowach, ani regulaminach kwestii przeniesienia prawa do towaru, że na mocy art. 544 par. 1 i art. 548 par. 1 kodeksu cywilnego „wydanie rzeczy następuje z chwilą powierzenia jej przez sprzedawcę przewoźnikowi z poleceniem dostarczenia jej do miejsca przeznaczenia uzgodnionego wcześniej z kupującym. W tym momencie następuje też formalne spełnienie świadczenia przez sprzedawcę, a na kupującego przechodzą korzyści i ciężary związane z rzeczą" [Pokojska 2014, s. B3].

Jak powyżej przedstawiono podatnicy funkcjonują w niestabilnym otoczeniu prawnym w zakresie swojego podstawowego obowiązku – ustalenia momentu wymagalności podatku VAT. Przy znacznej złożoności litery prawa brak stabilności interpretacji przepisów powoduje rozbieżność stanowisk zajmowanych przez Ministerstwo Finansów w okresie czterech miesięcy od wejścia w życie nowych przepisów.

Podsumowując, przedsiębiorca musi podąć pierwszą decyzję, kiedy przy sprzedaży towarów wysyłanych do odbiorcy powstaje obowiązek podatkowy. Zagadnienie staje się bardziej skomplikowane, gdy po pokonaniu pierwszych, opisanych powyżej trudności, zdecyduje się on na sprzedaż do odbiorcy indywidualnego za granicę. W dalszej części artykułu postaram się przybliżyć kolejne pułapki związane z zastosowaniem przepisów prawa podatkowego przy sprzedaży wysyłkowej z terytorium kraju.

Definicja i zasady opodatkowania sprzedaży wysyłkowej

W obecnym handlu znaczącą część sprzedaży stanowi sprzedaż towarów konsumpcyjnych przez Internet, która dla potrzeb przepisów o VAT nazywana jest sprzedażą wysyłkową. Powołane przepisy ustawy o VAT przewidują szczególne zasady opodatkowania tzw. sprzedaży wysyłkowej. Należy zauważyć, że sprzedaż wysyłkowa w rozumieniu VAT nie jest (choć w pewnych przypadkach może być) sprzedażą wysyłkową w potocznym rozumieniu tego zwrotu. Sprzedaż wysyłkowa w rozumieniu VAT stanowi szczególny rodzaj transakcji wewnątrzwspólnotowej. Do sprzedaży wysyłkowej dochodzi wówczas, gdy sprzedawcą towarów jest podatnik podatku VAT z jednego państwa członkowskiego, natomiast nabywcą – podmiot z innego państwa członkowskiego, który nie jest obowiązany do rozliczania wewnątrzwspólnotowych nabyć towarów. Uściślając – zgodnie z art. 2 ust 24 ustawy o VAT przez „sprzedaż wysyłkową z terytorium kraju rozumie się dostawę towarów wysyłanych lub transportowanych przez polskiego podatnika lub na jego rzecz z terytorium kraju (Polski) na terytorium państwa członkowskiego inne niż terytorium kraju, które jest państwem przeznaczenia dla wysyłanego lub transportowanego towaru pod warunkiem, że dostawa dokonywana jest na rzecz:

1) unijnego podatnika lub unijnej osoby prawnej niebędącej podatnikiem, którzy nie mają obowiązku rozliczania wewnątrzwspólnotowego nabycia towarów;
2) każdego innego podmiotu niebędącego unijnym podatnikiem" [Ustawa o podatku od towarów i usług].

Należy zwrócić uwagę, że sprzedaż wysyłkowa występuje niezależnie od tego czy towary będące jej przedmiotem zostały uprzednio nabyte lub wytworzone w państwie członkowskim wysyłki, czy też były przedmiotem importu – art. 23 ust. 16 i art. 24 ust. 12 ustawy o VAT. Przepisy Vat-owskie określają w szczególny sposób zasady opodatkowania sprzedaży wysyłkowej.

Regulacja powyższego zagadnienia sprowadza się do wyznaczenia miejsca dokonania (a w konsekwencji państwa opodatkowania) dostawy towarów wykonywanej w ramach sprzedaży wysyłkowej. „Zasadą w przypadku sprzedaży wysyłkowej jest, iż dostawę wykonywaną w ramach sprzedaży wysyłkowej uznaje się za dokonaną na terytorium państwa przeznaczenia wysyłanych lub transportowanych towarów. Jest to zatem zasada odwrotna od obowiązującej przy „zwykłych" (krajowych) dostawach towarów, gdy miejscem dostawy jest najczęściej miejsce, w którym towary znajdują się w momencie rozpoczęcia wysyłki lub transportu do nabywcy (art. 22 ust. 1 pkt 1 ustawy o VAT). Oznacza to, że w przypadku sprzedaży wysyłkowej z terytorium kraju, dostawę towarów wykonywaną w jej ramach uznaje się za dokonaną na terytorium państwa członkowskiego przeznaczenia dla wysyłanych lub transportowanych towarów (art. 23 ust. 1 ustawy o VAT). Przyjęcie powyższej zasady ma na celu wyeliminowanie ewentualnych zakłóceń konkurencji spowodowanych dokonywaniem sprzedaży z państw członkowskich, w których obowiązują niższe stawki podatku do państw, w których obowiązują stawki wyższe. Na skutek bowiem powyższej zasady sprzedaż wysyłkowa opodatkowana jest w państwie faktycznej konsumpcji (na terytorium państwa, do którego dokonano dostawy towarów w ramach sprzedaży wysyłkowej)" [Krzywan, lex 71887].

Niemniej jednak stosowanie opisanej zasady w praktyce oznacza, że podatnik dokonujący sprzedaży wysyłkowej do jednego z państw unijnych obowiązany jest zarejestrować się w tym państwie, jako podatnik VAT i rozliczyć podatek VAT od sprzedaży wysyłkowej na terytorium tego państwa. Jest to uciążliwe i często niepraktyczne oraz kosztowne, zwłaszcza w przypadku sprzedaży wysyłkowej w niewielkim zakresie, lub sprzedaży do wielu krajów.

Od powołanych przepisów przewidziany jest wyjątek. Wyjątek ten sprowadza się do jej odwrócenia i określenia, że sprzedaż wysyłkową z terytorium kraju uznaje się za dokonaną i opodatkowaną w Polsce. Niemniej jednak wyjątek ten można zastosować - w przypadku sprzedaży wysyłkowej z terytorium kraju - jeżeli całkowita wartość towarów (innych niż wyroby akcyzowe) wysyłanych lub transportowanych do tego samego państwa członkowskiego w ramach sprzedaży wysyłkowej z kraju, pomniejszona o kwotę podatku:

1) jest w danym roku mniejsza lub równa od kwoty wyrażonej w złotych odpowiadającej kwocie ustalonej przez państwo członkowskie przeznaczenia dla wysyłanych lub transportowanych towarów;
2) w poprzednim roku podatkowym nie przekroczyła powyższej kwoty.

Limit, o którym mowa w przepisie, każde z państw członkowskich ustala z osobna. Przeliczenia tego limitu dokonuje się w oparciu o kurs średni waluty przyjętej przez dane państwo ogłoszony przez NBP na dzień 1 maja 2004 roku, w zaokrągleniu do 1000 zł (art. 23 ust. 10 ustawy o VAT). Aktualnie w państwach członkowskich obowiązują następujące limity wartości sprzedaży wysyłkowej (w walucie oraz w przeliczeniu kursem średnim euro ogłoszonym przez NBP na dzień 1 maja 2004 roku 4,8122):

1) Austria – 100.000 euro (481.000 zł),
2) Belgia – 100.000 euro (168.000 zł),
3) Bułgaria - 70.000 BGN (172.000 zł),
4) Chorwacja - 270.000 HRK (171.000 zł),
5) Czechy – 1.140.000 CZK (169.000 zł),
6) Cypr – 35.000 euro (168.000 zł),
7) Dania – 280.000 DKK (181.000 zł),
8) Estonia – 550.000 EEK (169.000 zł),
9) Finlandia – 35.000 euro (168.000 zł),
10) Francja – 100.000 euro (481.000 zł),
11) Grecja – 35.000 euro (168.000 zł),
12) Hiszpania – 35.000 euro (168.000 zł),
13) Holandia – 100.000 euro (481.000 zł),
14) Irlandia – 35.000 euro (168.000 zł),
15) Litwa – 125.000 LTL (174.000 zł),
16) Luksemburg – 100.000 euro (481.000 zł),
17) Łotwa – 24.000 LVL (177.000 zł),
18) Malta – 35.000 euro (168.000 zł),
19) Niemcy – 100.000 euro (481.000 zł),
20) Portugalia – 35.000 euro (168.000 zł),
21) Rumunia – 118.000 RON (139 000 zł),
22) Słowacja – 35.000 euro (168.000 zł),
23) Słowenia – 35.000 euro (168.000 zł),
24) Szwecja – 320.000 SEK (169.000 zł),
25) Węgry – 8.800.000 HUF (168.000 zł),
26) W. Brytania – 70.000 GBP (498.000 zł),
27) Włochy – 35.000 euro (168.000 zł).

Przekroczenie limitu (zarówno w przypadku sprzedaży wysyłkowej z terytorium kraju, jak i w przypadku sprzedaży wysyłkowej na terytorium kraju) powoduje, iż miejsce dokonania dostawy w ramach sprzedaży wysyłkowej ustalane jest na zasadach ogólnych, tj. sprzedaż wysyłkową uznaje się za dokonaną na terytorium państwa przeznaczenia wysyłanych lub transportowanych towarów. Przekroczenie limitu w danym roku podatkowym oznacza, że w kolejnym roku nie będzie możliwe skorzystanie ze zmiany miejsca świadczenia ustalanego na zasadach ogólnych. Przekroczenie limitów wartości sprzedaży opodatkowanej powoduje konieczność zmiany miejsca opodatkowania dostawy począwszy od dostawy, którą przekroczono tę kwotę.

Oczywiście – przepisy umożliwiają, w ramach kwot sprzedaży w limicie – na wybór kraju, w którym podatnik chce opodatkować dostawę. Zgodnie z regulacjami zawartymi w ustawie o VAT podatnik może – pomimo nieprzekroczenia ustawowych limitów wybrać opodatkowanie dokonanej przez siebie sprzedaży wysyłkowej w państwie przeznaczenia. „Przyczyną wyboru opcji jest najczęściej niższa stawka podatku VAT obowiązująca w państwie członkowskim przeznaczenia. Fakt ten może podatnikowi dokonującemu sprzedaży wysyłkowej zrekompensować uciążliwości związane z koniecznością rozliczenia podatku VAT w tym państwie. Przykładowo, polskiemu podatnikowi dokonującemu w ramach sprzedaży wysyłkowej dostawy do Niemiec towarów opodatkowanych w Polsce stawką podstawową może się opłacać wybór opcji. Pozwoli to mu stosować wobec sprzedawanych towarów obowiązującą w Niemczech stawkę 19%. Z tego samego powodu podatnikowi węgierskiemu może się kalkulować (stawką podstawową obowiązującą na Węgrzech jest 25%) wybór opodatkowania sprzedaży wysyłkowej w Polsce" [Krzywan, lex 71887].

Skorzystanie z opcji następuje poprzez zawiadomienie o tym fakcie właściwego naczelnika urzędu skarbowego. Zawiadomienie takie może być dokonane wobec jednego z krajów przeznaczenia. Niekoniecznie musi oznaczać wybór tej opcji do wszystkich krajów, do których dokonywana jest sprzedaż. Wybór opcji jest wiążący dla podatnika przez okres dwóch lat od pierwszej dostawy dokonanej w trybie przewidzianym opcją. Dopiero po upływie tego okresu możliwa jest rezygnacja. Podobnie jak w przypadku zawiadomienia o wyborze opcji, rezygnacja z opcji powinna nastąpić na piśmie.

Zasady ustalania miejsca świadczenia przy sprzedaży wysyłkowej obowiązują dla każdego podatnika w stosunku do każdego z państw członkowskich z osobna. Zarówno limit sprzedaży wysyłkowej (a w konsekwencji jego przekroczenie i utratę prawa do opodatkowania sprzedaży wysyłkowej w państwie wysyłki), jak i wybór opcji i rezygnacja z niej odnoszą się tylko

do konkretnego państwa, którego dotyczą. A zatem, przykładowo, przekroczenie przez polskiego podatnika kwoty granicznej w stosunku do jednego z państw członkowskich pozostaje bez wpływu na zasady opodatkowania sprzedaży wysyłkowej do pozostałych państw. Z kolei w przypadku podejmowania decyzji o wyborze opcji podatnik może skorzystać z tego uprawnienia w stosunku do jednego, kilku lub wszystkich państw członkowskich. Jeśli podatnik zdecyduje się na skorzystanie z opcji tylko w stosunku do niektórych z państw członkowskich, jak najbardziej możliwe jest późniejsze skorzystanie z opcji w stosunku do innych państw. Podobnie jest z rezygnacją z opcji. Rezygnacja taka może dotyczyć wszystkich państw członkowskich, może jednak również dotyczyć tylko kilku czy jednego państwa członkowskiego. Rezygnacja z opcji może następować także etapami. Wszelkie możliwe konfiguracje są dopuszczalne.

Powyżej opisane przepisy regulujące zasady opodatkowania sprzedaży wysyłkowej nie mają zastosowania do wszystkich towarów. Stosownie do art. 23 ust. 11 oraz art. 24 ust. 8 ustawy o VAT, przepisów dotyczących miejsca świadczenia przy sprzedaży wysyłkowej nie stosuje się do:

1) nowych środków transportu – w tym przypadku ma bowiem zawsze miejsce wewnątrzwspólnotowe nabycie nowych środków transportu,
2) towarów będących przedmiotem dostawy przez dokonującego ich dostawy lub na jego rzecz po montażu lub instalacji, w których przypadku miejscem dostawy jest państwo członkowskie montażu lub instalacji (art. 22 ust. 1 pkt 2 ustawy o VAT).

Ponadto w myśl art. 23 ust. 12 oraz art. 24 ust. 9 ustawy o VAT, w przypadku sprzedaży wysyłkowej, której przedmiotem są wyroby akcyzowe, dostawę towarów uznaje się w każdym przypadku:

1) za dokonaną na terytorium państwa członkowskiego przeznaczenia – w przypadku sprzedaży wysyłkowej z terytorium kraju (Polski),
2) za dokonaną na terytorium kraju – w przypadku sprzedaży wysyłkowej na terytorium kraju.

Stosownie zaś do art. 23 ust. 13 oraz art. 24 ust. 10 pkt 1 ustawy o VAT, omawianych przepisów nie stosuje się również w stosunku do towarów opodatkowanych według zasad określonych w art. 120 ust. 4 i 5 ustawy o VAT, a więc do towarów używanych, dzieł sztuki, przedmiotów kolekcjonerskich lub antyków, których dostawa opodatkowana jest w oparciu o marżę.

Dodatkowo, w myśl art. 24 ust. 10 pkt 2 ustawy o VAT przepisów dotyczących miejsca świadczenia sprzedaży wysyłkowej na terytorium kraju nie stosuje się również do towarów używanych, dzieł sztuki, przedmiotów ko-

lekcjonerskich lub antyków będących przedmiotem dostawy na aukcji (licytacji) w państwie członkowskim rozpoczęcia transportu lub wysyłki, jeżeli ich dostawa dokonywana jest przez organizatora aukcji (licytacji) oraz zastosowano do niej szczególne zasady opodatkowania podatkiem VAT obowiązujące w państwie członkowskim rozpoczęcia transportu lub wysyłki, stosowane do dostaw towarów dokonywanych przez organizatora aukcji (licytacji), wyłączające uznanie dostawy towarów za czynność odpowiadającą wewnątrzwspólnotowej dostawie towarów.

Podsumowując tą część opisywanego zagadnienia pierwsze trudności pojawiające się ze stosowaniem powyżej opisanych przepisów wiążą się z koniecznością:

- Stosowania niejednolitych zasad tej samej sprzedaży – bowiem w zależności od kierunku sprzedaży (tzn. kraju wysyłki), jak i czasu sprzedaży (przed przekroczeniem limitu i po przekroczeniu limitu) występuje obowiązek opodatkowania sprzedaży w różnych krajach tj. raz w Polsce, a innym razem – za granicą.
- Znajomości zasad i ponoszenia kosztów rejestracji oraz rozliczania podatku w obcym kraju.
- Monitorowania i prognozowania poziomu sprzedaży na rynkach, na których podatnik zaczyna sprzedawać. Niedostosowanie przepisu wiąże się brakiem czasu do opodatkowania sprzedaży za granicą po powstaniu takiego obowiązku np. od nowego roku, czy choćby od następnego miesiąca po miesiącu, w którym limit został przekroczony. Zgodniebowiem z powołanymi przepisami wraz z przekroczeniem limitu podatnik ma obowiązek już następną sprzedaż rozliczyć poza granicą kraju wysyłki. Pojawia się pytanie: czy rozwijający się podatnik ma wcześniej projektować swoją strukturę organizacyjną w taki sposób, aby być przygotowanym na przekroczenie limitów w różnych krajach i ponosić z tego tytułu koszty? Czy może ma wstrzymywać od pewnego momentu sprzedaż i tracić dochody, aby po przekroczeniu limitu mieć czas na zorganizowanie możliwości zgodnego z prawem innego kraju dokumentowania i opodatkowania sprzedaży? Czy może ma ponosić ryzyko czasowego niedostosowania stosowanych przez siebie rozwiązań i dokonywać sprzedaży na zasadach dotychczasowych pomimo przekroczenia limitu w konkretnym kraju?

Dokumentowanie sprzedaży wysyłkowej

Sprzedaż wysyłkowa z terytorium kraju musi być bezwzględnie dokumentowana fakturami. Wynika to z art. 106b ust. 1 pkt 2 ustawy o VAT. Nie dotyczy to jednak wszelkiej sprzedaży wysyłkowej, która podlega opodatkowaniu podatkiem VAT w Polsce (ze względu na znajdujące się na terytorium kraju miejsce świadczenia określone na podstawie przepisów art. 23 i 24 ustawy o VAT). Sprzedaż wysyłkowa z terytorium kraju, która podlega opodatkowaniu podatkiem VAT poza Polską (ze względu na znajdujące się poza terytorium kraju miejsce świadczenia określone na podstawie przepisów art. 23 i 24 ustawy o VAT) nie stanowi sprzedaży w rozumieniu tej ustawy, a w konsekwencji nie jest dokumentowana polskimi fakturami. Taka sprzedaż wysyłkowa nie stanowi również czynności, o których mowa w art. 106a pkt ustawy o VAT. Powinna być ona zatem udokumentowana w sposób określony w państwie członkowskim opodatkowania.

Przepisy określające zasady wystawiania faktur zawierają jeszcze jeden przepis szczególny dotyczący sprzedaży wysyłkowej z terytorium kraju i sprzedaży wysyłkowej na terytorium kraju. Otóż jak wynika z art. 106e ust. 6 ustawy o VAT, transakcje takie nie mogą być dokumentowane fakturami uproszczonymi. A zatem faktury dokumentujące sprzedaż wysyłkową z terytorium kraju podlegającą opodatkowaniu podatkiem VAT w Polsce muszą zawsze zawierać pełną treść.

Na podatnikach dokonujących sprzedaży wysyłkowej z terytorium kraju, gdy miejscem jej dokonania jest państwo przeznaczenia ciążą dodatkowe obowiązki. Zgodnie z art. 23 ust. 14 ustawy o VAT, warunkiem uznania sprzedaży wysyłkowej z terytorium kraju za dostawę dokonaną na terytorium państwa członkowskiego przeznaczenia jest posiadanie przez podatnika, przed upływem terminu do złożenia deklaracji za dany okres rozliczeniowy (miesiąc lub kwartał) następujących dokumentów (jeżeli dokumenty te łącznie potwierdzają dostarczenie towarów do nabywcy znajdującego się na terytorium państwa członkowskiego przeznaczenia dla wysyłanych lub transportowanych towarów):

- dokumentów przewozowych otrzymanych od przewoźnika (spedytora) odpowiedzialnego za wywóz towarów z terytorium kraju – w przypadku, gdy przewóz towarów jest zlecany przez podatnika przewoźnikowi;
- dokumentów potwierdzających odbiór towarów poza terytorium Polski.

Jeśli dokumenty powyższe nie potwierdzają jednoznacznie dostarczenia towarów do nabywcy znajdującego się na terytorium państwa członkowskiego

przeznaczenia dla wysyłanych lub transportowanych towarów, dokumentami wskazującymi, że wystąpiła dostawa towarów na terytorium państwa członkowskiego przeznaczenia dla wysyłanych lub transportowanych towarów mogą być również inne dokumenty otrzymywane przez podatnika w tego rodzaju dostawie towarów, tzw. dokumenty pomocnicze (przy czym przyjmuje się, że z dokumentów pomocniczych można korzystać również w sytuacji, gdy brak jest jednego lub więcej z dokumentów podstawowych). Dokumentami takimi, zgodnie z art. 23 ust. 15 ustawy o VAT, są w szczególności:

1) korespondencja handlowa z nabywcą, w tym jego zamówienie;
2) dokument potwierdzający zapłatę za towar, z wyjątkiem przypadków, gdy dostawa ma charakter nieodpłatny lub zobowiązanie jest realizowane w innej formie; w takim przypadku inny dokument stwierdzający wygaśnięcie zobowiązania.

Jeżeli warunek dotyczący otrzymania dokumentów opisanych powyżej, potwierdzających dostawę z terytorium kraju nie jest spełniony (tj. podatnik nie otrzyma przed upływem terminu do złożenia deklaracji wymaganych dokumentów), podatnik nie wykazuje dostawy w ewidencji VAT za dany okres rozliczeniowy (jak również w deklaracji VAT). W takiej sytuacji:

1) dostawa jest wykazywana w kolejnym okresie rozliczeniowym (w ewidencji VAT oraz deklaracji VAT), jako sprzedaż poza terytorium kraju – jeśli przed upływem terminu do złożenia tej deklaracji podatnik otrzyma wymagane dokumenty;
2) dostawa jest wykazywana w kolejnym okresie rozliczeniowym (w ewidencji VAT oraz deklaracji VAT), jako sprzedaż na terytorium kraju (w przypadku sprzedaży opodatkowanej stawka podstawową) – jeżeli przed upływem terminu do złożenia tej deklaracji podatnik nie otrzyma wymaganych dokumentów (art. 23 ust. 15a ustawy o VAT).

W tym drugim przypadku późniejsze otrzymanie dokumentów wskazujących, że wystąpiła dostawa towarów na terytorium państwa członkowskiego przeznaczenia dla wysyłanych lub transportowanych towarów, uprawnia podatnika do dokonania korekty podatku należnego w ramach deklaracji VAT za miesiąc/kwartał, w którym podatnik otrzymał te dokumenty (art. 23 ust. 15b ustawy o VAT).

Podsumowując tę część opisanego zagadnienia – podatnik napotyka na szereg problemów:

- po pierwsze – musi wdrożyć różne systemy dokumentowania sprzedaży – obowiązujące w różnych krajach;

- po drugie – co jest niezwykle trudne – opodatkowanie sprzedaży w kraju przeznaczenia nie zwalnia automatycznie podatnika z opodatkowania danej sprzedaży w Polsce. Musi on bowiem udowodnić (udokumentować) – w określonych przepisami terminach oraz w określony sposób, że dostarczył towar do finalnego odbiorcy. Jest to proces niezwykle trudny i kosztowny, bo jeśli weźmiemy pod uwagę, że przedmiotem rozważań są tysiące drobnych wysyłek – często zamykających się w kwotach kilkudziesięciu złotych, przesyłanych przez kurierów – to koszty gromadzenia dokumentacji związanych z każdą z tych drobnych wysyłek może stanowić znaczącą część kwoty, którą sprzedawca jest w stanie uzyskać ze sprzedaży. Z reguły sprzedaży wysyłkowa – konsumentowi kojarzy się możliwością uzyskania niskiej ceny zakupu zatem koszty administracyjne sprzedaży nie powinny być wysokie. A konieczność sprostania wymogom określonym w przepisach jest bardzo kosztowna. Zatem przepisy w tym zakresie – choć zrozumiałe często mogą być barierą w dokonywaniu takiej sprzedaży ze względu na zbyt wysokie koszty ich zastosowania.

Obowiązek dokumentowania obrotu przy pomocy kasy fiskalnej przy sprzedaży wysyłkowej

Co do zasady - w myśl art. 111 ust. 1 ustawy o VAT, podatnicy obowiązani są prowadzić ewidencję obrotu i kwot podatku należnego przy zastosowaniu kas rejestrujących (fiskalnych) w zakresie sprzedaży dokonywanej na rzecz osób fizycznych nieprowadzących działalności gospodarczej oraz rolników ryczałtowych. Niemniej jednak – na mocy Rozporządzenia Ministra Finansów z dnia 29 listopada 2012 roku w sprawie zwolnień z obowiązku prowadzenia ewidencji przy zastosowaniu kas rejestrujących [Dz. U. poz. 1382], przewidzianych zostało szereg zwolnień od powyższego obowiązku. Zgodnie z §3 ust.1 pkt1 rozporządzenia, zwalnia się z obowiązku ewidencjonowania (za pomocą kas fiskalnych) do dnia 31 grudnia 2014 roku podatników, u których kwota obrotu realizowanego na rzecz osób fizycznych nieprowadzących działalności gospodarczej oraz rolników ryczałtowych nie przekroczyła w poprzednim roku podatkowym kwoty 20.000 zł, a w przypadku podatników rozpoczynających w poprzednim roku podatkowym dostawę towarów lub świadczenie usług na rzecz osób fizycznych nieprowadzących działalności gospodarczej oraz rolników ryczałtowych, jeżeli kwota obrotu z tego tytułu nie przekroczyła, w proporcji do okresu wykonywania tych czynności w poprzednim roku podatkowym, kwoty 20.000 zł. Wskaza-

ne w poprzednim akapicie zwolnienie traci moc po upływie dwóch miesięcy następujących po miesiącu, w którym podatnik przekroczył 20.000 obrotu realizowanego na rzecz osób fizycznych nieprowadzących działalności gospodarczej oraz rolników ryczałtowych.

Oprócz powołanego zwolnienia, które ze względu na niski limit kwoty najczęściej nie będzie miało zastosowania w omawianym zagadnieniu – „w myśl §2 ust.1 rozporządzenia w związku z poz. 36 załącznika do powołanego rozporządzenia zwalnia się z obowiązku ewidencjonowania - do dnia 31 grudnia 2014 roku - dostawę towarów w systemie wysyłkowym (pocztą lub przesyłkami kurierskimi), pod warunkiem, że zapłaty za wykonaną czynność dokonano w całości za pośrednictwem poczty, banku lub spółdzielczej kasy oszczędnościowo-kredytowej (odpowiednio na rachunek bankowy podatnika lub na rachunek podatnika w spółdzielczej kasie oszczędnościowo-kredytowej, której jest członkiem), a z ewidencji i dowodów dokumentujących zapłatę jednoznacznie wynika, jakiej konkretnie czynności dotyczyła i na czyją rzecz została dokonana (dane nabywcy, w tym jego adres)" [Paweł Łabno – odpowiedź – lex 190193].

Podsumowując - teoretycznie zasady stosowania kas fiskalnych są przejrzyste tj. przy prowadzeniu sklepu internetowego można skorzystać ze zwolnienia z ewidencjonowania sprzedaży za pomocą kasy fiskalnej, ale:

po pierwsze – obowiązujące zwolnienie jest przewidziane wyłącznie do końca 2014 roku. Co prawda historia ww. zwolnienia pokazuje, że jest ono cały czas przedłużane, niemniej jednak nie potwierdza to stabilizacji uwarunkowań podatkowo – prawnych dla przedsiębiorców, potwierdzając chaos legislacyjny, w wyniku którego przedsiębiorcy co roku zastanawiają się jakie będą mieli obowiązki związane z prowadzonym przez siebie biznesem;

po drugie – w przypadku dobrowolnego wprowadzenia kasy fiskalnej – pojawiają się problemy związane z datą, w której sprzedaż ta powinna na kasie być zafiskalizowana – o czym była mowa wcześniej – tj. przy omawianiu daty obowiązku podatkowego przy sprzedaży towarów;

po trzecie – problemem jest prowadzenie ewidencji zwrotów towarów, których kasa fiskalna nie przyjmuje. Zwroty towarów – które są zagwarantowane prawnie nabywcy przy sprzedaży wysyłkowej – trzeba zestawiać ręcznie – dołączając do zestawienia otrzymane zwrotnie paragony/faktury. Jest to znowu czynność teoretycznie łatwa w realizacji, ale powodująca dużą czasochłonność – biorąc pod uwagę, że przy miesięcznych wysyłkach ok 7.000 sztuk – mamy statystycznie 12% zwrotów – to oznacza – prowadzenie ręczne rejestru zwrotów – w ilości około 840 sztuk;

po czwarte – przepis rozporządzenia umożliwiający zastosowanie zwolnienia z ewidencji za pomocą kas fiskalnych nakłada obowiązek prowadzenia ewidencji otrzymanych zapłat, z której jednoznacznie wynika, jakiej konkretnie czynności dotyczyła i na czyją rzecz została dokonana (min. dane nabywcy, w tym jego adres). Prowadzenie takiej ewidencji rodzi liczne niebezpieczeństwa. Należy pamiętać, że bardzo często w drodze zakupów internetowych konsumenci nabywają dobra „wrażliwe" – tj. suplementy diety, bieliznę czy inne przedmioty, o których zakupie nie chcieliby informować publicznie. Zatem prowadzenie takiej ewidencji obliguje do zachowania szczególnych środków ostrożności oraz stosowania licznych zabezpieczeń związanych z ochroną tych danych.

Obecnie bardzo często przy zakupach internetowych wykorzystuje się pośredników płatniczych typu min.: payu, paypal, dotpay, przelewy24 do ściągania pieniędzy od indywidualnego klienta. Dlaczego sprzedawcy/nabywcy korzystają z przykładowo wymienionych pośredników? i jakie to rodzi konsekwencje? Sprzedawcy korzystają z pośredników, gdyż pośrednik daje konsumentowi gwarancję zwrotu pieniędzy przy zgłoszonym braku dostawy. Zatem biorąc pod uwagę specyfikę sprzedaży wysyłkowej przez Internet – tj. dużą ilość odbiorców indywidualnych, którzy dokonują zakupów danego produktu często incydentalnie, a zatem często niemogących nabrać zaufania do dostawcy – zachowanie sposobu płatniczego zapewniającego bezpieczeństwo nabywcy jest często warunkiem dojścia transakcji do skutku. Jednakże wpłata klienta na rachunek pośrednika płatniczego nie jest równoznaczna z wpłatą pośrednika na rachunek bankowy sprzedawcy. Sposób i częstotliwość wpłat przez pośrednika na rachunek dostawcy zależy od uzgodnionych zasad współpracy między pośrednikiem a sprzedawcą. Strony mogą na przykład uzgodnić, że pośrednik płatniczy wpłaca zebrane pieniądze z dowolną częstotliwością, tj. raz w tygodniu lub raz dziennie. Oczywiście pośrednik nie wpłaca indywidualnych wpłat dokonanych przez nabywców na rachunek bankowy sprzedawcy. Pośrednik dokonuje wpłat w tzw. „paczkach" zawierających kilka/kilkanaście lub kilkadziesiąt wpłat, po pomniejszeniu o swoją prowizję, przeliczoną umownym kursem na walutę rozliczenia. Podsumowując możemy spotkać się z sytuacją, że sprzedaż na rzecz finalnych odbiorców dokonana jest w różnych walutach i o różnym czasie, a wpłata pośrednika na rachunek sprzedawcy realizowana jest w uzgodnionej walucie – np. walucie lokalnej (PLN), po pomniejszeniu o należną pośrednikowi prowizję za usługi płatnicze i przewalutowanie. Zatem w momencie otrzymania wpłaty na rachunek nie ma bezpośredniego powiązania z dokumentem sprzedaży lub dostawy przez sprzedawcę. Trudno jest zatem stoso-

wać zwolnienie z obowiązku rejestracji sprzedaży na kasie fiskalnej. A w sytuacji, gdy firmy nie stosują zwolnienia z obowiązku stosowania kas fiskalnych – czyli fiskalizują całą swoją sprzedaż – muszą uważać, aby nie zafiskalizować transakcji sprzedaży opodatkowanej w kraju odbiorcy.

Ewidencja sprzedaży wysyłkowej

W nawiązaniu do powyżej opisanych problemów stosowania przepisów prawa podatkowego najczęściej sklepy internetowe dokumentują swoją sprzedaż ujmując ją w całości na kasie fiskalnej. Dąży się, aby moduł kasa fiskalna był zsynchronizowany z tzw. „panelem zamówień" i systemem wysyłek. Najczęściej bezpośrednio z „panelu zamówienia" – po złożeniu przez klienta zamówienia i zaakceptowaniu przez niego płatności - przekazywane są dane do zdjęcia ze stanu magazynowego towaru w celu jego zapakowania i jak najszybszego nadania do wysyłki, a do wysyłanej paczki dodawany jest wystawiony paragon lub faktura. Dokumenty sprzedaży przeliczane są kursem z dnia poprzedzającego dany dzień tj. dzień wydania i sprzedaży. Jeśli mamy do czynienia ze sprzedażą zagraniczną faktura wystawiana jest w walucie obcej i przeliczana na kwotę w PLN (przy czym wtedy nie ma obowiązku wystawiania paragonu fiskalnego). Następnie – po czasie sprzedawca otrzymuje wpłatę „paczki" pieniędzy w innej kwocie i winnej walucie, niż waluta sprzedaży, bez opisu których faktur sprzedaży czy paragonów dana wpłata dotyczy. W praktyce najczęściej kwoty wpłat są otrzymane z opóźnieniem i w mniejszych kwotach. Pojawia się pytanie – czym są i jak rozliczać różnice? Teoretycznie wiadomo, że różnice związane są z kosztami pośrednika – na które później sprzedawca otrzymuje fakturę, ale również z różnicami kursowymi. I tu w rozliczeniach dochodzi kolejna trudność związana ze stosowaniem prawa podatkowego, a mianowicie z ustaleniem podatkowych różnic kursowych. „Dodatnie różnice kursowe zdefiniowano w art. 15a ust. 2 ustawy o CIT [(Dz.U.2011.74.397 ze zm.] i art. 24c ust. 2 ustawy o PIT [Dz. U. 2012.361 ze zm.]. Zgodnie z powołanymi przepisami powstają one, jeżeli kwota przychodu należnego, wyrażonego w walucie obcej po przeliczeniu na złote według kursu średniego ogłoszonego przez NBP jest niższa od kwoty tego przychodu w dniu jej otrzymania (zapłaty) w walucie obcej, przeliczonej według faktycznie zastosowanego kursu waluty z tego dnia.

Według takich samych zasad, lecz na skutek odwrotnego kierunku zmiany kursu walutowego, powstają ujemne różnice kursowe. Mowa o nich jest w art. 15a ust. 3 ustawy o CIT i art. 24c ust. 3 ustawy o PIT. Ujemne różnice

kursowe powstają przede wszystkim wtedy, gdy przychód należny jest wyższy od otrzymanego, a koszt poniesiony jest niższy od kosztu w dniu zapłaty" [Koc, Waślicki, lex 93834]. Zatem zgodnie z powołanymi przepisami - różnice kursowe akceptowalne przez prawo podatkowe powstają wyłącznie wtedy gdy sprzedaż w walucie wiąże się z wpływem pieniędzy na rachunek bankowy sprzedawcy w walucie. W opisanej sprzedaży taka sytuacja często nie ma miejsca, gdyż niejednokrotnie sprzedaż w różnych walutach – co prawda „zbierana" jest przez pośrednika płatniczego w walutach, ale następnie wpłacana jest na rachunek bankowy sprzedawcy w PLN, lub odwrotnie – sprzedaż w PLN, otrzymana przez pośrednika płacowego w PLN – wpłacana jest na rachunek sprzedawcy w walucie. Przy czym sprzedawca nie może zidentyfikować – które „paczki" wpłat podlegają której zasadzie, gdyż sprzedawca nie może narzucić pośrednika płacowego odbiorcy – a tym samym nie może ująć w jeden spójny system zasad rozliczeń dotyczący konkretnego kierunku sprzedaży. To nabywca finalny wybiera, podczas składania zamówienia, sposób płatności i pośrednika. Zatem – przy braku powiązania konkretnego wydania z konkretnym „kawałkiem" wpłaconej „paczki" – nie ma możliwości udowodnienia, że różnice kursowe są różnicami podatkowymi, bądź nie. Problematyczna staje się również dokładna wycena należności od pośredników płacowych na dany dzień bilansowy, rzutująca finalnie na sprawozdanie finansowe prezentowane także dla celów rachunkowych. Albowiem trudno jest też ustalić na przełomie okresów rozliczeniowych – jaka powinna zostać na dany dzień należność od konkretnego pośrednika płacowego, gdyż wpłaty z różnych krajów oraz z różnych banków nabywców wpływają na rachunek pośrednika w różnych terminach. Można zatem jedynie w przybliżeniu ustalić, że należność, która powinna zostać na dzień bilansowy wynosi określoną kwotę, a różnica do pozostałego salda jest rachunkową różnicą kursową. Takich problemów można by było uniknąć przy kompletnym powiązaniu: „panelu zamówień" związanego z systemem sprzedaży oraz systemem wpłat. Teoretycznie jest to możliwe, gdyż w przypadku komercyjnego obrotu systemy rachunkowe już to potrafią robić. Wyróżnikiem, po którym łączona jest transakcja najczęściej jest numer faktury. W analizowanym jednakże przypadku wpłaty nie posiadają „numeru faktury", gdyż dokonywane są w spłatach tzw. „paczek" łączących kilkaset transakcji. Oczywiście samo zagadnienie jest proste do rozwiązania w przypadku jednostkowych transakcji – niemniej jednak biorąc pod uwagę masowość sprzedaży oraz brak w opisie wpłaty od pośrednika wyróżnika w postaci numeru dokumentu sprzedaży – zagadnienie staje się bardzo skomplikowane. Najczęściej systemy płatnicze przesyłają równolegle do „przekazanych

paczek" wpłat dzienne zestawienia, które prezentują listę indywidualnych wpłat znajdujących się w „paczce" według numeru faktury, czy numeru zamówienia. Niemniej jednak listy te są przez każdego pośrednika przesyłane w innym formacie IT, według różnych kursów, w różnych walutach oraz z inną konfiguracją zawartych w nich danych. Zatem informatycznie nie da się przygotować jednego szablonu, który obsługiwałby pomocnicze listy przesyłane przez pośredników do każdej otrzymanej wpłaty.

Zatem często firmy zajmujące się sprzedażą internetową na szeroką skalę – upraszczają rachunkowość – przyjmując w saldzie należności a dzień bilansowy średnią sprzedaż z ostatnich dni roku – wpisując przyjęte uproszczenie do stosowanej przez siebie polityki rachunkowości, a dla celów podatkowych – rozliczają różnice powstałe po stronie MA – w przychody podatkowe, a po stronie WN – w koszty niepodatkowe. Przy czym dokonują takiego rozliczenia raz na koniec roku, a nie na koniec każdego miesiąca – również przy uwzględnieniu odpowiedniego zapisu w polityce rachunkowości. Oczywiście taki sposób rozliczeń może budzić wątpliwości przy ewentualnej kontroli skarbowej, natomiast jest on często stosowany gdyż zastosowanie klasycznego porównania konkretnej sprzedaży z konkretną, przypisaną do niej wpłatą jest – ze względu na ilość transakcji oraz różnorodność sposobu raportowania albo niemożliwe do zastosowania albo zbyt kosztowne.

Podsumowanie

Polscy przedsiębiorcy starają się elastycznie dostosować się do wymagań klientów znajdujących się na globalnym rynku. Internet otwiera niemalże nieograniczone możliwości rozwoju oraz poszerzania rynków zbytu i docierania do klientów zlokalizowanych w innej części świata. Należałoby postulować jedynie do regulatora o zmniejszanie barier prawno-podatkowych związanych z tą dziedziną. Jest ona bowiem bardzo mobilna, zatem brak uproszczeń w regulacjach może być przyczyną do ucieczki w inne miejsca na świecie.

Bibliografia

Bartosiewicz A., Kubacki R. (2013), *VAT 7* – komentarz, wyd. Wolters Kluwer Polska Sp. z o.o.

Koc S., Waślicki T., *Różnice kursowe w świetle prawa podatkowego i bilansowego*, lex 93834.

Krzywan T., *Sprzedaż wysyłkowa w podatku od towarów i usług*, wydawnictwo lex 71887.

Łabno P. – odpowiedź – lex 190193.

Militz M. (2014), *Nowe zasady powstawania obowiązku podatkowego w VAT – ułatwienia czy utrudnienia?*. Przegląd Podatkowy nr 2/2014.

Pokojska A. (2014), *Decyduje data wydania towaru przewoźnikowi*, „Dziennik Gazeta Prawna" z 12 maja 2014, B3.

Polski rynek e-commerce rośnie w szybkim tempie, rozwijając się pomimo obecnego spowolnienia w gospodarce realnej – WWW.inwestor.msp.gov.pl/si/polska-gospodarka/wiadomosci-gospodarcze/25090,doc

Raport *The Internet Economy in G-20,* The Boston Consulting Group, www.ecommercepolska.pl

Rozporządzenie Ministra Finansów z dnia 29 listopada 2012 r. w sprawie zwolnień z obowiązku prowadzenia ewidencji przy zastosowaniu kas fiskalnych (publikacja Dz.U.2012.1382).

Sachs K., Namysłowski R. (2008), *Dyrektywa VAT,* wyd. Wolters Kluwer Polska Sp. z o.o.

Ustawa o CIT – ustawa z dnia 15 lutego 1992 roku „o podatku dochodowym od osób prawnych" (publikacja Dz. U. z 2011 r., nr 74, poz. 397 ze zm.).

Ustawa o PIT – ustawa z dnia 26 lipca 1991 roku o podatku dochodowym od osób fizycznych (publikacja Dz. U. z 2012 r., nr 361 ze zm.).

Ustawa z dnia 11 marca 2004 roku „o podatku od towarów i usług" (publikacja: Dz. U. z 2011 r. nr 177, poz. 1054 ze zm.)

Wpływ E-commerce na gospodarkę – www.deloitte.com/view/pl_PL/pl/dla-prasy/Raporty

www.mf.gov.pl – strona internetowa Ministerstwa Finansów

Zmiany w zakresie określania momentu powstania obowiązku podatkowego w VAT od 1 stycznia 2014 r., Ministerstwo Finansów, WWW.mf.gov.pl

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 83-96

Edyta Średzińska
Urząd Skarbowy w Brodnicy

Zasady odliczania podatku od towarów i usług (VAT) od pojazdów samochodowych po 31 marca 2014 roku

Principles of VAT deductions on vehicles after 21 March 2014

Abstract: As the result of the amendments to VAT Act of 1 April 2014 the amendments concerning VAT tax settlements on company cars were introduced. The objects were given additional evidence obligations and it became possible to correct input tax in the case of a change of a vehicle usage. Learning about the new principles is going to have a significant influence on honesty in VAT settlement and keeping accounts.

Key words: Evidence obligation, correction of input tax, full VAT deductibility, 50% VAT deductibility.

Wstęp

W dniu 17 grudnia 2013 r., Rada Unii Europejskiej wydała decyzję wykonawczą, dzięki której Polska uzyskała zgodę na czasowe pogorszenie sytuacji podatników w porównaniu ze stanem sprzed 1 maja 2014 r., czyli przed wejściem Polski do Unii Europejskiej. W decyzji tej zostały określone warunki dalszego stosowania przez Polskę ograniczeń w odliczeniu naliczonego podatku VAT związanego z nabyciem niektórych aut osobowych oraz związanych z nimi wydatkami. Wydanie decyzji przez Radę Unii Europejskiej upoważniło Polskę do wprowadzenia krajowych przepisów określających nowe zasady odliczania podatku VAT, w tym także nowe ograniczenia w zakresie wydatków dotyczących określonych pojazdów. Odstępstwo to wynika z art. 26 ust. 1 lit. a) i art. 168 dyrektywy 2006/112/WE w sprawie wspólnego systemu podatku od wartości dodanej (Dz. Urz. UE L 353 z 28.12.2013, s. 51).

Wprowadzone zmiany wynikają również z konieczności dostosowania przepisów o podatku od towarów i usług do tez wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 lipca 2012 r. w sprawie C-160/11 Bawaria Motors.

Celem artykułu jest przedstawienie nowych zasad odliczania podatku naliczonego VAT od wydatków związanych z określonymi pojazdami samochodowymi. Jak również możliwość wykorzystywania przez podatników VAT samochodów osobowych i innych pojazdów samochodowych do 3,5 tony zarówno do celów służbowych jak i prywatnych.

Nowe zasady i ograniczenia w tym zakresie, które w większości obowiązują od 1 kwietnia 2014 r., zostały wprowadzone:

- Ustawą z dnia 7 lutego 2014 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz. U. z 2014 r., poz. 312),
- Rozporządzeniem Ministra Finansów z dnia 19 marca 2014 r. zmieniającym rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2014 r., poz. 369),
- Rozporządzeniem Ministra Finansów z dnia 21 marca 2014 r. w sprawie wzoru informacji o pojazdach samochodowych wykorzystywanych wyłącznie do działalności gospodarczej (Dz. U. z 2014 r., poz. 371),
- Rozporządzeniem Ministra Finansów z dnia 27 marca 2014 r. w sprawie pojazdów samochodowych uznawanych za wykorzystywane wyłącznie do działalności gospodarczej podatnika (Dz. U. z 2014 r., poz. 407).

Definicja pojazdu samochodowego

Pomimo przejściowego charakteru regulacji, które mają obowiązywać do końca 2016 roku (z możliwością ich przedłużenia), ustawodawca dodał do słownika ustawy o podatku od towarów i usług definicję „pojazdu samochodowego". Zgodnie z art. 2 pkt 34 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2011 r. nr 177, poz.1054 ze zm.), od 1 kwietnia 2014 roku, przez pojazdy samochodowe – rozumie się pojazdy samochodowe w rozumieniu przepisów o ruchu drogowym o dopuszczalnej masie całkowitej nieprzekraczającej 3,5 tony. Zatem na potrzeby podatku VAT za pojazd samochodowy będzie uznany każdy pojazd silnikowy (wyposażony w silnik, z wyjątkiem motoroweru i pojazdu szynowego), którego konstrukcja umożliwia jazdę z prędkością przekraczającą 25 km/h, inny niż ciągnik rolniczy, którego dopuszczalna masa całkowita nie przekracza 3,5 tony. Odesłanie do przepisów ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2012 r., poz. 1137 ze zm.) eliminuje spory i wątpliwości uznania lub nieuznania za pojazd samochodowy takich pojazdów jak motocykle czy quady, które od 1 kwietnia 2014 roku na płaszczyźnie ustawy o podatku od towarów i usług zaliczane są kategorii pojazdów samochodowych.

Natomiast pojazdy samochodowe o dopuszczalnej masie całkowitej przekraczającej 3,5 tony, wykorzystywanie przez podatników w działalności gospodarczej, nie są uznawane za pojazdy samochodowe na gruncie ustawy o VAT.

Ograniczenie w odliczaniu podatku naliczonego

Celem ustawodawcy było ograniczenie możliwości odliczenia podatku naliczonego z 60% do 50% kwoty podatku wynikającego z faktur dokumentujących nabycie, w tym także wewnątrzwspólnotowe nabycie, wytworzenie oraz import pojazdów samochodowych, a także najem, dzierżawę, leasing, itp. takich pojazdów. Zasady te wynikają z nowego brzmienia art. 86a ustawy o podatku od towarów i usług. Ograniczenie to nie dotyczy jednak wszystkich pojazdów wykorzystywanych przez podatnika, a jedynie tych, które jednocześnie wykorzystywane są na potrzeby działalności gospodarczej i dla celów prywatnych, czyli do tzw. celów mieszanych. Zmiany dotyczą również podatku naliczonego z faktur dokumentujących inne wydatki, związane z tego typu pojazdami, które do tej pory nie podlegały ograniczeniom. Odliczenie 50% kwoty podatku naliczonego dotyczy także faktur paliwowych oraz faktur dokumentujących wydatki eksploatacyjne, takich jak zakup części zamiennych, naprawa, konserwacja, ubezpieczenie, itp.

Przy czym dodać należy, że na podstawie art. 12 ustawy nowelizującej, do końca czerwca 2015 roku przedłużono zakaz odliczania podatku naliczonego od zakupu paliwa do niektórych pojazdów. Dotyczy to paliw silnikowych, oleju napędowego oraz gazu, wykorzystywanych do napędu:

1) samochodów osobowych;
2) innych niż samochody osobowe pojazdów samochodowych o dopuszczalnej masie całkowitej nieprzekraczającej 3,5 tony, w których liczba miejsc (siedzeń) łącznie z miejscem dla kierowcy wynosi:
   a) 1 – jeżeli dopuszczalna ładowność jest mniejsza niż 425 kg,
   b) 2 – jeżeli dopuszczalna ładowność jest mniejsza niż 493 kg,
   c) 3 lub więcej – jeżeli dopuszczalna ładowność jest mniejsza niż 500 kg.

Dopuszczalna ładowność pojazdu oraz liczba miejsc (siedzeń), powinna wynikać z dokumentów wydanych zgodnie z przepisami o ruchu drogowym. Jeżeli w tych dokumentach nie będzie określonej dopuszczalnej ładowności lub liczby miejsc, pojazd uznany będzie jako samochód osobowy.

Zatem od 1 kwietnia 2014 r. nie przysługuje nawet ograniczone prawo do odliczenia podatku VAT od zakupu paliwa do samochodu osobowego oraz innego pojazdu samochodowego wykorzystywanego do celów miesza-

nych, jeżeli od takiego zakupu nie przysługiwało prawo do odliczenia podatku VAT przed 1 kwietnia 2014 roku.

Zmiany w zakresie odliczenia 50% mają swoje plusy i minusy. Są korzystne gdyż nie ma limitu kwotowego wartości odliczenia podatku VAT, a także dają możliwość odliczenia podatku naliczonego z faktur paliwowych. Niekorzystne jednak jest ograniczenie ze 100% do 50% możliwości odliczenia podatku VAT z faktur dokumentujących wydatki eksploatacyjne.

Pełne odliczenie podatku naliczonego

Pojazdy uprzywilejowane. Od 1 kwietnia 2014 r. ograniczeń przy odliczaniu podatku naliczonego nie stosuje się do pojazdów tzw. uprzywilejowanych. Zgodnie z art. 86a ust. 4 pkt 2 ustawy o VAT, za pojazdy samochodowe uznawane za wykorzystywane wyłącznie do działalności gospodarczej podatnika uważa się takie, których konstrukcja wyklucza ich użycie do celów niezwiązanych z działalnością gospodarczą lub powoduje, że ich użycie do celów niezwiązanych z działalnością gospodarczą jest nieistotne. Do tej grupy pojazdów na podstawie art. 86a ust 9 pkt 1 i 2 ustawy należą:

1) pojazdy samochodowe, inne niż samochody osobowe, mające jeden rząd siedzeń, który oddzielony jest od części przeznaczonej do przewozu ładunków ścianą lub trwałą przegrodą:
   a) klasyfikowane na podstawie przepisów o ruchu drogowym do podrodzaju: wielozadaniowy, van lub
   b) z otwartą częścią przeznaczoną do przewozu ładunków;
2) pojazdy samochodowe, inne niż samochody osobowe, które posiadają kabinę kierowcy z jednym rzędem siedzeń i nadwozie przeznaczone do przewozu ładunków, jako konstrukcyjnie oddzielne elementy pojazdu.

Spełnienie wymagań dla tej grupy pojazdów stwierdza się na podstawie dodatkowego badania technicznego przeprowadzonego przez okręgową stację kontroli pojazdów, potwierdzonego zaświadczeniem wydanym przez tę stację oraz dowodu rejestracyjnego pojazdu zawierającego adnotację o spełnieniu tych wymagań. Wynika to z zapisu art. 86a ust.10 pkt 1 ustawy. Warto dodać, że nie istnieje obowiązek dostarczenia do urzędu skarbowego zaświadczenia wydanego przez okręgową stację kontroli pojazdów. Istnieje jednak obowiązek przeprowadzenia takiego badania nawet w przypadku, gdy badanie takie przeprowadzone było przed 1 kwietnia 2014 r.. Wymóg ponownego badania nie dotyczy jedynie pojazdów samochodowych, innych niż samochody osobowe, mające jeden rząd siedzeń, który oddzielony jest od

części przeznaczonej do przewozu ładunków ścianą lub trwałą przegrodą klasyfikowane na podstawie przepisów o ruchu drogowym do podrodzaju: wielozadaniowy, van. Tylko dla tych pojazdów samochodowych wcześniejsze badanie techniczne zachowuje swoją aktualność. Ponadto na podstawie przepisów przejściowych art. 9 ust. 1 ustawy z dnia 7 lutego 2014r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz. U. z 2014 r., poz. 312), badanie techniczne pojazdów używanych przed 1 kwietnia 2014 r. należy przeprowadzić w terminie najbliższego okresowego badania technicznego, nie później jednak niż przed upływem 3 miesięcy licząc ten termin od 1 kwietnia 2014 r.

Pojazdy specjalne. Podobnie jak w przypadku tzw. pojazdów uprzywilejowanych, ograniczeń przy odliczaniu podatku naliczonego nie stosuje się do pojazdów specjalnychczyli do pojazdów samochodowych uznawanych za wykorzystywane wyłącznie do działalności gospodarczej podatnika, których konstrukcja wyklucza ich użycie do celów niezwiązanych z działalnością gospodarczą lub powoduje, że ich użycie do celów niezwiązanych z działalnością gospodarczą jest nieistotne. Zgodnie z art. 86a ust. 9 pkt 3 ustawy o podatku od towarów i usług, do pojazdów specjalnych zalicza się pojazdy określone dla następujących przeznaczeń:

- agregat elektryczny/spawalniczy,
- do prac wiertniczych,
- koparka, koparko-spycharka,
- ładowarka,
- podnośnik do prac konserwacyjno-montażowych,
- żuraw samochodowych,

jeżeli z dokumentów wydanych zgodnie z przepisami o ruchu drogowym wynika, że dany pojazd jest pojazdem specjalnym.

Na mocy delegacji zawartej w art. 86a ust. 16 ustawy z dnia 7 lutego 2014 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw (Dz. U. z 2014 r., poz. 312), Minister Finansów w rozporządzeniu z dnia 27 marca 2014 r. w sprawie pojazdów samochodowych uznawanych za wykorzystywane wyłącznie do działalności gospodarczej podatnika (Dz. U. z 2014 r., poz. 407), określił inne niż wymienione powyżej pojazdy samochodowe uznawane za wykorzystywane wyłącznie do działalności gospodarczej podatnika. Zgodnie z par. 2 tego rozporządzenia za pojazdy specjalne uznaje się pojazdy o przeznaczeniu:

– pogrzebowym,
– bankowóz – wyłącznie typu A i B,

jeżeli mają jeden rząd siedzeń albo ich dopuszczalna masa całkowita jest większa niż 3 tony. Ponadto pojazdy o przeznaczeniu pogrzebowym powinny posiadać dokumenty o spełnieniu wymagań określonych w par. 4 pkt 1 rozporządzenia Ministra Zdrowia z dnia 27 grudnia 2007 r. w sprawie wydawania pozwoleń i zaświadczeń na przewóz zwłok i szczątek ludzkich (Dz. U. nr 249, poz. 1866). Natomiast pojazdy o przeznaczeniu bankowóz – wyłącznie typu A i B, dokumenty potwierdzające wymagania określone w załączniku nr 3 lub 4 do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 7 września 2010 r. w sprawie wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych i transportowanych przez przedsiębiorców i inne jednostki organizacyjne (Dz. U. nr 166, poz. 1128 ze zm.).

Pozostałe pojazdy samochodowe. Do pojazdów samochodowych wykorzystywanych wyłącznie do działalności gospodarczej podatnika mogą być również zaliczane pozostałe pojazdy samochodowe, w tym samochody osobowe. Jednakże w takim przypadku podatnicy muszą stworzyć wewnętrzne zasady używania tych pojazdów, zapewniające wykorzystywanie ich wyłącznie na potrzeby działalności oraz prowadzić szczegółową ewidencję potwierdzającą wykorzystywanie pojazdu wyłącznie na potrzeby działalności gospodarczej.

Regulamin korzystania z samochodów służbowych może być wprowadzony przez pracodawcę – podatnika na takich samych zasadach jak regulamin pracy. Treść regulaminu może być bardzo różna, w zależności od woli i potrzeb pracodawcy. Jednakże w każdym regulaminie powinny znaleźć się standardowe postanowienia dotyczące tego, którzy pracownicy są uprawnieni do korzystania z samochodów służbowych oraz jakie samochody są przyznawane pracownikom na poszczególnych stanowiskach.

Ponadto w celu odliczenia pełnego podatku VAT, całość przebiegu samochodu musi mieć pokrycie w prowadzonej przez podatnika ewidencji. W przepisach ustawy o podatku od towarów i usług zamieszczona została specyfikacja danych, jakie muszą znaleźć się w ewidencji. Stanowi o tym art. 86a ust. 7 ustawy, zgodnie z którym ewidencja powinna zawierać:

1) numer rejestracyjny pojazdu samochodowego;
2) dzień rozpoczęcia i zakończenia prowadzenia ewidencji;
3) stan licznika przebiegu pojazdu samochodowego na dzień rozpoczęcia prowadzenia ewidencji, na koniec każdego okresu rozliczeniowego oraz na dzień zakończenia prowadzenia ewidencji;

4) wpis osoby kierującej pojazdem samochodowym dotyczący każdego wykorzystania tego pojazdu, obejmujący:
   a) kolejny numer wpisu,
   b) datę i cel wyjazdu,
   c) opis trasy (skąd – dokąd),
   d) liczbę przejechanych kilometrów,
   e) imię i nazwisko osoby kierującej pojazdem

   - potwierdzony przez podatnika na koniec każdego okresu rozliczeniowego w zakresie autentyczności wpisu osoby kierującej pojazdem, jeżeli nie jest ona podatnikiem;
5) liczbę przejechanych kilometrów na koniec każdego okresu rozliczeniowego oraz na dzień zakończenia prowadzenia ewidencji.

W przypadku, gdy pojazd samochodowy udostępniony zostanie osobie, która nie jest pracownikiem podatnika wpis, w zakresie osoby kierującej pojazdem samochodowym, zgodnie z art. 86a ust. 8 ustawy,

1) jest dokonywany przez osobę, która udostępnia pojazd;
2) obejmuje:
   a) kolejny numer wpisu,
   b) datę i cel udostępnienia pojazdu,
   c) stan licznika na dzień udostępnienia pojazdu,
   d) liczbę przejechanych kilometrów,
   e) stan licznika na dzień zwrotu pojazdu,
   f) imię i nazwisko osoby, której udostępniony został pojazd.

Ewidencja przebiegu pojazdu prowadzona dla celów podatku od towarów i usług nie wyznacza żadnego limitu podatku do odliczenia. Jednakże jeżeli wystąpi niezgodność pomiędzy liczbą kilometrów wykazanych w ewidencji i faktycznie przejechanych, podatnik utraci prawo do odliczenia w całości podatku naliczonego. Zatem nawet sporadyczne wykorzystanie pojazdu w innym celu pozbawi podatnika prawa do odliczenia 100% podatku naliczonego VAT.

Warto także wskazać, że ewidencja przebiegu pojazdu dla potrzeb podatku od towarów i usług nie zawiera wymogu podpisu, co może sugerować, że nie musi być prowadzona w formie papierowej, a może być prowadzona także w wersji elektronicznej.

Na mocy art. 86a ust. 12 ustawy o podatku od towarów i usług, podatnicy wykorzystujący wyłącznie do działalności gospodarczej pojazdy samochodowe, dla których są obowiązani prowadzić ewidencję przebiegu pojaz-

du, mają obowiązek złożyć naczelnikowi urzędu skarbowego informację o tych pojazdach w terminie 7 dni od dnia, w którym poniosą pierwszy wydatek związany z tymi pojazdami. W przypadku, gdy podatnik zaprzestanie prowadzenia takiej ewidencji, będzie także zobowiązany do poinformowania o tym fakcie organu podatkowego. Informacja taka powinna być przekazana nie później niż przed dniem dokonania zmiany. Wzór tej informacji (VAT-26) stanowi załącznik do Rozporządzenia Ministra Finansów z dnia 21 marca 2014 r. w sprawie wzoru informacji o pojazdach samochodowych wykorzystywanych wyłącznie do działalności gospodarczej (Dz. U. z 2014 r., poz. 371). Informacja VAT-26 zawiera dane podatnika oraz dane pojazdów samochodowych wykorzystywanych przez niego wyłącznie do działalności gospodarczej, czyli z pełnym odliczeniem VAT, a także datę poniesienia pierwszego wydatku na samochód. Dodatkowa pozycja – data zmiany wykorzystania, jest wypełniana jeżeli informacja VAT-26 jest składana jako aktualizacja.

Kary za niedopełnienie formalności i błędy

Warto tu zaznaczyć, że od 1 kwietnia 2014 roku zmianie uległy także przepisy ustawy z dnia 10 września 1999 r. – Kodeks Karny Skarbowy [Dz. U. z 2013 r., poz.186 ze zm.]. Zgodnie z dodanym art. 56a Kks podatnik, który nie złożył informacji VAT-26 albo złożył ją po terminie lub podał w niej dane niezgodne ze stanem rzeczywistym, a dokonał pełnego odliczenia podatku VAT, podlega karze grzywny do 720 stawek dziennych. Minimalne wynagrodzenie w 2014 roku wynosi 1680 zł. Zatem najwyższy wymiar grzywny może wynieść nawet 16 128 000 zł. Kary nie można jednak nakładać na podatnika, który złoży informację po terminie, ale przed dniem rozpoczęcia czynności sprawdzających w zakresie podatku VAT, doręczenia zawiadomienia o zamiarze wszczęcia kontroli podatkowej lub postępowania kontrolnego w ramach kontroli skarbowej w zakresie podatku VAT lub wszczęcia postępowania podatkowego w zakresie podatku od towarów i usług.

Tak więc podatnik, który zdecyduje się na odliczenie 100% podatku VAT będzie musiał wykazać się niezwykłą skrupulatnością oraz dbałością o wszelkie szczegóły i terminy. Grzywna taka nie grozi podatnikom, którzy będą korzystali z ograniczonego prawa do odliczenia podatku naliczonego.

Korygowanie podatku naliczonego

W związku z uchyleniem z dniem 1 kwietnia 2014 roku par.3 ust.1 pkt 20 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie

zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r., poz.1722 ze zm.), na podstawie którego do końca marca 2014 roku, korzystała ze zwolnienia dostawa samochodów osobowych oraz innych pojazdów samochodowych przez podatników, którym przy ich nabyciu przysługiwało prawo do obniżenia kwoty podatku należnego o podatek naliczony w wysokości 50% lub 60%, nie więcej jednak niż odpowiednio 5 lub 6 tys. zł, ustawodawca wprowadził do ustawy o podatku od towarów i usług poprzez art. 90b, tzw. system korekt podatku naliczonego.

Korekta taka wystąpi w przypadku zmiany wykorzystania pojazdu samochodowego w okresie 60 miesięcy od dnia jego nabycia, importu lub oddania w używanie. A dla pojazdów o wartości nie wyższej niż 15 000 zł okres korekty wyniesie 12 miesięcy. W ramach korekty podatnik może być zobligowany lub uprawniony do skorygowania VAT naliczonego. Chyba, że zmiana wykorzystania pojazdu samochodowego nastąpi po okresie korekty, czyli po upływie 60 miesięcy lub w przypadku pojazdów o wartości do 15 000 zł po 12 miesiącach.

Pamiętać jednak należy, że korekta zwiększająca podatek naliczony, powodowana zmianą przeznaczenia pojazdu samochodowego wiąże się z obowiązkiem zaprowadzenia ewidencji przebiegu pojazdu oraz złożenia do naczelnika urzędu skarbowego informacji VAT-26. Przy czym niezachowanie terminu i złożenie informacji po upływie 7 dni od dnia zaprowadzenia ewidencji będzie skutkowało tym, że moment korekty będzie odpowiadał dopiero dacie złożenia informacji VAT-26.

Korekta podatku naliczonego dokonywana jest w rozliczeniu za okres, w którym nastąpiła zmiana, a przy wyliczeniu proporcji przyjmuje się, że nowe wykorzystanie dotyczy już całego miesiąca, w którym ta zmiana nastąpiła.

Przykład 1. Podatnik nabył samochód osobowy w dniu 10 kwietnia 2014 r., który będzie wykorzystywał zarówno do celów prywatnych jak i do prowadzonej działalności gospodarczej (w całości opodatkowanej podatkiem VAT). Dane wynikające z faktury:

- cena netto – 100 000 zł,
- podatek VAT – 23 000 zł.

W deklaracji dla podatku od towarów i usług za miesiąc kwiecień 2014 roku podatnik odliczył podatek naliczony w wysokości 11 500 zł (23 000 x 50%).

Podatnik w dniu 23 lutego 2015 r. zmienia wykorzystanie tego samochodu. Będzie wykorzystywał go wyłącznie do prowadzonej działalności gospodarczej (w całości opodatkowanej podatkiem VAT). Wszelkie formalności względem urzędu skarbowego zostały dopełnione.

Podatnik z tego tytułu w rozliczeniu za miesiąc luty 2015 r. będzie miał prawo do podwyższenia kwoty podatku naliczonego do odliczenia o kwotę 9 583 zł, wg wyliczenia:

- kwota podatku VAT wynikająca z faktury – 23 000 zł,
- kwota podatku naliczonego faktycznie odliczona – 11 500 zł,
- kwota podatku nieodliczona – 11 500 zł,
- liczba miesięcy okresu korekty – 60,
- liczba miesięcy pozostałego okresu korekty (60 – 10) = 50,
- kwota korekty (11 500/60) x 50 = 9 583 zł.

Przykład 2. Podatnik nabył samochód osobowy w dniu 10 kwietnia 2014 roku, który będzie wykorzystywał tylko do prowadzonej działalności gospodarczej (w całości opodatkowanej podatkiem VAT). Wszelkie formalności względem urzędu skarbowego zostały dopełnione. Dane wynikające z faktury:

- cena netto – 70 000 zł,
- podatek VAT – 16 100 zł.

W deklaracji dla podatku od towarów i usług za miesiąc kwiecień 2014 r. podatnik odliczył podatek naliczony w wysokości 16 100 zł.

Podatnik w dniu 23 listopada 2017 r. zmienia wykorzystanie tego samochodu. Będzie wykorzystywał go do celów mieszanych.

Podatnik w rozliczeniu za miesiąc listopad 2017 roku będzie zobowiązany obniżyć kwotę podatku naliczonego do odliczenia o kwotę 2 281 zł, wg wyliczenia:

- kwota podatku VAT wynikająca z faktury – 16 100 zł,
- kwota podatku naliczonego faktycznie odliczona – 16 100 zł,
- kwota podatku naliczonego do odliczenia, jaka przysługiwałaby w chwili nabycia gdyby pojazd wykorzystywany był do celów mieszanych (16 100/50%) = 8 050 zł,
- liczba miesięcy okresu korekty – 60,
- liczba miesięcy pozostałego okresu korekty (60 – 43) = 17,
- wielkość korekty (8 050 / 60) x 17 = (-) 2 281zł.

Przykład 3. Podatnik nabył samochód osobowy w dniu 15 maja 2014 roku, który będzie wykorzystywał zarówno do celów prywatnych jak i do prowadzonej działalności gospodarczej (opodatkowanej podatkiem VAT i zwolnionej). Dane wynikające z faktury:

- cena netto – 100 000 zł,
- podatek VAT – 23 000 zł, ponadto
- obroty z opodatkowanej działalności gospodarczej w obrotach z całej działalności gospodarczej za 2013 rok stanowiły – 90%.

W deklaracji dla podatku od towarów i usług za miesiąc maj 2014 roku podatnik odliczył podatek naliczony w wysokości 10 350zł., tj. (23 000 x 50%) = 11 500 zł; 11 500 zł x 90% = 10 350 zł.

Podatnik w dniu 23 marca 2015 roku zmienia wykorzystanie tego samochodu. Będzie wykorzystywał go wyłącznie do prowadzonej działalności gospodarczej (opodatkowanej podatkiem VAT i zwolnionej). Wszelkie formalności względem urzędu skarbowego zostały dopełnione.

Podatnik z tego tytułu w rozliczeniu za miesiąc marzec 2015 roku będzie miał prawo do podwyższenia kwoty podatku naliczonego do odliczenia o kwotę 8 625 zł, wg wyliczenia:

- kwota podatku VAT wynikająca z faktury – 23 000 zł,
- kwota podatku naliczonego faktycznie odliczona – 10 350 zł,
- kwota podatku naliczonego do odliczenia, jaka przysługiwałaby w chwili nabycia gdyby pojazd wykorzystywany był wyłącznie do działalności gospodarczej – z uwzględnieniem proporcji (23 000 x 90%) = 20 700 zł,
- liczba miesięcy okresu korekty – 60,
- liczba miesięcy pozostałego okresu korekty (60 – 10) = 50,
- kwota korekty (0 350/ 60) x 50 = 8 625 zł.

Przykład 4. Podatnik prowadzący działalność gospodarczą w zakresie handlu detalicznego nabył w październiku 2012 r. samochód osobowy. Dane wynikające z faktury:

- cena netto – 80 000 zł,
- podatek VAT – 18 400 zł.

Podatek naliczony, który został odliczony w deklaracji dla podatku od towarów i usług za miesiąc październik 2012 r. wyniósł 6 000 zł.

W kwietniu 2014 r. podatnik sprzedaje ten samochód (zgodnie z przepisami jest to sprzedaż opodatkowana). Podatnik w rozliczeniu za miesiąc kwiecień 2014 roku będzie miał prawo podwyższyć kwotę podatku naliczonego do odliczenia o kwotę 8 680 zł, wg wyliczenia:

- kwota podatku VAT wynikająca z faktury – 18 400 zł.,
- kwota podatku naliczonego faktycznie odliczona – 6 000 zł,

- kwota podatku nieodliczona – 12 400 zł,
- liczba miesięcy okresu korekty – 60,
- liczba miesięcy pozostałego okresu korekty (60 – 18) = 42,
- kwota korekty (12 400/ 60) x 42 = 8 680 zł.

Na podstawie powyższych przykładów możemy zauważyć, że przepisy dotyczące korekt korzystne są dla podatników, którzy nabyli pojazd samochodowy objęty limitem odliczenia podatku naliczonego. Przy sprzedaży takiego pojazdu, w okresie obowiązywania korekty, co prawda nie będą mogli korzystać ze zwolnienia i będą zobowiązani opodatkować całą sprzedaż podatkiem VAT, jednakże będą mieli możliwość odzyskania części podatku VAT, który uprzednio nie stanowił podatku naliczonego.

Wyłączenie opodatkowania użytku prywatnego

Na podstawie art. 8 ust 5 Ustawy o podatku od towarów i usług, w przypadku wykorzystania przez podatnika do celów innych niż działalność gospodarcza, np. na cele prywatne podatnika lub jego pracowników, pojazdów samochodowych objętych wprowadzonym 50% ograniczeniem odliczenia podatku naliczonego, wyłączono konieczność rozliczania podatku VAT. W takiej sytuacji podatnik nie będzie miał obowiązku opodatkowania podatkiem VAT użytku prywatnego. Także w przypadku wykorzystywania pojazdu samochodowego do celów prywatnych także nie będzie opodatkowana, w sytuacji, gdy transakcja nabycia nie była opodatkowana podatkiem od towarów i usług lub korzystała ze zwolnienia, natomiast podatnikowi przysługiwało ograniczone 50% odliczenie podatku naliczonego z tytułu nabycia, importu lub wytworzenia części składowych do tego pojazdu. Ponadto zgodnie z art. 8 ust. 6 ustawy, wyłączenie z opodatkowania podatkiem VAT dotyczy również użytku na cele inne niż działalność gospodarcza pojazdów użytkowanych na podstawie umów najmu, dzierżawy, leasingu lub innej umowy o podobnym charakterze, w stosunku do których przysługiwało ograniczone 50% odliczenie podatku VAT.

Z analizy tych przepisów wynika, że zasada wyłączenia opodatkowania użytku prywatnego nie jest stosowana w przypadku gdy:

- podatnik posiadał pełne prawo do odliczenia podatku zarówno przy nabyciu pojazdu, jak i zakupionych do niego części składowych;
- podatnik posiadał pełne prawo do odliczenia podatku przy nabyciu pojazdu, natomiast przy nabyciu części składowych do tego pojazdu miał ograniczone prawo do 50%;

- podatnik nie posiadał prawa do odliczenia podatku przy nabyciu pojazdu, natomiast przy nabyciu części składowych do tego pojazdu miał pełne prawo odliczenia podatku VAT.

Ustawą nowelizującą VAT, na podstawie art. 7, wyłączono również obowiązek opodatkowania podatkiem od towarów i usług użytku prywatnego pojazdów zakupionych przed dniem 1 kwietnia 2014 roku objętych wówczas ograniczonym 50% lub 60% prawem do odliczenia podatku naliczonego, nie więcej jak odpowiednio 5 000zł. lub 6 000zł.

Zachowanie praw nabytych

Realizując poszanowanie praw nabytych, ustawodawca w art. 13 ustawy nowelizującej VAT, umożliwił podatnikom kontynuację odliczania na zasadach sprzed 1 kwietnia 2014 roku podatku naliczonego z faktur wystawianych w ramach umowy najmu, dzierżawy, leasingu lub innej umowy o podobnym charakterze, w stosunku do których na dzień poprzedzający wejście w życie ustawy czyli na 31 marca 2014 roku, przysługiwało im nieograniczone prawo do odliczenia podatku VAT.

Zgodnie z regulacjami przejściowymi, jeżeli umowa najmu, dzierżawy, leasingu lub inna o podobnym charakterze, została zawarta przed 1 kwietnia 2014 r. i do tego dnia pojazd został wydany, pod warunkiem zarejestrowania takiej umowy w urzędzie skarbowym w terminie 30 dni od daty wejścia ustawy, czyli do 2 maja 2014 roku, podatnik ma prawo do odliczania całego podatku VAT z faktur leasingowych. Prawo do odliczenia podatku naliczonego jest skuteczne wyłącznie do opłat od czynszu najmu, dzierżawy lub rat leasingowych. Natomiast podatek VAT od pozostałych wydatków takich jak zakup paliwa czy eksploatacja jest odliczany na nowych zasadach. W przypadku, gdy umowa była już raz rejestrowana w organie podatkowym, a dotyczy to umów zawartych w 2010 r., podatnik aby móc korzystać z pełnego odliczenia był zobowiązany po raz drugi zarejestrować taką umowę w urzędzie skarbowym. W sytuacji użytkowania przez podatnika na podstawie umowy leasingu samochodu osobowego, gdzie przysługiwało częściowe odliczenie podatku VAT w wysokości 60% nie więcej jak 6.000 zł, rejestracja w urzędzie takiej umowy nie była wymagana. Jednakże od 1 kwietnia 2014 r. podatnik wykorzystujący taki pojazd zarówno do działalności gospodarczej jak i do celów prywatnych ma prawo do odliczania 50% kwoty wynikającej z faktury dokumentującej wydatki związane z używaniem tego pojazdu, nawet w sytuacji, gdy do 31 marca 2014 r. wykorzystał obowiązujący wówczas limit w wysokości 6 000 zł.

Zakończenie

Analizując nowe zasady odliczania i rozliczania wydatków dotyczących pojazdów samochodowych można stwierdzić, że kolejna zmiana przepisów daje podatnikom możliwość odliczenia relatywnie wyższego podatku VAT od zakupu takich pojazdów. Jednakże wymogi, jakie stawia ustawodawca by móc skorzystać z pełnego odliczenia podatku VAT, są tak restrykcyjne, że z pewnością spowodują ograniczenia w odliczaniu VAT-u.

Ograniczenia w zakresie odliczania podatku naliczonego VAT z tytułu nabycia i wykorzystywania samochodów osobowych oraz pojazdów konstrukcyjnie im podobnych stosowane są w wielu krajach Unii Europejskiej. Według statystyk w 19 państwach Unii Europejskiej stosowane są ograniczenia w odliczaniu podatku VAT. W 6 państwach UE stosuje się częściowe ograniczenie, natomiast w 13 państwach, co do zasady stosuje się całkowity zakaz odliczania podatku z tytułu nabycia tego typu pojazdów.

Dla zidentyfikowania zjawiska:

- Włochy – ograniczenie do 40% prawa do odliczenia;
- Rumunia, Wielka Brytania, Łotwa, Belgia, Hiszpania – ograniczenie do 50% prawa do odliczenia;
- Bułgaria – całkowite ograniczenie w odliczaniu (możliwość odliczenia podatku tylko w przypadku, gdy pojazd jest wynajmowany);
- Estonia – obecnie nie ma ograniczeń w prawie do odliczenia podatku VAT w zakresie samochodów i paliwa do ich napędu. Planowane są zmiany w zakresie ograniczeń od 1 lipca 2014 roku.

Literatura

Dyrektywa 2006/112/WE w sprawie wspólnego systemu podatku od wartości dodanej (Dz. Urz. UE L 353 z 28.12.2013).

Ustawa z dnia 10 września 1999 r. – Kodeks Karny Skarbowy [Dz. U. z 2013 r., poz. 186 ze zm.].

Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2011 r. Nr 177, poz. 1054 ze zm.)

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 97-111

Maria Lefik
Społeczna Akademia Nauk

Rachunek bankowy podstawą rozliczeń pieniężnych przez Internet –korzyści i zagrożenia

The bank account as the basis of financial settlements via the Internet-profits and risks

Abstract: The article focuses on some of the dilemmas related to legal solutions adopted by the Polish legislator after Poland implemented EU directive concerning payment services.

In the article the author attempts to formulate a definition of the Internet banking. The author points to the benefits and threats resulting from using the Internet by both banks and customers. In recent years, despite a number of concerns related to using the Internet, the society's interest in the Internet banking and resulting benefits has increased noticeably.

Key-words: the Internet, Internet banking, Internet bank document.

Wprowadzenie

Na przełomie XX–XXI wieku rozpoczął się szybki rozwój technologii telekomunikacyjnych, a w szczególności informatycznych. Swym zasięgiem zaczęły one obejmować niemal wszystkie dziedziny życia, powodując zmianę wymagań oraz oczekiwań ludzi i instytucji. Zjawiskiem, które szczególnie silnie zarysowało się na polskim rynku, okazał się wzrost popularności i zastosowania Internetu, zarówno w sferze prywatnej, jak i działalności gospodarczej.

Internet stał się powszechnie używanym medium komunikacyjnym, w którym zaczęto dostrzegać narzędzie innowacyjne budujące prestiż i konkurencyjność.

Dokonujące się przemiany nie ominęły również systemu bankowego, który – ze względu na fakt działania w sferze usług – starał się podążać za wszelkimi zmianami otoczenia zewnętrznego. To banki jako jedne z pierw-

szych uczestników rynku finansowego wdrażały nowe technologie do dystrybucji produktów bankowych i budowy fundamentów bankowości internetowej, z wykorzystaniem posiadanej już bazy rachunków bankowych.

Celem artykułu jest prezentacja krajowych regulacji prawnych określających instytucję rachunku bankowego w kontekście świadczenia usług płatniczych w ramach wewnętrznego rynku unijnego z uwzględnieniem rozliczeń pieniężnych dokonywanych za pośrednictwem Internetu.

Polskie regulacje prawne umowy rachunku bankowego

Umowa rachunku bankowego jest jedną z najszczegółowiej uregulowanych i opisanych umów w polskim prawie i piśmiennictwie prawniczym. To efekt przyjętych rozwiązań ustawowych samej umowy rachunku bankowego, jak i jej ogromnego znaczenia w obrocie gospodarczym i rozliczeniach pieniężnych transakcji handlowych.

W ostatnich latach zdaje się, że wyłącznie tradycyjne podejście do interpretacji rachunku bankowego nie zawsze podąża za praktycznymi wyzwaniami i zadaniami tej umowy. Wynika to w dużej mierze z nieuwzględnienia w dotychczas przyjętych interpretacjach umowy rachunku bankowego (płatniczego)[1] [art. 2 pkt 25 ustawy z 19.08.2011 o usługach płatniczych, Dz. U. nr 199 poz. 1175 z póz. z.] zdarzeń z dziedziny prawa nowych technologii, a w szczególności powszechnie stosowanej bankowości internetowej *(e-banking)*.

Zatem zasadnym wydaje się włączenie w zakres analizy umowy rachunku bankowego szerokiej regulacji usług płatniczych z uwagi na rodzaje świadczeń, które mają zastosowanie w ramach wykonania tej umowy. Dla kompleksowego rozważania tematu w artykule uwzględniono niektóre wzajemne zależności, jakie zachodzą pomiędzy umową rachunku bankowego bankowości internetowej i usług płatniczych [Bajor 2011, s. 274–282].

W polskim prawie podstawowe regulacje umowy rachunku bankowego zostały zawarte w tytule XX Kc (art. 725–733) [Ustawa z 23 04.1964 r. – Kodeks cywilny, Dz. U. Nr 16, poz. 93 z póz. zm.], jako jednej z umów nazwanych. Wskazane w art. 725 *essentialia negotii* sprowadzają się do kwestii, że przez umowę rachunku bankowego bank zobowiązuje się względem posia-

[1] Rachunek płatniczy – rachunek prowadzony dla jednego lub większej liczby użytkowników służący do wykonywania transakcji płatniczych, przy czym przez rachunek płatniczy rozumie się także rachunek bankowy oraz rachunek członka spółdzielczej kasy oszczędnościowo-kredytowej, jeżeli rachunki te służą do wykonywania transakcji płatniczych.

dacza rachunku do przechowywania jego środków pieniężnych oraz do przeprowadzania na jego zlecenie rozliczeń pieniężnych. Istota regulacji kodeksowej stanowi także, że rozwiązania tutaj zawarte nie uchybiają przepisom o rozliczeniach pieniężnych, a w przypadku banków za aktualne uznać przepisy prawne obejmujące „Rozdział 4" prawa bankowego [Ustawa z 29.08.1997 r. – Prawo bankowe, Dz. U. z 2012 poz. 1376 z póz. zm.], Ustawę o usługach płatniczych, a także zarządzenie Nr 13/2013 Prezesa NBP w sprawie sposobu przeprowadzania rozrachunków międzybankowych z 24.05.2013 r.

Rozważania uregulowań rachunku bankowego w prawie bankowym są dwojakiego rodzaju: po pierwsze w „Rozdziale 3" prawa bankowego uregulowane zostały kwestie związane z poszczególnymi rodzajami rachunków bankowych, a także zagadnienia dot. małoletnich i rachunków wspólnych, generalnie poza art. 52 dotyczącym form i treści umowy oraz art. 61 obejmującym regulacje skutków utraty oznaczonych dokumentów, ale regulacje te nie mają większego znaczenia dla omawianego tematu.

Po drugie w „Rozdziale 4" prawa bankowego zostały uregulowane rozliczenia pieniężne przeprowadzane za pośrednictwem banków, które to ze swojej natury stanowią rozliczenia płatnicze w rozumienie ustawy o usługach płatniczych. Dlatego też za każdym razem dla rozstrzygnięcia sporu prawnego konieczne będzie dualistyczne rozpatrywanie tych dwóch regulacji łącznie.

Analizę ustawy o usługach płatniczych należy rozpocząć od znoszenia barier dla płatności w ramach wspólnego rynku Unii Europejskiej [Grabowski 2013, s. 104–106]. Regulacja usług płatniczych w ramach Unii obejmuje wiele aktów prawnych, ale najważniejszy z nich to Dyrektywa Parlamentu Europejskiego z 2007 r., w skrócie określana dyrektywą PSD[2] , która stanowi istotny element jednolitego systemu płatności w ramach rynku wewnętrznego, w szczególności poprzez ustanowienie wspólnych standardów świadczenia usług płatniczych przez podmioty dotychczas nieregulowane (nowe pojecie instytucji płatniczej) oraz szeroką gamę podmiotów już regulowanych, takich jak banki. Przytoczona dyrektywa ma charakter ścisłej implementacji, przy czym państwa członkowskie zachowały szerokie możliwości zastosowania rozwiązań krajowych. Polski ustawodawca zdecydował się na dokona-

[2] Chodzi o Dyrektywę 2007/64/ WE Parlamentu Europejskiego i Rady z 13.11.2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą Dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylającą Dyrektywę 97/5/WE (dyrektywa o usługach płatniczych) [Dz. Urz. UE L 319 z 5.12.2007 r. s. 1 ze zm.], określaną jako dyrektywa PSD – (*Payment Services Directive).*

nie transpozycji przepisów PSD do prawa polskiego w formie jednego, odrębnego aktu prawnego, ustawy o usługach płatniczych, zwanej dalej ustawą (UsłPłU)[3] . Ustawa łączy w sobie przepisy o charakterze prywatnoprawnym i publicznoprawnym oraz charakteryzuje się bardzo dużą bliskością sformułowań z dyrektywą unijną, ale bardzo małą korelacją z krajowymi przepisami zawartymi dotychczas w kodeksie cywilnym i prawie bankowym.

Świadczą o tym chociażby:

- całkowicie nowe i nieznane polskiemu prawu nazewnictwo w stosunku do już funkcjonujących od szeregu rozwiązań prawnych w tej materii np. płatnik, usługi płatnicze czy autonomiczna definicja umowy ramowej[4], (art. 1 ust 2 pkt. 31 UsłPłU), która nie może być utożsamiana z takim samym pojęciem w prawie polskim [Romanowski 2010, s. 133].
- wprowadzenie przepisów, które stanowią powtórzenie już obowiązujących konstrukcji prawnych *(superfluum)*; ma to miejsce przy regulacji skutków wykonania nieautoryzowanej transakcji, gdzie regulacje umieszczone w ustawie pokrywają się z przepisami kodeksu cywilnego o zobowiązaniach;
- brak dostrzeżenia przez ustawodawcę polskiego, że pomimo dosłownego transponowania rozwiązań przejętych przez dyrektywę, norma wynikająca z nowych przepisów oraz z przepisów dotychczasowych będzie różniła się od samej regulacji PSD – ma to miejsce m.in. w przypadku obowiązku informacyjnego dotyczącego zmiany umowy ramowej o usługi płatnicze.

Podsumowując – podwójny obowiązek prawny w tej materii będzie obejmował regulacje prawne obowiązujące w kodeksie cywilnym i ustawie prawo bankowe, co do samej istoty rachunku bankowego oraz przepisy w ustawie

[3] Ustawa o usługach płatniczych – w świetle art. 3 ustawy przez usługi płatnicze rozumie się m.in.. działalność polegającą na przyjmowaniu wpłat gotówki i dokonywaniu wypłat gotówki z rachunku płatniczego, wykonywaniu transakcji płatniczych, wykonywaniu transakcji płatniczych w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu, wydawaniu instrumentów płatniczych, świadczeniu usługi przekazu pieniężnego, wykonywaniu transakcji płatniczych, w przypadku których zgoda płatnika na wykonywanie transakcji udzielna jest przy użyciu urządzenia telekomunikacyjnego, cyfrowego lub informatycznego.

[4] Umowa ramowa – umowa o usługę płatniczą, regulująca wykonanie indywidualnych transakcji płatniczych, która może zawierać postanowienia w zakresie prowadzenia rachunku bankowego. Jak podnosi się w doktrynie „jedną z cech charakterystycznych umowy ramowej jest brak ścisłego oznaczenia świadczenia. Nie przesądza ona ani w ogólnej wielkości przyszłych świadczeń, ani w szczególności terminów ich spełnienia".

o usługach płatniczych, a to z kolei powoduje szereg wątpliwości interpretacyjnych i małą przejrzystość obowiązujących regulacji prawnych. Dodatkowym niejako źródłem rozwiązań prawnych jest wprowadzanie przez same banki komercyjne samoregulacji dla klientów – w postaci regulaminów bankowych, wzorów umów i formularzy. Ponadto w przypadku wątpliwości, każda czynność płatnicza w polskim porządku prawnym będzie wymagała kompleksowego oglądu i zinterpretowania zlecenia płatniczego, z uwzględnieniem regulaminów bankowych wiążących bank i klienta. Powiązania pomiędzy regulacjami PSD i UuIPłU mają charakter semiimperatywny tzn. postanowienia umów o usługi płatnicze nie mogą być mniej korzystne dla użytkowników niż przepisy ustawy (art. 8 ust.1).

Dlatego też zastosowanie wszystkich rozwiązań materialnych, co do danej usługi płatniczej wymaga każdorazowej szczegółowej analizy treści danej usługi oraz umowy ramowej, na podstawie której ma być ona dokonana, włącznie z uwzględnieniem okoliczności jej dokonania. Taka sytuacja powoduje, że w praktyce weryfikacja wszystkich wspomnianych elementów jest wysoce utrudniona i niezwykle czasochłonna. W mojej ocenie, wobec tak znacznego skomplikowania materii ustawy o usługach płatniczych, ustawodawca, wprowadzając stosunkowo ważny akt prawny dla funkcjonowania usług bankowych, powinien sobie zadać dodatkowy trud bardziej precyzyjnego i spójnego uregulowania zakresów zastosowania dotychczasowych przepisów, zawartych w kodeksie cywilnym i prawie bankowym oraz nowych, podyktowanych obowiązkiem wprowadzeniem dyrektywy unijnej. W rezultacie, wobec automatycznego skopiowania przez polski parlament przepisów PSD do treści ustawy o usługach płatniczych, uzasadniona wydaje się praktyka dużej części sektora bankowego, które wolą stosować standardy bezpośrednio zawarte w PSD do wszystkich transakcji dokonywanych na terytorium UE, niż skupiać każdorazowo uwagę na możliwości zastosowania ustawowych wyłączeń dla danej transakcji i sytuacji jej zawarcia i realizacji.

Dla porównania należy nadmienić, że transpozycja dyrektywy PSD do prawa angielskiego też została dokonana w drodze odrębnego aktu prawnego – The Payment Regulations (PSR) 2009[5] [Iwański 2014, s. 15]. W angielskim prawie finansowym wcześniej już wielką rolę odgrywały uchwały i rekomendacje krajowego organu nadzoru finansowego zebrane w zbiorach

[5] Implementacja przepisów PSD w Wielkiej Brytanii została dokonana w formie dwóch odrębnych aktów. Regulacją PSR 209 zostały objęte Anglia, Szkocja, Walia i Irlandia Północna, natomiast dla Gibraltaru przyjęto osobny akt – *Financial Services* (EEA), *(Payment Services*) Regulations 2010.

Handbooks[6] [Iwański 2014, s. 15–16], które mogły znaleźć zastosowanie do świadczenia usług płatniczych i które jednocześnie były przedmiotem praktycznej edukacji instytucji finansowych i ich klientów.

W przeciwieństwie do ustawodawcy angielskiego, ustawodawca niemiecki transpozycję przepisów dyrektywy PSD dokonał w drodze ich wkomponowania w istniejący system przepisów prawnych[7]. Tym samym niemiecka implementacja po pierwsze opiera się na pojęciach używanych w dotychczasowych przepisach prawnych, których znaczenie i interpretacja była dotychczas znana – i daleka jest od dosłownego przepisywania dyrektywy PSD, albowiem uznano, ze przepisy o identycznym brzmieniu prowadziłyby do zbędnego zdublowania regulacji w tej materii.

Podobnie jak w przypadku implementacji niemieckiej, ustawodawca francuski zdecydował się na transpozycję polegającą na wkomponowaniu rozwiązań PSD w istniejący system prawa krajowego. Co ciekawe, na poziomie ustawowym francuska implementacja wyraźnie oddziela regulację odnoszącą się do umów rachunku bankowego, pełniącego funkcje rachunku płatniczego, od wymogów odnoszących się do innych umów ramowych[8].

Oceniam również, że wprowadzenie przez Polskę omawianej dyrektywy unijnej do obowiązującego prawa nie jest szczęśliwym rozwiązaniem, z uwagi na brak poszanowania już utrwalonych przez prawo i praktykę, konstrukcji reżimów prawnych. Bardzo często wprowadzenie na ich miejsce regulacji niezrozumiałych dla beneficjentów i budzących wątpliwości interpretacyjne wśród samych prawników i pracowników banków nie budzi zaufania klientów do banków i stanowi niebezpieczeństwo dla płynnego obrotu pieniężnego.

---

[6] Organ nadzoru finansowego: *The Financial Services Authority* (FSA), zastąpionego w 2013 r. przez dwa kolejne organy: *The Financial Conduct Authority* oraz *Prudential Regulation Authority*.

[7] Trzon regulacji stanowią przepisy Podtytułu 3 usytuowanego w Księdze 2 Sekcji 8 Tytule 12 niemieckiego KC (*Bűrgerliches Gesetzbuch* – BGB), obejmującego §675c 676c BGB. Przepisy publicznoprawne zostały natomiast włączone do właściwych ustaw szczegółowych tj. ustawy z 10.07.1961 prawo bankowe (*Kreditwesengesetz* – KWG*)* oraz ustawy 25.06.2009 o nadzorze nad świadczeniem usług płatniczych (Zahlungsdiensteaufsichtsgesetz – ZAG).

[8] W piśmiennictwie francuskim podkreśla się, że konieczność taka wynika choćby z fundamentalnej różnicy konstrukcyjnej między rachunkiem bankowym, tworzącym specyficzną więź obligacyjną pomiędzy bankiem a posiadaczem rachunku bankowego a rachunkiem płatniczym, będącym *zwykłym* zobowiązaniem płatniczym, por. [L. de Pellegars 2010, Nr 134, s. 14].

Przedstawiona konkluzja nie oznacza, że jestem przeciwna wprowadzeniu cytowanej dyrektywy unijnej – moje wątpliwości to głownie bezkrytyczna forma je wprowadzenia.

Bankowość internetowa

Świadczenie usługi elektronicznej[9] jest definiowane, jako wykonanie usługi bez jednoczesnej obecności stron – czyli na odległość – poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresja cyfrową, przechowywaniem danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej[10].

Bankowość elektroniczna *(e-banking)* jest formą usługi, polegającą na umożliwieniu uprawnionego dostępu do rachunku bankowego za pomocą urządzenia elektronicznego: komputera, bankomatu, telefonu, terminalu linii telekomunikacyjnych [Kosiński, Nowak 2011, s. 82–88]. Przytoczone rozważania są podstawą do podzielenia usług bankowości elektronicznej na trzy rodzaje:

- bankowość terminalową (operacje dokonywane za pomocą kart płatniczych),
- bankowość telefoniczną (operacje wykonywane przy użyciu telefonów stacjonarnych oraz komórkowych),
- bankowość internetową (operacje wykonywane za pomocą sieci Internet).

W dalszej części artykułu to właśnie tej ostatniej bankowości zamierzam poświęcić najwięcej uwagi.

Istnieje bardzo dużo definicji bankowości internetowej. Bankowością internetową [http:/mfiles.pl/pl/index.php/bankowościnternetowa] nazywamy operacje bankowe dokonywane przez klienta za pośrednictwem Internetu.

[9] Reguluje to Ustawa z dnia 18 lipca 2002 o świadczeniu usług drogą elektroniczną, tekst jednolity, Dz. U. 2013, poz. 1422

[10] W rozmienieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, tekst jednolity Dz. U. 2014 poz. 243.

Do realizacji operacji bankowych za pośrednictwem Internetu[11] [Patterson 2002 s. 130] wymagany jest jedynie komputer z dostępem do Internetu, wyposażony w przeglądarkę. Bankowością internetową określa się wszelkiego rodzaju przedsięwzięcia biznesowe wykorzystujące Internet do prowadzenia działalności bankowej. Bankowość internetowa jest niejako formą świadczenia usług za pośrednictwem ogólnodostępnej sieci Internet, z wykorzystaniem standardowego oprogramowania przeglądarki www) lub oprogramowania dedykowanego do komunikacji z bankiem (systemy home/corporate banking) [*Usługi bankowości elektronicznej dla…,* 2010, s. 24].

Należy również zaznaczyć, że bankowość internetowa to jeden z instrumentów bankowości elektronicznej, będący kombinacją technologicznych i organizacyjnych innowacji, zapewniający rozszerzenie tradycyjnych form usług finansowych oraz kreujący całkowicie nowe usługi świata cyberprzestrzeni.

Jak dotychczas brak jest jednak prawnej legalnej definicji bankowości internetowej i dlatego też bankowość internetową uznaje się za pojęcie pozaprawne. W praktyce jednak funkcjonuje pojecie bankowości internetowej, zarówno w języku prawniczym, jak i w dokumentach używanych w relacjach banku z klientem. Niezależnie od tego, co już napisano o bankowości internetowej i w jakim stopniu termin ten znany jest opinii publicznej, treść tego medium trzeba rozważać na gruncie praktyki bankowej oraz wcześniejszego pojęcia usług bankowości elektronicznej i prawideł rządzących funkcjonowaniem rachunku bankowego[12].

Z wzorców umów w obszarze prawniczym można wywieść szczególne cechy bankowości internetowej [Iwański 2014, s. 51–53]:

– udostępnienie posiadaczowi rachunku bankowego bankowości internetowej ma zawsze podstawę umowną i z reguły nie stanowi ona regulacji zawartej w odrębnej umowie (nazwanej czy nienazwanej), lecz jedynie jej uszczegółowienie czy modyfikacje umowy rachunku bankowego już istniejącej w postaci *accidentalia negotii;*

[11] INTERNET (sieć wewnętrzna) wewnętrzny system internetowy, oparty na tej samej technologii co Internet – przeglądarki, hiperłącza banery, itd. ale ograniczony do sieci prywatnej. Sieci wewnętrznych używa się do poprawienia sprawności komunikacji wewnętrznej i do korzystania z bazy danych. Internet jest szczególnie przydatny w bankach, gdzie często występują szeroko rozgałęzione sieci oddziałów. Pracownicy mogą uzyskać na przykład dzięki niemu dostęp instrukcji postępowania, wytycznych, materiałów źródłowych, opisów produktów.

[12] Za takim stwierdzeniem przemawia analiza wzorców umów bankowych świadczących usługi bankowości internetowej za pośrednictwem rachunku bankowego.

- poruszanie się w środowisku bankowości internetowej powinno być możliwe za pomocą standardowych urządzeń i oprogramowania, które umożliwiają dostęp do stron internetowych. To przesłanka różniąca bankowość internetową od innych form bankowości elektronicznej, a mianowicie od bankowości terminalnej oraz telefonicznej;
- bankowość internetowa opiera się na komunikacji za pośrednictwem portalu internetowego konkretnego banku[13] [Bańko 2007 s. 580];
- dostęp do portalu internetowego oraz inicjowanie rozliczeń pieniężnych przez posiadacza rachunku bankowego możliwe jest po spełnieniu przez niego określonych warunków identyfikacji i uwierzytelnienia, które zostały ustalone z bankiem w umowie;
- za pośrednictwem bankowości internetowej posiadacz rachunku bankowego może skorzystać z dwóch podstawowych funkcji. Po pierwsze poprzez portal internetowy posiadacz rachunku pozyskuje różne informacje, począwszy od wysokości dostępnych środków pieniężnych na rachunku bankowym, poprzez historię dokonywanych informacji, jak i dokonywanie innych czynności jak np. nieudane próby logowania się do systemu.

Druga, jakże ważna możliwość, to dokonywanie poprzez portal internetowy za pośrednictwem rachunku rozliczeń pieniężnych z wykorzystaniem polecenia przelewu, zapłaty. Strony tj. bank i posiadacz rachunku umawiają się bowiem, że dyspozycja złożona przez posiadacza jako podmiot prawidłowo zidentyfikowany stanowi jego oświadczenie woli.

W przypadku umowy rachunku bankowego objętego bankowością internetową, ustawa o usługach płatniczych znajduje zastosowanie w odniesieniu do umowy rachunku bankowego, jako umowy ramowej, w tym również do bankowości internetowej, jako instrumentu płatniczego, a do usług płatniczych dokonywanych za pośrednictwem tej umowy wówczas, gdy spełniają kryteria z UsłPłU. W praktyce są to najczęstsze przypadki, kiedy w oparciu o umowę rachunku bankowego klient może dokonywać transakcji wynikających z ustawy o usługach płatniczych oraz transakcji pozostających poza jej zasięgiem (dot. rachunków wielowalutowych umożliwiających dokonywanie transakcji w walutach państw członkowskich, jak i innych walutach np. frank szwajcarski). Innymi słowy, jeśli dana transakcja płatnicza będzie spełniała kryteria ustawy o usługach płatniczych, to jej podstawowym źródłem regulacji będzie ta ustawa, natomiast inne przepisy, takie jak kodeks cywilny czy

[13] „Portal" w Internecie – witryna [*Wielki słownik wyrazów bliskoznacznych* PWN, 2007].

prawo bankowe, będą miały zastosowanie w przypadku braku konkretnej regulacji w UsłPłU.

Podsumowując powyższe rozważania, można by się pokusić o jedynie praktyczno-techniczne sformułowanie terminu bankowości internetowej. Zatem bankowość internetowa jest formą usługi polegającej na umożliwieniu posiadaczowi rachunku bankowego, na podstawie zawartej umowy, dostępu – za pośrednictwem urządzeń standardowych i oprogramowania do stron internetowych i portalu internetowego banku – do przeglądu tegoż rachunku bankowego i składania bankowi zleceń płatniczych. Tak sformułowany zapis mógłby stać się w przyszłości alternatywą do legalnej konstrukcji prawnej.

Korzyści i zagrożenia bankowości internetowej

Osoby decydujące się na korzystanie z usług bankowości internetowej mogą liczyć na szereg udogodnień, jakich nie oferują im banki „stacjonarne". Tak jak w przypadku korzyści osiąganych przez bank, dzielą się one na finansowe i pozafinansowe.

Pierwsze z wymienionych profitów wynikają bezpośrednio z korzyści ekonomicznych, z jakimi spotykają się usługi bankowe w sieci. Z kolei fakt obniżenia kosztów działalności banku przekłada się bezpośrednio na opłaty ponoszone przez jego klientów. Zainwestowanie banku w bankowość internetową pozwala na oszczędność pieniędzy i wiąże się ze znacznie mniejszymi kosztami bieżącego utrzymania. Nakłady inwestycyjne, związane z uruchomieniem banku internetowego, są porównywalne z wydatkami ponoszonymi na otwarcie filii banku „stacjonarnego" i wynoszą średnio 6–7 mln zł[14]. Duże znaczenie mają tutaj wydatki ponoszone na promocję i reklamę, które mogą wśród wymienionych powyżej opłat wynieść nawet 60% [Grzechnik 2000, s. 32–38].

Prowadzenie bankowości w Internecie pozwala na obniżenie kosztów stałych funkcjonowania banku, co pozytywnie wpływa na wynik finansowy, albowiem bank oferujący usługi w sieci nie wymaga rozbudowanej struktury oddziałów, a także jego siedziba nie musi się mieścić w ekskluzywnej i kosztownej dzielnicy miasta – to prowadzi do redukcji kosztów związanych z utrzymaniem nieruchomości oraz ich wyposażenia.

[14] Takiej kwoty pieniędzy wymagała realizacja projektu Volkswagen Bank Dietek; na jej wysokość składają się opłaty za sprzęt, software, szkolenia, marketing itp. – koszty te mają charakter zmienny i wykazują z reguły tendencję rosnącą [www.bankier.pl].

Banki świadczące usługi przez Internet zatrudniają często mniejszą liczbę pracowników *back Office*, a także obniżają koszty stałe poprzez wykorzystanie outsourcingu [Borcuch 2011, s. 106–111].

Sprzedaż usług za pośrednictwem Internetu pozwala bankowi zmniejszyć koszty zmienne dzięki zwiększonej wydajności obsługi klientów. To następnie daje możliwość automatyzacji czynności bankowych, szczególnie rozliczeniowych i załatwienia większej liczby klientów w tej samej jednostce czasu. Ograniczona jest „okienkowa" obsługa Klienta, występuje zmniejszenie banku zapotrzebowania na druki, broszury i opłaty pocztowe.

Banki świadczące usługi w sieci mogą liczyć, obok korzyści ekonomicznych, na szereg dogodności niezwiązanych bezpośrednio z ich finansami, gdyż są one następstwem globalnego charakteru Internetu, jako wiodącego kanału dystrybucji usług rozliczeniowych, depozytowych, kredytowych i dającego szanse dotarcia do regionów, w których otwarcie tradycyjnego oddziału banku byłoby nieopłacalne ze względu na małą liczbę mieszkańców.

Bankowość internetowa wyróżnia się bardzo wysoką elastycznością. Wiąże się ona zarówno z łatwością rozbudowy serwisu, jak i dostosowania go do zmieniającego się rynku. Wykorzystywanie specjalistycznych aplikacji CRM[15] [Bronkowski, Hościłowicz, Widelska 2007, s. 110] pozwala na agregacje danych marketingowych i ich analizę, co daje możliwość dopasowania świadczonych usług do oczekiwań klientów, nawet z możliwością personalizacji ofert usług bankowych.

Obecność banku w sieci czyni go bardziej prestiżowym i sprawia, że postrzegany jest on jako nowoczesny. Owa wyjątkowość i oczywistość, jakbyśmy ją nie nazwali, likwiduje zagrożenia w postaci kradzieży i fałszerstw, które towarzyszą tradycyjnej obsłudze klientów banku. Ponadto brak obsługi kasjerskiej i automatyzacja transakcji, eliminując częściowo możliwość popełnienia błędu przez pracownika banku, przenosi tę odpowiedzialność na klienta, gdyż to on sam wypełnia zlecenie i odpowiada za ewentualne błędy wynikające z nieprawidłowego wprowadzenia danych do systemu [Gostomski 2009, s. 200–205]. Obok wymienionych profitów finansowych

[15] System CRM – (ang.) *Customer Relationnship Management* w literaturze przedmiotu wyróżnia się wiele podejść do koncepcji zarządzania relacji z klientami – od systemu komputerowego do kompleksowego systemu zarządzania przedsiębiorstwem. Można przyjąć, że CRM to analizowanie działalności wszystkich działów przedsiębiorstwa z punktu widzenia tworzenia korzyści zapewnionych klientowi. CRM to zbiór strategii i metod, których podstawowym celem jest zwiększenie lojalności klientów oraz zmniejszenie kosztów obsługi, promocji i sprzedaży.

bankowość internetowa proponuje wiele korzyści *stricte* pozaekonomicznych, jak: ciągły dostęp do rachunków bankowych, możliwość zarządzania zgromadzonymi środkami przez dwadzieścia cztery godziny na dobę w ciągu całego tygodnia. Innym atutem jest globalny zasięg banku internetowego, co przejawia się w tym, że niezależnie od miejsca, wszędzie tam, gdzie istnieje dostęp do Internetu, istnieje też możliwość wglądu w rachunki bankowe. Ponadto korzystanie z bankowości wirtualnej zapewnia komfort jej użytkownikowi, nie wymaga bowiem instalowania skomplikowanego w obsłudze oprogramowania, a kontakt ze środowiskiem wirtualnym następuje za pośrednictwem przejrzystego interfejsu strony www. Transakcje realizowane są stosunkowo szybko z wyłączeniem wyczekiwania w kolejkach oraz wszystkie transakcje płatnicze i zarządcze własnymi środkami pieniężnymi można zrealizować w miejscu pracy bądź w domu, oszczędzając czas i pieniądze.

Zagrożenia w bankowości internetowej objawiają się głownie z występowaniem lęku związanego z wykorzystaniem komputerów. Dotyczy to w zdecydowanej większości ludzi starszych oraz z małych miast i środowisk wiejskich.

Globalna sieć postrzegalna jest przez liczną grupę ludzi, jako miejsce popisu dla oszustów i złodziei, a głośne przypadki nadużyć w cyberprzestrzeni przedstawiane przez media tylko utwierdzają potencjalnych klientów o braku potrzeby posługiwania się Internetem w składaniu zleceń płatniczych bądź w ogóle przechowywaniu czasowo wolnych środków pieniężnych w banku. Typowe przestępstwa urzędników bankowych najczęściej polegają na samowolnych pożyczkach (np. w formie wypłat), przestępczych manipulacjach komputerowych, na fałszowaniu poleceń przelewu czy na transferach za granicę zgromadzonych w Polsce środków płatniczych poprzez zawieranie z firmami zagranicznymi fikcyjnych umów. Ogólnie rzecz ujmując, zarządy banków najbardziej obawiają się nowych form oszustw, a szczególnie tych, których jeszcze nie rozpoznali i które stosunkowo trudno jest przewidzieć [Wójcik 2008, s. 55 i in.]

Awaryjność i problemy z funkcjonowaniem portali transakcyjnych banków to także przeszkody stanowiące zagrożenia dla rozwoju bankowości internetowej. Zdarzają się, lecz stosunkowo rzadko, sytuacje braku dostępu klienta do swoich oszczędności z powodu niewystarczającej wydolności systemów informatycznych banku – zdarzenia te, natychmiast nagłaśniane przez środki masowego przekazu, również niekorzystnie odbijają się na zaufaniu do konkretnego banku i systemu bankowości komercyjnej.

Poważną barierą dla realizowania rozliczeń pieniężnych przez Internet jest wzmożona konkurencja na rynku elektronicznym, to z kolei powoduje, że z jednej strony banki komercyjne mogą systematyczne doskonalić systemy informatyczne i uatrakcyjniać swoje oferty na rynki zagraniczne, ale z drugiej muszą one zdać sobie sprawę, że i podobnie postępują banki w innych krajach, a to z kolei daje możliwość dotarcia hakerów już nie tylko do banku krajowego, ale i do banków i innych instytucji finansowych na drugim końcu świata [Borcuch 2013, s. 21–23]. Inną przeszkodą dla bankowości internetowej jest fakt, że w bardzo wielu sytuacjach dokumenty bez potwierdzenia w postaci pieczątki instytucji je wystawiającej, czy też odręcznego podpisu jej pracownika, nie są akceptowane.

W obliczu najróżniejszych zagrożeń wynikających z bankowości internetowej leżących zarówno po stronie banków jak i klientów, niezaprzeczalnym zadaniem tych pierwszych jest zapewnienie skutecznych mechanizmów zapewniających wysoki poziom bezpieczeństwa zarówno dla oszczędności klienta, jak i składanych przez nich zleceń płatniczych. Bezpieczeństwo komunikacji w bankowości wirtualnej ma przede wszystkim na celu zapewnienie integralności danych przesyłanych przez Internet oraz niedopuszczenie do sytuacji, w której osoby postronne mogłyby odczytać poufne informacje. Główne metody zapewniające bezpieczeństwo transakcji internetowych to szyfrowana transmisja danych, stosowanie metod uwierzytelnienia transakcji w połączeniu z identyfikatorem przypisanym klientowi poprzez hasło stałe, jednorazowe i certyfikaty cyfrowe skojarzone z hasłem. Ważnym elementem, który nie może być pominięty w procesie bezpieczeństwa jest komputer klienta, jak każdy inny narażony jest on na szkodliwe działanie wirusów i aktów włamywaczy internetowych. Natomiast informowanie klienta przez bank o wszelkich zmianach, które miały miejsce na jego rachunku i przesyłanie ich m.in. w formie wiadomości tekstowych np. na jego telefon komórkowy daje możliwość szybszej reakcji z jego strony na ewentualne niezgodności – w przypadku uzyskania dostępu przez osobę nieuprawnioną.

Zakończenie

Zasadniczym celem zaprezentowanego artykułu było dowiedzenie w polskich rozwiązaniach prawnych szczególnej roli umowy rachunku bankowego (płatniczego) w bieżących rozliczeniach pieniężnych za pośrednictwem Internetu.

Wyrażam negatywną ocenę polskiego ustawodawcy w kwestii transpozycji przepisów dyrektywy unijnej w zakresie usług płatniczych do polskiego

prawa finansowego. W krajowym prawie finansowym funkcjonująca już do dziesiątek lat instytucja rachunku bankowego stanowiła jedną z najbardziej transparentnych i opisanych w doktrynie oraz orzecznictwie konstrukcję prawną. Brak poszanowania tego dorobku przy wdrażaniu prawa unijnego niesie za sobą negatywne skutki dla obrotu gospodarczego, nierówności stron umowy rachunku bankowego i w konsekwencji znacznego zachwiania i tak już nadwątlonej reputacji banków na rynku finansowym. Jedynym i słusznym rozwiązaniem *de lege ferenda* powinno być uporządkowanie regulacji obrotu pieniężnego w jednym kompletnym i czytelnym akcie prawnym na wzór nieniecki czy ewentualnie francuski.

Procedura ujednolicenia analizowanej materii wymagała by jedynie inkorporacji tych konstrukcji prawnych, które na gruncie polskiego prawodawstwa dotychczas nie wystąpiły. Całościowa regulacja tych kwestii winna obejmować odniesienie do umowy rachunku bankowego i usług płatniczych, a to z kolei czyniłoby całokształt otoczenia prawnego usług finansowych bardziej przejrzystym i czytelnym dla każdego uczestnika obrotu pieniężnego.

Jak każde medium, tak i również Internet nie jest w swojej istocie doskonały, bo korzystając z jego dobrodziejstwa klienci narażeni są na najróżniejsze niebezpieczeństwa, ale również na co dzień odnoszą z tego tytułu rozmaite korzyści. Rachunek bankowy (płatniczy) z przypisaną funkcją internetową jest podstawowym instrumentem, za pośrednictwem którego są przeprowadzane aktualne w kraju rozliczenia pieniężne. Studiując różne publikacje i opracowania, można dojść do wniosku, że przy zachowaniu maksimum staranności po stronie klienta bankowości internetowej i samego banku, istnieje zdecydowanie więcej korzyści dla obu stron rozliczeń pieniężnych. Dowodem niech będzie raport ZBP[16], z którego wynika, że liczba aktywnych klientów bankowości internetowej na koniec 2013 wynosiła 12,4 mln osób. Jest to 9,2% więcej niż rok wcześniej i należy dodać, że tylko w ostatnim kwartale ubiegłego roku przybyło pól miliona aktywnych uczestników bankowości internetowej. Jednocześnie ZBP podaje, że na koniec ubiegłego roku liczba klientów indywidualnych, posiadających umowy umożliwiające dostęp od usług bankowości internetowej, wynosiła blisko 23 mln. Największym bankiem internetowym jest PKO BP, który ma podpisanych z klientami 6130 tys. umów, ale to w mniejszych bankach, takich jak: ING BSK SA czy BZ WBK i PEKAO SA klienci częściej logują się na rachunek bankowy ROR przez Internet.

[16] Na podstawie Raportu PRNews.pl: Rynek bankowości internetowej – IV kw. 2013.

Według badań przeprowadzonych na zlecenie Komisji Europejskiej w 2009 r. jeden na trzech obywateli UE korzystał z bankowości internetowej i przewiduje się, że proporcja ta wzrośnie do poziomu dwóch na trzech obywateli do roku 2020[17].

Literatura

Bańko M. (2007), *Wielki słownik wyrazów bliskoznacznych*, Wyd. Naukowe PWN, Warszawa.

Bajor B. (2011), *Bankowość elektroniczna – studium prawne*, Wydawnictwo Naukowe SCHOLAR, Warszawa.

Borcuch A. (2011), *Bankowość elektroniczna*, CeDuWu, Wydawnictwo Naukowe U.W., Warszawa.

Borcuch A. (2013), *Społeczność wirtualna a wirtualny obieg pieniądza,* CeDeWu Wydawnictwo Naukowe U.W, Warszawa.

Brokowski H, Hościłowicz E, Wielska U, *Zarządzanie marketingowe we współczesnym handlu i usługach* , Wyższa Szkoła Finansów i Zarządzania w Białymstoku, Białystok.

Gostomski E. (2009), *Jestem nowy,* Bankowy Ośrodek Doradztwa i Edukacji, Poznań.

Grabowski M. (2013), *Instrumenty płatnicze*, Wydawnictwo Naukowe CeDuWu Wydawnictwo Naukowe U.W., Warszawa.

Grzechnik J. (2000), *Bankowość internetowa*, Wydawnictwo Internetowe Centrum Promocji Gdańsk.

Iwański W. (2014), *Umowa rachunku bankowego objętego bankowością internetową z punktu widzenia nowej regulacji usług płatniczych*, Wydawnictwo C.H.Beck, Warszawa.

Kosiński B., Nowak A.Z. (2011), *Podstawy współczesnej bankowości* CeDeWu, Wydawnictwo Naukowe U.W. Warszawa.

Patterson R. (2002), *Kompendium terminów bankowych po polsku i angielsku,* Fundacja Rozwoju Rachunkowości w Polsce, Warszawa.

Romanowski M (2010), [w:] Bagińska E, *System Prawa Prywatnego*, *Prawo zobowiązań – umowy nienazwane,* t. 9*,* red. W.J. Karnet, Warszawa.

Wójcik J.W. (2008), *Oszustwa finansowe – zagadnienia kryminologiczne i kryminalistyczne,* Wydawnictwo J.W. Wójcik, Warszawa.

Dyrektywa 2007/64/Deparlamentu Europejskiego i Rady z 13.11.2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i uchylająca dyrektywę 97/5/WE (PSD), Dz. Urz. UE L319 z 12.2007 r., s. 1.

Ustawa z 23.4.1964 – Kodeks cywilny, Dz. U. Nr 16 poz. 93 ze zm.

Ustawa z 29.08.1997 r. – Prawo bankowe, Dz. U. z 2012 poz. 1376 ze zm.

Ustawa z 19.08.2011 o usługach płatniczych, Dz. U. Nr 199, poz. 1175 ze zm.

Ustawa z 1807.2002 o świadczeniu usług droga elektroniczną – tekst jednolity, Dz. U. 2013 poz. 1422.

Ustawa z 16.07.2004 Prawo telekomunikacyjne – tekst jednolity, Dz. U. 2014, poz. 243.

[17] Informuje o tym Komunikat z 11.01.2012 r. opublikowany na stronie Komisji Europejskiej pod adresem http:/europa.eu/rapid/pressReleasesAction (dostęp 1.11.2013).

Ochrona danych osobowych w zasobach informatycznych

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 115-128

Ireneusz Grabowski
Uniwersytet Mikołaja Kopernika w Toruniu
Barbara Kamińska
Społeczna Akademia Nauk

Kopia bezpieczeństwa danych elektronicznych jako podstawowy element Systemu Zarządzania Bezpieczeństwem Informacji w Firmie

A backup of the electronic data as an essential element of the Information Security Management System within the Enterprise

Abstract: The universality and accessibility of information technology causes then more and more information is created, transmitted and stored in the digital form. Therefore, secure processing, and storage of the electronic data in each enterprise is not only a need but rather by the necessity of both the legal conditions and the natural need to ensure security of the data. Ensuring proper archiving (including backup) for each company must be a continuous process and certainly it must be carefully adapted to the needs, enterprise capabilities and financial resources of a specific organization. Thanks the deployed, proven, but especially effective procedures for performing backup and secure data storage there is a guarantee of the protection business-critical data on the circumstances of accident, damage or loss of data.

The article presents selected aspects related to the topic of security of electronic data policy implementation in the companies, especially by performing backup of the data. The legislative requirements for the safe storage of data, organizational aspects of backup in the company, technical aspects and procedures for optimal selection and implementation of how to perform the backup in small and medium-sized enterprises are presented.

Key words: data safety, backup, data storage, medium-sized enterprises.

Wstęp

W obecnych czasach, rzetelna i co najważniejsze dostępna informacja, niejednokrotnie stanowi o możliwości efektywnego działania i właściwego rozwoju organizacji. Coraz częściej widać, że w warunkach wysokiej konkurencyjności, największymi dobrami firmy stają się jej pracownicy oraz właśnie posiadane informacje. Widać też, że wykorzystanie informacji jest związane z funkcjonowaniem przedsiębiorstwa ściślej niż kiedykolwiek wcześniej.

Przetwarzanie informacji wiąże się z koniecznością przetwarzania, przesyłania i zapisu danych. Naturalną formą przechowywania i przesyłania danych jest obecnie postać elektroniczna. Rozwój technologii informatycznych, ich powszechność i łatwa dostępność, zmiany prawne, powodują, że niemal 70% dokumentów, jakie powstają obecnie w firmach lub są tworzone przez użytkowników prywatnych w Polsce i na Świecie, ma postać cyfrową. Szacuje się, że 90% z nich nigdy nie zostanie wydrukowanych i pozostaną one jedynie w formie elektronicznej. Koniecznie trzeba w tym miejscu dodać, że ze względu na informatyzację przedsiębiorstw, powszechność dostępu do Internetu oraz wykorzystanie systemów informatycznych do zarządzania przedsiębiorstwem, tradycyjne powiązanie informacji oraz danych z dokumentem przestaje być wystarczające. Przetwarzane i zapisywane informacje bezpośrednio wiążą się z bazami danych stanowiącymi podstawę systemów informatycznych przedsiębiorstwa, ich strukturami, konfiguracją systemów zarządzania i sterowania, konfiguracją sieci, serwerów, komputerów, dostępu do danych i Internetu, a także z innymi formami zapisu informacji, takimi jak zdjęcia, filmy, nagrania audio czy wreszcie poczta e-mail oraz szeroko rozumiane zasoby WWW. Dlatego też dla każdej firmy (bez względu na jej wielkość, branżę czy obszar działania), instytucji czy jednostki administracyjnej, utrata, czasowy brak dostępu lub przekłamanie danych zgromadzonych i przetwarzanych w systemach elektronicznych jest poważnym problem obejmującym obszar finansowy, prawny i administracyjny. Utrata kluczowych dla działania instytucji danych będących np. bazą klientów, danych z programów magazynowych, finansowo-księgowych, czy danych kadrowych może poważnie utrudnić wykonywanie działań biznesowych lub wręcz uniemożliwić w przypadku całkowitego braku odtworzenia utraconych danych, dalsze prowadzenie działalności gospodarczej doprowadzając nawet do bankructwa firmy. Nawet krótkotrwała utrata danych powoduje przestoje w pracy, jej dezorganizację, bezpośrednie i pośrednie straty materialne.

Dlatego też w tym kontekście tworzenie kopii bezpieczeństwa danych (backup)[1] przechowywanych w postaci elektronicznej stanowi ważny element zarządzania bezpieczeństwem danych w ramach polityki bezpieczeństwa realizowanej w firmie.

[1] Pod pojęciem backupu rozumiemy kopię bezpieczeństwa na bieżąco przetwarzanych danych (a także systemu operacyjnego i zainstalowanych aplikacji) z serwera, stacji roboczych lub innych urządzeń gromadzących i przetwarzających dane w postaci elektronicznej. W razie wystąpienia awarii taka czynność pomaga w krótkim czasie przywrócić system informatyczny do stanu z ostatniego poprawnego backupu.

Brak odpowiednich procedur ochrony danych elektronicznych, w tym wykonywania kopii zapasowej, sposobu przywracania utraconych danych powoduje w sytuacji awaryjnej czasochłonne a przede wszystkim kosztowne działania pozwalające, jeśli jest to w ogóle możliwe, na przywrócenie działania firmy do stanu sprzed awarii. „Stare" przysłowie informatyczne mówi, że „*Ludzie dzielą się na tych, którzy wykonują kopie zapasowe i na tych, którzy dopiero będą je wykonywali*" i niestety jego aktualność ciągle nie maleje.

Dostępne statystyki dotyczące zabezpieczenia danych w organizacjach są ciągle bardzo niepokojące. Przeprowadzone przez Instytut Rozwoju Technologii Informatycznych badania, wśród kadry zarządzającej małymi i średnimi przedsiębiorstwami pokazały, że: 67% respondentów nie archiwizuje regularnie kluczowych danych. 81% spośród tych, którzy zadeklarowali, iż regularnie archiwizują dane, przyznało się, iż zdarza się im nie wykonać archiwizacji przez okres dłuższy niż 30 dni! [http://pomocit.blogspot.com/2008_04_01_archive.html].

Artykuł omawia podstawowe aspekty pozwalające na zrozumienie złożoności problemu konstrukcji zabezpieczenia danych za pomocą kopii bezpieczeństwa. Przedstawione też zostały zasady i procedury pozwalające na zaprojektowanie, wybór, wdrożenie i utrzymanie najlepszego rozwiązania dla małych i średnich przedsiębiorstw.

Skala i złożoność problemu

Problem zabezpieczenia danych elektronicznych, w szczególności w kontekście wykonywania kopii zapasowych tych danych jest niestety zagadnieniem bardzo złożonym, co wynika z bardzo wielu czynników [Białas 2007]. Trzeba podkreślić, że wiele z nich to nie problemy techniczne czy typowo informatyczne. Niestety to właśnie postrzeganie informatycznych aspektów zagadnienia wykonywania kopii bezpieczeństwa, jako procesu zbyt skomplikowanego, wskazywane są jako jedna z głównych przyczyn niewykonywania takich kopii przez przedsiębiorców. Jedną z podstawowych przyczyn złożoności problemu jest znaczne skomplikowanie i złożoność obecnych infrastruktur informatycznych. Przykładem może być infrastruktura rozproszona lub dostępna tylko czasowo, która praktycznie nie pozwala na wdrożenie jednoznacznych procedur pozwalających na efektywne wykonywanie kopii bezpieczeństwa. Dodatkowo kopiowanie (backup) nie obejmuje tylko danych, które są składowane na serwerze, ale często mamy do czynienia z kilkoma serwerami, z różnymi systemami operacyjnymi np. z rodziny Windows, Linux, licznymi stacjami roboczymi oraz komputerami przeno-

śnymi, czy smartfonami. Wszystkie te elementy produkują i przetwarzają dane elektroniczne, które muszą być także zabezpieczane przed utratą. Kolejny aspekt, to konieczność uwzględnienia potrzeby kopiowania „w locie" danych z „otwartych", czyli takich, które są właśnie przetwarzane przez użytkowników, zbiorów czy baz danych np.: SQL, MySQL, Oracle [http://docs.oracle.com/cd/E12151_01/nav/portal_booklist.htm]. Następny problem to ograniczenia zasobów, np. pojemności dysków twardych, systemów do backupu, przepustowości sieci, braku lub zbyt małej mocy (procesor, pamięć RAM) serwerów dedykowanych do wykonywania kopii bezpieczeństwa, czy ograniczeń systemów operacyjnych, systemów baz danych lub oprogramowania. Bardzo ważnym aspektem jest też wielkość firmy. Im większa firma tym trudniej zaplanować, wdrożyć i realizować procedury związane z bezpieczeństwem danych elektronicznych, w tym z kopią bezpieczeństwa. Nie bez znaczenia jest też fakt, że tworzenie kopii bezpieczeństwa to proces długotrwały, praktycznie ciągły, który musi być zaplanowany na lata. I tutaj od razu pojawia się tzw. czynnik ludzki, który powoduje, że problem zaniechania, zaniedbania, niewykonywania obowiązków przez pracowników może doprowadzić do katastrofy nawet bardzo dobrze zaplanowanego i wdrożonego systemu zabezpieczenia poprzez backup danych. Takie sytuacje także należy uwzględnić poprzez zaplanowanie odpowiednich procedur sprawdzających efektywność i jakość wykonywanej archiwizacji. Ostatnie lata wskazują na kolejny problem związany z przechowywaniem danych. Jest nim bardzo duża dynamika zmian w technologiach, zarówno technicznego jak i programowego zapisu danych. Zmieniają się nośniki, urządzenia do zapisu, sposoby ich obsługi zarówno z poziomu systemu operacyjnego jak i oprogramowania. Zmieniają się także same struktury danych, sposób ich przetwarzania, kompresji czy algorytmów odczytu. Prowadzi to coraz częściej do problemu użycia danych, do których dostęp jest niemożliwy np. ze względów zmiany technologii czy oprogramowania. Do podobnej grupy problemów można też zaliczyć tzw. „dark data" [Tiano Luigi], czyli dane i informacje tworzone i przechowywane przez przedsiębiorstwa na różnych nośnikach i w różnych technologiach przez wiele lat, podczas typowych działań biznesowych, które są na ogół nieużywane w bieżących procesach biznesowych a potencjalnie mogłyby przynosić firmie korzyści, gdyby zostały zebrane i przeanalizowane w odpowiedni sposób. Często takie dane nie są w ogóle zabezpieczane przed utratą. Innym aspektem jest konieczność spojrzenia całościowego na całe zagadnienie. Procedury wykonywania kopii bezpieczeństwa podobnie jak wszystkie systemy bezpieczeństwa podlegają ważnej zasadzie, a mianowicie – powinny być wdrożone kompleksowo,

a żaden element nie może być zaniedbany, gdyż cały system bezpieczeństwa jest tak wytrzymały, jak jego najsłabsze ogniwo.

Bardzo dużym problemem przy planowaniu i wdrażaniu systemów zabezpieczenia danych, który jest elementem Systemu Zarządzania Bezpieczeństwem Informacji – ISMS (ang. *Information Security Management System*) [Dhillon, Backhouse, 2000], czy w szerszym kontekście polityki bezpieczeństwa danych elektronicznych, jest także mała świadomość i wiedza dotycząca zagrożeń i konsekwencji utraty danych elektronicznych zarówno pracowników jak i kadry zarządzającej i właścicieli oraz brak najzwyklejszych intuicji i podstawowego instynktu samozachowawczego. Wynika to między innymi z braku ogólnej wiedzy informatycznej, dynamiki zmian technologii komputerowych, ich skomplikowania, ale równocześnie z łatwej dostępności i powszechności tych technologii. Brak świadomości zagrożeń i ich skutków jest bardzo dużą barierą we wdrażaniu polityki bezpieczeństwa i oczywiście jej elementu, jakim jest wykonywanie kopii bezpieczeństwa. Bardzo łatwo popełnia się błąd zakładający, że dopóki brakuje odnotowanych symptomów, iż bezpieczeństwo systemu zostało naruszone, możemy spać spokojnie. I niestety bardzo trudno wytłumaczyć np. właścicielowi firmy, że skoro przez ostatnich 10 lat „nic się nie stało" z danymi, a nawet, jeśli coś zginęło, to utrata była mało dotkliwa, że właśnie w tym momencie należy wydać środki oraz przedsięwziąć kroki w celu zabezpieczenia danych poprzez kopię bezpieczeństwa wykonywaną profesjonalnie i zgodnie ze sztuką. Jak widać, jest to problem bardziej socjologiczny, psychologiczny lub może edukacyjno-pedagogiczny niż informatyczny.

Uwarunkowania prawne

Każda organizacja, bez względu na rozmiar czy zakres działalności, w mniejszym lub większym stopniu podlega różnym regulacjom prawnym. Część z nich dotyczy także archiwizacji danych. Jednak to, jakie ustawy i rozporządzenia obejmują daną organizację, zależy od wielu czynników, m.in. od rodzaju prowadzonej działalności. Z tego względu opis aspektów prawnych, odnoszących się do archiwizacji danych, został przedstawiony jedynie w sposób ogólny. To w interesie każdej z firm jest określenie, jakim podlega regulacjom. Dla przykładu: dla instytucji finansowych mamy Bazylee II, dla służby zdrowia – HIPPA, w USA obowiązuje Sarbanes-Oxley (SOX), itd.[2] W Polsce istnieje szereg aktów prawnych, które dotyczą ochrony infor-

[2] BAZYLEA II to obowiązujące w Europie od 2007 roku przepisy dotyczące kapitału własnego, oceny i analizy ryzyka operacyjnego oraz ryzyka wypłacalności klienta przy udzie-

macji. Dla każdego rodzaju organizacji można zidentyfikować kilka lub kilkanaście przepisów prawnych, które zawierają w sobie wymagania związane z bezpieczeństwem informacji, określających obowiązki i kary, które grożą organizacji nieprzestrzegającej przepisów. Dla przykładu wiele grup zawodowych obowiązuje wymóg zachowania tajemnicy zawodowej, która nakazuje zapewnienie określonym informacjom odpowiedniej ochrony, dotyczy to np. tajemnicy lekarskiej, bankowej, skarbowej, itp. Brak spełnienia tych wymogów może być przyczyną nieprzyjemnych konsekwencji – od kar finansowych aż do kary pozbawienia wolności. W ustawodawstwie polskim istnieje wiele wymagań wynikających z przepisów normatywnych, które obligują do zachowania odpowiedniego bezpieczeństwa informacji przy jej przetwarzaniu, jest to między innymi „Ustawa o ochronie danych osobowych" (Dz. U. nr 133, poz. 883), która także odnosi się do archiwizacji danych, np. rozdział 5 pt. „Zabezpieczenie danych osobowych", art. 36. punkt 1.: „Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem". Zatem można przyjąć, że jednym z obowiązków administratora danych powinno być przygotowanie i wdrożenie tzw. polityki bezpieczeństwa, która powinna zawierać m.in.: wykaz budynków lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych; określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Oprócz polityki bezpieczeństwa organizacja może także stworzyć instrukcję zarządzania systemem informatycznym, który służy do przetwarzania danych osobowych. Instrukcja może zawierać na przykład takie informacje jak: procedury tworzenia kopii zapasowych zbiorów danych, sposób i miejsce ich przechowywania, a także wszelkich innych elektronicznych nośników informacji, procedury wykonywania przeglądów i konserwacji

laniu kredytu. Ustawa o ubezpieczeniach zdrowotnych i odpowiedzialności z tym związanej – (HIPPA). Od 1996 roku Health Insurance Portability and Accountability Act reguluje kwestie postępowania z dokumentacją medyczną oraz zapewnia ochronę sfery prywatności i bezpieczeństwo informacji. Ustawa SARBANES–OXLEY (SOX) Od 2002 roku ustawa definiuje kwestie przejrzystości i nadzoru krytycznych procesów dla celów prawidłowego kierowania przedsiębiorstwem i bilansowania.

systemu i nośników informacji. Reguluje to Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych [Dz. U. z 2004 r. nr 100, poz. 1024]. Przechodząc do kolejnych regulacji prawnych wymienić można wiele innych przepisów dotyczących bezpieczeństwa danych, jak np.: Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, która określa, jakie informacje urząd ma obowiązek udostępniać, a więc, posługując się pojęciami charakterystycznymi dla bezpieczeństwa informacji, zapewnić ich dostępność oraz pod jakimi warunkami informacje te nie są udostępniane. Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji określająca wymagania, co do poufności w zakresie przekazywania, ujawniania lub wykorzystania cudzych informacji stanowiących tajemnicę przedsiębiorstwa. Wymagania, co do bezpieczeństwa informacji stawiają także przepisy ustawy z dnia 29 września 1994 r. o rachunkowości, nakazując stosowanie odpowiedniego systemu służącego ochronie danych i ich zbiorów. Jednakże należy dodać, że podstawowym aktem normatywnym, który dotyczy wszystkich obywateli naszego kraju i instytucji jest Konstytucja RP. To na jej podstawie w drodze ustaw zostały wprowadzone rozwiązania związane z zapewnieniem bezpieczeństwa zarówno w zakresie poufności informacji, jak i jej dostępności oraz integralności [Zawistowski 2012].

Przywołane akty normatywne pokazują jak ważne jest postępowanie z przepisami obowiązującego prawa, przyjętych uwarunkowań normatywnych oraz własnych standardów. Takie postępowanie chroni przed naruszeniem przepisów prawa karnego, cywilnego czy zobowiązań wynikających z ustaw lub jakichkolwiek wymagań w zakresie bezpieczeństwa informacji. Dlatego też organizacja, która chce należycie zabezpieczyć swoje dane powinna zastosować podejście, w ramach którego będzie rozważnie zarządzać posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji.

Planowanie i projektowanie kopii bezpieczeństwa danych

Jak już wspomnieliśmy wcześniej zabezpieczenie danych poprzez wykonywanie kopii bezpieczeństwa jest elementem szerszego kontekstu, a mianowicie polityki bezpieczeństwa systemów komputerowych, która powinna być wdrożona w przedsiębiorstwie. Jak każdy element polityki bezpieczeństwa musi być on odpowiednio zaprojektowany. Od jakości projektu zależeć będzie funkcjonowanie, efektywność i niezawodność procedury backupu.

Dlatego też projekt taki powinien zostać stworzony przez osoby posiadające odpowiednią wiedzę oraz doświadczenie w tej tematyce. Ponieważ procedura wykonywania kopii bezpieczeństwa jest ściśle związana ze specyfiką firmy, jej obszarem działania, potrzebami, strukturą organizacyjną, kompetencjami i liczbą pracowników oraz oczywiście posiadanym budżetem, proste kopiowanie rozwiązań wdrożonych w innych firmach jest bardzo niewłaściwym podejściem do problemu. Dlatego też w dalszej części artykułu największy nacisk położony zostanie właśnie na elementy związane z projektowaniem procedur wykonywania kopii bezpieczeństwa. Omówione zostaną tylko najważniejsze elementy, na które należy zwrócić szczególną uwagę podczas opracowywania wyżej wymienionych procedur. W pierwszym kroku trzeba koniecznie określić główne przyczyny utraty lub przekłamania danych. Do najważniejszych należą:

- błąd ludzki, czyli przypadkowe lub celowe usunięcie danych przez pracowników lub osoby postronne (nieupoważnione), błędne wprowadzenie danych, nieświadome działania prowadzące do przekłamania danych;
- celowe działanie: kradzież, włamanie, sabotaż, w tym wynik działania wszelkiego rodzaju złośliwego i szkodliwego oprogramowania (wirusy, robaki, trojany itd.);
- błędy oprogramowania, czyli wadliwe działanie aplikacji przetwarzających wrażliwe dane, ale także systemów operacyjnych;
- awarie sprzętu, czyli utrata danych na skutek wadliwego działania lub awarii sprzętu komputerowego (np. usterka dysku twardego, usterka komputera, zasilacza, serwera, elementów struktury sieciowej, itp.);
- klęski żywiołowe, wypadki: ogień, woda, uderzenie pioruna, zawalenie budynku, itp. Ten ostatni element jest często niesłusznie pomijany przy projektowaniu procedury backupu.

Wiedząc już, co może nam grozić (oczywiście także w odniesieniu do specyfiki działania naszej firmy) przystępujemy przy projektowaniu backupu do określenia następujących podstawowych elementów.

Pierwszy z nich to określenie informacji, danych, które powinny być zabezpieczone przed utratą poprzez ich backup. Podstawową rolę odgrywa tu specyfika firmy, system informatyczny oraz użytkownik decydujący, jakie dane mają kluczowe znaczenie dla działalności przedsiębiorstwa. Jak już wspomniano wcześniej koniecznie trzeba włączyć do backupowanych danych także systemy operacyjne, struktury baz danych, ustawienia i konfigurację sieci, drukarek i innych elementów systemu informatycznego.

Kolejny element to odpowiedni dobór czasu i cyklu archiwizacji. To wbrew pozorom nie tylko wybór godzin, w których wykonywana będzie

kopia bezpieczeństwa, czy określenie częstotliwości jej wykonywania. Bardzo pomocne w tym aspekcie jest zrozumienie i uwzględnienie dwóch podstawowych kwestii. Pierwsza to odpowiedź na pytanie „ile danych możemy stracić?" To tzw. (RPO (*Recovery Point Objective*) – określający moment w przeszłości, w którym po raz ostatni została wykonana kopia danych i do którego momentu działalności będzie można wrócić. Określamy w tym miejscu ile danych w przypadku wystąpienia awarii możemy odtworzyć z wydruków, pamięci pracownika, e-maili, itp. W zależności od specyfiki firmy może to być kilka tygodni, dni, godzin lub w systemach ciągłego działania, przetwarzających dużo danych w czasie rzeczywistym, kilka lub ułamki sekund. Kolejne pytanie, na które musimy sobie odpowiedzieć w tym kontekście to „ile możemy „wytrzymać" bez danych/systemu". Określa to tzw. RTO (*Recovery Time Objective*) będący maksymalnym czasem po awarii, potrzebnym do przywrócenia działania aplikacji, systemów i procesów biznesowych. I tak jak w przypadku RPO czas ten może się wahać od kilku dni do ułamków sekundy w zależności od rodzaju prowadzonej działalności. Przy wyborze czasu i częstotliwości backupu należy pamiętać, żeby zapewnić jego jak największą automatyzację oraz niekolidowanie z bieżącą pracą systemu. Uwzględnienia wymaga też długość wykonywania samej kopii bezpieczeństwa oraz świadomość, że system backupu będzie pracował przez wiele miesięcy i lat.

Kolejnym aspektem jest odpowiedni wybór nośnika oraz oprogramowania służącego do archiwizacji. Zarówno wybór nośników, jak i oprogramowania zależy od potrzeb oraz możliwości danej organizacji. W przypadku oprogramowania, w małych firmach może okazać się całkowicie wystarczające wykonywanie kopii za pomocą narzędzi wbudowanych, np. w system operacyjny z rodziny Windows czy Linux lub prostych skryptów powłoki systemowej. W większych firmach warto zainwestować w dedykowane oprogramowanie (dostępne są także wersje *open source*). W kwestii nośników, na których będziemy wykonywać kopię, wybór jest bardzo szeroki: od płyt CD/DVD, dysków zewnętrznych, macierzy dyskowych, systemów RAID, po backupy taśmowe i dedykowane serwery backupowe. Wybór ten będzie zależał od ilości przetwarzanych i gromadzonych danych, ale także od RPO i RTO.

Następny punkt, to wybór metody przeprowadzania archiwizacji oraz liczby kopii oraz ustalenie czasu i sposobu przechowywania archiwów. Tak jak poprzednio kluczowe są tu wielkości RPO i RTO, wymuszające np. konieczność backupu w czasie rzeczywistym, lub jego jak największą automatyzację. Oczywiście aspekt finansowy też ma tutaj ogromne znaczenie np. dla doboru liczby nośników, uwzględniając ich zużycie w czasie. Wybór miejsca

i sposobu przechowywania nośników z kopiami bezpieczeństwa musi podlegać podstawowym procedurom związanym z tajnością danych i aspektami prawnymi – przetwarzaniem danych osobowych oraz zabezpieczeniem tych nośników przed zniszczeniem, np. w wyniku pożaru, zalania wodą, czy kradzieży. Podstawową zasadą jest przechowywanie nośników z kopią bezpieczeństwa w wodo/ognioodpornych sejfach oraz dodatkowych kopii poza siedziba firmy.

Właściwy dobór metody zapewnienia poufności i integralności archiwizowanych danych, to kolejny ważny aspekt projektowania kopii bezpieczeństwa. Oprócz zapewnienia dostępności, integralność archiwizowanych informacji jest ich bardzo ważnym atrybutem. Informacje, które zostały celowo lub przypadkowo zmodyfikowane, tracą swoją wartość i będą generować kolejne błędy. Dlatego też należy rozważyć wdrożenie pewnych mechanizmów, zapewniających weryfikację integralności, takich jak np. naliczanie sum kontrolnych dla pewnych partii informacji – plików, katalogów, archiwów czy dysków. Szczególnie wrażliwe informacje powinny dodatkowo być podpisywane cyfrowo w celu zapewnienia ich integralności. Jeżeli archiwizowane dane wymagają zapewnienia poufności, to należy je w odpowiedni sposób zaszyfrować, co niestety wprowadza dodatkowe techniczne problemy takie jak wydłużenie czasu wykonywania i dostępu do kopii bezpieczeństwa czy zapewnienie polityki zarządzania kluczami szyfrującymi.

Ostatnim z głównych punktów mających wpływ na projekt backupu danych w przedsiębiorstwie jest oszacowanie oraz umieszczenie w budżecie odpowiednich środków finansowych. Muszą one uwzględniać nie tylko koszty sprzętu i oprogramowania koniecznego do wykonywania kopii bezpieczeństwa, ale także koszt projektu, wdrożenia, zakupu i odnawiania nośników oraz dodatkowych obowiązków pracowników związanych z wykonywaniem kopii bezpieczeństwa. Niestety koszty te mogą być znaczące, dlatego tak ważnym elementem jest odpowiedni projekt przygotowany dla konkretnej organizacji. Z praktyki wiadomo też, że nadmierne oszczędzanie np. na jakości nośników (taśmy do streamerów, płyty DVD, dyski twarde), automatyzacji procesu backupu, czy wynagrodzeniach pracowników odpowiedzialnych za wykonywanie kopii mogą okazać się pozorne i w konsekwencji prowadzić do utraty informacji.

Proste rozwiązania dla małych i średnich przedsiębiorstw

Opierając się na definicji określonej w ustawie z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej [Dz. U. nr 173, poz. 1807] charakte-

ryzującej firmy z sektora MSP ze względu na liczbę zatrudnionych, można wyodrębnić trzy grupy przedsiębiorstw: mikro -zatrudniające średniorocznie mniej niż 10 pracowników, małe – zatrudniające średniorocznie mniej niż 50 pracowników oraz średnie zatrudniające średniorocznie mniej niż 250 pracowników. Popularność form prawnych MSP jest różna. Najczęściej funkcjonują w formie przedsiębiorstw rodzinnych (osób fizycznych) lub spółek osobowych nieposiadających osobowości prawnej. Zdecydowanie mniej firm sektora MSP działa jako spółki kapitałowe [Skowronek-Mielczarek 2007]. Dokonując głębszej charakterystyki omawianych przedsiębiorstw należy nadmienić, że działalność szczególnie małych podmiotów, odnosi się najczęściej do rodzaju więzi i stopnia wzajemnego zaufania, wielkości posiadanych i potrzebnych zasobów finansowych, skali i ryzyka prowadzenia działalności oraz innych ciężarów fiskalnych itp. [Bućko, Filipowicz, Wąsik 2000]. Niewątpliwie wpływa to na specyfikę zarządzania w tego rodzaju firmach. Cechą charakterystyczną polskich przedsiębiorstw należących do omawianego sektora, a w szczególności firm mikro jest dominująca pozycja właściciela oraz niski stopień formalizacji działań. Zwykle właściciel niewielkiej firmy zarządza nią osobiście, rzadko decydując się na delegowanie uprawnień i odpowiedzialności, co wiąże się z tzw. słabą strukturyzacją ról. Jej symptomy, to między innymi brak jasno określonych procedur, co sprzyja podejmowaniu decyzji przypadkowych, spontanicznych nie zawsze efektywnych [Konieczny, Schmidtke, 2007]. Stąd tak duży odsetek firm tego sektora (85%) boryka się z różnymi problemami, m.in. dotyczącymi kosztów tworzenia kopii zapasowych i odtwarzania danych. 83% wskazuje na braki funkcjonalne, a 80% uznaje dostępne rozwiązania za zbyt skomplikowane [http://www.egospodarka.pl]. Tak jak podaliśmy w poprzednim rozdziale system wykonywania kopii bezpieczeństwa musi być dostosowany do specyfiki przedsiębiorstwa, co zapobiega jego niedoskonałości, niewydolności czy nadmiarowości. W praktyce bardzo często okazuje się, że w sektorze MSP proste rozwiązania oparte na wykonywaniu kopii bezpieczeństwa w sposób rozproszony na prostych nośnikach zewnętrznych typu DVD, dyski zewnętrzne, napędy taśmowe przy użyciu narzędzi wbudowanych w system operacyjny czy oprogramowanie firmowe oraz dodatkowe jasne określenie procedur i obowiązków pracowników jest wystarczające, przynajmniej w początkowym okresie wykonywania kopii bezpieczeństwa.

Pełne zabezpieczenie wymaga jednak dodatkowych procedur w postaci archiwizacji w czasie rzeczywistym w systemach dyskowych typu RAID (ang. *Redundant Array of Independent Disks*, Nadmiarowa macierz niezależnych dysków) [Arpaci-Dusseau, Remzi H.; Arpaci-Dusseau, Andrea C.] oraz scentra-

lizowanych rozwiązań w postaci serwerów bakupowych. Taka centralizacja zasobów, które będą podlegały archiwizacji pozwala też na efektywną automatyzację procesu wykonywania kopii bezpieczeństwa. Konieczne w takim wypadku jest wykorzystanie specjalistycznego oprogramowania pozwalającego na wykonywanie, ewentualne odtwarzanie i zarządzanie kopiami bezpieczeństwa. Warto zwrócić też uwagę na to, że wspomniany tu system mirroringu czy replikacji realizowany w czasie rzeczywistym na macierzach typu RAID nie zastąpi klasycznego backupu na zewnętrznych nośnikach. Tylko backup pozwala na spojrzenie wstecz i powrót do wersji danych sprzed określonego czasu. Daje to zabezpieczenie głównie przed kasowaniem plików, wirusami lub błędami ukrytymi w programie bądź strukturze danych. Systemy redundancyjne, przy całej swojej doskonałości, naiwnie duplikują także wirusy czy błędy. Dlatego też na pełen system ochrony danych w systemach pamięci masowych przedsiębiorstw sektora MSP składa się kilka elementów:

1. Macierz RAID i replikacja w czasie rzeczywistym – zabezpiecza system np. przed awarią twardego dysku.
2. Urządzenie zapisu taśmowego, dysk zewnętrzny lub zewnętrzna macierz RAID z odpowiednimi procedurami cyklicznego zapisu danych – chroni system przed ogólną awarią (w tym całkowitą awarią macierzy RAID), klęską żywiołową np. powódź, pożar. Dzięki przechowywaniu backupów z różnych dni możemy odtworzyć stan np. sprzed awarii, która spowodowała niespójność danych.
3. Dane, które nie podlegają zmianom i są rzadko używane, powinny być archiwizowane na tanich urządzeniach zewnętrznych – także po to, by przyspieszyć dostęp do aktualnie przetwarzanych danych poprzez odciążenie aplikacji, bazy danych, systemu operacyjnego, sprzętu czy sieci.

Ze względu na olbrzymią liczbę dostępnych na rynku różnego rodzaju rozwiązań, zarówno sprzętowych jak i programowych oraz dużą dynamikę zmian, dokładniejszy ich opis w tym artykule jest bezzasadny.

Warto może na koniec tego rozdziału przedstawić stosunkowo nowe rozwiązania, które pojawiły się na rynku wraz z rozwojem technologii i dostępu do szerokopasmowego łącza internetowego, a polegające na wykonywaniu zdalnych kopii zapasowych danych firmowych w szeroko rozumianych zasobach sieciowych i Internetowych w tym tzw. chmurze [Mell, Grance, 2011]. Rozwiązania takie oferowane są coraz częściej przez firmy zewnętrzne i są bardzo atrakcyjną alternatywą dla klasycznych sposobów wykonywania kopii bezpieczeństwa. Wykonywanie w tej technologii kopii bezpieczeństwa polega na tworzeniu za pomocą specjalnego oprogramowania kopii dokumentów z komputera lub serwerów firmowych poprzez przesłanie

ich, najczęściej szyfrowanym połączeniem, na zewnętrzne serwery. Szyfrowanie następuje jeszcze przed wysłaniem plików na serwer, dlatego tylko właściciel danych ma do nich wgląd. Wiąże się to oczywiście w koniecznością posiadania łącza internetowego oraz kosztami, najczęściej w postaci abonamentu, zakupu takiej usługi. Rozwiązania te charakteryzują się łatwością obsługi, dużą automatyzacją, niezawodnością i skalowalnością (mogą być wykorzystane zarówno dla pojedynczego komputera jak i większej ich liczby) i z pewnością będą coraz częściej wybieranymi rozwiązaniami w sektorze MSP.

Podsumowanie

W artykule starano się przedstawić najważniejsze aspekty związane z zabezpieczeniem danych elektronicznych w przedsiębiorstwach MSP przy pomocy kopii bezpieczeństwa. O tym jak ważnym elementem polityki bezpieczeństwa w przedsiębiorstwie jest backup przekonał się każdy, kto w kluczowym momencie działań biznesowych utracił dostęp (nawet chwilowo) do kluczowych danych. Wbrew pozorom podstawowe zabezpieczenie danych za pomocą backup'u nie jest ani trudne, ani zbyt kosztowne, pod warunkiem, że zostanie zaplanowane przez osoby czy firmy posiadające odpowiednią wiedzę. Niestety należy pamiętać, że nawet najlepiej przygotowany i wdrożony system backupu danych, ze względu na jego długi czas życia, musi być cały czas pielęgnowany, udoskonalany i dopasowywany do zmieniających się realiów. Dodatkowo należy okresowo przeprowadzać testy odtwarzania wybranych losowo danych, gdyż archiwum, którego nie można odtworzyć (uszkodzenie, brak umiejętności), stwarza pozorne poczucie bezpieczeństwa, co może być bardziej szkodliwe i frustrujące w chwili wystąpienia awarii niż brak takiej kopii bezpieczeństwa. Bardzo ważnym elementem procedury tworzenia backupu jest osoba odpowiedzialna za wykonywanie, sprawdzanie i konserwację kopii bezpieczeństwa. Warto podkreślić, że tradycyjne formy wykonywania kopii bezpieczeństwa na serwerach firmowych i nośnikach zewnętrznych, coraz częściej są uzupełniane lub zastępowane przez nowe rozwiązania technologiczne takie jak backup w chmurze, czy na serwerach firm zewnętrznych specjalizujących się w zabezpieczaniu danych. Te nowe rozwiązania i możliwości są szczególnie atrakcyjne dla firm z sektora MSP, gdzie wielkość i przyrost przetwarzanych danych jest stosunkowo niewielki, a koszt takiego backupu (najczęściej abonament) jest rozłożony w czasie.

Na koniec należy podkreślić, że ciągle bardzo ważnym krokiem w celu poprawy sytuacji w firmach MSP jest dotarcie z czytelną informacją do przedsiębiorców i właścicieli, w celu uświadomienia im znaczenia dostępności informacji i danych elektronicznych dla efektywnego działania ich firmy.

Podstawa to zauważenie problemu i podjęcie kroków w celu jego rozwiązania. Jak pokazaliśmy w artykule, pomimo ewidentnego znaczenia zabezpieczenia danych poprzez wykonywanie kopii bezpieczeństwa, sytuacja w sektorze MSP jest bardzo zła. Dlatego konieczne jest edukowanie, budowanie intuicji związanych z bezpieczeństwem systemów komputerowych nie tylko wśród kadry zarządzającej, ale także wśród zwykłych pracowników, którym ta wiedza przyda się także w życiu prywatnym. Przecież praktycznie każdy z nas przetwarza i „produkuje" dane w postaci elektronicznej, takie jak zdjęcia, e-maile, dokumenty, których utrata może być bardzo dotkliwa.

Literatura

Arpaci-Dusseau, Remzi H.; Arpaci-Dusseau, Andrea C. (2014), *Operating Systems: Three Easy Pieces [Chapter: RAID], Arpaci-Dusseau Books.*

Białas A. (2007), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. Wydawnictwo Naukowo-Techniczne, Warszawa.

Bućko J., Filipowicz J., Wąsik L.T. (2000), *Ekonomika przedsiębiorstwa*, Wydawnictwo Politechniki Radomskiej, Radom.

Dhillon G., Backhouse J., (2000), *Information system security management in the new millennium*, Communications of the ACM Volume 43 Issue 7.

Konieczny O., Schmidtke R. (2007), *Inwestycja w kadry. Perspektywa małych i średnich przedsiębiorstw,* Wydawnictwo WYG International Sp. z o.o., Kraków.

Mell P., Grance T. (2011), *The NIST Definition of Cloud Computing* NIST Special Publication 800-145, September, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

Skowronek-Mielczarek A. (2007), *Małe i średnie przedsiębiorstwa. Źródła finansowania*, C.H.Beck, Warszawa.

Tiano Luigi, Dark Data – Big Data's evil twin?, http://www.1cloudroad.com/darkdata/

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.).

Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej [Dz. U. nr 173, poz. 1807]

Zawistowski T. (2012), *Bezpieczeństwo informacji*, FRDL, Warszawa.

http://www.egospodarka.pl/97160,Sektor-MSP-tworzenie-kopii-zapasowych-to-klopot,1,39,1.html,

http://pomocit.blogspot.com/2008_04_01_archive.html

http://docs.oracle.com/cd/E12151_01/nav/portal_booklist.htm

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 129-146

Dariusz Wiśniewski
Urząd Miejski Brodnica

Bezpieczeństwo informacji oraz ochrona przed ich wyciekiem na przykładzie wybranego Urzędu Miejskiego

Information security and DLP (data leak prevention) in a selected city office

Abstract: The security of data processing in computer systems plays a significant role. It applies also to self-government units. It is essential to recognize dangers and locate and define the application which influence the work of a given institution. The author presents electronic turnover of documents and examples of hackers' attacks in the office, threats to the local network and attempts to eliminate those threats through securing the net.
Key words: information classification, information identification, locatingand defining application, integrated service system in the office, threats in a local network, network security.

Wstęp

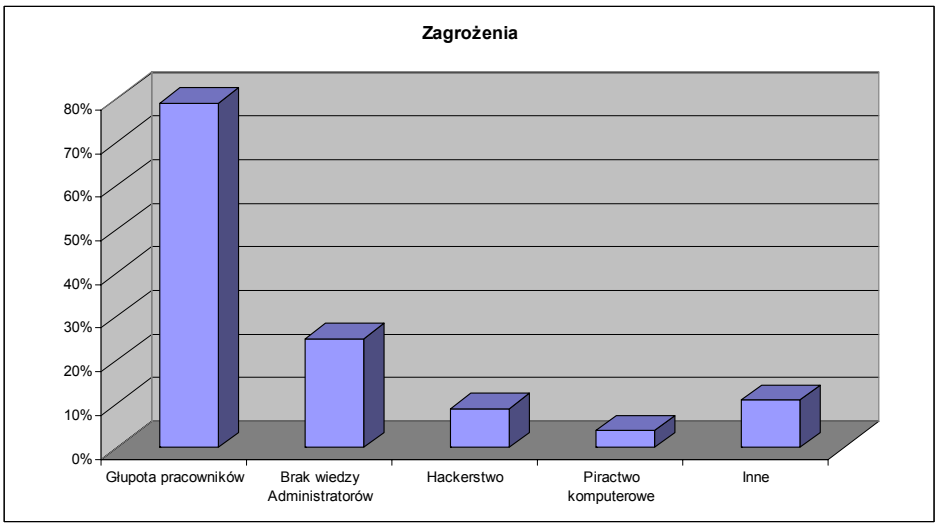
W dobie informatyzacji jednostek samorządowych, jakim jest Urząd Miejski, znaczącą rolę ma bezpieczeństwo przetwarzanych w systemach komputerowych informacji. Ich ochronę wymuszają również ustawy między innymi Ustawa o Ochronie Danych Osobowych, Ustawa o Informatyzacji Podmiotów Publicznych, Ustawa o prawie autorskim i prawach pokrewnych.

Dokument ten ma na celu pokazanie w pigułce na przykładzie danego Urzędu Miejskiego pewien typ podejścia do ochrony informacji. Na temat bezpieczeństwa informacji istniej wiele opracowań oraz książek, dlatego też ten dokument jest tylko sygnalizacją i ewentualnym wskazaniem do szerszego zagadnienia, z którym można się spotkać w danych instytucjach samorządowych. Podejście to z pewnością nie jest jedyne i nie jest idealne, ale należy pamiętać, że „Informacja bezpieczna to taka, której nie ma", a informacja, która istnieje jest zawsze narażona na pewne niekorzystne działania. Należy się przed nimi zabezpieczyć i przeznaczyć na to bezpieczeństwo środki finansowe i intelektualne zgodnie z zasadą – „tak silne środki, jaka ważne są

dla nas informacje", czyli nic innego jak ryzyko – „Proces zarządzania ryzykiem w systemie teleinformatycznym prowadzi się w celu zapewnienia i utrzymania na poziomie akceptowalnym przez kierownika danej jednostki organizacyjnej bezpieczeństwa informacji przetwarzanych w tym systemie" [http://isap.sejm.gov.pl/DetailsServlet?id=WDU20111590948].

Postaram się wskazać środki, które przynajmniej w pewnym stopniu pozwolą na zabezpieczenie informacji przed ich utratą czy wyciekiem. W całym cyklu zabezpieczeń należy pamiętać, że najważniejszą rolę w bezpieczeństwie informacji pełni osoba wytwarzająca tę informacje czy też przetwarzająca je.

Rysunek 1. Pogląd na zagrożenie



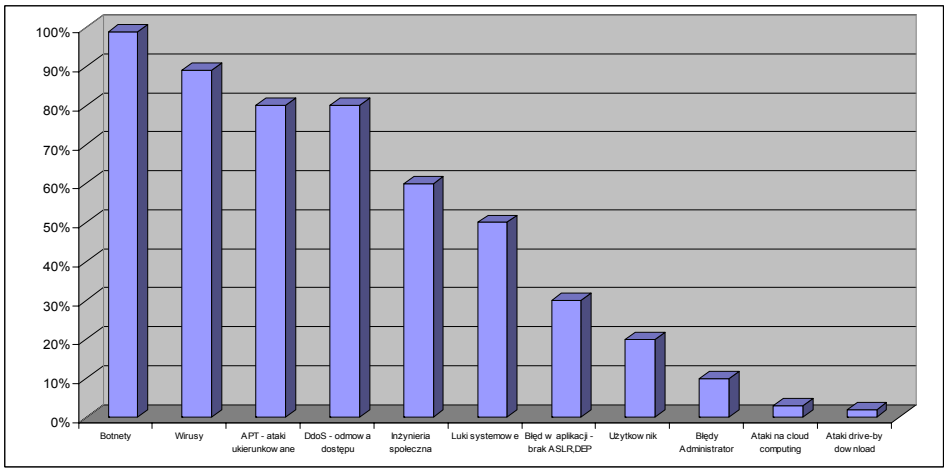
Źródło: opracowanie własne.

Oczywiście trzeba się zastanowić czy w dzisiejszych czasach instytucje samorządowe takie jak Urząd Miejski są wstanie w pełni kontrolować dostęp do informacji przez siebie wytwarzanych czy też przetwarzanych. Moim zdanie takiej 100% pewności nie ma i raczej nigdy jej nie osiągniemy. Właśnie, dlatego należy dołożyć wszelkich starań, stosując pewne środki bezpieczeństwa, aby w procesie przetwarzania informacji utrzymać kontrolę nad nimi w jak najwyższym stopniu no i zgodnie z ryzkiem – na poziomie akceptowalnym przez kierownictwo. Co powoduje brak takiej pełnej świadomości bezpieczeństwa informacji? Spójrzmy na wykres pewnych badań („badanie przeprowadzone w Krakowie 15 maja 2009 r. podczas konferencji, Confidence 2009 na grupie 275 specjalistów IT" [materiały konferencyjne].

Oczywiście dziś ten pogląd na zagrożenia może już być inny. Moim zdaniem świadomość zagrożeń przez pracowników od roku 2009 znacząco się poprawiła na lepsze poprzez wprowadzanie w jednostkach samorządowych polityk bezpieczeństwa informacji oraz szkoleń.

Zastanówmy się również, jakie zagrożenia mogą wystąpić w roku 2014 – wykres ten (rys. 2) został sporządzony przeze mnie na podstawie własnych doświadczeń oraz niektórych wyników statystycznych przedstawianych przez różne źródła. Zostały one ustawione wg skali ważności zwrócenia na nie szczególnej uwagi pod względem instytucji, jaką jest Urząd Miejski – 100% ważne 1% monitorowane przez okresowe sprawdzanie logów. Oczywiście w każdej instytucji te doświadczenia mogą być inne, a zatem i wykres będzie przedstawiał inną ważność zagrożeń.

Rysunek 2. Zagrożenia w skali ważności



Źródło: opracowanie własne.

Klasyfikacja informacji i co musimy zapewnić informacji

Informacje możemy sklasyfikować na różne sposoby, w zależności od przechowywania, przetwarzania czy prawa dostępu do niej. Na potrzeby tego artykułu przyjmijmy klasyfikacje przedstawioną poniżej.

Klasyfikacja informacji:

1. Informacje publiczne – ogólnie dostępne – integralność, rozliczalność.
2. Finansowe – poufność, integralność, rozliczalność.
3. Informacje przedsiębiorstwa – poufność, integralność, rozliczalność.
4. Dane osobowe – poufność, integralność, rozliczalność.
5. Niejawne – poufność, integralność, rozliczalność.

Co trzeba zapewnić informacji:

1. **Poufność** – dostęp do danej informacji powinny mieć tylko osoby czy instytucje do niej upoważnione.
2. **Integralność** – musimy zadbać oto aby informacja nie została przez nieupoważnione osoby zmieniona.
3. **Rozliczalność** – musimy wiedzieć koto i kiedy przetwarzał daną informację.
4. **Dostępność** – musimy zadbać o dostęp do informacji osobom upoważnionym zawsze gdy jest to niezbędne.

Biorąc pod uwagę naszą klasyfikacje informacji można przypisać do niej pewne zapewnienia:

– Informacja publiczna – integralność, rozliczalność a w pewnych warunkach również dostępność, np. informacje w Biuletynie Informacji Publicznych;
– Finansowe, informacje przedsiębiorstwa, dane osobowe, niejawne – poufność, integralność, rozliczalność;

Jak identyfikujemy informacje w Urzędzie

W Urzędzie Miejskim identyfikacja informacji polega na wypełnieniu poniższej tabelki przez poszczególne wydziały. Tabela ta być może nie jest idealnym rozwiązaniem, ale pozwala w sposób dość szybki zlokalizować daną informację i jej zabezpieczenia.

Lp.	*Rodzaj informacji*	*Dane osobowe*	Wrażliwość informacji [i]	*Osoba przetwarzająca informacje*	Forma przetwarzania[ii] informacji		Uprawnienia[iii] osób przetwarzających informacje		*Sposób przechowywania informacji*	*Sposób archiwizowania informacji*	Stosowany system zabezpieczenia dostępu do informacji[iv]
					elektroniczna[v]	*papie-rowa*	*elektronicznie*	*papie-rowo*			
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
1.											

Jakie aplikacje są w Urzędzie pod szczególną ochroną

W systemie teleinformatycznym ważną rolę pełni zlokalizowanie i określenie aplikacji, które mają znaczący wpływ na funkcjonowanie danej instytucji. Na przykładzie Urzędu Miejskiego możemy wyróżnić następujące aplikacje ważne z punktu widzenia przetwarzania informacji:

1. EOD (Elektroniczny Obieg Dokumentów), który jest zintegrowany z EPUAP utrata np. *Dostępności* spowodowała by brak możliwości załatwienia spraw drogą elektroniczną przez klienta.
2. Zintegrowany System Obsługi Urzędu w skład, którego wchodzą min:
   - Ewidencja Ludności (finanse, grunty, nieruchomości);
   - Gospodarka odpadami;
   - Pojazdy;
   - Psy.

   Utrata np. *integralności* mogła by spowodować błędne naliczanie zobowiązań i należności.;
3. Biuletyn Informacji Publicznej, utrata *dostępności* czy *integralności* spowodowałaby podawanie błędnych lub fałszywych informacji lub brak dostępu do tych informacji przez lokalne społeczeństwo;

Należy również pamiętać o ochronie własności intelektualnej. Lokalizacja i rejestr używanych aplikacji w instytucjach pozwala na legalne użytkowanie programów czy informacji. Użytkowanie legalnego oprogramowania minimalizuje również zagrożenia wycieku informacji lub innego rodzaju ataków na sieci teleinformatyczne instytucji. Jedną z najbardziej rozpowszechnionych form przenoszenia różnego rodzaju złośliwego oprogramowania są nielegalne oprogramowania. Dobrą metodą jest stosowanie oprogramowania zbierającego informacje o zainstalowanych programach oraz o próbie ich instalacji przez użytkownika bez wiedzy Administratora systemu w danej jednostce. Dużą rolę pełni też Polityk Bezpieczeństwa wdrożona w Urzędzie Miejskim, która określa zasady instalacji, użytkowania programów czy informacji chronionych prawem autorskim.

Ochrona na styku Internetu oraz w sieci lokalnej Urzędu

Obecnie większość informacji jaką się przetwarza wymaga łączności z Internetem. Jednym z przykładów aplikacji w Urzędzie Miejskim, która korzysta z tego łącza jest CEIGD (Centralna Ewidencja i Informacja o Dzia-

łalności Gospodarczej). Do działania tej aplikacji jest wymagane łącze internetowe, a więc wszelkiego rodzaju ataki na takie łącze destabilizują prawidłową pracę Urzędu. Dlatego tak ważna jest ochrona na styku Internet – Sieć lokalna.

Jeśli chodzi o bezpieczeństwo sieci lokalnej obecnie można zauważyć znaczącą poprawę w różnych instytucjach. W Urzędzie Miejskim takie bezpieczeństwo określa Polityka Bezpieczeństwa Informacji.

Postaram się pokrótce przybliżyć możliwości zabezpieczeń w takich sieciach. Jednocześnie pragnę zaznaczyć, że wszystkie tu podane metody nie są wzięte z konkretnej Instytucji min Urzędu Miejskiego ze względu na to, iż uważam, że takie informacje nie powinny być nigdzie publikowane, o czym często zapominają Administratorzy sieci czy instytucje obsługujące Urzędy Miejskie pod względem teleinformatycznym. Przykłady, które podam będą hipotetyczne, ale jednocześnie zbliżone do realiów, w jakich znajdują się Urzędy Miejskie czy jednostki administracji samorządowej.

Zagrożenia – przykłady ataków w Urzędzie

Przykłady tu wymienionych ataków są ułożone wg moim zdaniem ważności zwrócenia na nie uwagi:

1) APT „Advanced Persistent Threat" – są to ataki ukierunkowane na konkretny cel np. Urząd Miejski w celu wydobycia konkretnych informacji lub sparaliżowania prawidłowej pracy. Jak mogą wyglądać poszczególne etapy takiego ataku:
   - zbieranie informacji o Urzędzie (pracownikach, stosowanych systemach, urządzeniach sieciowych, oprogramowaniu, polityce bezpieczeństwa, …) – *już chyba wiemy teraz dlaczego nie należy takich informacji podawać do publicznej wiadomości – ponieważ pierwszą część ataku zrobilibyśmy sami;*
   - przygotowanie odpowiednich metod do zebranych informacji – np. inżynieria społeczna, sprawdzenie jakie luki ma stosowane oprogramowanie, odpowiednio spreparowany e-mail ze złośliwym oprogramowaniem, zaproponowanie programu do przetestowania przez Urząd, …
   - po udanym wstrzyknięci złośliwego oprogramowania atakujący przejmuje jedną ze stacji bez świadomości użytkownika czy Administratora sieci;
   - następny atak jest już atakiem z sieci lokalnej; atakujący może bardzo długo pozostawać w sieci lokalnej i otwierać sobie następne drogi dostępu czy tylne furtki;

Tak więc widać na tym przykładzie jak ważną rolę spełnia ochrona informacji choćby o systemach teleinformatycznych. Proszę zwrócić uwagę jak często w zamówieniach publicznych taka informacja występuje – czyli ten pierwszy krok ataku APT.

2) DDoS – „Distributed Denial of Service" – atak polegający na odmowie usług; polega na wyssaniu wszystkich wolnych zasobów łącza, atak zazwyczaj następuje z dużej ilości komputerów. Ataki tego typu często uniemożliwiają dostęp dla użytkownika do danej strony internetowej lub danego serwera świadczącego jakieś usługi np. strona BIP.
3) Wirusy – tu chyba wszyscy wiemy, że chodzi o złośliwe oprogramowanie, mogą one stanowić pierwsze wejście do innych ataków komputerowych.
4) Phishing – wyłudzanie pewnych informacji, do których dana osoba nie powinna mieć dostępu; tu stosuje się zazwyczaj inżynierie społeczną. Przykładem może być wykonanie przez atakującego telefonu do pracownika Urzędu i powołanie się na firmę obsługującą daną jednostkę pod względem teleinformatycznym (część nie uświadomionych pracowników może podać nawet nazwę konta i hasło do niego).
5) Pharming – bardziej zaawansowana forma Phishingu – częstym przykładem tego ataku jest skierowanie użytkownika na fałszywą stronę i wyłudzenie loginu i hasła. Jak do niedawna dziecinnie prosty był taki atak niech świadczy fakt, iż wystarczy w systemie w jednym tylko pliku dokonać wpisu przekierowującego dany adres na inną stronę, chodzi tu o plik *hosts*. Plik ten znajduje się w systemie Windows w katalogu *windows\system32\drivers\etc*. Można spróbować wykonać to samemu:
   - edytujemy plik *windows\system32\drivers\etc\host* z uprawnieniami do zapisu
   - na końcu dopisujemy tak jak w przykładzie niżej jedną linijkę:

   # 127.0.0.1 localhost

   # ::1 localhost

   213.180.141.140 www.wp.pl

   - zapisujemy plik;
   - w przeglądarce internetowej wpisujemy www.onet.pl, jeśli wszystko poszło dobrze to ku naszemu zdziwieniu zamiast na onecie wylądowaliśmy na stronie wirtualnej polski. Tu widać jak ważne jest, aby użytkownik logował się do systemu z ograniczonymi uprawnieniami, które uniemożliwią wykonanie takiego wpisu.

6) Backdor – luka w systemie bezpieczeństwa umożliwiająca późniejsze wykorzystanie; np. przejęcie kontroli nad komputerem.
7) Ataki na Cloud-computing – stosunkowo nowe ataki na zasoby przechowywane w tak zwanej „chmurze"; czyli jak zwykle chodzi o kradzież informacji.
8) Ataki driver-by download – polegają na łączeniu się przez przeglądarkę internetową do strony, na której został umieszczony exploit (exploit wykorzystuje błędy w oprogramowaniu w celu przejęcia kontroli nad procesem).

Z przykładów podanych wyżej widzimy, że informacja jest ważna i należy ją chronić. Moim zdaniem w instytucjach i jednostkach samorządowych jest zbyt mała dbałość o nie przekazywanie informacji dotyczących systemów teleinformatycznych. Powinno też być zmienione prawo dotyczące przetargów na systemy teleinformatyczne tak, aby informacje o nich były chronione.

Innymi słowy mówiąc *„wiem co masz to znajdę tam lukę"*.

Zagrożenia w sieci lokalnej

Sieć lokalna jest tak samo zagrożona jak sam styk z Internetem. Często wydaje się nam, że jeśli dobrze chronimy się od strony Internetu to lokalnie nic nam nie grozi – moim zdaniem taki tok rozumowania jest błędny. Sieć lokalną należy tak samo dobrze chronić, postaram się pokrótce przedstawić podstawowe zagrożenia w tej sieci.

1) Brak świadomości pracowników. Jak widać na wykresie rys. 1. jeszcze niedawno fachowcy od IT podawali to zagrożenie, jako najczęściej występujące. Obecnie ta sytuacja już częściowo się zmienia, ale zawsze ten czynnik ludzki będzie miał dość duży wpływ na bezpieczeństwo w sieciach lokalnych i nie tylko. Przykładem na takie zagrożenie niech będą przechowywane, czy zapisywane hasła do systemów, programów i innych zasobów. W niektórych jednostkach można powiedzieć, że te hasła są wszędzie: w kalendarzu, na ścianie, pod klawiaturą, na ekranie żółta karteczka, aby lepiej było widać.
2) Inżynieria społeczna. Są to metody stosowane przez osoby chcące uzyskać dostęp do informacji wykorzystujące łatwowierność lub niewiedzę pracownika. Przykładem niech będzie krążąca wśród Administratorów historyjka jak Pani N zmarł mąż i podczas pogrzebu otrzymuje telefon od osoby udającej pracownika danej firmy o potrzebie podania jej loginu i hasła – w takim stresie osoba ta podała wszystkie potrzebne dane.

3) Atak MAC Flooding. Polega na zakłóceniu pracy przełączników. Ponieważ dane o adresach MAC przechowywane są w pamięci CAM (content-addressable memory) atak ten polega na przepełnieniu tej pamięci. Po przepełnieniu pamięci urządzenie zachowuje się jak koncentrator – czyli pakiety są przekierowywane na wszystkie porty, a tym samy łatwo podsłuchać informacje jakie tam krążą.
4) Atak ARP Spoofing. Atak tego typu pozwala na przechwycenie danych w pewnym segmencie sieci. Polega on na przesyłaniu w sieci odpowiednich spreparowanych pakietów ARP, które zawierają sfałszowane adresy MAC. W wyniku takich działań pakiety zamiast trafiać do prawdziwego odbiorcy trafiają do osoby atakującej. Nie podaję tutaj szczegółów tego ataku – można go znaleźć w Internecie lub wielu wydaniach książkowych o bezpieczeństwie w sieciach lokalnych.
5) Ataki Spanning Tree Protocol. Przykładem takiego ataku może być stacja robocza połączona dwoma łączami do sieci lokalnej. Można wtedy wymusić wyznaczenie jej na Root Bridge i w takim przypadku znaczna część ruchu będzie płynęła przez tą stację roboczą.

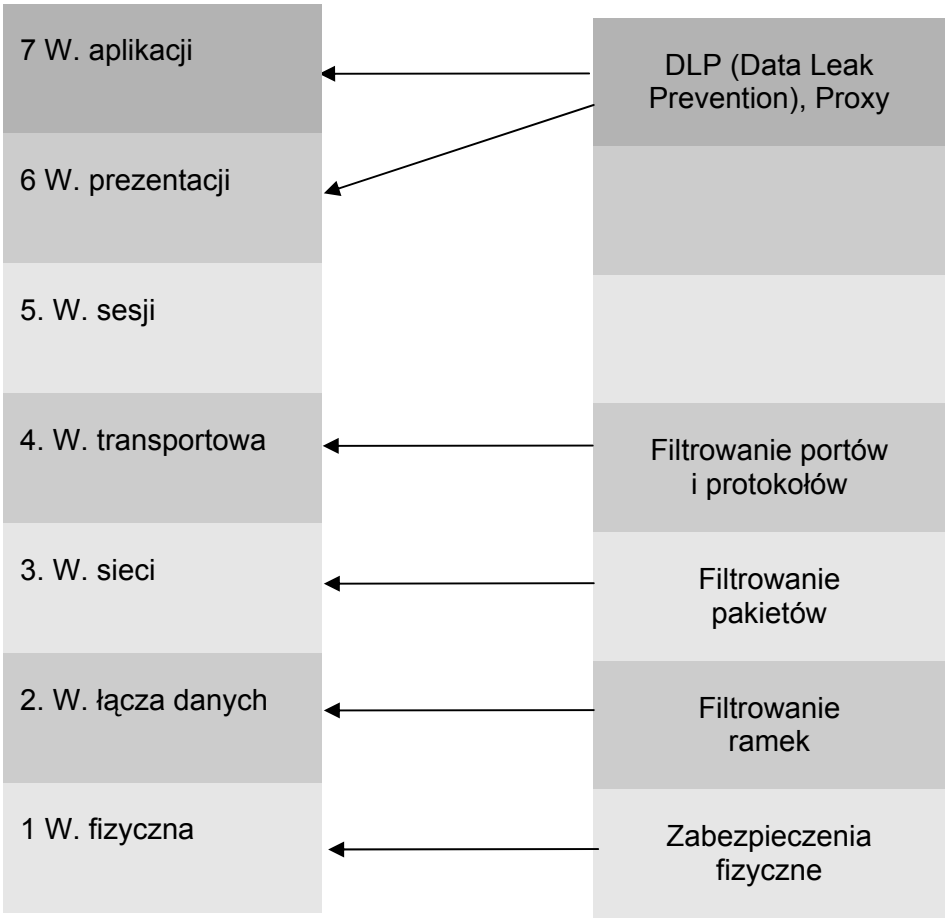
Oczywiście jest to tylko zasygnalizowanie części podatności sieci lokalnych na ataki od środka. Zainteresowanych tą tematyką odsyłam do literatury umieszczonej na końcu tego opracowania. Jak Państwo zauważyli nie poruszyłem tu nawet zagrożenia tak oczywistego jak wirusy – ale myślę, że dzisiejsza świadomość użytkownika jest już na tyle duża, że tak trywialne fakty można opuścić.

Ochrona na styku sieci lokalnej Urzędu a Internetem

Mamy już kropelkę informacji o zagrożeniach, więc można posilić się o próbę ich wyeliminowania poprzez zabezpieczenie sieci. Należy mieć świadomość, takie jest moje zdanie, że nie ma idealnej metody zabezpieczenia się przed atakami – można tylko je zminimalizować i liczyć na to, „że nam się to nie przytrafi".

Zanim zaczniemy omawiać kolejne możliwe zabezpieczenia spójrzmy jak to wygląda na modelu OSI (rys. 3). Z prawej strony widzimy jakie zabezpieczenie w danej warstwie należy przyjąć. W dzisiejszych czas oprócz ochrony w warstwach 1–4 podstawową ochronę należy zastosować w warstwach wyższych, czyli w warstwie aplikacji czy prezentacji.

Rysunek 2. Zabezpieczenia w modelu OSI

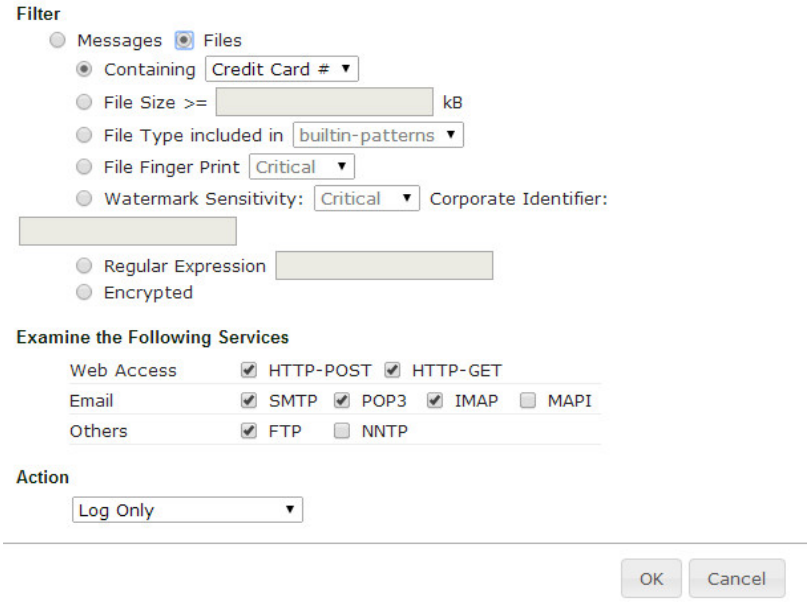


Źródło: opracowanie własne.

Dzisiejszy firewall powinien umożliwiać ochronę w warstwach wyższych, przed stawie tutaj jeden z podstawowych mechanizmów ochrony w tej warstwie, a mianowicie DLP, który chroni przed wyciekami wrażliwych informacji.

1) DLP (Data Leak Prevention) – ochrona przed wyciekami. Jak pokazane jest na modelu OSI zabezpieczenie to działa na warstwach 7,6. Zobaczmy na przykładzie jednego z dostępnych na rynku firewalli, co można przy pomocy DLP chronić:

Rysunek 3. Ustawienia DLP



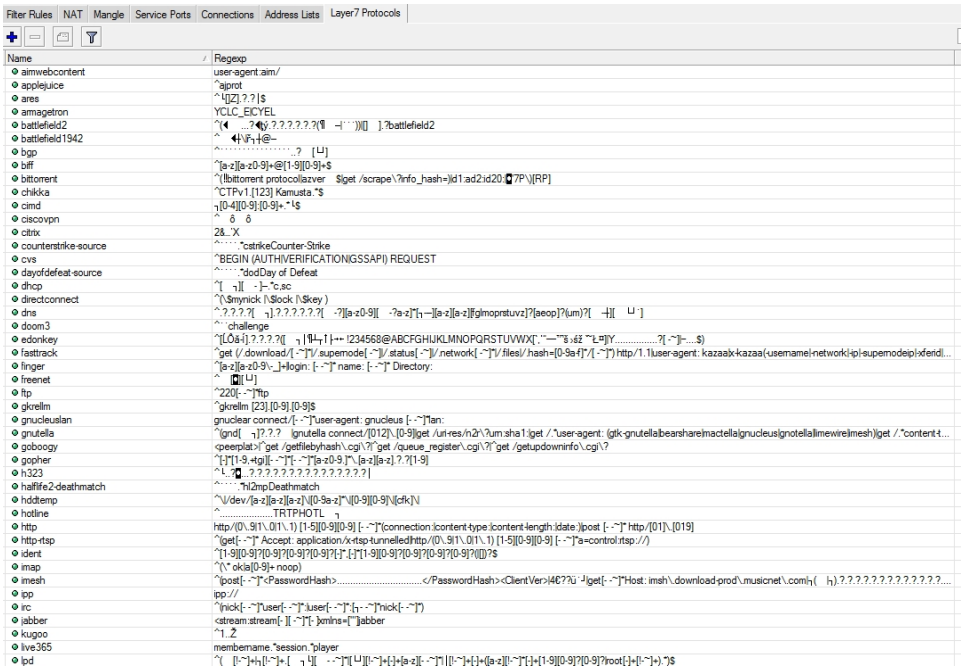
Źródło: opracowanie własne.

- - zabezpieczenie przed wyciekiem nr kard kredytowych;
- - można określić warunek wielkości pliku;
- - typ pliku np. określamy, że pliki z rozszerzeniem doc nie mogą wyjść poza jednostkę;
- - sumy kontrolnej pliku
- - znaku wodnego na dokumencie np. dokument z danym znakiem wodnym nie może opuści jednostki;
- możemy określić dowolną zawartość pliku, która jest w dokumencie i na tej podstawie zezwolić lub zabronić wyjścia poza jednostkę;
- możemy również ustawiać różnego rodzaju akcje – czyli czy plik ma być zapisany w logach, czy chcemy zapisać cały plik, czy ma być zablokowany, czy też można go wysłać;
- podobne ustawienia stosujemy również do przesyłanych informacji czy to drogą meilową czy komunikatorami;

2) Ważną ochroną w warstwie 7, 6 jest ochrona konkretnych aplikacji. Możemy zabronić z korzystania z tych aplikacji np. Gadu-Gadu lub pozwolić na ich komunikację. Zobaczmy jak to można zrobić na routerze Mikrotik:

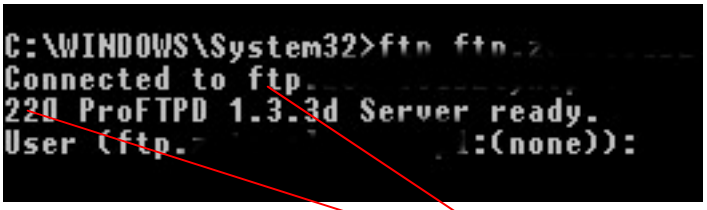
a) na początku musimy zdefiniować *regexp* (sygnatury);

Rysunek 5. Ochrona w warstwie 7 (Mikrotik)



Źródło: Internet.

Popatrzmy na sygnaturę protokołu ftp *regexp="^220[\t-\r -~]*ftp*



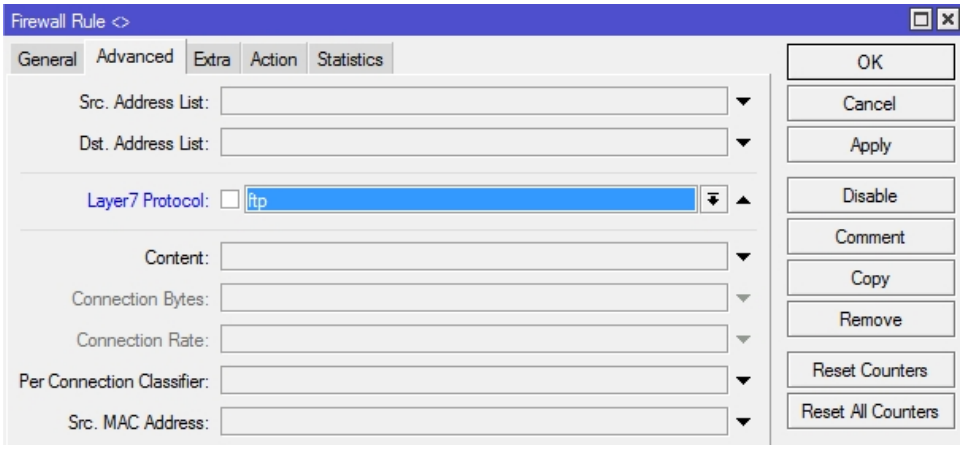
220 oraz ftp zazwyczaj występują podczas zgłoszenia się serwer ftp

Jak widać, można zdefiniować dowolne wystąpienia ciągów znaków w pakiecie i na tej podstawie dokonywać określonych czynności przez firewall. Odrzucenie pakietów czy ich akceptacja nie ma nic wspólnego z otwartym portem – w przypadku ftp 21.

b) Następnie dodajemy regułę do firewalla;

Rysunek 7. Firewall (Mikrotik) - Advanced

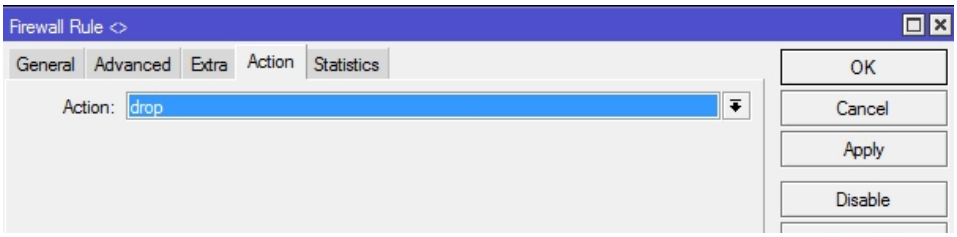
podajemy zdefiniowaną sygnaturę



Źródło: opracowanie własne.

Co z takim pakietem ma się stać (np. wycięty)

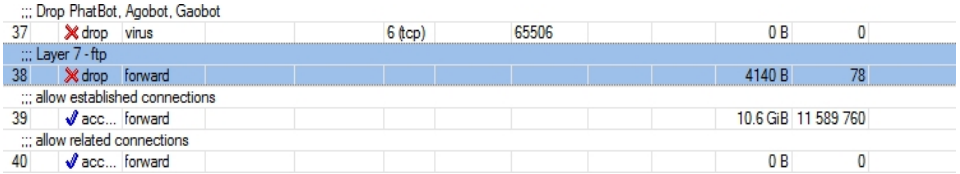
Rysunek 8. Firewall (Mikrotik) - Action



Źródło: opracowanie własne.

Jak widzimy pakiety tak oznaczone są usuwane.

Rysunek 9. Firewall (Mikrotik)



Źródło: opracowanie własne.

3). IDS (*Intrusion Detection System*) – technologia ta służy do wykrywania zagrożeń płynących z sieci zewnętrznych. W różnych w zależności o danego sprzętu są różnie zaimplementowane. Podstawowa rola, jaką ma ta funkcja spełniać to:
   - analiza ruchu sieciowego pod względem ataków;
   - zapisywanie tych informacji w logach;
   - podejmowanie wcześniej zadeklarowanych działań w zależności od rodzaju ataku;

4) IPS (*Intrusion Prevention Systems*) – to technologia łącząca firewall i IDS. Służy do zapobiegania atakom z wewnątrz jaki i zewnątrz sieci. Podstawowa rola to:
   - analiza ruchu sieciowego i wykrywania ataków;
   - zbieranie informacji o atakach (np. z różnych sensorów umieszczonych w systemie);
   - zapis tych informacji oraz ich wizualne przedstawianie;
   - podejmowanie decyzji w razie wykrytego ataku o blokadzie ruchu.

Ochrona w sieci lokalnej

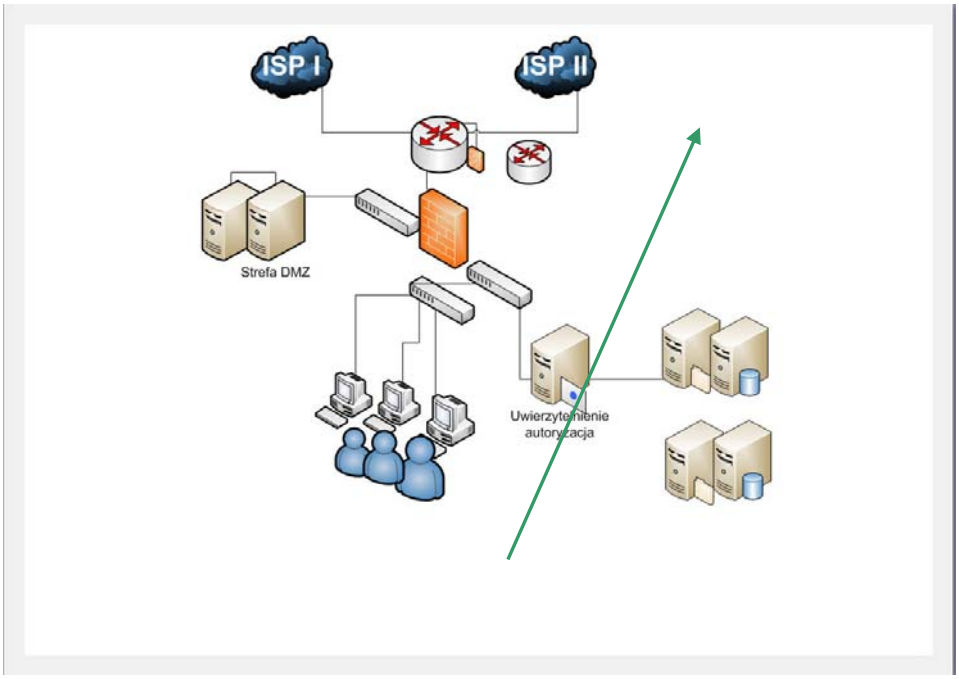
Chipotetyczny model sieci lokalnej

Teoretycznie można przyjąć taki prosty model ochrony w sieci lokalnej:

- zabezpieczenie przed utratą dostępu do Internetu przez backupowe łącze od dwóch dostawców *ISP I, ISP II;*
- router (failover) z podstawową minimalną wstępną ochroną sieci (np. filtracja pakietów, ograniczanie spamu itp.)
- firewall (failover) skonfigurowany minimum na 3 porty – strefa DMZ, sieć lokalna, dostęp do Internetu;
- firewall powinien być tak skonfigurowany, aby nawiązanie połączenia z siecią zewnętrzną było możliwe tylko przez nawiązanie sesji od strony sieci lokalnej.

Taki model jest bardzo uproszczony. Jednak patrząc na realia w niektórych jednostkach samorządowych mógłby być dobrym rozwiązaniem pod warunkiem zastosowania wszystkich omówionych powyżej technik (rys. 10).

Rysunek 4. Schemat sieci lokalnej



Źródło: opracowanie własne.

Ochrona przed atakami ARP

Najczęstsze ataki typu arp to: arp MITM, Arp DoS, arp flooding, arp hijacking. Oto kila porad, które warto znać, aby zminimalizować ataki tego typu:

a) ochrona przed możliwością dołączenia do naszej sieci lokalnej (bez naszej wiedzy) stacji roboczej;
b) stosowanie szyfrowania w sieciach – przechwycone pakiety będą trudne do odczytania;
c) stosowanie przełączników zamiast koncentratorów;
d) dowiązanie na stałe adresów mac w tablicy;
e) wykrywanie sniffingu np. test ARP, test ICMP, pomiar czasu opóźnienia czy metoda reflektometryczna;
f) stosować VLAN-y;

Ochrona sieci lokalnej przed innymi atakami

Należy również pamiętać przed stosowaniem:

a) programów antywirusowych chroniących nas przed robakami, wirusami, backdoorami, trojanami, rootkitami itp.;

b) stosować wewnętrzne serwery DNS co częściowo może nas chronić przed atakami Man-in-the-Middle;

c) aktualizować systemy;

d) sprawdzać integralność plików; przykładowe narzędzia to Tripwire dla systemu Linux, FastSum dla systemu Windows;

e) stosować ochronę fizyczną przed dostępem do serwerów czy stacji roboczych dla nieupoważnionych osób;

Zasady pracy w sieci dla pracownika Urzędu

Podstawową ochroną w sieci lokalnej, jest określenie podstawowych zasad pracy z tą siecią, czyli Polityka Bezpieczeństwa. Omówię tu kilka wybranych aspektów dotyczących takiej podstawowej ochrony:

1. **Uwierzytelnienie** – czyli stwierdzenie, że dany komputer, dana osoba jest tą za którą się podaje;
   - może to być certyfikat, login i hasło, biometryka, itp.;
   - np. w systemie Windows możemy włączyć uwierzytelnienie 802.1X, jak to zrobić: w konsoli cmd wpisujemy *services.msc* w oknie wyszukujemy *Automatyczna konfiguracja sieci przewodowej* a następnie *uruchom* – zamykamy okienko; w połączeniach sieciowych wybieramy nasze połączenie i wybieramy *właściwości* wybieramy kartę uwierzytelnienie a w polu wyboru *włącz uwierzytelnienie metodą IEEE 802.1X*.
2. **Autoryzacja** – jest to proces nadawania uprawnień – czyli nic innego jak określamy do czego ma dostęp dana osoba, komputer i z jakimi uprawnieniami.
3. **Siła hasła –** należy zadbać o siłę hasła podczas procesu uwierzytelniania, autoryzacji. Hasła powinny dziś spełniać przynajmniej następujące założenia:
   - długość hasła – min. 8 znaków ;
   - złożoność – duża litera, mała litera, liczba, znak typu: !, ?, &, …;
   - czas ważności hasła – nie powinien być większy niż 30 dni;
4. W sieci należy wdrożyć metody zabezpieczenia przed nieupoważnionym używaniem nośników wymiennych. Obecnie na rynku istnieje szereg te-

go typu rozwiązań np. Symantec Endpoint Protection, Statlook, …, jeśli pracujemy z AD (Active Directory) możemy to robić przez GPO.

5. Możemy również uruchomić serwer NAP (Network Access Protection) – jest to serwer sprawdzający czy dany klient podłączający się do sieci spełnia przez nas określone warunki bezpieczeństwa – jeśli tych warunków nie spełnia nie zostaje dopuszczony do pracy w sieci, aż do momentu spełnienia tych warunków, np. stara baza sygnatur antywirusowych, brak uaktualnień, itp.
6. Dobrą zasadą jest szyfrowanie danych na nośnikach, przede wszystkim zewnętrznych. Zgubienie, czy utrata takiego nośnika z innych powodów znacząco ogranicza możliwość odczytania danych na nim zgromadzonych.

Zakończenie

Jaka widać z tego, krótkiego opracowania zagrożeń w sieciach lokalnych czy rozległych jest bardzo dużo. Tematyka jest tak rozległa, że praktycznie na każdy poruszony tutaj problem można napisać oddzielną książkę. Jak wspomniałem na wstępie to opracowanie jest tylko sygnalizacją zagrożeń, które istnieją w sieciach. Należy pamiętać, że o nowych zagrożeniach dowiadujemy się dopiero po fakcie, czasami po kilku latach, przykładem może tu być dziura w OpenSSL, o której dowiedzieliśmy po 2 latach od wystąpienia. Należy pamiętać, że dzisiaj istnieje możliwość odczytania większości informacji zaszyfrowanej, a więc i ta metoda nie daje stuprocentowej pewności bezpieczeństwa informacji. W artykule na stronie hack.pl (http://hack.pl/aktualnosci/sekrety-staran-nsa-aby-dorwac-i-zhackowac-administratorow-systemow.html) można przeczytać, że różnego rodzaju agencje śledzą aktywność na różnego rodzaju portalach społecznościowych Administratorów sieci, tak więc należy pamiętać o ukrywaniu w pewien sposób swojej tożsamości w sieci rozległej jaką jest internet.

Tak więc na zakończenie tego krótkiego referatu motto dla wszystkich zajmujących się próbą ochrony swoich sieci:

„ Paranoja jest twoim przyjacielem”

i ma to sens o tyle, że trzeba w sieci widzieć wszędzie zagrożenie.

Literatura

Szmit M., Gusta M., Mariusz Tomaszewski M. (2005), *101 zabezpieczeń przed atakami w sieci komputerowej*, Wyd. Helion.

Agresja i Ochrona (2000), Robomatic.

Wikipedia; http://pl.wikipedia.org/

Sekurak; http://sekurak.pl

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 147–164

Małgorzata Domańska
Społeczna Akademia Nauk

Działalność Gminy w zakresie gromadzenia, przetwarzania i ochrony danych osobowych

Activities of Municipalities in the collection, processing and protection of personal data

Abstract: Municipality as the main unit of the local government, fulfills a number of functions, including taxable and non-taxable incomes, investments, maintenance of schools, financing of social care, as well as organization of public life. To perform the tasks, it is necessary to collect, process and store tax data, both private persons and companies (business partners), at the same time providing proper protection of the data, by implementation of a security system for the IT data. In this field, the government is also responsible for data protection within the range of granted authorizations used by the Committee of the Municipal Council, Municipal Council, Supreme Chamber of Control (NIK), Regional Chamber of Account under performing internal control or audit. The data must be also secured and controlled in the scope of disclosing them to public knowledge. The purpose of the article is the discussion of widely understood "security policy", including threats analysis and data processing risk assessment. The article is a result of researches and experience of the author as well as the team of other persons related to the subject.

Key words: finance, protection of personal data, local government.

Wprowadzenie

Gmina, jako podstawowa jednostka samorządu terytorialnego spełnia liczne funkcje polegające na realizowaniu dochodów podatkowych i niepodatkowych, realizacji wydatków bieżących oraz inwestycji, utrzymania szkół, finansowania pomocy społecznej, kultury i sportu, a także organizowania życia publicznego lokalnej społeczności. W tej sytuacji niezbędne jest gromadzenie, przetwarzanie i archiwizowanie danych dotyczących podatków – zarówno osób fizycznych (mieszkańców) jak i podmiotów gospodarczych, kontrahentów oraz zapewnienie ochrony danych, jak też wdrożenie odpowiedniej polityki bezpieczeństwa systemem informatycznym.

Na tym tle Gmina staje przed wyzwaniem ochrony danych, również w przypadku realizacji uprawnień Rady Gminy, Komisji Rady Gminy, Najwyższej Izby Kontroli, Regionalnej Izby Obrachunkowej w zakresie pełnienia funkcji kontrolnych przez te organy, ale również wielu zapytań w systemie informacji publicznej.

Celem artykułu jest omówienie zasad szeroko rozumianej „polityki bezpieczeństwa", w tym analiza zagrożeń i ocena ryzyka przetwarzania danych osobowych i firm. Artykuł jest wynikiem badań i doświadczeń własnych autora oraz zespołu innych osób nad problematyką bezpieczeństwa.

Organizacja i działalność samorządu terytorialnego

Samorząd terytorialny to podstawowa forma organizacji lokalnego życia publicznego, której działalność sprowadza się do samodzielnego wykonywania zadań, które służą zaspokajaniu zbiorowych potrzeb wspólnoty samorządowej. Podstawową jednostką samorządu terytorialnego jest Gmina, która wykonuje wszystkie zadania samorządu terytorialnego w interesie mieszkańców, niezastrzeżone dla innych jednostek samorządu terytorialnego. Zadania publiczne służące zaspokajaniu zbiorowych potrzeb wspólnoty samorządowej wykonywane są przez gminę jako zadania własne i odnoszą się głównie do pogłębiania i poprawy warunków funkcjonowania społeczności [Domańska 2013, s. 78]. Jednakże samorządy wykonują wiele innych zadań powierzonych oraz zleconych m.in. w zakresie administracji publicznej, oświaty czy pomocy społecznej. Jednostki samorządu terytorialnego wykonują zadania za pośrednictwem organów stanowiących i wykonawczych. Są wyposażone w niezbędne narzędzia i środki umożliwiające wykonywanie zadań, do realizacji których zostały powołane, czyli zaspokajania potrzeb społeczności lokalnej. Zadania gmin odnoszą się głównie do pogłębiania i poprawy warunków funkcjonowania społeczności lokalnej poprzez realizację założonych zadań, zawartych w ustawie o samorządzie gminnym, która reguluje organizację samorządu terytorialnego [Dz. U. z 2013 r. poz. 594]. Zadania dotyczą głównie zagadnień z zakresu:

- ładu przestrzennego, gospodarki nieruchomościami;
- ochrony środowiska, przyrody i gospodarki wodnej;
- dróg gminnych, ulic, mostów, placów oraz organizacji ruchu drogowego;
- wodociągów, zaopatrzenia w wodę, kanalizacji, usuwania i oczyszczania ścieków komunalnych;

- utrzymania porządku i czystości oraz urządzeń sanitarnych, wysypisk i unieszkodliwiania odpadów komunalnych;
- zaopatrzenia w energię elektryczną i cieplną,
- ochrony zdrowia, pomocy społecznej, polityki prorodzinnej;
- wspierania rodziny i systemu pieczy zastępczej, budownictwa mieszkaniowego;
- edukacji, kultury, kultury fizycznej i sportu oraz ochrony zabytków i opieki nad nimi;
- targowisk i hal targowych, zieleni gminnej i zadrzewień;
- cmentarzy gminnych, porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej, utrzymania obiektów i urządzeń obiektów użyteczności publicznej oraz obiektów administracyjnych;
- wspierania i upowszechnianie idei samorządowej, promocji gminy i współpracy z organizacjami samorządowymi, współpracy ze społecznościami pozarządowymi.

Gmina realizując ustawowo określone zadania, gromadzi i przetwarza dane osobowe, które z mocy ustawy podlegają ochronie. Należą do nich m.in. dane:

- dotyczące osób fizycznych, podatników, podmiotów gospodarczych, kontrahentów, firm zamieszczone w różnego rodzaju rejestrach, skorowidzach, kartotekach, zbiorach księgowych, wykazach lub też innych systemach ewidencyjnych;
- zawarte w programach informatycznych (finansowo-księgowych, wymiarowych, podatkowych, kadrowo-płacowych, ewidencji ludności, działalności gospodarczej, pomocy społecznej, itp.);
- utworzone w zbiorach danych oraz poza nimi (zbiory zarejestrowane u Generalnego Inspektora Ochrony Danych Osobowych (GIODO) przetwarzane przez Gminę);
- współpracujących ze sobą sieci, urządzeń, programów, technik przetwarzania informacji i oprogramowania (np. elektroniczny system obiegu dokumentów).

Są to głównie dane podlegające ochronie i dotyczą przede wszystkim danych podatników, danych osobowych osób fizycznych, osób prawnych, procedur związanych z zamówieniami publicznymi (przetargi), szkół, ośrodków pomocy społecznej, ośrodków zdrowia oraz pozostałych związanych z realizacją zadań publicznych. Jako przykład mogą posłużyć *rejestry zbiorów*

danych gromadzone i przetwarzane przez Gminę. Możemy wśród nich wyróżnić m.in. zbiory zawierające dane osobowe podlegające ochronie w jednostkach oświatowych, np.:

- rejestr rodziców, którzy otrzymują dofinansowanie na dowóz dziecka do szkoły;
- rejestr uczniów, którzy otrzymują pomoc materialną;
- rejestr awansu zawodowego nauczycieli oraz tych, którzy otrzymują dofinansowanie do kształcenia czy tych, którym udzielono pomocy zdrowotnej;
- rejestr dofinansowań do kształcenia młodocianego pracownika;
- arkusz organizacyjny szkoły;
- system informacji oświatowej (SIO).

Z kolei w zakresie gospodarki nieruchomościami oraz podatków i opłat lokalnych takie dane stanowić będą m.in.:

- wykazy podatników podatku od nieruchomości, rolnego, leśnego, od środków transportowych,
- wykazy nieruchomości,
- rejestry wymiarowe,
- ewidencja decyzji w sprawie zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej,
- ewidencja wydanych decyzji w sprawie umorzenia, odroczenia bądź rozłożenia na raty.

Kolejnym przykładem jest gospodarka komunalna i ochrona środowiska. W tym segmencie mamy do czynienia m.in. z danymi podlegającymi ochronie głównie w zakresie wykazu wydawanych decyzji środowiskowych, wykazu przydomowych oczyszczalni ścieków, wykazu danych zawartych w złożonych deklaracjach w sprawie opłaty za gospodarowanie opadami.

Newralgiczne obszary w zakresie ochrony danych osobowych zawiera pomoc społeczna. Zgodnie z zapisami ustawy z dnia 12 marca 2004 r. o pomocy społecznej w postępowaniu w sprawie przyznawania świadczeń z pomocy społecznej należy kierować się głównie dobrem osób korzystających z pomocy społecznej i ochroną ich dóbr osobistych [Piskorz-Ryń 2007, s. 82]. W myśl zapisów ustawy nie można podawać do wiadomości danych osobowych osób korzystających z pomocy społecznej, a także charakteru przyznanego świadczenia (np. pomoc rzeczowa, zasiłek stały, zasiłek okresowy, zasiłek celowy).

Jak ważne w sferze omawianej płaszczyzny jest umiejętne i efektowne zarządzanie ryzykiem, analiza zagrożeń oraz ocena ryzyka procesu gromadzenia, przetwarzania i ochrony danych osobowych, ich ujawnienie mogłoby doprowadzić do utraty kontrahentów czy procesów sądowych. Zagrożenia to zjawiska wywołane działaniem człowieka (umyślne, nieumyślne) lub sił wyższych (przyrody, środków trwałych itp.), które powodują, że poczucie bezpieczeństwa maleje bądź zupełnie zanika [Generalny Inspektor Ochrony Danych Osobowych 2009, ABC zagrożeń …, s. 97]. Analiza i ocena z kolei obejmuje identyfikację i zweryfikowanie ewentualnych zagrożeń mogących wystąpić na poszczególnych procesach przetwarzania danych (gromadzenie, utrwalanie, opracowywanie, zmienianie, udostępnianie, przechowywanie, usuwanie). Prowadzona w sposób systematyczny i uporządkowany pozwala na wprowadzenie odpowiednich procedur oraz zabezpieczeń, które zminimalizują prawdopodobieństwo ich wystąpienia [Pilc, *Kontrola przestrzegania przepisów o*…, s. 7] w obszarze działalności danego samorządu (gminy). Wśród zagrożeń można wyróżnić:

1. Zagrożenia zasobów sieciowo-komputerowych spowodowane głównie umyślną działalnością sieciową (może być połączona z działalnością przestępczą, a także włamaniami hakerów, posiadających obszerną wiedzę informatyczną i umiejętnie wykorzysujących uchybienia w sieci oraz oprogramowaniu), poprzez rozsyłanie np. spamu czy też złośliwego oprogramowania, powodująca:
   - ujawnienie informacji, a w konsekwencji utratę poufności, oznaczającą ochronę przed nieautoryzowanym dostępem do odczytu,
   - modyfikację informacji, czyli utratę integralności i nienaruszalności, rozumianej jako ochrona danych przed ich nieautoryzowanym zmodyfikowaniem [Ogólne własności bezpieczeństwa informacji…],
   - brak dostępu do informacji czy systemu dla uprawnionych użytkowników [Pilc, *Kontrola przestrzegania przepisów o*…, s. 8], a więc utratę dostępności zasobów.
2. Działania umyślne fizyczne, dokonywane poprzez bezpośrednią obserwację, podsłuch lub kradzież posiadanych zasobów.
3. Działania przypadkowe, będące wynikiem pomyłki, pominięcia użytkowników systemu lub wynikające z problemów technicznych, np. wad sprzętu i oprogramowania, awarie, przerwy i zakłócenia w sieci energetycznej.
4. Problemy organizacyjne, wynikające ze złej organizacji pracy użytkowników systemów, braku wdrożonych odpowiednich procedur postępowań

(polityka bezpieczeństwa), braku organizacji infrastruktury informatycznej, niewystarczająca wiedza oraz niewłaściwe monitorowanie zabezpieczeń i utrzymywanie posiadanych zasobów.

5. Błędów ludzkich, wynikających głównie z nieprzestrzegania podstawowych zasad bezpieczeństwa – polityki bezpieczeństwa, braku świadomości wystąpienia zagrożeń, zapisywania haseł w miejscach łatwo dostępnych dla innych użytkowników systemu, pomyłkowe skasowanie danych czy nieprawidłowe użytkowanie i administrowanie systemu [Pilc, *Kontrola przestrzegania przepisów o*…, s. 9].

Podstawowym elementem wyeliminowania zagrożeń jest analiza ryzyka. Polega ona głównie na zidentyfikowaniu dla danego obszaru przetwarzania (środowisko informatyczne, zabezpieczenia fizyczne obiektów, nośników danych, serwerów, stacji roboczych, mediów transmisyjnych, itp.) naturalnych zagrożeń i oszacowanie potencjalnych skutków ich wystąpienia. Oprócz tego na wyszukaniu i zastosowaniu środków zmniejszających prawdopodobieństwo lub skutki ich wystąpienia [Analiza ryzyka cz. 2].

Procesy takie mogą przebiegać według różnych schematów. Można np. skorzystać ze schematów wskazanych w polskich normach technicznych dotyczących zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo systemów informatycznych, np. wg normy PN-I-13335-1, gdzie zarządzanie ryzykiem jest jednym z kilku elementów procesu zarządzania bezpieczeństwem systemów teleinformatycznych, których celem jest udzielenie odpowiedzi na następujące pytania:

- co złego może się wydarzyć?
- jakie jest prawdopodobieństwo, że wydarzy się coś złego?
- jakie skutki dla systemu informatycznego i organizacji będą miały te wydarzenia?
- jak i ile możemy zmniejszyć straty? [Generalny Inspektor Ochrony Danych Osobowych 2009, ABC zagrożeń…, s. 67].

Należy pamiętać, że ryzyko można zmniejszyć, niwelować, ale nie jest możliwe całkowite jego wyeliminowanie. W zarządzaniu ryzykiem istotna jest odpowiedź na pytanie, do jakiego poziomu można i warto je obniżać. Okazuje się, że na pewnym poziomie dodawanie nowych zabezpieczeń jest znacznie kosztowniejsze niż wzrost wartości bezpieczeństwa, które można osiągnąć. Ryzyko należy obniżać do poziomu, w którym jednostka będzie mogła ponieść ciężar strat spowodowanych przez zrealizowanie się zagroże-

nia i kontynuować swoją działalność? [Generalny Inspektor Ochrony Danych Osobowych 2009, ABC zagrożeń…, s. 68].

Możemy je minimalizować poprzez umiejętne zarządzanie ryzykiem, czyli monitorowanie ryzyka, zidentyfikowanie newralgicznych obszarów ryzyka, podejmowanie odpowiednich środków w celu jego ograniczenia, dobór odpowiednich systemów informatycznych, zapewnienie odpowiednich szkoleń oraz nakładów finansowych na IT, które mogą przełożyć się na ewentualne koszty związane z utratą danych. Ponadto poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych adekwatną do zagrożeń oraz kategorii danych objętych ochroną [Pilc, *Kontrola przestrzegania przepisów o*…, s. 10]. W szczególności będzie to zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem zapisów ustawy oraz zmianą, utratą, kradzieżą, uszkodzeniem lub zniszczeniem [Generalny Inspektor Ochrony Danych Osobowych 2007, ABC bezpieczeństwa…, s. 5]. Ponadto przyjęcie odpowiedniej dokumentacji opisującej sposób przetwarzania danych oraz środki ochrony ich przetwarzania, a także powołanie administratora bezpieczeństwa informacji, który będzie nadzorował przestrzegania stosowania środków (technicznych i organizacyjnych) zapewniających ochronę posiadanych danych osobowych.

Żeby skutecznie zabezpieczyć system należy usunąć „wszystkie" jego słabości i podatność na znane rodzaje ataków, jak również ataki, które mogą pojawić się w najbliższej przyszłości, zaś aby skutecznie zaatakować – wystarczy znaleźć jedną słabość danego systemu i stosownie ją wykorzystać [Generalny Inspektor Ochrony Danych Osobowych 2009, ABC zagrożeń …, s. 33].

Tak więc obok ustawy o samorządzie gminnym, samorząd wykonując swoje zadania uwzględnia zapisy wielu innych ustaw. Należą do nich m.in. ustawa o finansach publicznych [Dz. U. z 2013r. poz. 885], o dostępie do informacji publicznej [Dz. U. z 2001 r. nr 112, poz. 1198] oraz o ochronie danych osobowych [Dz. U. z 2002 r. nr 101, poz. 926].

Dostęp do informacji publicznej

Konstytucyjna ochrona prywatności oraz danych osobowych zawarta jest w ustawie z 29 sierpnia 1997 roku o ochronie danych osobowych. Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Nikt nie może być zobowią-

zany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby [Konstytucja Rzeczypospolitej Polskiej]. Organy władzy publicznej w ramach prowadzonej działalności nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych [Konstytucja Rzeczypospolitej Polskiej]. Jeżeli osoba zainteresowana zwróci się z wnioskiem w oparciu o ustawę o dostępie do informacji publicznej o udzielenie informacji np. o podanie kosztów realizacji zadania w zakresie opieki nad bezdomnymi zwierzętami, Gmina jest zobowiązana do udzielenia tej informacji w trybie przewidzianym w ustawie. Inaczej jest w sytuacji, gdy zainteresowany zwróci się z wnioskiem o udzielenie informacji dotyczącej np. wynagrodzenia osób, które zobligowane są do składania oświadczeń majątkowych. Wówczas Gmina nie ma obowiązku udzielania takiej informacji, lecz odesłania zainteresowanego do Biuletynu Informacji Publicznej (BIP), gdyż w myśl zapisów ustawy o dostępie do informacji publicznej (art. 10 ust. 1) informacja, która nie została udostępniona w BIP, udostępniana jest na wniosek zainteresowanego. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Ograniczenie natomiast prawa dostępu do informacji publicznej, zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa [art. 51 Konstytucji Rzeczypospolitej Polskiej].

W tym momencie przytoczone zostanie pojęcie informacji publicznej. Ustawodawca określił, iż jest to każda informacja dotycząca osoby fizycznej, pozwalająca na określenie tożsamości tej osoby, np. imię i nazwisko, data urodzenia, adres zamieszkania, wysokość osiąganych dochodów, stan konta bankowego, informacje o mieniu ruchomym czy nieruchomościach i inne. Definicja niby klarowana, a jednak sprawia problemy. W praktyce powstał problem, czy nr identyfikacyjny *pesel* jest daną osobową. Numer ewidencyjny *pesel* występując samodzielnie, w świetle definicji danych zawartej w ustawie o ochronie danych osobowych, nie jest informacją umożliwiającą identyfikację określonej osoby, mimo że zawiera dane o urodzeniu tej osoby, jej numer porządkowy i liczbę kontrolną. Gdyby jednak numer ten występował wraz z imieniem i nazwiskiem, wówczas, przy spełnieniu również innych wymogów, znalazłyby zastosowanie przepisy ustawy o ochronie danych osobowych. Z tych powodów, odpowiadając na pytanie, czy pozostaje w zgodzie z ustawą wykorzystywanie numeru *pesel* do znakowania przedmiotów (np. rowerów, telewizorów), Generalny Inspektor uznał, że umieszczanie wyłącznie numeru ewidencyjnego na tych przedmiotach nie podlega rygorom

ustawy [Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999–31.12.1999, s. 13].

Warto zaznaczyć, że termin „dane osobowe" kojarzony jest wyłącznie z danymi osobowymi: imię, nazwisko, pesel, NIP, adres zamieszkania. A to zdecydowanie zawęża krąg informacji, które można uznać za dane osobowe. Jeżeli np. powiemy, że chodzi o Jana Nowaka z Warszawy, mieszkającego przy ul. Krochmalnej, to osobom postronnym trudno byłoby ustalić, o jaką konkretnie osobę chodzi. Ale jeśli w jakiejś małej miejscowości, w której wszyscy się znają, mieszka jeden Jan Nowak, to nawet gdy nie podamy adresu, wszyscy będą wiedzieć, o jakiego Nowaka chodzi [Serzyski, Które dane podlegają ochronie?]. Jak wynika z przytoczonego przykładu przy rozstrzyganiu, które informacje mogą stanowić dane osobowe, należy oddzielnie analizować wiele czynników mających wpływ na możliwości zidentyfikowania danej osoby.

Przykładowo Gminy (Rady Gmin) wypełniając obowiązek wynikający zapisów ustawy o utrzymaniu czystości i porządku w gminach, określiły wzory deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi. Osoba składająca deklarację obowiązana była podać m.in. swoje dane osobowe. W niektórych przypadkach określając wzór ww. deklaracji, gminy zobligowały osoby wypełniające deklarację do podawania zbyt szerokiego zakresu danych osobowych, nieadekwatnego do celu ich przetwarzania. W toku przeprowadzonych kontroli przez GIODO stwierdzono, iż oprócz imienia i nazwiska, numeru PESEL, adresu zamieszkania i adresu nieruchomości, której dotyczy deklaracja, pozyskiwano dane osobowe właścicieli nieruchomości w następującym zakresie: nazwisko rodowe, data urodzenia, imię ojca, imię matki, numer księgi wieczystej nieruchomości, numer geodezyjny działki oraz numer PESEL przedsiębiorcy będącego osobą fizyczną [Sprawozdanie z działalności GIODO w roku 2013, s. 27] .

Gminy wskazywały, że pozyskują dane osobowe obejmujące nazwisko rodowe, datę urodzenia, imię ojca, imię matki oraz numer księgi wieczystej nieruchomości na wypadek konieczności wystawienia wobec zobowiązanego tytułu wykonawczego, w przypadku zalegania przez niego z zapłatą zobowiązania z tytułu opłaty za gospodarowanie odpadami komunalnymi. Generalny Inspektor uznał, że pozyskiwanie powyższych danych osobowych oznacza gromadzenie tych danych „na zapas", w celu ich ewentualnego wykorzystania w postępowaniu egzekucyjnym, tj. wystawienia tytułu wykonawczego. Jak wskazał Wojewódzki Sąd Administracyjny w Warszawie w uzasadnieniu wyroku z dnia 1 grudnia 2005 r. (sygn. II SA/Wa 917/2005), gromadzenie danych osobowych na wypadek, gdyby w przyszłości zaszła potrzeba ich wykorzystania nie może być uznane za zgodne z przepisami

o ochronie danych osobowych [Sprawozdanie z działalności GIODO w roku 2013, s. 27].

Analizując informację publiczną ważnym jest zdefiniowanie informacji przetworzonej. Jest to informacja, której udzielenie wymaga zebrania lub zsumowania informacji znajdujących się w dokumentach dostępnych, np. w Urzędzie Gminy. Jest to więc informacja, dla której udzielenia zawsze jest konieczne wykonanie jakiejś dodatkowej pracy intelektualnej na potrzeby konkretnego wniosku [Piskorz-Ryń 2007, s. 74]. Przykładem takiej informacji jest udzielenie informacji przetworzonej na pytanie dotyczące np. *poniesienia rocznych kosztów utrzymania samochodu służbowego w Urzędzie*. Takich informacji Urząd nie jest w stanie udzielić od razu. Jej sporządzenie wymaga sporządzenia zestawień tabelarycznych lub też innych, gdyż wydatki ewidencjonowane są zgodnie z klasyfikacją budżetową, która stanowi jednolity system symboli cyfrowych i nazw stosowanych dla zapewnienia przejrzystości przepływu środków [Domańska 2012, s. 25], odpowiednio dział, rozdział, paragraf. Udostępnienie takiej informacji wymaga ponadto wykazania szczególnie istotnego interesu publicznego, np. w przypadku podejrzenia niegospodarnego wydatkowania środków publicznych bądź też niezgodnie z przeznaczeniem.

Jawność działania Gminy i jej organów a problemy ochrony danych osobowych

W myśl zapisów ustawy o samorządzie gminnym działalność gminy i jej organów jest jawna. Występujące ograniczenia jawności mogą wynikać wyłącznie z innych ustaw. Jawność działania organów gminy przejawia się głownie poprzez prawo dostępu obywateli do uzyskiwania informacji, wstępu na sesje Rady Gminy i posiedzenia jej komisji, a także dostępu do dokumentów wynikających z wykonywania zadań publicznych, w tym protokołów posiedzeń organów gminy i komisji rady gminy. Tak więc obywatel ma prawo do otrzymywania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne [Opaliński 2014, s. 27]. Jednakże zasady dostępu do dokumentów i korzystania z nich określa statut gminy. Dla przykładu w Gminie Ozorków w myśl zapisów Statutu przebieg obrad sesji Rady Gminy i posiedzeń jej komisji mogą być rejestrowane za pomocą urządzeń do utrwalania obrazu i dźwięku. Osoba, która chce przeprowadzić rejestrację obrazu lub dźwięku, przed rozpoczęciem sesji lub komisji Rady Gminy, składa wniosek do przewodniczącego posiedzenia o umożliwienie takiej rejestracji. Prowadzący obrady wyznacza miejsce dokonywania rejestracji obrazu lub dźwięku mając na uwadze prawidłowe

prowadzenie posiedzenia i nie zakłócanie jego przebiegu [Uchwała nr XII/85/03 Rady Gminy w Ozorkowie z 29 października 2003 r.].

Jawność finansów publicznych przejawia się przede wszystkim w zapewnieniu wszystkim obywatelom i organizacjom swobodnego dostępu do informacji o działalności władz publicznych, a co za tym idzie do informacji o gospodarowaniu środkami publicznymi. Nakazuje taką konstrukcję budżetu, szczególnie na etapie planowania, by możliwe było łatwe rozpoznanie źródeł i wielkości dochodów oraz kierunków i wielkości wydatków [Czarny 2006, s. 29]. Zasada jawności to również tworzenie warunków dla społecznej kontroli gospodarki środkami publicznymi. Realizując tę zasadę, samorząd powinien poinformować mieszkańców o założeniach budżetu, kierunkach polityki społecznej i gospodarczej oraz sposobach wykorzystania środków budżetowych. Dlatego też *uchwała budżetowa* oraz *sprawozdanie z jej wykonania* podlegają ogłoszeniu (art. 33 ustawy o finansach publicznych). Zasada jawności (przejrzystości, transparentności) budżetu funkcjonuje jako generalna i ogólna zasada gospodarowania publicznymi zasobami [Świderek 2014, s. 58] i przejawia się m.in. poprzez:

1) jawność debat budżetowych,
2) jawność debat nad sprawozdaniami z wykonania budżetów,
3) podawanie do publicznej wiadomości kwot dotacji udzielanych z budżetów samorządu,
4) jawność debaty nad projektem uchwały w sprawie wieloletniej prognozy finansowej;
5) podawanie do publicznej informacji dotyczących zakresu zadań lub usług wykonywanych lub świadczonych przez jednostkę oraz wysokości środków publicznych przekazanych na ich realizację, oraz zasad odpłatności za świadczone usługi;
6) zapewnianie radnym danej jednostki samorządu terytorialnego dostępu do dowodów księgowych i dokumentów inwentaryzacyjnych, z zachowaniem przepisów o rachunkowości oraz o ochronie danych osobowych;
7) udostępnianie wykazu podmiotów spoza sektora finansów publicznych, którym ze środków publicznych została udzielona dotacja, dofinansowanie realizacji zadania lub pożyczka, lub którym została umorzona należność wobec jednostki sektora finansów publicznych;
8) udostępnianie corocznych sprawozdań dotyczących finansów i działalności jednostek organizacyjnych należących do sektora finansów publicznych;

9) podejmowanie, w głosowaniu jawnym i imiennym, uchwał organu wykonawczego jednostki samorządu terytorialnego dotyczących gospodarowania środkami publicznymi.

Działalność gminy oraz gminnych jednostek jest jawna i podlega ścisłej kontroli. Regionalna Izba Obrachunkowa, jako organ nadzoru dokonuje kontroli pod względem legalności i zgodności z prawem. Najwyższa Izba Kontroli z kolei pod względem gospodarności. Rada Gminy natomiast wykonuje kontrolę pod względem celowości wydatkowania środków publicznych. Radny i każda zainteresowana osoba ma prawo do dostępu do każdej informacji publicznej, czyli informacji o sprawach publicznych dotyczących wykonywania zadań publicznych lub gospodarowania majątkiem gminy. Dostęp do informacji może być jednak ograniczony. Ustawodawca bowiem nałożył pewne ograniczenia w zakresie dostępu do jawności w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie danych osobowych i innych tajemnicach ustawowo chronionych, które zostały omówione w dalszej części artykułu.

Najczęściej spotykanymi przypadkami odmowy udzielenia informacji jest tajemnica służbowa, przedsiębiorcy, pomocy społecznej, postępowania administracyjnego oraz prawo do prywatności.

Prawo do prywatności można zdefiniować jako prawo człowieka do samodzielnego dysponowania informacjami o swoim życiu osobistym i bez ingerencji z zewnątrz podejmował decyzje o tym, czy i w jakim zakresie będzie się dzielił z innymi swoimi myślami, uczuciami i faktami ze swojego życia osobistego [Piskorz-Ryń, s. 81]. Jednakże prawo do prywatności nie chroni osób pełniących funkcje publiczne, aczkolwiek pojęcie to nie zostało zdefiniowane w odniesieniu do samorządu terytorialnego. Ogólnie zakłada się, iż są to osoby składające oświadczenia majątkowe na podstawie ustaw ustrojowych. Z badań wynika, że osobom pełniącym funkcje publiczne przysługuje ograniczona ochrona prawna. Jednakże biorąc pod uwagę ograniczenia ustawowe w dostępie do informacji publicznej, w związku z ochroną sfery prywatnej zarówno radnym jak i pozostałym zainteresowanym nie udostępnia się informacji dotyczących wynagrodzeń i innych informacji zawartych w aktach osobowych pracowników niebędących osobami pełniącymi funkcje publiczne. Mogą być udostępniane jedynie informacje zbiorcze, ale przygotowane w taki sposób, by na ich podstawie nie można było ustalić wielkości zarobków poszczególnych osób, potrąceń dokonywanych z wynagrodzenia, jak i innych informacji przekazywanych przez pracowników, dotyczących życia rodzinnego [Piskorz-Ryń, s. 82].

Następnym wyłączeniem, do którego radny i pozostali zainteresowani nie mają prawa wglądu ani kontroli jest ustawa o pomocy społecznej. W myśl jej zapisów nie należy podawać do wiadomości nazwisk osób korzystających z pomocy społecznej oraz rodzaju i zakresu przyznanego świadczenia (np. zasiłek stały, zasiłek okresowy, zasiłek celowy, pomoc rzeczowa). Tak więc radni podczas czynności kontrolnych nie mają prawa do dostępu do informacji o osobach, które otrzymały lub ubiegały się o pomoc z opieki społecznej, a także o do informacji zebranych podczas przeprowadzania wywiadu środowiskowego, ani dokumentów przedkładanych ośrodkowi pomocy społecznej [Piskorz-Ryń, s. 82]. Mogą jedynie otrzymać informacje o charakterze zbiorczym.

Tajemnica przedsiębiorstwa to nieujawnione do informacji publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne posiadające wartość gospodarczą, co do których przedsiębiorca podjął działania niezbędne w celu zachowania ich poufności [Piskorz-Ryń, s. 79].

Tajemnica przedsiębiorcy stanowi podstawę odmowy dostępu do informacji publicznej, chyba że sam przedsiębiorca zrezygnował z ochrony (zrzekł się przysługującego mu prawa) [Piskorz-Ryń, s. 80].

Tajemnica postępowania administracyjnego z kolei zapewnia ochronę wglądu w akta postępowania administracyjnego. Wyjątkiem mogą być dane zawarte w aktach, ale muszą mieć związek z wykonywaniem zadań publicznych lub pełnieniem funkcji publicznej [Wyrok Sądu Najwyższego z 24.06.2003 r., sygn. akt IIIRN 95/02].

W tym miejscu należy zaznaczyć, iż ograniczenia nie dotyczą osób posiadających poświadczenie bezpieczeństwa. Jest to dokument tworzony na podstawie ustawy o ochronie informacji niejawnych [Dz. U z 2010 r. nr 182, poz. 1228], umożliwiający dostęp danej osobie do informacji niejawnej (objętej klauzulą tajności).

Realizacja polityki bezpieczeństwa i ocena zagrożeń

Zasady jawności oraz zasady dostępu do informacji publicznej realizowane przez Gminę przekładają się na przetwarzanie danych osobowych. Ustawa o ochronie danych osobowych określa prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Zbiorem, jest każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy też podzielony funkcjonalnie [Generalny Inspektor Ochrony Danych Osobowych 2011, ABC rejestracji…, s. 6].

Przykładem może być zbiór akt postępowania administracyjnego zawierający dane stron, ich adresy i inne informacje. Spełnia wskazane kryteria i wobec tego jest zbiorem danych w rozumieniu ustawy. Ważnym więc elementem identyfikacji zasobów informatycznych jest wskazanie nazw zbiorów danych oraz systemów informatycznych używanych do ich przetwarzania [Generalny Inspektor Ochrony Danych Osobowych 2007, ABC bezpieczeństwa…, s. 12]. Na gminie ciążą zatem takie same obowiązki, jak na innych administratorach danych, w szczególności zaś obowiązek właściwego zabezpieczenia danych. Z racji wykonywania przez gminy zadań, w ich jednostkach organizacyjnych prowadzone są różnego rodzaju zbiory, z których wymienić można, np. rejestr nieruchomości, ewidencję gruntów, rejestr decyzji administracyjnych, rejestr pozwoleń i decyzji budowlanych, ewidencję ludności, ewidencję przedpoborowych, ewidencję podatków i windykacji, rejestr danych zawartych w złożonych deklaracjach w sprawie opłaty za gospodarowanie opadami, rejestr decyzji w sprawie zwrotu podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej, rejestr pojazdów i inne, które podlegają rejestracji w prowadzonym przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) ogólnokrajowym rejestrze zbiorów danych osobowych.

Zbiory te prowadzone są na podstawie różnych aktów prawnych i służą realizacji odmiennych celów. Ponieważ inna jest ich specyfika, zbiory te wymagają określonych nazw, różnych procedur dostępu i konieczne jest więc stosowanie w odniesieniu do nich różnych zabezpieczeń. Ponadto, zbiory znajdujące się w posiadaniu gminy są niejednokrotnie wykorzystywane przez niektóre instytucje [Sprawozdanie z działalności GIODO za okres od 01.01.1999–1.12.1999, s. 17] (np. urzędy stanu cywilnego, Policję, Straż Miejską, ośrodki pomocy społecznej, itp.).

W celu ochrony danych osobowych wymagane są odpowiednie środki bezpieczeństwa. Należą do nich m.in. polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. W obecnym czasie wykonywanie zadań publicznych przez gminy odbywa się głównie przy użyciu komputera. Baza informatyczna zatem stanowi zbiór wszelkich informacji związanych z działalnością gminy, a także ważny zasób informacji i danych osobowych. W celu ich ochrony niezbędne jest stosowanie jak najmniej zawodnych metod i technik uwierzytelniania, wykorzystywanych najczęściej w oparciu o:

- posiadaną wiedzę, czyli *CO WIEM?* (np. identyfikator, hasło, pin);

- posiadaną rzecz, czyli autoryzacja *CO MAM?* (np. klucz, token, karta kredytowa, karta mikroprocesorowa);
- posiadaną cechę, czyli sprawdzanie *KIM JESTEM?* (np. odcisk palca, siatkówka oka, charakterystyka głosu) [Pilc, s. 22].

W celu ochrony danych osobowych w samorządach ustanawia się administratora danych osobowych. Jest to podmiot lub osoba, która jest odpowiedzialna i decyduje o celach i środkach przetwarzania danych osobowych oraz systemów informatycznych. Realizuje przyjętą politykę bezpieczeństwa oraz zarządzanie systemem informatycznym. Poprawnie zdefiniowana i wdrożona polityka bezpieczeństwa zawiera m.in.:

- wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych [Dz. U. z 2004r. Nr 100, poz. 1024].

Z kolei wybrane elementy instrukcji zarządzania systemem informatycznym przedstawia tabela 1.

Tabela 1. Elementy instrukcji zarządzania systemem informatycznym

Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
Sposób, miejsce i okres przechowywania: elektronicznych nośników informacji zawierających dane osobowe, kopii zapasowych, sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Źródło: Opracowanie własne na podstawie Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

W kwestii bezpieczeństwa informatycznego w zakresie programów komputerowych w odniesieniu do prowadzenia ksiąg rachunkowych zgodnie z art. 10 ustawy o rachunkowości jednostka powinna posiadać również dokumentację opisującą przyjęte zasady rachunkowości, a w szczególności w przypadku prowadzenia ksiąg rachunkowych przy użyciu komputera – wykaz zbioru danych tworzących księgi rachunkowe na informatycznych nośnikach danych z określeniem ich struktury, wzajemnych powiązań oraz ich funkcji w organizacji ksiąg rachunkowych i w procesach przetwarzania danych oraz opisu systemu informatycznego, zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, programowych zasad ochrony danych, w szczególności zabezpieczenia dostępu danych i systemu ich przetwarzania, określenie wersji oprogramowania i daty rozpoczęci jego eksploatacji. Ponadto określenie systemu służącego ochronie danych i ich zbiorów, w tym dowodów księgowych, ksiąg rachunkowych i innych dokumentów stanowiących podstawę dokonanych w nich zapisów [Dz. U. z 2013 r. poz. 330].

Powyższe wskazuje jak ważne jest wprowadzenie odpowiedniej polityki bezpieczeństwa i zarządzania systemem informatycznym. Jak ważna jest funkcja administratora danych osobowych, który jest odpowiedzialny za przestrzeganie przyjętych postanowień. Polityka bezpieczeństwa połączona z umiejętnym zarządzaniem systemem informatycznym stanowi o prawidłowym zarządzaniu zasobami ludzkimi i informacyjnymi w samorządzie. Wymaga właściwej identyfikacji posiadanych zasobów oraz określenia miejsca i sposobu ich przechowywania. Wybór natomiast odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i rozpowszechnianiem zależny jest od zastosowanych nośników informacji, rodzaju używanych urządzeń, sprzętu komputerowego i oprogramowania [Generalny Inspektor Ochrony Danych Osobowych 2007, ABC bezpieczeństwa…, s. 10] w danej jednostce.

Zakończenie

Z przedstawionych rozważań wynika, że jednostki samorządu terytorialnego w zakresie prowadzonej działalności wykorzystują wiele instrumentów z zakresu tematyki ochrony danych osobowych, a mianowicie gromadzenie, przetwarzanie i ochronę danych osobowych zarówno osób fizycznych jak i podmiotów gospodarczych. Artykuł akcentuje wybrane zagadnienia dotyczące gromadzenia danych osobowych, ich przetwarzania, a w konsekwencji szeroko rozumianej ochrony. Wskazuje jakimi narzędziami dysponują jednostki samorządu terytorialnego w gromadzeniu, przetwarzaniu i ochronie

danych osobowych, na które w czasie informatyzacji położony jest szczególny nacisk, a więc identyfikacja wybranych gromadzonych danych podlegających ochronie, analiza zagrożeń i ocena ryzyka przetwarzania danych oraz wymagane środki bezpieczeństwa w Gminie. Ponadto akcentuje wybrane zagadnienia dotyczące uprawnień organów kontroli – Regionalnej Izby Obrachunkowej i Najwyższej Izby Kontroli oraz Rady Gminy i Komisji w zakresie jawności i przejrzystości finansów publicznych z uwzględnieniem ochrony danych osobowych. Jednocześnie prezentuje przykładowe elementy polityki bezpieczeństwa oraz instrukcji zarządzania bezpieczeństwem systemu informatycznego służącego do transferu danych osobowych oraz kontrolę wymaganych zabezpieczeń. Najważniejsze jest jednak to, aby Gmina zdawała sobie sprawę jak ważna jest edukacja (szkolenia) w zakresie polityki bezpieczeństwa, gdyż niejednokrotnie sami dostarczamy pewnych informacji w wyniku nieświadomego działania. Ważnym jest zapewnienie bezpiecznego dostępu do informacji publicznej, jawności i transparentności finansów publicznych. Powoduje to efektywne wykorzystanie środków publicznych, przy jednoczesnym wprowadzeniu ograniczeń w tym zakresie (tajemnica służbowa, tajemnica prywatności, tajemnica przedsiębiorcy i przedsiębiorstwa). Należy dodać, że zapewnienie bezpieczeństwa wymaga dużych nakładów finansowych, ale należy je przełożyć na ewentualne koszty związane z utratą danych. Zatem gromadzenie, przetwarzanie i ochrona danych osobowych nie może być celem samym w sobie, musi być wkomponowane w całościowy program działalności Gminy.

Bibliografia

Analiza ryzyka cz. 2, http://12all3.elettery.pl/preview.php?c=3732&m=3856&previewtype=html.

Czarny A. (2006), *System finansów publicznych* [w:] Podstawy finansów publicznych, Redaktorzy: K. Brzozowska, Czarny A., Zbaraszewski W., Stowarzyszenie Naukowe Instytut Gospodarki i Rynku, Szczecin.

Domańska M. (2012), *Klasyfikacja budżetowa jako istotny element zarządzania jednostka budżetową na przykładzie Gminy Ozorków,* [w:] M. Wypych (red.) Finansowe aspekty zarządzania organizacjami, T.XIII Zeszyt 18, Łódź.

Domańska M. (2013), *Uwarunkowania efektywnej gospodarki finansowej w jednostce samorządu terytorialnego*, [w:] A. Jackiewicz, Ł. Sułkowski, (red), Dylematy rozwoju przedsiębiorczości w aspekcie regionalnym, T. XIV Zeszyt 8, Łódź.

Generalny Inspektor Ochrony Danych Osobowych (2007), opracowanie Kaczmarek A., *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Wydawnictwo Sejmowe, Warszawa.

Generalny Inspektor Ochrony Danych Osobowych (2009), opracowanie Kaczmarek A., *ABC zagrożeń danych osobowych w systemach teleinformatycznych,* Warszawa.

Generalny Inspektor Ochrony Danych Osobowych (2011), *ABC rejestracji zbiorów danych osobowych,* Wydawnictwo Sejmowe, Warszawa.

Generalny Inspektor Ochrony Danych Osobowych (2011), opracowanie Pilc B., *ABC zasad kontroli przetwarzania danych osobowych,* Warszawa.

Ogólne własności bezpieczeństwa informacji, http://wazniak.mimuw.edu.pl/images/1/19/Bsi_03_wykl.pdf.

Opaliński B. (2014), *Dostęp do informacji publicznej w polskich przepisach prawnych,* [w:] Dostęp do informacji publicznej Praktyczne wskazówki w świetle obowiązujących przepisów i orzecznictwa pod red. P. Szustakiewicza, Wyd. C.H. Beck Warszawa.

Pilc B., *Kontrola przestrzegania przepisów o ochronie danych osobowych - obowiązki i uprawnienia przedszkoli jako administratorów danych osobowych*, http://konferencja.dyrektorszkoly.pl/edutrendy2012/pdf/Prezentacja_Kntrola_Przedszkoli_pilc.pdf.

Piskorz-Ryń A. (2007), *Dostęp radnych do informacji w procesie kontroli,* [w:] Działalność kontrolna rady gminy i komisji ze wzorami pism, regulaminów, programów i protokołów pod red. Z. Majewskiego, Wyd. 2, MUNICIPIUM SA, Warszawa.

Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024).

Serzyski M., *Które dane podlegają ochronie?*, http://e-czytelnia.abrys.pl/?mod=tekst&id=10435.

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013.

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych za okres 01.01.1999–31.12.1999.

Świderek I. (2014), *Budżet jednostki samorządu terytorialnego,* [w:] M. Kaczurak-Kozak, P. Walczak, M. Culepa (red.), Vademecum głównego księgowego jednostki finansów publicznych, Redaktorzy: Wyd. C.H .Beck, Warszawa.

Ustawa z dnia 12 marca 2004r. o pomocy społecznej (Dz. U. z 2004r. Nr 64, poz. 593 z późn. zm.).

Ustawa z dnia 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003r. nr 153, poz. 1503 z późn. zm.).

Ustawa z dnia 27 sierpnia 2009r. o finansach publicznych (Dz. U. z 2013 r. poz. 885 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926 z późn. zm.).

Ustawa z dnia 29 września 1994r. o rachunkowości (Dz. U. z 2013r. poz. 330 z późn. zm.).

Ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz. U. z 2010 r. nr 182, poz. 1228).

Ustawa z dnia 6 września 2001r. o dostępie do informacji publicznej (Dz. U. z 2001 r. nr 112, poz. 1198 z późn. zm.).

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2013r. poz. 594 z późn. zm.).

Wyrok Sądu Najwyższego z 24.06.2003 r., sygn. akt III RN 95/02.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 165-177

Grzegorz Sowa
Społeczna Akademia Nauk

Bezpieczeństwo systemów informatycznych biznesu

Business Information Systems Security

Abstract: As the world becomes more interconnected, organizations are feeling a greater need for network security. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, and make rational decisions about expenditures. Network security must provide five important services: access, confidentiality, authentication, integrity, nonrepudiation. Common internet attacks methods are broken down into categories: eavesdropping, viruses, worms, trojans, pishing, spoofing, Denial of Service. Different defense and detection mechanisms were developed to deal with these attacks: cryptographic systems, firewalls, Intrusion Detection Systems, anti-malware software, Secure Socket Layer. Advance authentication employs the use of following factors: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric).

Key-words: network, cybersecurity, business, media, outsourcing, password, cloud.

Wprowadzenie

W czasach gospodarki opartej na Internecie bezpieczeństwo systemów informatycznych jest coraz ważniejsze a narzędzia jego zapewnienia coraz bardziej złożone. W artykule dokonano przeglądu typowych zagrożeń i najpopularniejszych metod obrony oraz aktualnych tendencji w zarządzaniu ryzykiem w tym zakresie. Zwrócono uwagę na nowe niebezpieczeństwa związane z otwartymi formatami danych i aktywnymi stronami internetowymi.

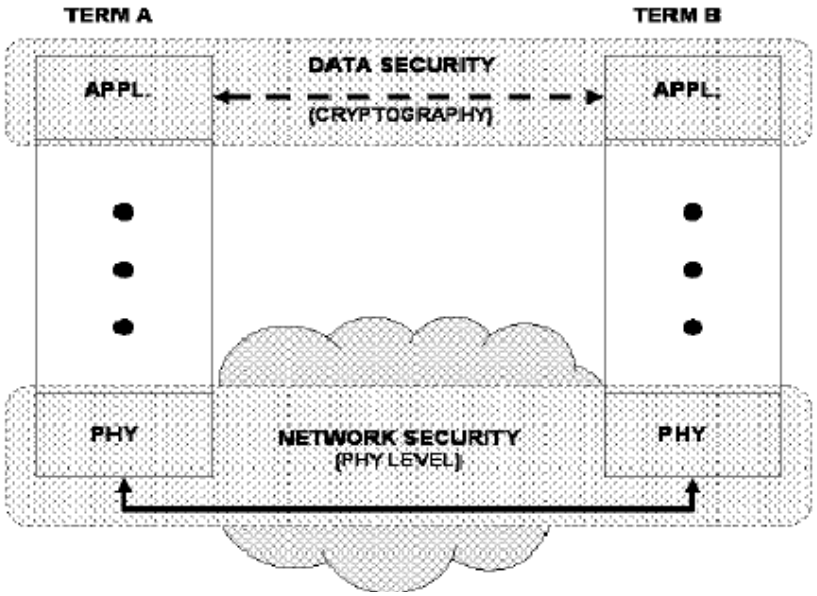
Bezpieczeństwo w sieci – ogólne zasady

Jeszcze dwadzieścia parę lat temu komputery personalne pracowały przeważnie bez połączenia z Internetem. Sieci były już jednak powszechnie używane w przedsiębiorstwach i podstawowe pojęcia bezpieczeństwa sieciowego sformułowano w klasycznej pracy Dowda i McHenry'ego [1998, s. 24–28]:

- Ograniczenie dostępu: do sieci powinny mieć dostęp jedynie upoważnione osoby;
- Poufność: dane w sieci powinny pozostać prywatne, znane tylko swoim właścicielom i osobom wskazanym przez nich;
- Autentykacja: osobowość użytkowników powinna być potwierdzona – są tymi, za których się podają;
- Integralność: dane nie mogą być modyfikowane w czasie transmisji;
- Niezaprzeczalność: użytkownik sieci nie może twierdzić, że z niej nie korzystał – dostęp jest udokumentowany.

Należy odróżnić bezpieczeństwo danych od bezpieczeństwa sieci. Bezpieczeństwo danych może zapewnić np. ich szyfrowanie – nawet podsłuchanie transmisji nie pozwala poznać nam jej treści. Jednakże należy pamiętać o postępie kryptografii – coś co było dobrym zabezpieczeniem kilka – kilkanaście lat temu, dziś może być złamane. Zatem pomocne jest, oprócz zaszyfrowania danych, mieć również bezpieczne sieci, aby danych nie można było łatwo podsłuchać. O ile bezpieczeństwo danych lokujemy na poziomie aplikacji, bezpieczeństwo sieci to poziom fizyczny – drugi koniec popularnego modelu OSI (Open System Interconnection) – rys. 1.

Rys. 1 Bezpieczeństwo sieci w modelu OSI



Źródło: [Priyank… , 2013 s. 2].

Podstawowe rodzaje zagrożeń sieciowych to:

- Przechwytywanie transmisji przez nieupoważnione osoby (podsłuch – 'eavesdropping');
- Wirusy – samoreplikujące się programy o różnych funkcjach, rozchodzące się w sieci;
- Robaki ('worms') – w odróżnieniu od wirusów nie wymagają plików do propagacji (spam w sieci generowany jest często przez robaki);
- Trojany – wirusy ukryte w niewinnie wyglądających plikach, których otwarcie uruchamia je;
- Phishing – wyłudzanie poufnych informacji przy pomocy np. fałszywych stron internetowych;
- Spoofing – podszywanie się pod różne elementy oprogramowania pozwalające np. na nieuprawniony dostęp do danych, modyfikację plików;
- Odmowa usług (Denial of Service DOS) – blokowanie systemu przez żądanie nadmiernych ilości odpowiedzi;
- Scams – podszywanie się pod zaufaną osobę celem np. wyłudzenia pieniędzy;
- Hijacking – włamanie się na stronę celem umieszczenia własnych treści.

Specyficzne zagrożenia powodowane są przez skracanie adresów URL. Ich prawdziwa, fizyczna długość jest często kłopotliwa, więc różne serwisy (np. tinyurl.com) pozwalają przetłumaczyć je na krótsze odpowiedniki; jesteśmy potem przekierowywani na właściwą stronę. Na przykład adres:

http://www.theemployerhandbook.com/2011/07/study-more-employees-allowed-t.html może zostać skrócony do: http://tinyurl.com/q4wax9h. Kłopot polega na tym, że wtedy nie widać od razu, jeżeli jesteśmy kierowani na niepożądane strony internetowe (reklamy, pornografia itp.)

Standardowe narzędzia zabezpieczania to: szyfrowanie danych, firewalle (komputery lub programy blokujące zewnętrzny dostęp do sieci prywatnych), systemy wykrywania włamań (IDS – Intrusion Detection Systems), oprogramowanie skanujące (wykrywanie wirusów), bezpieczne protokoły takie jak SSL (Secure Socket Layer) gwarantujące bezpieczeństwo transmisji pomiędzy przeglądarką a stroną internetową (np. udostępniającą funkcje przelewów bankowych).

Reakcja na próbę włamania może być pasywna lub aktywna. Pasywna polega na kontroli wprowadzanych informacji np. haseł. Aktywna reakcja to na przykład zamykanie systemu po wykryciu próby włamania – np., gdy ktoś kilkakrotnie wprowadzi błędne hasło.

Polityka bezpieczeństwa

Pisząc o polityce bezpieczeństwa, dobrze jest przyjrzeć się poczynaniom doświadczonych w tym zakresie organizacji. Zasady polityki bezpieczeństwa rządu USA sformułowano w dokumencie *Framework for Improving Critical Infrastructure Cybersecurity* [2014] wydanym w styczniu 2014 przez Narodowy Instytut Standardów i Technologii. Na uwagę zasługuje metodyczne podejście do zagadnienia i abstrahowanie od szczegółów technologicznych. Jako podstawowe funkcje systemu bezpieczeństwa określono:

- Identyfikację.
- Ochronę.
- Wykrywanie.
- Odpowiedź.
- Odzyskanie.

Poszczególnym funkcjom przypisano konkretne normy (najczęściej standardy ISO), które powinny być przestrzegane. Głównym wątkiem dokumentu jest zarządzanie ryzykiem: należy zdawać sobie sprawę, że zawsze ono występuje i stosownie do jego prawdopodobieństwa starać się minimalizować straty.

Dostępne są również ogólne zalecenia bezpieczeństwa FBI [*CJIS Security Policy,* 2013], mają one już bardziej od rządowych techniczny charakter. Nie wgłębiając się w biurokratyczne szczegóły można wskazać kilka ciekawych cech polityki bezpieczeństwa FBI.

Opisane są metody reagowania na włamania i naruszenia zasad bezpieczeństwa. Zakładając, że całkowite bezpieczeństwo jest niemożliwe, coś zawsze się będzie działo, organizacja powinna się cały czas uczyć na błędach. Incydenty mają być opisywane i organizować należy szkolenia jak ich w przyszłości uniknąć.

Pracownicy dzieleni są na kategorie: wszyscy zatrudnieni, posiadający fizyczny i logiczny dostęp do informacji oraz informatycy. Wymagany poziom szkoleń i kompetencji odpowiednio rośnie. Wszelkie zdarzenia w systemie (logowanie udane i w szczególności – nieudane) powinny być ewidencjonowane, co umożliwi audyt i ewentualne śledztwo. Każde zdarzenie musi mieć zapisany dokładny czas. Stosowane są rozbudowane mechanizmy ograniczenia dostępu do informacji dla poszczególnych pracowników.

Szczególnie ograniczany i kontrolowany jest dostęp zdalny do zasobów (np. baz danych) oraz dostęp z prywatnych urządzeń pracowników (tak

zwany przypadek BYOD: *bring your own devices*). Ograniczone jest używanie urządzeń bezprzewodowych; podkreśla się ryzyko stosowania telefonów komórkowych; należy przechodzić na technologię VOIP – pakietowej transmisji głosu przez Internet. Stosować należy technologię VPN – wirtualnych sieci prywatnych. Szczególne ryzyko niesie też używanie urządzeń używających do transmisji danych częstotliwości radiowych (standard Bluetooth); stosowane powinny być jedynie w bezpiecznych lokalizacjach.

W dokumencie przypomniano powszechnie znane zasady wyboru haseł (op. cit. s. 52):

1. Co najmniej 8 znaków.
2. Nie może to być słowo ze słownika lub nazwa geograficzna.
3. Nie może być takie same jak identyfikator użytkownika.
4. Nie powinno być ważne dłużej niż 3 miesiące.
5. Nie powinno być identyczne jak 10 ostatnich haseł.
6. Nie należy go wyświetlać w czasie wprowadzania.
7. Nie wolno go transmitować poza bezpiecznymi lokalizacjami.

Rozbudowane są zasady autentykacji. Przy dostępie do bardziej poufnych danych lub jakichkolwiek wątpliwościach stosowana jest zaawansowana autentykacja. Poza loginem i hasłem stosuje się wtedy systemy biometryczne (odcisk palca, tęczówka oka itp), szyfrowanie przy pomocy klucza publicznego, tokeny programowe i sprzętowe. Analizowana jest typowa aktywność użytkownika (np. sposób korzystania z klawiatury), badana jest znajomość unikalnych faktów z biografii.

Ogólną zasadą jest autentykacja, co najmniej dwu elementowa, z zestawu trzech pozycji (po. op. cit s. 53):

1. Coś co powinieneś znać (np. hasło).
2. Coś co powinieneś mieć (np. token).
3. Coś czym jesteś (np. odcisk palca).

W dokumencie drobiazgowo opisano zasady ochrony nośników danych. W szczególności np. złomowanie niepotrzebnych pamięci musi być poprzedzone ich starannym kasowaniem (przynajmniej trzykrotny zapis kasujący lub demagnetyzacja); zalecane jest też fizyczne niszczenie (cięcie).

Dopuszcza się przetwarzane w chmurze, z zastrzeżeniem że dane nie mogą być pod żadnym pozorem skanowane w celach analitycznych – na przykład w celu usprawnienia działania centrum obsługi, nie mówiąc już o reklamie (op. cit. s. 70). Podkreślono znaczenie oddzielenia (również fizycznego – oddzielne serwery) baz danych od usług od interfejsów – np. publicznie dostępnych stron www.

Bezpieczeństwo przetwarzania w chmurze

Dzielenie zasobów komputerowych ma historię znacznie dłuższą niż Internet. W czasach, gdy komputery w miastach liczono na sztuki, przetwarzaniem danych zajmowały się usługowe ośrodki obliczeniowe, wykonujące usługi na rzecz różnych przedsiębiorstw. Późniejszy rozwój sieci rozległych stopniowo doprowadził do ery wszechobejmującej Sieci. Zatem i problemy bezpieczeństwa przetwarzania danych w sieciach były rozpoznawane i rozwiązywane stopniowo.

Obecny poziom sieci transmisji danych pozwala powszechnie przetwarzać je na wynajętych serwerach, których geograficzna lokalizacja jest sprawą drugorzędną – ważna jest odległość (czas transmisji) mierzona „po sieci". Ponadto same aplikacje mogą być dzierżawione albo mieć postać komponentów wynajmowanych do jednorazowego użycia. Tego typu podejście ma liczne zalety (brak konieczności kupowania kosztownych licencji, sprzętu, zatrudniania fachowców) ale rodzi poważne wyzwania w zakresie bezpieczeństwa, poufności danych i oczywiście ich dostępności. Zagadnienia fizycznego bezpieczeństwa danych, konfiguracji aplikacji, doboru i nadzoru nad personelem informatycznym są w rękach dostawcy usług, którego przeważnie na oczy nie oglądamy. Takie obawy są jednym z głównych hamulców rozwoju przetwarzania w chmurze. Jednakże bliższe przyjrzenie się zagadnieniu pozwala rozwiać wiele z tych wątpliwości.

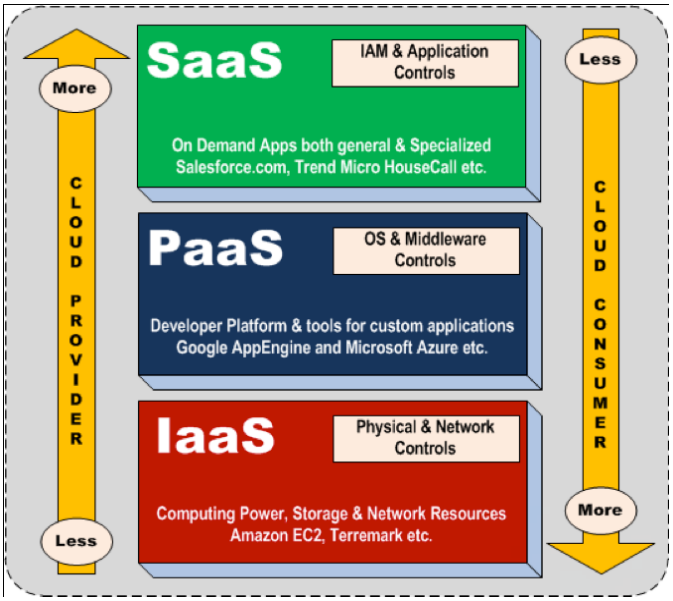
Przetwarzanie w chmurze, jak zdefiniowano w źródłowej publikacji Mell i Grance [2011, s. 2–3], ma postać trzech modeli:

- Usługa wynajmu aplikacji (Software as a Service – SaaS). Aplikacja należy tu do dostawcy usług, klient nie ma nad nią kontroli, korzysta z niej wywołując ją ze swoich komputerów personalnych, przeważnie przy wykorzystaniu przeglądarki internetowej.
- Usługa wynajmu platformy, na której działa aplikacja (Platform as a Service – PaaS). Klient wykorzystuje komputery, sieci, kompilatory, biblioteki procedur itp. należące do dostawcy usług, dla eksploatacji swojej aplikacji.
- Usługa wynajmu infrastruktury aplikacji (Infrastructure as a Service – IaaS). Klient otrzymuje dostęp do komputerów i sieci, na których eksploatuje swoją aplikację, często na swoich systemach operacyjnych.

W zależności od modelu przetwarzania, różny jest poziom odpowiedzialności za bezpieczeństwo. W modelu IaaS dostawca usług jest odpowie-

dzialny tylko za bezpieczeństwo infrastruktury, podczas gdy w modelu SaaS odpowiada również za aplikację – rys. 2.

Rysunek 2 Modele przetwarzania w chmurze



Źródło: *Best practices*… [2013, s. 5].

Kontrola danych i aplikacji może mieć postać kontroli administracyjnej, fizycznej i logicznej. Kontrola administracyjne polega na pisemnym sformułowaniu zasad bezpieczeństwa, procedur, standardów i zaleceń stwarzających ogólne ramy, w których eksploatowany jest system informatyczny zarządzania. Jeżeli odpowiedzialność przekazujemy dostawcy usług, powinniśmy znać jego standardy w tym zakresie. Kontrola fizyczna u dostawców usług polega na ochronie fizycznego dostępu do ich centrów przetwarzania danych. Są to najczęściej duże obiekty i ich ochrona jest na wysokim poziomie.

Najciekawszym rodzajem kontroli jest kontrola logiczna. Używamy tu specjalizowanego oprogramowania dla nadzoru i kontroli dostępu do naszych danych. Elementami kontroli logicznej są hasła, systemy uprawnienia do dostępu, szyfrowanie danych, systemy zabezpieczające przed nieuprawnioną modyfikacją programów i danych, firewalle.

Typowe zabezpieczenia obejmują:

- Dawanie użytkownikom tylko takich uprawnień, jakich naprawdę potrzebują.
- Rozdzielenie zadań między różne osoby. Zasada oczywista w księgowości ale znana też informatykom [zobacz np. Clark, 2013, s. 3]. Informatyczny aspekt tego rozwiązania to zapewnienie że jedna osoba nie będzie miała możliwości logowania się pod różnymi identyfikatorami – nieco trudne do praktycznej realizacji w sieciach rozległych.
- Wymuszanie stosowania mocnych haseł (minimalna długość, znaki niealfabetyczne, okresowa zmiana).
- Wieloetapowa i różnorodna (dodatkowe urządzenia fizyczne (np. tokeny fizyczne lub wirtualne – na telefonach komórkowych), głos, odcisk palca), autentykacja zwłaszcza uprzywilejowanych użytkowników.
- Szyfrowanie krytycznych danych, administrowanie kluczami.
- Programy antywirusowe.
- Kontrola integralności plików (np. wszelkiego rodzaju funkcje skrótu – sumy kontrolne itp.).
- Inspekcje logów (dzienników dostępu do systemu).

Reakcja na ataki może być wieloraka [Ellison 2013]:

- Ograniczenie prawdopodobieństwa i możliwych strat, odzyskiwanie danych.
- Transfer odpowiedzialności (np. ubezpieczenie).
- Ignorowanie mało istotnych zagrożeń.
- Unikanie – aktywne przeciwdziałanie.

Ważna jest regularna i natychmiastowa aktualizacja narzędzi ochrony (np. programów antywirusowych). Czasem jest to pracochłonne i uciążliwe, duże ośrodki serwisowe mogą zapewnić tu wyższy poziom bezpieczeństwa, robią to rutynowo w ramach najbardziej podstawowych zadań.

Warto podkreślić, że u dostawcy usług chmury nawet administratorzy nie powinni mieć możliwości logicznego dostępu do danych użytkownika [zob. Rashmi, 2013 s. 5]. Ponadto wszelkie dostępy są rejestrowane i kontrolowane a użytkownicy mogą też szyfrować swoje dane przed przesłaniem ich na serwery.

Odpowiedzialność za bezpieczeństwo możemy przedstawić w postaci następujących poziomów [*Best practices*…, 2013, s. 11]:

1. Bezpieczeństwo fizyczne (kontrola dostępu, awaryjne zasilanie).

2. Bezpieczeństwo sieci (segmentacja sieci, sieciowe systemy kontroli i wykrywania dostępu).
3. Kontrola bezpieczeństwa serwerów (ochrona przeciwwirusowa, zarządzanie aktualizacjami, kontrola integralności plików, ewidencja dostępów, firewalle).
4. Bezpieczeństwo aplikacji (ochrona przed nieupoważnionym dostępem).
5. Ochrona danych (szyfrowanie, narzędzie bezpiecznej transmisji).

Jeżeli dane gromadzone są w chmurze, musimy liczyć się z tym, że mogą znaleźć się na serwerach podlegających lokalnemu prawodawstwu (np. w USA Patriot Act umożliwia dostęp do wielu danych). Klienci mogą sobie życzyć, aby jednak określić fizyczną lokalizację danych.

Reasumując, przetwarzanie w chmurze stwarza duże szanse, ale nie eliminuje zagrożeń dla bezpieczeństwa. Musimy być ciągle świadomi potencjalnych niebezpieczeństw i rozumieć podział odpowiedzialności pomiędzy nas a dostawcę usług.

Kompleksowe rozwiązanie problemu bezpieczeństwa zapewnia intranet – sieć wewnątrzorganizacyjna zbudowana przy pomocy technologii internetowych, ale odcięta od Internetu. Takie rozwiązanie pozbawia nas jednak możliwości łatwego kontaktu z zewnętrznymi klientami i korzystania z wielu ogólnie dostępnych usług sieciowych.

Media społecznościowe jako źródła zagrożeń bezpieczeństwa

Podstawową cechą mediów społecznościowych jest to, że publikowane treści dostarczane są przez użytkowników. Popularność tych narzędzi stwarza zupełnie nowe możliwości badań marketingowych oraz daje szanse na dotarcie do precyzyjnie znanych grup odbiorców; o wadze tych informacji świadczy wartość firm w rodzaju FaceBooka, Twittera, Google, których głównym zasobem są informacje o potencjalnych klientach.

Innym aspektem jest korzystanie z mediów społecznościowych przez pracowników; pociąga to za sobą wiele zagrożeń dla bezpieczeństwa danych firmy. Mówiąc najkrócej leżą one w obszarach: zagrożenia reputacji firmy, wycieku informacji, utraty wartości intelektualnych, naruszenia praw autorskich, naruszenia prywatności [Shullich 2011, s. 1].

Pierwszym z brzegu przykładem może być lokalizacja wielkich centrów przetwarzania danych; jest ona często poufna (*security by obscurity*), a już publikowanie ich zdjęć w jakichkolwiek otwartych serwisach (zwłaszcza w wa-

runkach, gdy telefony mają często GPS) łamie tę pierwszą barierę dostępu [Shulich, 2011, s. 27].

Ocenia się [*State of the Net 2010*, 2010], że „Więcej niż połowa użytkowników mediów społecznościowych udostępnia w sieci informacje, które stwarzają dla nich ryzyko stania się celem cyberkryminalistów". Jak zatem organizacje mogą oczekiwać od pracowników, że będą chronić dane firmy, skoro nie chronią oni własnych? Dość znaczna część firm (około 30% w USA w roku 2011 – [Meyer, 2011] zakazuje pracownikom korzystania w pracy z mediów społecznościowych, ale egzekwowanie takich zakazów jest trudne, ocenia się że lepiej zmierzyć się inaczej z problemem.

Operatorzy mediów społecznościowych dostarczają również usług przetwarzania w chmurze (np. Google Docs), zatem zakresy szans i zagrożeń zachodzą tu na siebie.

Zasady bezpieczeństwa – studium przypadku

Przyjrzyjmy się praktycznym zasadom zapewnienia bezpieczeństwa w firmie. Łatwo można sobie wyobrazić trzy dość typowe sytuacje [Pruit 2013, s. 3]:

- nasz mail zawierający poufne informacje został przez sekretarkę pomyłkowo przesłany do konkurenta naszego klienta;
- arkusz kalkulacyjny, nad którym długo pracowaliśmy został uszkodzony;
- laptop, z którym idziemy na ważne spotkanie otwiera się z czarnym ekranem.

Powyższe przykładowe scenariusze opisują naruszenie jednego z trzech składników tak zwanej triady bezpieczeństwa informacji:

1. Poufność.
2. Integralność.
3. Dostępność.

Proste zasady bezpieczeństwa informacji polegają na tym, że „informacja powinna być znana jedynie upoważnionym osobom, powinna być autentyczna w sposób możliwy do zweryfikowania, kompletna, dostatecznie dokładna, wiarygodna i dostępna, kiedy jest potrzebna" [Pruit, 2013 s. 3]. Atak powinien być sklasyfikowany: osoba z wnętrza organizacji, klient, dostawca, specjalista, powszechny wirus lub robak internetowy.

Bezpieczeństwo poczty elektronicznej jest naruszone praktycznie na dwa sposoby: nasz e-mail omyłkowo zostaje wysyłany (np. opcja *forward*) tam, gdzie nie powinien lub następuje zagubienie smartfona z adresami i danymi. Telefony komórkowe mają minimalne zabezpieczenia a przechowują i trans-

mitują coraz więcej informacji. Ich zagubienie jest najpowszechniejszym źródłem wycieku danych. Należy również pamiętać o potrzebie robienia kopii bezpieczeństwa przechowywanych w nich danych na innych urządzeniach.

Bezpieczeństwo haseł jest zawsze ważne. Niemal 100% ataków typu APT (*advanced persistent threat*) następuje poprzez skradzione hasła i inne identyfikatory [*MTrends*…,2013 s. 20-26]. Bazy danych wykradzionych haseł mają pojemność mierzoną w terabajtach. Należy zatem przynajmniej stosować znane, rozsądne reguły: długie, złożone hasła, różne hasła w różnych miejscach, okresowa ich zmiana, w razie wątpliwości zaawansowane metody autentykacji.

Szyfrowanie jest powszechne w transmisji danych, możemy nie być tego świadomi. Ale szyfrować należy również wrażliwe dane w bazach danych, zwłaszcza przechowywane w chmurze.

Publicznie dostępne sieci bezprzewodowe (hotele, dworce, restauracje) stwarzają poważne zagrożenia bezpieczeństwa: informacje może być podsłuchana, przechwycone mogą być hasła.

Wpływ niedoskonałości oprogramowania na bezpieczeństwo

Bezpieczeństwo aplikacji staje się coraz bardziej złożone. W czasach globalizacji firmy mieszczą się na różnych kontynentach, pracują w trybie 24/7 przy wykorzystaniu Internetu i urządzeń mobilnych, mają wiele centrów danych i najrozmaitszych systemów, które muszą ze sobą współpracować. Koordynuje się aplikacje utworzone w różnych językach programowania, porozumiewające się przy pomocy różnych sieciowych protokołów. Wydłużenie łańcuchów logistycznych zacieśnia współpracę z partnerami biznesowymi – chcemy automatycznie mieć dostęp do danych o zapasach naszych dostawców i odbiorców.

Strony internetowe były kiedyś statyczne: użytkownik żądał informacji (strony, zdjęcia, filmu) i serwer ją mu dostarczał. Gdy Internet stał się miejscem aktywności biznesowej, klientom należało dostarczyć narzędzie do wprowadzania danych i zadawania zapytań – dialogu ze stroną. W kodzie HTML pojawiły się skrypty pisane w różnych językach programowania (Perl, Visual Basic). Aplikacja taka mogła mieć dostęp do baz danych i dostarczać dynamiczną zawartość. Kolejnym krokiem było pojawienie się appletów – prostych programów, które instalują się na komputerach klientów; większość wykorzystywane jest do wyświetlania reklam. Następnym etapem było poja-

wienie się języka Java Script, którego programy realizowane są bezpośrednio w przeglądarkach. Potem pojawiły się serwlety i technologia Java Server Faces – generowanie odpowiedzi dla klienta po stronie serwera.

W wyniku upowszechnienia się dynamicznych stron internetowych powstają specyficzne zagrożenia. Różnorodne poziomy integracji w kodzie strony HTML wywołań języka Java Script i Java [zob. Goncalves 2013, s. 15–316] zwiększają podatność aplikacji na nieautoryzowany dostęp. Importowanie kodu HTML z najróżniejszymi dodatkami może prowadzić nie tylko do wyświetlenie niewinnej zawartości, ale spowodować poważne zagrożenie dla systemu (XSS: Cross – Site Scripting).

Warto sobie uświadomić nowe zagrożenia. Inżynieria systemów oprogramowania od wielu lat kładzie nacisk na możliwość integracji heterogenicznych systemów informatycznych. Jest to bardzo ułatwione przez stosowanie otwartych formatów danych; wszechobecnym standardem jest tu XML. Jednak, jeżeli dane przechowujemy w postaci plików tekstowych, każdy może je odczytać (oczywiście zabezpieczeniem może być szyfrowanie) i ponadto, w przypadku XML, dodatkowo łatwo zinterpretować. Zatem z punktu widzenia bezpieczeństwa lepiej byłoby przechowywać dane wewnątrz aplikacji [zob. Clark 2014, s. 1], w formatach trudnych do interpretacji. To jest jednak horror dla każdego integratora systemów.

Oprogramowanie powinno być starannie testowane na okoliczność prób ataków. Stosuje się tutaj testy „białej skrzynki" – analizę kodu; to muszą robić programiści oraz „czarnej skrzynki" – robią to użytkownicy systemu.

Nie tylko błędy użytkowników obniżają bezpieczeństwo systemów informatycznych. Aplikacje powinny być tworzone w taki sposób, aby zmniejszyć prawdopodobieństwo udanych ataków.

Podsumowanie

Nie ma całkowicie bezpiecznych samochodów, nigdy systemy komputerowe nie będą całkowicie bezpieczne. Metody zapewniania bezpieczeństwa zmieniają się szybko, pozostają jednak w mocy ogólne zasady. Bezpieczeństwo kosztuje a stosowanie reguł bywa uciążliwe, kto jednak zaniedbuje nawet elementarne zasady bezpieczeństwa, doczeka się kłopotów.

Bibliografia

Best Practices for Security and Compliance with Amazon Web Services, (2013), A Trend Micro White Paper I, April 2013.

Clark D. (2014), *Some thoughts on accountable systems,* 2nd International Workshop on Accountability: Science, Technology and Policy, January 29-30, 2014, MIT Computer Science and Artificial Intelligence Laboratory, Cambridge, MA USA.

Criminal Justice Information Services (CJIS) Security Policy (2013), U. S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, Version 5.2, 8/9/2013.

Dowd P.W., McHenry J.T. (1998), *Network security: it's time to take it seriously*, Computer, vol.31, no.9, Sep 1998.

Ellison R. J. (2013), *Security and Project Management*, (2013), US Department of Homeland Security, August 06, 2013.

Framework for Improving Critical Infrastructure Cybersecurity, (2014), National Institute of Standards and Technology, February 12, 2014.

Goncalves A. (2013), *Beginning Java EE 7,* Apress 2013.

Mell P., Grance T. (2011), *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145.

Meyer E.B. [2011] *Tweet this! More employers now allow social networking at work*, July 13, 2011, http://www.theemployerhandbook.com/2011/07/study-more-employees-allowed-t.html

M Trends. Attack the ecurity gap. 2013 Threat Report.(2013), Mandiant.com.

Priyank S., Kreena M., Shikha S. (2013), *Network Security,* International Journal of Scientific and Research Publications, Volume 3, Issue 8, August 2013.

Pruitt M. (2013), *Security Best Practices for IT Project Managers*, SANS Institute Reading Room, June 18, 2013.

Rashmi, Sahoo G., Mehfuz S., (2013) *Securing Software as a Service Model of Cloud Computing: Issues and Solutions,* International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013

Shullich R. (2011), *Risk Assessment of Social Media,* SANS Institute Reading Room.

State of the Net 2010, (2010), June 2010 Consumer Report Magazine .

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 179-199

Joanna Krygier
Społeczna Akademia Nauk

Pozyskiwanie danych marketingowych w Internecie – możliwości, problemy i zagrożenia

Acquisition of Marketing Data on the Internet - the Opportunities, Problems and Threats

Abstract: With unlimited storage of information resources and its interactive nature, the Internet has become in recent years one of the most important sources of knowledge about the market.

With various kinds of remote tools of marketing communication and virtual points of contact between the company and the client, the network allows for a relatively quick and easy data acquisition marketing, in particular consumers' personal data. On one hand, this creates unprecedented on this scale opportunities to establish and maintain personal contact with customers, on the other, raises a number of risks and technical, organizational and legal side problems for entities operating commercially in the virtual space. This article presents the most commonly used methods of online marketing data collection and emphasises on the problem of security of the data and legal aspects of the acquisition and processing of data.

Key-words: marketing data, Internet, acquisition and processing of data.

Wstęp

Dynamicznie zmieniające się warunki otoczenia, w jakich przyszło funkcjonować współczesnym przedsiębiorstwom, zmuszają je do poszukiwania wciąż nowych sposobów skutecznego konkurowania na globalnym rynku. Wiedza o kliencie stała się jednym z najważniejszych narzędzi marketingowych. Dzięki ciągłej dwustronnej komunikacji z rynkiem przedsiębiorstwa mogą na bieżąco poznawać jego potrzeby i oczekiwania, by jak najpełniej je zaspokajać. Potrzeby te zmieniają się w bardzo dynamiczny sposób, dlatego konieczne jest stosowanie narzędzi umożliwiających stały kontakt i swobodną wymianę informacji z klientem, wśród których najskuteczniejszym okazuje się Internet. Dodatkową trudność sprawia fakt, iż klienci oczekują indywidualnego podejścia i maksymalnego dostosowania poziomu obsługi do swo-

ich oczekiwań. Sprostanie tym wyzwaniom rodzi konieczność nieustannego gromadzenia i przetwarzania ogromnych ilości danych o klientach. Dzięki rozwojowi odpowiednich narzędzi technologii informacyjnych możliwa stała się tzw. masowa indywidualizacja w podejściu do obsługi klienta, prowadząca do pełniejszego zaspokojenia jego potrzeb.

Niniejszy artykuł ukazuje możliwości wynikające z wykorzystywania narzędzi internetowych do pozyskiwania cennych danych marketingowych oraz wskazuje na zasadnicze problemy, jakie wiążą się z zapewnieniem ich bezpieczeństwa oraz legalnym wykorzystywaniem. W szczególności dotyczą one przedsiębiorstw obsługujących rynki konsumenckie, których strategie zakładają prowadzenie działań opartych na marketingu bezpośrednim czy marketingu baz danych[1].

Zmiany w podejściu do założeń marketingowych

Ostatnie lata przyniosły radykalne zmiany ekonomiczne, społeczne i kulturowe w otoczeniu przedsiębiorstw. Globalna konkurencja, wyraźna dominacja mediów cyfrowych oraz dynamika zmian w obszarze potrzeb i oczekiwań rynku narzucają konieczność prowadzenia z otoczeniem rynkowym swoistego dialogu, którego celem jest szybkie reagowanie na wszelkie zachodzące w nim zmiany. Interakcja z rynkiem stała się świadomym i celowym działaniem przedsiębiorstw. Wśród założeń stanowiących podstawę współczesnego marketingu należy wymienić między innymi [Grzesiowski 1997]:

- indywidualne podejście do relacji z klientem,
- podmiotowość klienta,
- personalizację i partnerstwo,
- zwrot w kierunku marketingu bezpośredniego,
- koncentrowanie się na budowaniu długotrwałych więzi z klientem znanym z imienia i nazwiska,
- nową komunikację z klientem: zastąpienie monologu reklamy bezpośrednim dialogiem z klientem.

[1] Marketing oparty na bazie danych (ang.: *database marketing*) – polega na użyciu bazy danych do prowadzenia analiz marketingowych w celu budowy strategii oddziaływania na nabywców [Trojanowski 2010, s. 33].

Powyższe założenia oparte na koncepcji CRM (ang. *Customer Relationship Management*)[2] wymagają niezwykle skrupulatnego odnotowywania każdego istotnego szczegółu dotyczącego klienta, począwszy od jego danych personalnych, poprzez historię kontaktów z firmą i zakupów, wymagania i oczekiwania, aż po zwyczaje, sposoby spędzania wolnego czasu, upodobania czy zainteresowania. Proces ten byłby niezwykle żmudny, a niejednokrotnie niemożliwy do przeprowadzenia bez wsparcia ze strony odpowiednich technologii informacyjnych. Dziś przedsiębiorstwa mają do dyspozycji zaawansowane systemy klasy CRM, posiadające rozbudowaną funkcjonalność, często zintegrowane z większymi kompleksowymi rozwiązaniami. Przykładami dostępnych na rynku systemów tego rodzaju są m.in. SAP CRM oraz Microsoft Dynamic CRM. Te i podobne rozwiązania pozwalają na zorganizowanie, zautomatyzowanie oraz skoordynowanie procesów biznesowych dotyczących sprzedaży, działań marketingowych, w tym obsługi klienta oraz obsługi serwisowej, co zasadniczo ma prowadzić do wzrostu przychodów przedsiębiorstwa, zwiększenia jego udziału w rynku, zwiększenia zysków i skuteczniejszego utrzymywania klienta.

Internet jako źródło wiedzy o klientach

Wykorzystanie technologii informacyjnych w działalności przedsiębiorstw dało początek zupełnie nowym możliwościom kontaktu klienta z firmą. Interaktywny charakter mediów cyfrowych oraz digitalizacja mediów tradycyjnych wpłynęły znacząco na sposób komunikacji z klientem. Przede wszystkim zasługi w tym zakresie należy przypisać komercyjnemu wykorzystaniu sieci Internet, z którą, dzięki urządzeniom mobilnym, dzisiejsi konsumenci mogą mieć niemal nieprzerwaną łączność. Możliwość interaktywnej komunikacji oraz stały dostęp do informacji daje im sposobność do aktywnego uczestnictwa w rynku i swobodnej wymiany opinii. Charakterystyczna staje się tzw. wielokanałowość komunikacji marketingowej, polegająca na realizowaniu kampanii marketingowych z jednoczesnym wykorzystaniem wielu różnych środków przekazu. U jej podstaw leżą zachowania samych konsumentów, którzy przeszukując zasoby informacyjne w celu np. dokonania zakupu, przemieszczają się po bardzo wielu różnych źródłach informacji, do łączności z którymi wykorzystują najczęściej kilka urządzeń dostępowych:

[2] CRM (ang. *Customer Relationship Management*) – koncepcja zarządzania przedsiębiorstwem, oparta na doskonałej znajomości klientów i dostosowaniu działań organizacji i produktów do ich potrzeb [Gwiazda 2014].

komputery stacjonarne, smartfony czy, coraz częściej, tablety. Według danych TNS Polska w styczniu 2014 r. 44% użytkowników telefonów komórkowych posiadało smartfony. [*Marketing mobilny w Polsce 2013 2014*, 2014], a sprzedaż tabletów w 2013 r. sięgnęła 1,8 mln, wykazując gwałtowną tendencję wzrostową [*Marketing mobilny. Raport* 2013, s. 29]. Potencjalnie możliwe jest więc, że klienci zapoznają się np. poprzez smartfon z ofertą nadesłaną pocztą elektroniczną, a zakup zrealizują w sklepie internetowym za pośrednictwem tabletu czy komputera stacjonarnego.

W ostatnich latach Internet stał się więc medium o bodaj największym udziale w gromadzeniu i dostarczaniu informacji o klientach, stwarza bowiem różnorodne możliwości kontaktu pomiędzy firmami a rynkiem oraz generuje okazje do działania, udostępniając jednocześnie narzędzia służące podtrzymywaniu łączności z klientem. W odpowiedzi na powstałą w związku z tym potrzebę zarządzania danymi i informacjami pozostawianymi w Sieci przez klientów jest rozwinięcie omówionych wcześniej systemów klasy CRM do rozwiązania mającego na celu synchronizację wielorakich punktów kontaktu z klientem w środowisku eCommerce. Mowa tu o tzw. eCRM (ang. *Electronic Customer Relationship Management*).

O ile konsumenci przyzwyczajeni są już do tego, że inicjowanie kontaktu z firmą czy marką (niezależnie od tego, która strona go inicjuje) może odbywać się za pomocą wielu różnych środków komunikacji, to Internet stanowi swoisty katalizator tego procesu komunikacji. Większość działań konsumenta przed podjęciem decyzji o zakupie sprowadza się do przejrzenia oferty na stronie internetowej firmy bądź jej profilu na portalu społecznościowym czy zapoznania się z opiniami społeczności internetowych. Finalizacja procesu zakupu odbywa się z udziałem Internetu lub w tradycyjnym w punkcie sprzedaży. W przypadku płatności gotówką w punkcie sprzedaży, do realizacji transakcji najczęściej nie są wymagane żadne dane, jeśli oczywiście klient nie zamawia dodatkowych usług, natomiast realizacja zamówienia złożonego przez Internet najczęściej wymaga od klienta pozostawienia w bazie wielu informacji, w tym danych osobowych. Jest to znakomita okazja dla przedsiębiorstwa, by pozyskać od klienta informacje, które mogą być w przyszłości ponownie wykorzystywane.

Metody pozyskiwania danych marketingowych w Internecie

Internet stwarza ogromne możliwości w zakresie poznawania rynku. Sytuacji, w których użytkownik Internetu pozostawia swoje dane do dyspozycji innym podmiotom, jest wiele. Dokonując zakupu w sklepie internetowym czy korzystając z usług internetowych, zmuszony jest on wypełnić od-

powiedni formularz zawierający dane osobowe takie jak imię, nazwisko czy adres zamawiającego. Znacznie więcej cennych danych zawierają internetowe formularze wypełniane przy okazji składania aplikacji w systemie pośrednictwa pracy. Najprostszą formą pozostawiania swoich danych w internetowej bazie jest dopisanie swojego adresu e-mail do listy dystrybucyjnej w celu otrzymywania newslettera. Lista adresów e-mail jest jednym z najczęściej wykorzystywanych przez przedsiębiorstwa narzędzi marketingu bezpośredniego (ang. *direct marketing*) polegającego na wysyłaniu indywidualnych komunikatów do przedstawicieli grupy docelowej w celu uzyskania ich bezpośredniej reakcji w postaci realizacji zakupu. Forma ta ułatwia klientom dokonywanie zakupów z pominięciem osobistego kontaktu ze sprzedającym. Tradycyjnymi formami direct marketingu są wszelka marketingowa korespondencja prowadzona z klientem, periodyki dla klientów czy sprzedaż katalogowa. Rozwój Internetu, jako środowiska marketingowego stworzył warunki dla rozwoju wielu nowych form marketingu bezpośredniego. Podobnie jak przekazy reklamowe, komunikaty direct marketingu docierają do klienta drogą elektroniczną: poprzez wspomniany e-mailing, produktową stronę internetową czy – finalnie – w pełni funkcjonalny sklep internetowy, gdzie realizuje się ostateczny cel kampanii marketingu bezpośredniego – zakup. Takie rozwiązania są niejednokrotnie skuteczniejsze, szybsze i tańsze od direct marketingu realizowanego w sposób tradycyjny. Dzięki swej prostocie, łatwości dotarcia do klienta oraz niewielkim kosztom e-mail marketing jest dziś jedną z najbardziej popularnych metod pozyskiwania klientów oraz utrzymywania z nimi stałego kontaktu.

Jednym z najczęściej wykorzystywanych sposobów pozyskiwania adresów e-mail w Internecie jest umieszczenie na firmowej stronie internetowej formularza zapisu i rejestracji. Potencjalny klient przeszukujący zasoby strony może być zainteresowany otrzymywaniem treści związanych z ofertą firmy, dlatego może chętnie dopisać swój adres email do listy dystrybucyjnej, wyrażając w ten sposób zgodę na prenumeratę elektronicznego newslettera. Z chwilą, gdy adres email klienta znajdzie się w bazie danych, przedsiębiorstwo może w regularny sposób wysyłać do niego informacje na temat nowości produktowych, promocji czy ofert specjalnych. Może również tą drogą zbudować stałą relację ze swoim klientem, proponując mu różnego rodzaju dodatkowe usługi stanowiące rozszerzenie standardowej oferty czy inne elementy motywujące do regularnych zakupów [zob. Ossowski 2013].

Innym sposobem jest umieszczenie w formularzu wypełnianym przy okazji zakupów elektronicznych pola wyboru (ang. *checkbox*) z formułą wyrażającą akceptację otrzymywania informacji o charakterze marketingowym,

dzięki czemu firma będzie mogła w przyszłości nie tylko utrzymać kontakt z klientem, ale także realizować kolejne kampanie crosssellingowe[3] czy upsellingowe[4].

Bardzo popularne w ostatnim czasie portale społecznościowe są znakomitym źródłem nowych kontaktów. Coraz częściej firmy działające w Sieci wykorzystują listy ich fanów na takim portalu (jeśli oczywiście udało się takich fanów pozyskać) jako potencjalnych klientów. Współpraca z firmą partnerską w zakresie wymiany barterowej przestrzeni reklamowej w e-mail marketingu to jeszcze inny sposób pozyskania danych nowych klientów. Taka forma współpracy pozwala na wykorzystanie już istniejącej bazy adresów e-mail klientów firmy partnerskiej.

Opisując metody gromadzenia adresów e-mail warto też wspomnieć o aplikacjach mobilnych, które stały się bardzo popularnym narzędziem rozwiązującym szereg problemów użytkowników. Częste korzystanie z nich jest okazją do tego, by pozyskiwać dane osobowe klientów tym kanałem. Analogicznie do stron internetowych, aplikacje mobilne mogą zawierać notyfikacje z informacją o możliwości zaprenumerowania newslettera.

Skłonienie internautów do udostępnienia swoich danych wymaga ze strony firm zastosowania różnego rodzaju zachęt. Jest to szczególnie ważne, gdy przedsiębiorstwo chce uzyskać więcej danych niż tylko adres e-mail. Założenie konta w sklepie internetowym z równoczesnym wypełnieniem formularza danych osobowych przyspiesza i upraszcza proces składania kolejnych zamówień. Klient ma wgląd w historię zamówień, może monitorować status realizacji zamówienia, ma możliwość skorzystania z rabatów przy większym wolumenie zakupów, jest nagradzany za zakupy punktami wymienialnymi na produkty. Niektóre firmy (np. Drukuj24.pl) wprowadzają własne pseudowaluty będące odpowiednikiem punktów otrzymywanych przez klientów przy okazji realizowanych zakupów. Posiadając tzw. konto klienta w sklepie elektronicznym kupujący ma także możliwość składania reklamacji i śledzenia statusu realizacji reklamacji oraz zgłoszeń serwisowych. Otrzymywane w zamian za adres e-mail newslettery często zawierają informacje

[3] Crosselling (ang.) – Technika sprzedaży polegająca na oferowaniu klientowi dodatkowych opcji (tzw. dóbr komplementarnych) do zakupionego produktu, uzupełniające go. Istotną cechą tej techniki jest oferowanie ich klientowi po dokonaniu zamówienia [Ebiznesy.pl].

[4] Upselling (ang.) – Technika sprzedaży polegająca na podwyższaniu wartości sprzedawanego produktu poprzez namawianie klienta do kupienia dobra wyższej klasy, a więc droższego w drodze negocjacji, stopniowo oferując mu ulepszone wersje produktu, który chciał pierwotnie kupić [Ebiznesy.pl].

o tzw. kodach promocyjnych upoważniających do zakupów w sklepie internetowym ze specjalną zniżką bądź bez konieczności pokrywania przez klienta kosztów transportu. Takie rozwiązania stosuje np. dom sprzedaży wysyłkowej Bon Prix czy sieć sklepów wysyłkowych techniki i elektroniki Conrad Electronic (zob. rys. 1). Ponadto klient może otrzymywać różnego rodzaju kupony czy okresowo korzystać ze specjalnych promocji tylko dla stałych klientów (zob. rys. 2).

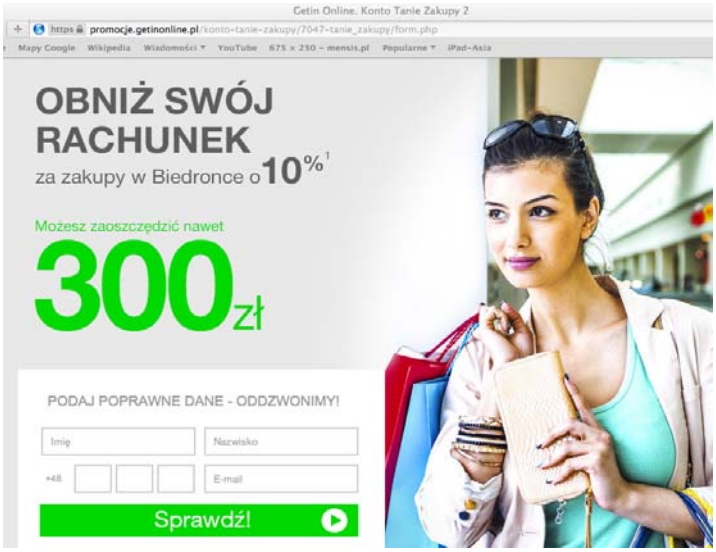
Rysunek 1 Okno z komunikatem zachęcającym do zaprenumerowania newslettera na stronie sieci sklepów Conrad Electronic

Źródło: http://www.conrad.pl.

Przy zakupie produktów cyfrowych, użytkownicy, którzy w zamian za udostępnienie swoich danych otrzymali konto klienta, mają prawo do ponownego pobrania zakupionego oprogramowania czy plików muzycznych. Ciekawym rozwiązaniem są modele sprzedażowe oparte o tzw. chmurę obliczeniową. W chmurze przechowywane są wersje zakupionych produktów o zawartości cyfrowej (e-czasopisma, ebooki, filmy, aplikacje, dokumenty), które klient może ponownie pobrać poprzez konto, przez które wcześniej dokonał ich zakupu. Dodatkowo użytkownik ma dostęp do tych treści

z wielu urządzeń dzięki możliwości synchronizacja danych.[5] Do najbardziej popularnych sklepów internetowych sprzedających produkty cyfrowe na takich zasadach należą m.in. Apple.com, Amazon.com i Google.com.

Rysunek 2 Przykład zachęty skierowanej do odbiorcy komunikatu w celu pozyskania jego danych osobowych



Źródło: Opracowanie własne.

Wśród licznych pomysłów na zachęcenie użytkowników Internetu do udostępnienia swoich danych wymienić należy także rozwiązania takie jak loterie, gry komputerowe, próbki (np. kursów językowych, szkoleń) czy e-vouchery pozwalające na zniżkowe zakupy w sklepach internetowych. Aby z nich skorzystać, należy wypełnić odpowiedni formularz, np. ankietę internetową, za pośrednictwem której firma może także zdobyć informacje na temat zakupionego i użytkowanego przez klienta produktu. Ciekawym rozwiązaniem zaproponowanym przez firmy Euro RSCG Marketing House oraz Digital One jest formuła zapraszania przyjaciela, pozwalająca na zdobycie danych kolejnych osób, które mogą potencjalnie stać się nowymi klientami [Wirtualnemedia.pl].

Poruszając temat pozyskiwania i wykorzystywania danych marketingowych w zamian za różnego rodzaju zachęty, nie sposób nie wspomnieć o programach lojalnościowych, których celem jest nakłonienie klienta do

[5] Więcej na temat chmur obliczeniowych w punkcie 4.4.

ponownych zakupów i podtrzymywanie z nim pozytywnych relacji poprzez obietnicę nagrody. Specjaliści w dziedzinie marketingu określają program lojalnościowy jako ogół działań mających na celu wytworzenie więzi pomiędzy klientem a firmą, opartej na dostarczaniu korzyści zarówno firmie jak i klientowi w postaci zwiększonej sprzedaży, pozyskania wartościowych klientów oraz dostarczenia im satysfakcji [Pawlikowska 2013, s. 212–213]. Programy lojalnościowe rozpowszechniły się także w Internecie, gdzie są doskonałym sposobem na pozyskiwanie danych o klientach, które służą lepszemu zaspokajaniu ich potrzeb. Żeby bowiem stać się uczestnikiem programu, należy wprowadzić do systemu swoje dane. Powszechność mediów cyfrowych oraz coraz częstsze wykorzystywanie urządzeń mobilnych przyczyniły się do stopniowej rezygnacji z tradycyjnych kart lojalnościowych na rzecz aplikacji lojalnościowych na urządzeniach mobilnych. Klient ma dzięki temu możliwość sprawowania większej kontroli nad bieżącym stanem gromadzonych punktów, posiadanymi uprawnieniami. Wszelkie czynności, które musi wykonać przy okazji realizacji kolejnej transakcji, są znacznie uproszczone, a on sam nie musi nosić przy sobie dużej ilości kart plastikowych należących do różnych programów lojalnościowych. Z rozwiązania w postaci internetowych programów lojalnościowych korzysta wiele sklepów internetowych (np. Drukuj24.pl) oraz firm świadczących usługi internetowe, np. banków, w śród których wymienić można mBank, Inteligo czy AlliorSync (obecnie T-mobile Usługi Bankowe).

Kolejnym przykładem wykorzystania Internetu jako źródła informacji o rynku są wyszukiwarki internetowe. Są one bardzo popularnym narzędziem stosowanym przez internautów w celu łatwego i szybkiego znalezienia szukanych stron www bez konieczności zapamiętywania i wpisywania dokładnego ich adresu w oknie przeglądarki internetowej. Wyszukiwarka rejestruje każde wejście na stronę za jej pośrednictwem oraz odnotowuje je w statystykach, co stwarza ogromne możliwości przechwytywania danych o użytkownikach. Z takiej możliwości korzysta najpopularniejsza wyszukiwarka na świecie, Google.com. W zamian za założenie konta w serwisie Google.com użytkownik otrzymuje unikalny adres e-mail i pakiet usług. Rejestracja w systemie wymaga podania danych identyfikujących użytkownika. Następnie każdorazowo po zalogowaniu w systemie Google użytkownik jest przez niego „śledzony": rejestrowane są wpisywane słowa kluczowe, zapytania, klikane linki, oglądane strony, realizowane zakupy, szczegóły dotyczące czasu i częstotliwości poszczególnych zachowań. Informacje te wykorzystywane są następnie, aby serwować danemu użytkownikowi na przeglądanych przez niego stronach internetowych reklamy powiązane z wcześniej odwie-

dzanymi przez niego witrynami. Taka metoda pozyskiwania danych jest dość kontrowersyjna z uwagi na częsty brak świadomości użytkowników kont w serwisie Google na temat działających tam mechanizmów.

Jedną z charakterystycznych cech Internetu, jako sieci komunikacyjnej jest jej mierzalność. W odniesieniu do działań marketingowych realizowanych za pośrednictwem Sieci przedmiotem pomiaru będą wszelkie zachowania internautów postrzeganych, jako klientów bądź potencjalnych klientów. Narzędziem, które doskonale sprawdza się w tej roli, są „cookies" (ang. ciasteczka), czyli niewielkie pliki tekstowe wysyłane przez odwiedzany serwis internetowy i zapisywane na urządzeniu końcowym (komputerze, laptopie, smartfonie), z którego użytkownik korzysta podczas przeglądania stron internetowych [oCiasteczkach.pl]. Informacje te są niezbędne do korzystania z pełnej funkcjonalności witryn internetowych. W sytuacji, gdy wymagana jest autoryzacja, np. podczas logowania do konta pocztowego czy sklepu internetowego, „cookies" pozyskują dane osobowe, które mogą być wykorzystane tylko i wyłącznie w celu identyfikacji i uwierzytelnienia użytkownika. Dzięki zastosowaniu procedur szyfrowania transmisji danych dane te są zabezpieczone przed nieuprawnionym dostępem. Ale wykorzystanie „ciasteczek" ma także swoje uzasadnienie marketingowe. „Cookies" identyfikują dane komputera i przeglądarki internetowej, dzięki czemu umożliwiają m.in. zapamiętywanie preferencji użytkowników i personalizowanie treści stron internetowych oraz reklam, ułatwiają kupującym w sklepach internetowych szybką i sprawną realizację zakupów dzięki zapamiętywaniu („przechowywaniu") w „koszyku" produktów, dzięki procedurze logowania umożliwiają korzystanie z wielu usług oraz dostępu do różnych informacji, kontrolują zawartość witryn (zwłaszcza reklam) pod kątem indywidualnych preferencji i zainteresowań użytkowników i dostarczają szczegółowych statystyk odwiedzalności stron www. Zestawienie omówionych wyżej metod pozyskiwania danych marketingowych w Internecie przedstawiono na rys. 3.

Wspomniane wcześniej portale społecznościowe, uznane nie tylko za znakomity kanał komunikacji z rynkiem, ale również za potencjalne źródło wiedzy o klientach, są coraz chętniej wykorzystywane przez instytucje bankowe w celu weryfikacji klientów pod kątem ich zdolności kredytowej. Nie jest to stricte informacja o charakterze marketingowym, jednak znacząco wpływa ona na kształt proponowanych klientowi produktów. W sposób nieoficjalny banki korzystają np. z portalu FaceBook, by zweryfikować informacje podawane przez klientów we wnioskach kredytowych. Informacje te dotyczą często prywatnego życia użytkowników, m.in. np. liczby członków rodziny na utrzymaniu czy faktu posiadania samochodu. Są one istotne

z punktu widzenia oceny obciążeń budżetu domowego, ale często niedostępne w żadnym oficjalnym rejestrze. Może się zatem zdarzyć, że w oparciu o nie właśnie bank nie udzieli klientowi kredytu lub udzieli go na warunkach innych niżby to miało wynikać z informacji podanych we wniosku kredytowym [Siwek 2010].

Rysunek 3. Sposoby pozyskiwania danych marketingowych w Internecie

Źródło: Opracowanie własne.

Problemy związane z gromadzeniem i przetwarzaniem informacji o klientach w Internecie

Narzędzia do gromadzenia i przetwarzania danych o klientach w Internecie – systemy eCRM. Gromadzenie i przetwarzanie danych rynkowych jest procesem ściśle powiązanym z potrzebą zarządzania relacjami z klientem, z którym firmy chcą nawiązać i utrzymywać długotrwałą więź. W Internecie mamy do czynienia z ogromną ilością danych generowanych przez klientów: wejścia na strony www, przeglądanie katalogów, logowanie w systemach, wysyłanie zapytań, formularzy, e-maili, składanie zamówień itd.. Wszystkie te fakty wymagają natychmiastowej rejestracji oraz odpowiedniej reakcji ze strony firm działających w środowisku eCommerce. Narzędziem, którego celem jest synchronizacja wielu punktów kontaktu z klientem w Internecie, są wspomniane systemy eCRM (Electronic Customer Relationship Management), będące rozszerzeniem zakresu rozwiązań CRM. Wśród obsługiwa-

nych przez eCRM funkcji znajdują się m.in. automatyczne e-mail respondery, personalizowany e-mailing, samoobsługowe bazy wiedzy (prezentacje produktów, listy FAQ), personalizowane stron www, ranking pożądanych produktów, rekomendacje, składanie ofert czy kosztorysowanie online [CRMreview.pl, 2013]. Oparte o bazy danych systemy eCRM stają się niezwykle skutecznym narzędziem w walce o lojalność klienta dzięki wysokiemu poziomowi automatyzacji i synchronizacji wielu procesów. Przede wszystkim eCRM stwarza możliwości szybkiej i wielokanałowej komunikacji z klientem oraz pozwala na lepszą personalizację ofert w czasie rzeczywistym. Odbywa się to w sposób automatyczny w oparciu o zgromadzone dane dotyczące zachowań i preferencji użytkownika, pozyskane dzięki możliwości śledzenia ruchów na stronie, historii zakupów oraz dzięki analizie wielu wskaźników, m.in. ekspozycji stron www, ponownych odwiedzin itp. [Porębska-Miąc 2008].

Prawne aspekty gromadzenia i przetwarzania danych osobowych w Internecie

Skuteczność działań marketingowych jest rezultatem ciągłego pozyskiwania oraz właściwego przetwarzania danych. W marketingu najczęściej mamy do czynienia z danymi statystycznymi dotyczącymi ogółem rynku czy poszczególnych jego segmentów. Inaczej jednak wygląda to w sytuacji stosowania narzędzi marketingu bezpośredniego na rynku konsumenckim. W tym szczególnym przypadku mamy bowiem do czynienia z danymi osobowymi, których gromadzenie i przetwarzanie wiąże się z określonymi obowiązkami oraz konsekwencjami. Prawo dopuszcza wykorzystanie danych osobowych w celach marketingu bezpośredniego. Art. 23 ust. 4 ustawy o ochronie danych osobowych precyzuje, iż marketing bezpośredni własnych produktów lub usług administratora danych jest prawnie usprawiedliwionym celem, dla którego dopuszczalne jest przetwarzanie danych osobowych [Ustawa o ochronie danych osobowych (Dz. U. z 1997 r., nr 133, poz. 883)]. Firmy gromadzące i przetwarzające dane osobowe swoich klientów w związku z prowadzoną przez nie działalnością komercyjną w Internecie (np. sklepy internetowe), zobowiązane są do przestrzegania określonych wymogów, m.in. do ochrony tych danych. Zgodnie z definicją zawartą w art. 6 ww. ustawy, danymi osobowymi określa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Za osobę możliwą do zidentyfikowania uważa się „osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników

określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne". Oznacza to, że danymi osobowymi są informacje, dzięki którym bez nadmiernych kosztów, działań i czasu możemy zidentyfikować daną osobę. W nielicznych przypadkach wystarczy tylko jedna informacja, by można było zidentyfikować konkretną osobę. Dotyczy to np. numeru PESEL czy informacji o kodzie DNA. Najczęściej jednak mamy do czynienia z sytuacjami, w których aby określić tożsamość osoby, należy zestawić ze sobą dwie lub więcej informacji (np. nazwisko, adres miejsca pracy). Każda z nich traktowana oddzielnie nie stanowi danych osobowych. Staje się nimi dopiero w połączeniu z pozostałymi danymi niezbędnymi do identyfikacji osoby [Jakubiec 2012].

W Internecie najczęściej mamy do czynienia z gromadzeniem danych w postaci adresów e-mail. Powstaje więc pytanie, czy taki adres można traktować jako dane osobowe. W myśl cytowanego wyżej zapisu art. 6 ustawy o ochronie danych osobowych adresy e-mail mogą stać się danymi osobowymi w sytuacji, gdy będą zawierały informacje pozwalające na zidentyfikowanie danej osoby bez nadmiernych kosztów i czasu. A zatem adres o abstrakcyjnym brzmieniu nie będzie spełniał kryteriów danych osobowych, ale już e-mail zawierający np. nazwisko jego użytkownika oraz nazwę firmy, którą reprezentuje, może być traktowany, jako dane osobowe. Podobna sytuacja będzie dotyczyła numeru IP komputera, który, zgodnie z opinią GIODO[6], w niektórych sytuacjach może być uznany za dane osobowe, gdyż, jeśli „jest na stałe lub na dłuższy okres czasu przypisany do konkretnego urządzenia, które przypisane jest z kolei konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową" [GIODO, *Czy adres IP*…].

Zatem zgodnie z interpretacjami GIODO, bazy danych zawierające zgromadzone od internautów adresy e-mail podlegają wymogowi rejestracji oraz ochrony danych osobowych [GIODO, *Czy należy zgłosić*…].

Wśród wymogów formalnych postawionych wobec podmiotów przetwarzających dane osobowe należy wymienić złożenie wniosku o wpisanie zbioru do rejestru zbiorów danych osobowych, oznaczenie administratora danych, określenie celu przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych, sposób zbierania oraz udostępniania danych, podanie informacji o odbiorcach lub kategoriach od-

[6] GIODO – Generalny Inspektor Ochrony Danych Osobowych, uprawniony m.in. do kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych a także prowadzenia rejestru zbiorów danych oraz udzielania informacji o zarejestrowanych zbiorach [*Zadania i kompetencje Generalnego Inspektora Ochrony Danych Osbowych*].

biorców, którym dane mogą być przekazywane, opis środków technicznych i organizacyjnych użytych w celu zabezpieczenia danych i dostępu do nich czy też podanie informacji o sposobie wypełnienia warunków technicznych i organizacyjnych [art. 41 ust. 1 ustawy o ochronie danych osobowych].

W przypadku uzyskania dostępu do utworzonego wcześniej przez kogoś innego zbioru (np. w drodze zakupu bazy danych) należy poinformować wszystkie osoby o przetwarzaniu ich danych osobowych oraz zgłosić fakt posiadania tego zbioru do GIODO.

Pozyskiwanie i gromadzenie danych osobowych w Internecie, podobnie jak w innych tego typu sytuacjach, wymaga uzyskania od osoby, której te dane dotyczą, zgody na ich przetwarzanie. Zgoda musi być w pełni świadoma i dobrowolna oraz musi być wyrażona w momencie wprowadzania danych. Ustawodawca nie określił szczegółowych zasad formułowania klauzuli zgody, ale z jej zapisu powinno w sposób niebudzący wątpliwości wynikać, w jakim celu i w jakim zakresie dane będą przetwarzane. Ponadto powinna tam znaleźć się dokładna nazwa (w przypadku osób fizycznych imię i nazwisko) oraz adres administratora tych danych. Osoba, która udostępnia swoje dane osobowe, powinna być poinformowana o tym, że ma prawo do wglądu w ich treść oraz do wprowadzania w nich zmian i ich usuwania.

Uzyskanie zgody stanowi podstawę przetwarzania danych osobowych. W przypadku braku takiej podstawy administratorowi danych grożą konsekwencje wynikające z przepisów karnych [art. 49 ustawy o ochronie danych osobowych].

W przypadku e-mail marketingu występują dwa różne rodzaje zgody, mianowicie opisana wyżej zgoda na przetwarzanie danych osobowych oraz zgoda na świadczenie usług drogą elektroniczną. Dopiero uzyskanie obu tych zgód z osobna pozwala na w pełni legalne wysyłanie informacji handlowej[7] na podany adres mailowy. Przepisy prawne regulujące problem rozsyłania drogą elektroniczną korespondencji o treści marketingowej (a więc e-mail marketingu) przyczyniły się do powstania tzw. *permission email marketingu*, czyli email marketingu realizowanego za zgodą odbiorcy. Pod tym pojęciem kryje się cała gama metod, których celem jest zachęcenie potencjalnego klienta do umieszczenia jego danych osobowych w specjalnym formularzu w celu otwarcia drogi do dalszej komunikacji sprzedażowej [Ossowski 2013]. Wysyłanie e-maili o treściach marketingowych bez uzyskania stosow-

[7] Zgodnie z art. 2 ustawy o świadczeniu usług drogą elektroniczną informacją handlową jest każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy.

nej zgody (tzw. „SPAM") jest czynem zabronionym, karanym grzywną. Spełnienie opisanych wyżej wymogów prawnych ma chronić dane osobowe użytkowników Internetu, jednakże praktyka pokazuje wiele sytuacji ignorowania zapisów prawa w tej kwestii. Najczęściej jest to konsekwencją braku świadomości wynikających z ustawy obowiązków. Tymczasem okazuje się, że zawarcie w wypełnianym przez potencjalnego klienta formularzu odpowiedniej klauzuli zgody na otrzymywanie korespondencji handlowej zapewnia wysoką skuteczność email marketingu (wysoki wskaźnik LTV[8], przy relatywnie niskim CAC[9], zwrot z email marketingu na poziomie ponad 4000%) [Ossowski 2013]. Do złych praktyk, niezgodnych z prawem, należy natomiast umieszczenie zapytania o zgodę już w samej treści wysyłanego komunikatu. Takie rozwiązanie może prowadzić do znacznego obniżenia skuteczności działań zmierzających do pozyskania nowego nabywcy. W wielu przypadkach problemem staje się też poprawne skonstruowanie treści klauzul zgody, ponieważ ustawodawca nie podaje gotowych rozwiązań. Często popełnianym błędem jest umieszczanie treści wszystkich niezbędnych zgód (w tym zgody na przetwarzanie danych, na przekazywanie danych innym podmiotom, na przesyłanie informacji handlowej drogą elektroniczną itp.) w jednej klauzuli (zob. rysunek 2). Takie oświadczenie woli z punktu widzenia administracyjnego jest nieważne i powoduje, że podmiot realizując swoje cele marketingowe w oparciu o posiadane dane, działa niezgodnie z prawem [PrawoMarketingu.pl].

Częstą praktyką jest umieszczanie w korespondencji e-mailingowej tzw. klauzuli marketingowej, dotyczącej przetwarzania danych osobowych przez podmioty trzecie. Uzyskanie takiej zgody pozwala na przekazanie (sprzedaż) bazy danych innym podmiotom, które będą te dane przetwarzały w ich imieniu i na ich rzecz. Zgoda ta jest dobrowolna i nie jest niezbędna do zawarcia transakcji, gdyż jej udzielenie nie może warunkować dostępu do usług. Niestety zdarza się, że niektóre podmioty wymuszają przy okazji zawierania transakcji zgodę na przetwarzanie danych w innych celach (np. marketingowych). Zgodę na otrzymywanie korespondencji handlowej można w każdym momencie odwołać. Wymaga to formy pisemnego powiado-

[8] LTV (ang. *Lifetime value of customer*) – wskaźnik określający "wartość życiową klienta", czyli przewidywaną sumę wydatków danego klienta na produkty bądź usługi oferowane przez firmę, w odniesieniu do kosztów wytworzenia produktu i kosztów związanych z pozyskaniem i obsługą klienta [Ossowski 2013].

[9] CAC (ang. *Cost to acquire a customer*) – koszt pozyskania klienta, zawierający w sobie wszelkie wydatki na marketing i reklamę, które doprowadziły do konwersji (np. koszt reklamy AdWords) [Ossowski 2013].

mienia usługodawcy, np. poprzez wypełnienie odpowiedniego formularza zamieszczonego na jego stronie internetowej.

Rysunek 4 Przykład połączonych klauzul zgody na przesyłanie informacji handlowej oraz na przetwarzanie danych osobowych

Źródło: Supercar.pl.

Podsumowując, ograniczenia i wymogi prawne związane z wykorzystywaniem baz danych użytkowników Internetu, w tym adresów e-mail, w celach sprzedażowych czy marketingowych stanowią częsty problem i nierzadko skłaniają do nadużyć.

Multiplikacja danych w Internecie a ich bezpieczeństwo

Udostępnianie danych osobowych w Sieci jest nierozerwalnie związane z procesem uwierzytelniania i autoryzacji, które w sytuacji komunikacji na odległość są niezbędne. Bezpieczeństwo danych w Internecie wiąże się więc z zapewnieniem bezpieczeństwa komunikacji. Poufność i autentyczność danych uzależniona jest od stopnia możliwości odczytu informacji transmitowanych w Sieci przez osoby niepowołane. Im słabsze zabezpieczenia tym większe prawdopodobieństwo zagrożenia dla autentyczności i integralności przesyłanych danych ze strony osób nieuprawnionych. Rzeczą podstawową jest więc zastosowanie przez system procedur pozwalających na identyfikację i uwierzytelnienie (autentykację) stron biorących udział w procesie komuni-

kacji, czyli weryfikację ich tożsamości. Dopiero po uwierzytelnieniu system może udzielić stronie autoryzacji, czyli przyznać jej odpowiednie uprawnienia (np. związane z dostępem do określonych zasobów). W praktyce oznacza to, że żeby użytkownik konta na danym serwisie internetowym mógł z niego w pełni korzystać, musi się uwiarygodnić podając w formularzu dane logowania. Internet, jako sieć publicznie dostępna, nie daje gwarancji bezpieczeństwa przesyłanych danych. Do komunikacji w Sieci konieczne są więc specjalne protokoły[10] (zasadniczo oparte o techniki kryptografii), dzięki którym bezpieczeństwo oraz integralność przesyłanych danych będzie zachowana [ComputerWorld.pl].

Wynikająca z powyższego konieczność pozostawiania w Internecie danych osobowych w celu zawarcia transakcji czy skorzystania z określonych usług bądź przywilejów, rodzi kolejny problem związany z ich bezpieczeństwem. Ilość odwiedzanych przez internautów miejsc w Sieci, przeglądanych serwisów, sklepów internetowych jest coraz większa, zatem i coraz więcej okazji do mnożenia sytuacji, w których ich dane są udostępniane. Im więcej podmiotów wchodzi w posiadanie tych danych, tym trudniej zabezpieczyć je przed niepowołanym dostępem. Pojawiała się więc potrzeba opracowania rozwiązań, które zwiększyłyby bezpieczeństwo danych poprzez uproszczenie procedur logowania i ograniczenie ilości wypełnianych formularzy.

Istnieją systemy, dzięki którym np. zawarcie transakcji przez Internet nie wymaga wpisywania danych osobowych do bazy e-sklepu. Do rozwiązań takich należą systemy płatności elektronicznych, za pośrednictwem których zarejestrowany i zalogowany klient wydaje jedynie dyspozycję przelewu gotówki na rzecz e-sklepu, w którym dokonał zakupu. Dzięki temu rozwiązaniu dane finansowe czy osobowe klienta (poza adresem e-mail i miejscem dostawy) nie są udostępniane sprzedawcy. Z punktu widzenia firmy prowadzącej działalność handlową w Internecie oznacza to, że nie musi ona prowadzić rejestru danych osobowych kupujących, w związku z tym nie dotyczy jej problemem wynikający z ustawowych obciążeń w zakresie ochrony tych danych. Obowiązek ten przejął na siebie podmiot trzeci. Przykładowym rozwiązaniem tego typu jest system PayPal, który pozwala na dokonywanie płatności elektronicznych w szybki i bezpieczny sposób. Klient korzystający z tego systemu, realizując przelew z tytułu zakupów w e-sklepie, nie musi każdorazowo wpisywać na nieznanych stronach internetowych często trudnych do zapamiętania wielu haseł, kodów, numerów PIN czy numerów kart

[10] Najpopularniejsze bezpieczne protokoły używane w sieci Internet to: SSL, SSH, IP Security.

kredytowych. Jedyną daną, jaką musi wprowadzić w systemie PayPal jest adres e-mail oraz hasło logowania [http://www.paypal.com].

Innym działającym na podobnych zasadach rozwiązaniem jest system opracowany dla jednego z serwisów e-commerce - Ceneo.pl. Serwis ten udostępnia użytkownikom zestaw narzędzi, dzięki którym mogą oni w sposób szybki i łatwy wyszukać interesujące ich produkty czy korzystne oferty. Bardzo ciekawym narzędziem jest system „Kup na Ceneo", dający możliwość realizacji zakupów online bezpośrednio w serwisie Ceneo.pl, bez konieczności wchodzenia na strony www e-sklepu, z którego pochodzi oferta. Kupujący może składać zamówienia w różnych sklepach w ramach jednej transakcji na Ceneo.pl. Nie musi też przechodzić przez procedurę rejestracji. Wypełnia tylko prosty formularz zamówienia, ewentualnie, jeśli jest użytkownikiem serwisu aukcyjnego Allegro.pl, może także zalogować się korzystając z założonego tam konta. Płatności dokonywane są za pomocą systemu szybkich płatności internetowych PayU lub za pobraniem. Proces zakupowy jest dzięki temu znacznie uproszczony i bezpieczniejszy niż w przypadku realizacji wielokrotnych zakupów w różnych sklepach. Dodatkowo wszystkie transakcje realizowane przez Ceneo są objęte tzw. Programem Ochrony Kupujących, który zapewnia konsumentowi rekompensatę finansową z tytułu nie otrzymania zakupionego towaru bądź w przypadku znacznych różnic pomiędzy opisem zawartym w ofercie a otrzymanym produktem. Dla internetowego sprzedawcy oznacza to, że może, oprócz skorzystania z dodatkowych form komunikacji marketingowej, wykorzystać także potencjał handlowy Ceneo.pl, jakim są miliony użytkowników odwiedzających serwis. To Ceneo przejmuje na siebie odpowiedzialność za bezpieczeństwo transakcji, administrując danymi swoich użytkowników, którzy zawierają transakcje z zarejestrowanymi w systemie sklepami internetowymi.

System Ceneo kieruje swoją ofertę do dużych sklepów w Sieci, którym poza zwiększeniem szans sprzedażowych szczególnie zależy na budowaniu pozytywnego wizerunku, natomiast małe podmioty mogą korzystać z rozwiązań dostępnych w systemie Allegro.pl, który oferuje im gotową infrastrukturę, łącznie z możliwością kontaktu z potencjalnymi klientami odwiedzającymi serwis. Tutaj, podobnie jak w Ceneo, obowiązek gromadzenia i przetwarzania danych klientów przejmuje na siebie Allegro.

Realizując e-mailing firma również może zmniejszyć ryzyko związane z utrzymywaniem rejestru danych osobowych klientów. Może zlecić wysłanie komunikatu innej firmie posiadającej bazę danych, pod warunkiem, że firma ta otrzymała stosowną zgodę osób, których dane przetwarza. Często tego typu usługi świadczone są przez wyspecjalizowane podmioty, np. porta-

le internetowe, udostępniające użytkownikom darmowe konta poczty elektronicznej.

Problem bezpieczeństwa danych w chmurze – rozwiązania typu SaaS

W ostatnim czasie bardzo rozpowszechnił się model tzw. chmury obliczeniowej (ang. C*loud Computing*), nazywany potocznie chmurą. Chmura to świadczona na zasadach outsourcingu usługa polegającą na zdalnym udostępnianiu mocy obliczeniowej urządzeń teleinformatycznych. Usługa ta jest dostępna na żądanie w dowolnej chwili oraz jest skalowalna [Jachimowicz 2013]. Szczególnie popularną formą chmury obliczeniowej jest SaaS (ang. *Software as a Service*) czyli oprogramowanie jako usługa. SaaS polega na udostępnianiu użytkownikom gotowej aplikacji bez konieczności ingerowania w jej wnętrze przez użytkownika. W praktyce oznacza to, że firma nie musi ponosić często wysokich kosztów z tytułu zakupu potrzebnego oprogramowania, ponieważ może z niego korzystać na zasadach usługi. Odpowiedni interfejs pozwala na zdalne łączenie się z serwerem usługodawcy (zazwyczaj poprzez sieć Internet) i swobodne korzystanie z wybranych w ramach usługi funkcjonalności systemu. W taki sposób można korzystać z dowolnego oprogramowania, np. z opisywanych wcześniej systemów CRM czy eCRM, za pomocą których gromadzone są i przetwarzane dane o klientach. Przykładem dostępnego przez Internet systemu do zarządzania relacjami z klientami jest CRM Online firmy Firmao, który pozwala zebrać w jednym miejscu dane obecnych i przyszłych klientów, wyznaczać i monitorować zadania związane z ich obsługą, katalogować informacje na temat kontaktów, transakcji czy akcji marketingowych [Firmao.pl]. Kluczowa staje się tutaj kwestia bezpieczeństwa danych, które za pośrednictwem usługi w chmurze są gromadzone i przechowywane fizycznie poza firmą będącą administratorem tych danych, a więc teoretycznie poza jej bezpośrednią kontrolą. Jednakże bezpieczeństwo danych (rozumiane tutaj zarówno, jako zabezpieczenie ich przed utratą jak i niepowołanym dostępem) jest dla firm świadczących usługi w chmurze sprawą priorytetową. Muszą one stosować restrykcyjne procedury i standardy bezpieczeństwa. Potencjalnie jest to rozwiązanie gwarantujące znacznie wyższy poziom zabezpieczenia danych niż w przypadku korzystania przez firmy z ich własnych zasobów.

Podsumowanie

Efektywna komunikacja z klientami i tworzenie z nimi długotrwałych relacji wymagają wykorzystania odpowiednich kanałów komunikacji bezpośredniej, z których najtańszym oraz najbardziej popularnym dziś jest Internet. Narzędzia marketingu bezpośredniego w Internecie, wspomagane również innymi nowoczesnymi środkami przekazu, stwarzają liczne możliwości komunikacji z klientami, dzięki którym przedsiębiorstwo może wejść w posiadanie cennych danych marketingowych, pozwalających na możliwe najlepsze poznanie klientów oraz optymalne przygotowanie oferty i spełniającą indywidualne oczekiwania obsługę. Realizacja tej strategii wymaga zatem działań opartych na pozyskiwaniu i przetwarzaniu danych osobowych klientów (do których także należą adresy poczty elektronicznej), co rodzi konieczność spełnienia określonych wymogów formalno-prawnych oraz techniczno-organizacyjnych, takich jak choćby konieczność zgłaszania rejestrów danych do GIODO, spełnienie wymogu uzyskania zgody na przetwarzanie danych czy wdrożenie narzędzi i procedur pozwalających na optymalne zarządzanie tymi danymi i stanowiących o ich bezpieczeństwie. W Internecie powstają liczne rozwiązania mające na celu zwiększenie bezpieczeństwa danych czy ograniczenie liczby nadużyć, jednak wciąż można spotkać wiele przypadków nieprawidłowości czy zaniedbań w tej materii, wynikających najczęściej z braku dostatecznej wiedzy menedżerów na temat ustawowych obowiązków związanych z przetwarzaniem danych konsumentów.

Bibliografia

ComputerWorld.pl, *Identyfikacja. Uwierzytelnianie* [online], http://www.computerworld.pl/artykuly/299422_1/Identyfikacja.uwierzytelnianie.i.autoryzacja.html, dostęp: 30.05.2014.

CRMreview.pl, *Zyski z dodania "e" do CRM*, 2013 [online], http://www.crmreview.pl/print.php?news=56, dostęp: 30.05.2014.

Ebiznesy.pl, *Cross-selling i up-selling – strategie sprzedaży* [online], http://ebiznesy.pl/e-marketing/cross-selling-i-up-selling-strategie-sprzedazy, dostęp: 30.05.2014.

GIODO, *Czy adres IP komputera należy do danych osobowych?* [online], http://www.giodo.gov.pl/319/id_art/2258/j/pl/, dostęp: 30.05.2014.

GIODO, *Zadania i kompetencje Generalnego Inspektora Ochrony Danych Osbowych* [online], http://www.giodo.gov.pl/138/id_art/1975/j/pl/, dostęp: 3-.05.2014.

Grzesiowski M. (1997), *Marketing konwencjonalny a nowy marketing* [online], http://www.sm.fki.pl/Maciej/ekonomia/Marketing%20klasyczny%20a%20nowy%20marketing.htm, dostęp: 23.05.2014.

Gwiazda E., *Gdy dwóch mówi to samo, to nie jest to samo, albo co to jest CRM?* [online], http://firmao.pl, [online], dostęp: 30.05.2014.

http://www.crm.pl, dostęp: 27.05.2014.

http://www.paypal.com, [online], dostęp: 30.05.2014.

Jachimowicz B. 2013, *Chmura obliczeniowa* [online], http://sicd.pl/teoria/chmura-obliczeniowa/, dostęp: 30.05.2014.

Jakubiec S. (2012), *Dane osobowe w marketingu internetowym* [online], http://websem.pl/dane-osobowe-w-marketingu-internetowym/, dostęp: 30.05.2014.

Marketing mobilny. Raport, 2013 [online], http://interaktywnie.com/biznes/artykuly/raporty-interaktywnie-com/raport-interaktywnie-com-marketing-mobilny-247487, s. 29, dostęp: 27.05.2014.

Marketing mobilny w Polsce 2013 2014 [on line], http://jestem.mobi/2014/02/smartfonizacja-w-polsce-2014-najwazniejsze-liczby-infografika/, (2014), dostęp: 27.05.2014.

oCiasteczkach.pl, *Czym są cookies?* [online], http://www.ociasteczkach.pl, dostęp: 30.05.2014.

Ossowski M. (2013), *Skuteczne pozyskiwanie klientów przez e-mail* [online], http://www.brief.pl/artykul,1227,skuteczne_pozyskiwanie_klientow_przez_email.html dostęp: 30.05.2014.

Pawlikowska D. (2013), *Programy lojalnościowe jako narzędzie wpływu na postawy i zachowania konsumentów*, [w:] A. Wiśniewska (red.), *Kształtowanie lojalności konsumenckiej*, Wyższa Szkoła Promocji, Warszawa.

Porębska-Miąc T. (2008), *Wykorzystanie technologii mobilnych w zarządzaniu relacjami z klientem, w: Systemy Wspomagania Organizacji* [online], http://www.swo.ae.katowice.pl/_pdf/412.pdf, dostęp: 25.05.2014.

PrawoMarketingu.pl, *Zgoda na przetwarzanie danych osobowych i przesyłanie informacji handlowych* [online], http://prawomarketingu.pl/zgoda-na-przetwarzanie-danych-osobowych-i-przesylanie-informacji-handlowych, dostęp: 30.05.2013 r.

Siwek K. (2010), *Banki weryfikują dane o klientach na portalach społecznościowych* [online], http://biznes.interia.pl/finanse-osobiste/news/banki-weryfikuja-dane-o-klientach-na-portalach,1528574,4141?utm_source=paste&utm_medium=paste&utm_campaign=firefox, dostęp: 30.05.2014.

Supercar.pl, [online], dostęp: 30.05.2014.

Trojanowski M., *Marketing bezpośredni. Koncepcja - zarządzanie - instrumenty*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2010.

Ustawa o ochronie danych osobowych, Dz. U. 1997 Nr 133 poz. 883.

Wirtualnemedia.pl, *Narzędzie do pozyskiwania danych osobowych* [online], http://www.wirtualnemedia.pl/artykul/narzedzie-do-pozyskiwania-danych-osobowych, dostęp: 30.05.2014.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 201-217

Anna Wierzbicka
Uniwersytet Łódzki

Ochrona danych osobowych w publicznych zakładach opieki zdrowotnej w Polsce

Personal data protection in Polish public healthcare

Abstract: The purpose of this article is to review the existing regulations concerning personal data protection with respect to the activities of Polish hospitals. A case study of the public health maintenance organization from Lodz region will allow to indicate the rules regarding patient personal data storage and processing. On the one hand, the regulations that are applicable in hospitals and must be obeyed by medical personnel due to the context of its work will be discussed. On the other hand an attempt to present the consequences that may result from not complying with the organizational and legal principles will be made.

Key words: personal data protection, patient rights, public health maintenance organization.

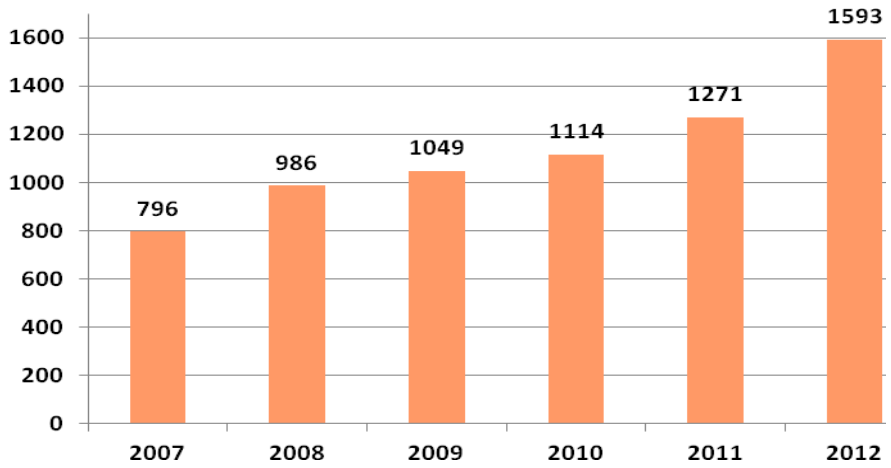
Wprowadzenie

Zgodnie z art. 12 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [Dz. U. 2002 r. nr 101, poz. 926, z późn. zm.] zadania związane m.in. z kontrolą zgodności przetwarzania danych z przepisami o ochronie danych osobowych, a także z wydawaniem decyzji administracyjnych i rozpatrywaniem skarg w sprawach wykonania przepisów o ochronie danych osobowych sprawuje Generalny Inspektor Ochrony Danych Osobowych (GIODO).

W roku 2012 do Departamentu Orzecznictwa, Legislacji i Skarg Biura GIODO wpłynęły 1593 skargi dotyczące naruszenia przepisów o ochronie danych osobowych, tj. o około 50% więcej niż w roku 2007 (rys. 1). W roku 2012 GIODO wydał 762 decyzje administracyjne, czyli o 41% więcej niż rok wcześniej. Sytuacja ta związana jest przede wszystkim ze zwiększeniem liczby skarg, w których skarżący coraz precyzyjniej artykułowali swoje oczekiwania wobec organu ds. ochrony danych osobowych w kwestii podjęcia

działań przewidzianych przez Kodeks postępowania administracyjnego i ustawę o ochronie danych osobowych [Sprawozdanie z działalności Generalnego… 2012].

Rys 1. Zestawienie porównawcze liczby skarg skierowanych do Generalnego Inspektora Ochrony Danych Osobowych w latach 2007–2012 r.



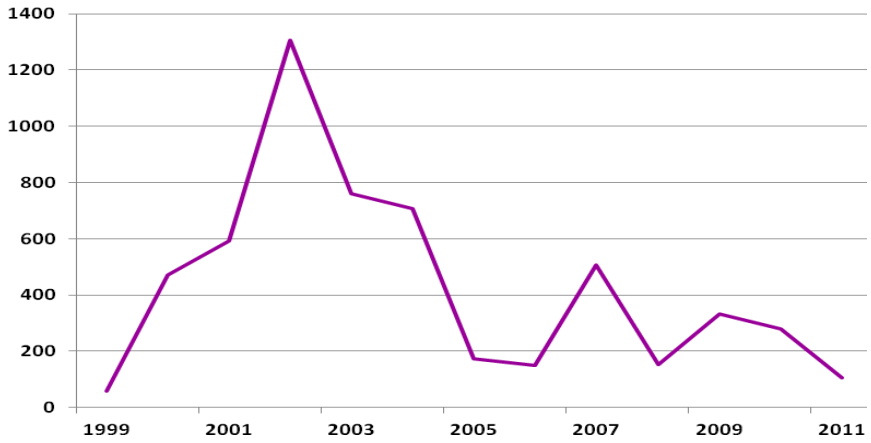
Źródło: Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012.

Jednocześnie, statystki prowadzone przez Policję wskazują, iż liczba przestępstw w zakresie nieprawidłowego administrowania lub nieuprawnionego przetwarzania danych osobowych [Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych] zmalała w roku 2011 w stosunku do roku 2002 o 1200 przypadków, tj. o 92% (rys. 2). Należy także zauważyć, iż w latach 2009–2011 liczba stwierdzonych przez Policję przestępstw zmalała o 68%, podczas gdy liczba skarg skierowanych do GIODO wzrosła w tym samym okresie o 21%.

Brak zbieżności kierunku zmian statystyk policyjnych z danymi podanymi przez GIODO tłumaczyć można zaobserwowanym spadkiem wykrywalności przez Policję przestępstw zdefiniowanych w art. 49-54 ustawy o ochronie danych osobowych. Wskaźnik wykrywalności z blisko 80% w roku 2009 zmalał do 43% w roku 2011 (rys. 3). Wśród wskazanych kategorii nie wyodrębniono sektora służby zdrowia, gdzie ochrona danych osobowych jest niezwykle istotna. Sektor ten z uwagi na specyfikę prowadzonej działalności

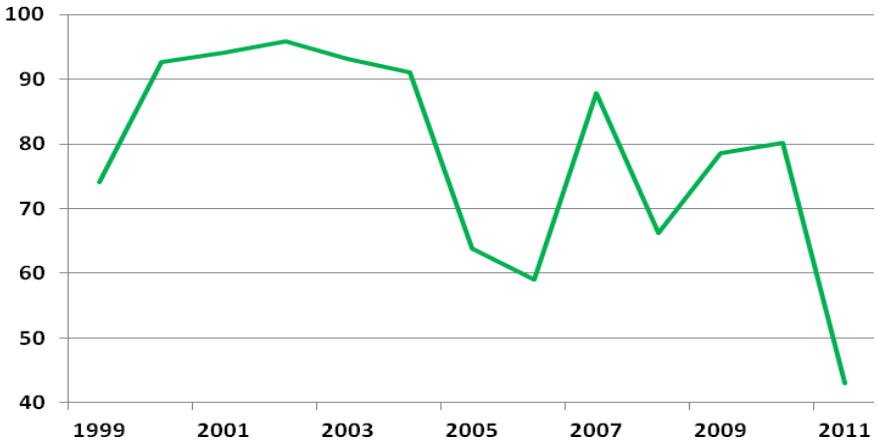
w swoich zasobach przechowuje tzw. dane wrażliwe[1], podlegające specjalnym zasadom przetwarzania i ochrony.

Rys. 2: Liczba przestępstw stwierdzonych w zakresie ochrony danych osobowych przez Policję w latach 1999–2011



Źródło: http://statystyka.policja.pl/

Rys. 3: Wskaźnik wykrycia przez Policję przestępstw w zakresie ochrony danych osobowych w latach 1999–2011 [w %].



Źródło: http://statystyka.policja.pl/

[1] Więcej informacji dotyczących danych wrażliwych znajduje się w 2 rozdziale niniejszego artykułu.

Wobec zarządzania danymi wrażliwymi w systemie ochrony zdrowia znacząca wydaje się ocena regulacji obowiązujących w polskich placówkach szpitalnych. W ramach niniejszej pracy ocenie poddane zostaną zasady dotyczące przechowywania i przetwarzania danych osobowych pacjentów. Analiza przeprowadzona zostanie na przykładzie samodzielnego publicznego zakładu opieki zdrowotnej z regionu łódzkiego.

Pojęcie oraz rodzaje danych osobowych

W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[2]. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań [Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, art. 6].

Za dane osobowe uznaje się m.in.: imię i nazwisko, datę urodzenia, dokładny adres, NIP, PESEL, nr paszportu, DNA, grupę krwi, stan konta, adres mailowy (zawierający dane, które umożliwiają zidentyfikowanie osoby; adresem e-mail nie będącym daną osobową jest np.: żabcia@wp.pl), adres IP komputera danej osoby, zdjęcia rentgenowskie, wyniki badań, fotografie. Za dane osobowe można zatem uznać wszelkie informacje, których wykorzystanie umożliwia zidentyfikowanie osoby fizycznej, mimo iż jej tożsamość nie jest znana.

Zgodnie ze stanowiskiem GIODO ustawa o ochronie danych osobowych ma zastosowanie tylko do przetwarzania danych osobowych osób żyjących, a odmowę udzielania informacji na temat osób zmarłych z powołaniem się na w/w ustawę należy uznać za nieuzasadnioną. W przypadku wykorzystania danych osób zmarłych (np. przesyłania ulotek reklamowych adresowanych do nieżyjącej osoby), osobom bliskim, których dobra osobiste, tj. na przykład kult pamięci o osobie zmarłej, zostały naruszone przysługuje prawo wystąpienia z powództwem cywilnym do sądu powszechnego [http://www.giodo.gov.pl/…].

[2] Osoba fizyczna – prawne określenie człowieka będącego uczestnikiem stosunków cywilnoprawnych. W Polsce zdolność prawna osób fizycznych rozpoczyna się z chwilą narodzin i trwa do momentu śmierci. Zdolność prawną mają zarówno dorośli, jak i dzieci, które np. mają prawo do dziedziczenia.

Wyróżnia się dwa rodzaje danych osobowych[3]:

- dane zwykłe;
- dane wrażliwe (sensytywne).

Zwykłe dane osobowe to m.in. imię i nazwisko, czy numer PESEL. Z kolei dane wrażliwe oznaczają dane szczególne, których przetwarzanie i ochrona podlegają specjalnym regulacjom. Zaliczamy do nich pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym[4].

Ustawodawca wskazuje, iż przetwarzanie danych zwanych sensytywnymi jest możliwe jedynie w określonych sytuacjach, w tym m.in. gdy:

1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie;
2) przepis szczególny innej ustawy zezwala na przetwarzanie takich danych bez zgody osoby, której dane dotyczą, i stwarza pełne gwarancje ich ochrony;
3) przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem;
4) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów;
5) przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą;
6) jest to niezbędne do prowadzenia badań naukowych, pod warunkiem anonimizacji[5] danych.

Za złamanie zakazu przetwarzania danych grozi grzywna, kara ograniczenia wolności albo pozbawienia wolności do 2 lat (w przypadku danych zwykłych) lub do 3 lat (w przypadku danych wrażliwych).

---

[3] Ustawa o ochronie danych osobowych nie wskazuje bezpośrednio rodzajów danych osobowych. Niemniej jednak podział ten jest powszechnie używany, w tym m.in. przez GIODO.

[4] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. nr 101, poz. 926, z późn. zm.) - art. 27.

[5] Ananimizajca to proces zapewniania anonimowości obiektów badania. Anonimizacja obniża jakość danych, może przyczyniać się do sztucznego zwiększania lub zmniejszania zmienności, jednak jest ona wymagana w celu zapewnienia respondentom gwarantowanej przez prawo, także polskie, poufności.

Ochrona danych osobowych na przykładzie szpitala z regionu łódzkiego

Ochrona danych osobowych pacjentów jest jednym z podstawowych obowiązków każdej placówki medycznej. Jest ona tym bardziej szczególna, że informacje o stanie zdrowia człowieka należą do danych wrażliwych.

Ze względu na swoją specyfikę przetwarzanie danych osobowych świadczeniobiorców usług medycznych wymaga szczególnych uregulowań. Na szczeblu międzynarodowym zasady dotyczące ochrony informacji o pacjentach określają m.in.: Konwencja 108 Rady Europy z 28 stycznia 1981 r. dotycząca ochrony osób w związku z automatycznym przetwarzaniem danych osobowych[6] oraz dyrektywy Unii Europejskiej zabraniające przetwarzania danych sensytywnych[7].

W Polsce normy dotyczące danych osobowych pacjentów (poza ogólnymi regulacjami opisanymi w ustawie o ochronie danych osobowych) precyzuje w szczególności rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania oraz ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r. nr 52, poz. 417 z późn. zm.)[8].

---

[6] Głównym zadaniem Konwencji jest wprowadzenie ujednoliconej ochrony danych osobowych w krajach europejskich. Konwencja stanowi, iż dane osobowe dotyczące zdrowia mogą być automatycznie przetwarzane tylko wówczas, gdy przepisy wewnętrzne zapewniają właściwą ochronę; http://www.giodo.gov.pl/plik/id_p/343/j/pl/ 25.02.2014 r.

[7] Dyrektywa 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (art. 8) zabrania państwom członkowskim UE przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego. W ramach przepisów unijnych do przetwarzania danych wrażliwych uprawnieni są pracownicy służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegający obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również zobowiązaną do zachowania tajemnicy; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pl:NOT, 25.02.2014 r.

[8] Zasady związane z przetwarzaniem dokumentacji medycznej zostały ujęte przez ustawodawcę także w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2011 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych, w rozporządzeniu Ministra Obrony Narodowej z dnia 18 grudnia 2009 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez Ministra Obrony Narodowej oraz sposobu jej przetwarzania oraz w rozporządzeniu Ministra Sprawiedliwości z dnia 2 lutego 2011 r. w sprawie rodzajów i zakresu

Przestrzeganie generalnych zasad ochrony danych osobowych leczonych chorych wymagane jest także na mocy regulacji wewnętrznych obowiązujących w poszczególnych SPZOZ[9]. Zasady ochrony dotyczące informacji o świadczeniobiorcach szpitala z regionu łódzkiego, będącego przedmiotem niniejszej analizy, ujęte są w Regulaminie Organizacyjnym, stanowiącym załącznik do Zarządzenia Wewnętrznego Dyrektora placówki. § 20 Regulaminu stanowi, iż do wspólnych zadań komórek organizacyjnych SPZOZ należy przestrzeganie przepisów o ochronie danych osobowych w zakresie gromadzonych informacji. Decyzją Dyrektora szpitala nadzór nad ochroną danych osobowych pacjentów spoczywa w gestii administratora systemu informatycznego oraz administratora bezpieczeństwa informacji. Pierwszy z nich odpowiada m.in. za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych w placówce medycznej, zarządza systemami informatycznymi w sposób zapewniający ochronę danych osobowych pacjentów w nich przetwarzanych, a także kontroluje przepływ informacji pomiędzy systemem informatycznym a siecią publiczną. Do zadań administratora bezpieczeństwa informacji należy z kolei ochrona i zapewnienie bezpieczeństwa danych przetwarzanych tradycyjnie, tj. papierowo, a także w systemach informatycznych oraz podejmowanie stosownych działań w przypadku naruszenia przepisów ustawy o ochronie danych osobowych i zapisów polityki bezpieczeństwa przetwarzania tychże danych w analizowanym szpitalu. W przypadku wykrycia jakichkolwiek zagrożeń, bądź stwierdzenia naruszeń bezpieczeństwa danych osobowych administrator zobowiązany jest niezwłocznie poinformować Dyrektora SPZOZ.

Regulamin Organizacyjny szpitala wskazuje także, iż do zadań personelu medycznego, poza działaniami wykonywanymi w ramach praktyki zawodowej, należy ochrona danych osobowych pacjentów zgodnie z obowiązującymi przepisami prawa. Lekarz udzielający świadczeń zdrowotnych, na mocy umowy o świadczeniu usług lekarskich, zobligowany jest do zachowania w tajemnicy informacji pozyskanych o pacjentach. SPZOZ ze swojej strony zobowiązuje się zapewnić swobodny dostęp do dokumentacji medycznej[10], którą lekarz winien systematycznie i czytelnie prowadzić z poszanowaniem przepisów prawa, wymogów Narodowego Funduszu Zdrowia i standardów

dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania.

[9] SPZOZ – samodzielny publiczny zakład opieki zdrowotnej.

[10] Definicja dokumentacji medycznej podana została w dalszej części tego rozdziału.

wewnątrzszpitalnych, dbając o ochronę danych osobowych zgodnie z instrukcjami bezpieczeństwa obowiązującymi w placówce.

Tajemnica lekarska obowiązuje cały personel medyczny, także ten nieuczestniczący bezpośrednio w kuracji pacjenta. Jednakże, specyfika wielu chorób, a także wszechobecny proces komputeryzacji powoduje, iż wiedzę o procesie hospitalizacji posiada również personel niemedyczny – informatycy, operatorzy sprzętu medycznego, pracownicy działu administracyjnego, itp. W sytuacji, w której dane dotyczące chorego dostępne są szerszemu gremium, mamy do czynienia z tzw. tajemnicą podzieloną[11]. Jako że dane medyczne winny być przetwarzane wyłącznie przez osoby zobowiązane do zachowania tajemnicy, analizowany szpital wprowadził stosowne zapisy również w umowach o pracę zawieranych z personelem niemedycznym. I tak SPZOZ poprzez sam fakt zatrudnienia takiego pracownika sprawuje nad nim bezpośrednią kontrolę w ramach stosunków służbowych.

Stosowne zapisy wprowadzone zostały także do umowy zawartej z zewnętrznym wykonawcą na wykonywanie opisów badań Tomografii Komputerowej (ang. *Computed Tomography* – CT) i przekazywanie ich w drodze transmisji danych. Strony tejże umowy oświadczają, że dokumentacja medyczna w tym wszelkie dane podlegają ochronie zgodnie z zapisami rozporządzeń w sprawie zasad prowadzenia i rodzajów dokumentacji medycznej oraz ustawie o ochronie danych osobowych. Strony oświadczają, że zarówno dokumentacja, jak i dane będą podlegały wszelkim rygorom, co do zasad ich przechowywania i w szczególności rygorów ich udostępniania. Szpital zabezpieczył się także w stosunku do wykonawcy robót budowlanych prowadzonych na terenie placówki. Wymagane jest, aby generalny wykonawca zobowiązał się zachować w tajemnicy w czasie trwania umowy, jak i po jej zakończeniu, wszystkie informacje dotyczące zamawiającego, jakie uzyska w toku realizacji przedmiotu umowy, w tym w szczególności informacje dotyczące danych osobowych pacjentów zamawiającego, jak również danych dotyczących prowadzonych przez zamawiającego procedur diagnostycznych.

Wymogiem ochrony danych osobowych oprócz personelu objęta jest także prowadzona w szpitalu dokumentacja medyczna rozumiana, jako dane i informacje medyczne odnoszące się do stanu zdrowia pacjenta lub udzielonych mu w zakładzie leczniczym świadczeń zdrowotnych.

Szpital z regionu łódzkiego, tak jak każdy SPZOZ, zobligowany jest do prowadzenia dokumentacji medycznej pacjentów, zapewnienia ochrony danych

[11] http://www.infodent24.pl/lexdentpost/lekarz-dentysta-w-roli-spowiednika,5970_0.html 25.02.2014.

zawartych w dokumentacji i udostępniania jej zgodnie z ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta [zgodnie z art. 18 ustawy z dnia 30 sierpnia 1991 r.]. Dokumentacja może zostać udostępniona jedynie [zgodnie z art. 26 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku…]:

1) pacjentowi lub jego przedstawicielowi ustawowemu bądź osobie upoważnionej przez pacjenta;
2) po śmierci pacjenta prawo do wglądu w dokumentację medyczną ma osoba upoważniona przez pacjenta za życia;
3) podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych;
4) organom władzy publicznej, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom krajowym zakresie wojewódzkim, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności kontroli i nadzoru;
5) ministrowi właściwemu do spraw zdrowia, sądom dyscyplinarnym, prokuraturom, lekarzom sądowym i rzecznikom odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem;
6) uprawnionym na mocy odrębnych ustaw organom i instytucjom, jeżeli badanie zostało przeprowadzone na ich wniosek;
7) organom rentowym oraz zespołom do spraw orzekania o stopniu niepełnosprawności, w związku z prowadzonym przez nie postępowaniem;
8) podmiotom prowadzącym rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów;
9) zakładom ubezpieczeń za zgodą pacjenta;
10) lekarzowi, pielęgniarce lub położnej, w związku z prowadzeniem procedury oceniającej podmiot udzielający świadczeń zdrowotnych na podstawie przepisów o akredytacji w ochronie zdrowia, w zakresie niezbędnym do jej przeprowadzenia;
11) szkole wyższej lub jednostce badawczo-rozwojowej do wykorzystania dla celów naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy.

Regulamin Organizacyjny (par. 95) analizowanej placówki leczniczej, zgodnie z wytycznymi ustawodawcy stanowi, iż dokumentacja medyczna jest udostępniana odpłatnie (poprzez sporządzenie jej wyciągów, odpisów lub kopii) lub też nieodpłatnie (do wglądu w szpitalu lub poprzez wydanie oryginału za pokwitowaniem odbioru z zastrzeżeniem zwrotu po wykorzystaniu, jeżeli uprawniony organ lub podmiot żąda udostępnienia oryginałów tej dokumentacji). Wysokość opłat za udostępnianie dokumentacji medycznej

określona jest w cenniku wprowadzonym zarządzeniem Dyrektora szpitala. Czas przechowywania dokumentacji został określony na okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkami określonymi w art. 29 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Po upływie wskazanych w ustawie okresów podmiot udzielający świadczeń zdrowotnych niszczy dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła.

Weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych dokonuje GIODO. W przypadku wykrytych niezgodności GIODO mocą wydanych decyzji może zobowiązać kontrolowaną placówkę do usunięcia uchybień.

Autorce nie udało się ustalić, czy w szpitalu będącym przedmiotem analizy stwierdzono jakiekolwiek niezgodności związane z przetwarzaniem danych osobowych pacjentów w odniesieniu do regulacji określonych zarówno przez ustawodawcę, jak i tych ujętych w Regulaminie Organizacyjnym szpitala. Niemniej jednak, dla przykładu warto przywołać decyzję GIODO nr DIS/DEC-174/12/14274 z dnia 6 marca 2012 r. Kontroli GIODO poddany został inny szpital niżeli ten z regionu łódzkiego[12]. W ramach działań prowadzonych przez Generalnego Inspektora od pracowników tegoż szpitala odebrano ustne wyjaśnienia. Ponadto skontrolowano systemy informatyczne oraz dokonano oględzin pomieszczeń, w których odbywa się przetwarzanie danych osobowych[13]. Na podstawie zebranych materiałów ustalono, iż szpital, jako administrator danych, naruszył przepisy o ochronie danych osobowych. Uchybienia polegały m.in. na:

- niezastosowaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, z uwagi na fakt, iż przechowywanie dokumentacji medycznej zawierającej dane osobowe pacjentów na otwartych półkach w pomieszczeniu, w którym są przyjmowani pacjenci szpitala, stwarza niebezpieczeństwo udostępnienia tych danych osobom nieupoważnionym, zabrania przez osobę nieuprawnioną, przetwarzania z naruszeniem ustawy oraz zmiany, utraty, uszkodzenia lub zniszczenia;

[12] Dane placówki, której dotyczy decyzja GIODO nie mogą być ujawnione.

[13] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., nr 100 poz. 1024).

- niezabezpieczeniu dokumentacji medycznej pacjentów z uwagi na fakt, iż w pomieszczeniu, w którym ją przechowywano nie zainstalowano czujek przeciwpożarowych (art. 36 ust. 1 ustawy).

W uzasadnieniu do postanowienia z dnia 15 lutego 2000 r., sygn. T. 28/99, Trybunał Konstytucyjny stwierdził, iż „zarówno materiały dokumentujące historię choroby pacjenta, jak również druki zaświadczeń lekarskich należą do danych chronionych tajemnicą służbową. Zakład pracy obowiązany jest zabezpieczyć właściwy tryb postępowania związany z obiegiem, gromadzeniem i przechowywaniem tych dokumentów, aby uniemożliwić osobom nieupoważnionym zapoznawanie się z treścią informacji zawartych w tych dokumentach". Wobec powyższego szpital poddany kontroli GIODO został zobowiązany do usunięcia stwierdzonych uchybień w procesie przetwarzania danych osobowych.

Etyczno-prawny wymiar tajemnicy lekarskiej

W parze z wymogami formalnymi dotyczącymi ochrony danych osobowych pacjentów idą zasady etyki lekarskiej, której podstawy formułuje starożytna przysięga Hipokratesa. Jej zapis, w odniesieniu do zagadnienia ochrony danych osobowych pacjentów, stanowi: „To, co w czasie leczenia lub poza moją praktyką w obcowaniu z ludźmi usłyszę i zobaczę, i co nie wolno powtarzać, przemilczę i będę strzec jak tajemnicy" [www.polscy-lekarze.net/].

Do dnia dzisiejszego dochowanie tajemnicy postrzegane jest, jako jedna z cnót, szczególnie poważanych w zawodzie medyka, będącego zawodem publicznego zaufania. W Polsce zakres tajemnicy lekarskiej określa art. 40 ust. 1 ustawy o zawodach lekarza i lekarza dentysty oraz art. 23 Kodeksu Etyki Lekarskiej. Zapisy obu dokumentów wskazują, iż tajemnicą objęte są wiadomości o pacjencie i jego otoczeniu uzyskane przez lekarza w związku z wykonywanymi czynnościami zawodowymi. Śmierć chorego nie zwalnia od obowiązku dochowania tajemnicy lekarskiej.

Powołany zapis ustawy o zawodach lekarza i lekarza dentysty wskazuje jednoznacznie, iż zachowanie tajemnicy lekarskiej stanowi obowiązek, a nie prawo osoby wykonującej zawód lekarza. Tajemnica nie jest wyrazem uprzywilejowania grupy zawodowej, lecz obowiązkiem związanym z wykonywaniem zawodu. Trybunał Konstytucyjny w wyroku z 22 listopada 2004 r. (sygn. akt SK 64/2003) zauważył, iż tajemnica zawodowa nie jest ustano-

wiona w interesie osoby wykonującej dany zawód, lecz w interesie osoby korzystającej z jej usług[14].

Ujawnienie przez lekarza danych objętych tajemnicą zawodową stanowi przestępstwo z art. 266 kodeksu karnego[15]. Z kolei za nieprzestrzeganie zasad Kodeksu Etyki Lekarskiej grozi postępowanie z zakresu odpowiedzialności zawodowej.

Podkreślenia wymaga fakt, iż lekarzowi występującemu w charakterze świadka w toku postępowania sądowego przysługuje prawo do zasłonięcia się tajemnicą zawodową. Zgodnie z art. 180 §2 k.p.k. osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej mogą być przesłuchiwane, co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. Ujawnienie tajemnicy lekarskiej może mieć miejsce w szczególnych przypadkach, określonych przez ustawodawcę[16]. Zastosowanie ma tutaj także art. 261 §2 k.p.c, który stanowi, iż świadek może odmówić odpowiedzi na zadane mu pytanie, jeżeli zeznanie mogłoby narazić jego lub jego bliskich na odpowiedzialność karną, hańbę lub dotkliwą i bezpośrednią szkodę majątkową albo, jeżeli zeznanie miałoby być połączone z pogwałceniem istotnej tajemnicy zawodowej.

W świetle powyższych przepisów, w ocenie Sądu Okręgowego w Lublinie, do ujawnienia tajemnicy lekarskiej doszło na sali sądowej podczas składania przez pozwaną wyjaśnień informacyjnych. Sprawa dotyczyła sporu pomiędzy dentystką (pozwana), a pacjentem (powód), któremu wykonana została skomplikowana usługa protetyczna, a z której to pacjent nie był zadowolony. W toku postępowania sądowego dentystka winna była skorzystać z prawa do odmowy odpowiedzi na pytanie (zgodnie z przywołanym powyżej art. 261 § 2 k.p.c.), tym bardziej, że przekazanie informacji o stanie jamy ustnej pacjenta nie mogło stanowić elementu obrony, jako że nie miało związku ze sprawą.

---

[14] Opinia prawna w przedmiocie tajemnicy lekarskiej w toku kontroli Urzędu Kontroli Skarbowej (Zespół Radców Prawnych Naczelnej Izby Lekarskiej, opinia nr NRL/ZRP/MK/961-1/69/2013 z dnia 10.01.2013 r.)

[15] Art. 266 §2 Kodeksu Karnego: Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację stanowiącą tajemnicę służbową lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

[16] Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2008 r., nr 136 poz. 857), art. 40, pkt. 2.

Zdaniem Sądu dentystka łamiąc tajemnicę lekarską, naruszyła dobro osobiste w postaci prywatności. Sąd uznał, że naruszenie było umyślne z uwagi na konieczność posiadania przez pozwaną wiedzy o istnieniu tajemnicy lekarskiej z racji wykonywanego zawodu. Sąd przyznał powodowi zadośćuczynienie w wysokości 1.000 zł [Krzymowski, Glosa do wyroku…].

Podsumowanie

W dobie rozwoju technologicznego kluczowym zagadnieniem staje się przetwarzanie i przechowywanie danych osobowych przy wykorzystaniu programów i urządzeń elektronicznych podłączonych do ogólnoświatowej sieci komputerowej. W ramach krajowego Programu Informatyzacji Ochrony Zdrowia opracowywana jest Elektroniczna Dokumentacja Medyczna[17]. Cyfryzacja ochrony zdrowia ma na celu zapewnienie szybkiego dostępu do informacji o stanie zdrowia leczonych chorych, a także zabezpieczenie danych przed ich zaginięciem. Wiąże się z tym duża oszczędność, zarówno czasu jak i kosztów związanych z przechowywaniem i powielaniem danych w formie papierowej.

Niezależenie od coraz to bardziej innowacyjnych metod, a także sprzętu pozwalającego na szybkie i sprawne zarządzanie danymi osobowymi, nie wolno zapomnieć, iż jednym z podstawowych uprawnień jednostki w państwie demokratycznym jest prawo do sprawowania kontroli nad gromadzonymi na jej temat informacjami[18]. Gwarantem tychże praw jest władza ustawodawcza, której domeną jest stanowienie powszechnie obowiązujących norm i przepisów.

Integralną częścią szeroko rozumianych praw człowieka są prawa pacjenta. Zgodnie z Deklaracją Praw Pacjenta[19] świadczeniobiorca usług medycznych ma prawo do intymności i poszanowania godności m.in. poprzez ochronę wszelkich informacji umożliwiających jego identyfikację. Ponadto

[17] Elektroniczna Dokumentacja Medyczna (EDM) – system informatyczny przechowujący całość lub wybrane elementy dokumentacji medycznej indywidualnej i zbiorczej. Pierwotnie przyjęty termin uruchomienia EDM to 1 sierpnia 2014 r., przesunięty na 1 stycznia 2017 r. – wówczas dokumentacja medyczna wszystkich rodzajów oraz w całym zakresie będzie musiała być prowadzona wyłącznie w formie elektronicznej, https://p1.csioz.gov.pl/38; http://www2.mz.gov.pl/wwwmz/index?mr=m17&ms=796&ml=pl&mi=796&mx=0&mt=&my=796&ma=032667 25.03.2014

[18] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.

[19] Karta Praw Pacjenta w oparciu o Deklarację Praw Pacjenta Światowej Organizacji Zdrowia (WHO).

pacjent może zażądać skorygowania, uzupełnienia, usunięcia, wyjaśnienia i/lub uaktualnienia dotyczących go osobistych i medycznych danych, które są niedokładne, niekompletne, dwuznaczne lub nieaktualne albo nieodpowiednie dla potrzeb rozpoznania, leczenia lub opieki. Unormowania dotyczące ochrony danych osobowych pacjentów muszą być respektowane przez wszystkie podmioty systemu ochrony zdrowia.

Analizowany szpital z regionu łódzkiego funkcjonuje w oparciu o określone przez ustawodawcę zasady, które zostały wdrożone w placówce na mocy stosownych regulaminów oraz zapisów w formalnych dokumentach. Zauważyć należy, iż władze szpitala mają wiedzę w zakresie wymogów niezbędnych dla sprawnego działania systemu ochrony danych osobowych, umieją dokonać poprawnej interpretacji przepisów prawa w tym zakresie, a także mają świadomość odpowiedzialności za poprawne zabezpieczanie danych sensytywnych, o czym świadczą m.in. stosowne zapisy w umowach z pracownikami oraz wykonawcami szpitala. Pomimo to, wskazane byłoby przeprowadzenie audytu istniejącej w szpitalu polityki bezpieczeństwa i systemu informatycznego, poprzez dokonanie dogłębnego przeglądu dokumentacji medycznej, a także weryfikację możliwości i zabezpieczeń technicznych. Właściwe wydaje się także prowadzenie regularnych szkoleń dla pracowników, które zwiększałyby świadomość, a tym samym odpowiedzialność personelu w zakresie poprawnego zabezpieczania danych osobowych pacjentów.

Można przypuszczać, iż placówki o tożsamym profilu działalności w całym kraju, z uwagi na wymogi ustawodawcy, wdrożyły zbliżone regulacje legislacyjne. Pomimo to, kontrole przeprowadzane przez GIODO[20]

[20] Przykładowe decyzje GIODO wskazujące uchybienia w procesie przetwarzania danych osobowych prze szpitale i nakazujące ich usunięcie: przywołana w artykule decyzja GIODO nr DIS/DEC-174/12/14274 z dnia 6 marca 2012 r., ponadto decyzje nr: DIS/DEC-174/12/14274 z dnia 6 marca 2012 r. (nakaz zabezpieczenia dokumentacji medycznej oraz zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mających na celu zabezpieczenie danych osobowych pacjentów znajdujących się na zaświadczeniach o niezdolności do pracy przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem); DIS/DEC – 933/34056/09 z dnia 18 września 2009 r. (nakaz przywrócenia stanu zgodnego z prawem, poprzez: usunięcie danych osobowych pacjentów, (…) które przetwarzane są bez zgody osoby, której dane dotyczą); DIS/DEC – 1207/44995/09 z dnia 3 grudnia 2009 r. (nakaz zabezpieczenia dokumentacji zawierającej dane osobowe przed jej udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem; opracowania procedury określającej sposób zabezpieczenia pomieszczeń i sposób postępowania z kluczami do

w placówkach medycznych w Polsce wskazują na występowanie uchybień w procesach przetwarzania i przechowywania danych osobowych leczonych chorych. Zidentyfikowane uchybienia są w dużej mierze zależne od wewnętrznego czynnika ludzkiego, który odgrywa kluczową rolę z jednej strony w odniesieniu do przestrzegania (pracownicy placówek), a z drugiej do egzekwowania przepisów (dyrekcja szpitali).

Istotnym problemem jest także kwestia zapewnienia bezpieczeństwa danych medycznych przed czynnikami zewnętrznymi. W IV kwartale 2013 r. firma FORTINET (dostawca zaawansowanych rozwiązań bezpieczeństwa sieciowego) we współpracy z Korporacją Badawczą Pretendent przeprowadziła wśród działów IT[21] polskich placówek medycznych badanie, którego wyniki wskazują, iż jedynie 17% szpitali ocenia, że dotychczasowe systemy informatyczne są na tyle dobre, by odeprzeć większość ataków hakerów. Informatycy narzekają na brak należytych środków i brak pewności, co do poziomu zabezpieczeń obecnie funkcjonujących systemów. Zwracają uwagę na konieczność dodatkowych zabezpieczeń w infrastrukturze informatycznej. Z kolei zaledwie 11% ankietowanych osób odpowiedzialnych za koordynację procesu informatyzacji w polskich szpitalach i dostosowywanie ich systemów IT do obowiązujących wymogów prawnych, zna dokładnie zapisy Ustawy o systemie informacji w ochronie zdrowia[22]. Niepokojący jest fakt, że aż 40% przebadanych określiło swój stan wiedzy na temat jej przepisów, jako „przeciętny".

Dlatego też, oprócz rozwiązań infrastrukturalnych szpitale zamierzają (zamiar deklaruje blisko 60% badanych szpitali [www.sarota.pl/pl/fortinet/1099-informatyzacja-…] zadbać o szkolenia dla personelu. Podejście takie, wsparte odpowiednim finansowaniem (ze środków własnych i/lub unij-

pomieszczeń oraz prowadzenie ewidencji wydawanych i zdawanych kluczy do pomieszczeń; uzupełnienia polityki bezpieczeństwa, prowadzonej w formie dokumentu o nazwie „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Szpitalu (…)", o wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe; nadania osobom zatrudnionym przy przetwarzaniu danych osobowych, upoważnień do przetwarzania danych osobowych; prowadzenie w Szpitalu (…), ewidencji osób upoważnionych do przetwarzania danych osobowych).

[21] Na pytania ankieterów odpowiadali pracownicy wyższego szczebla administracji odpowiedzialni za wdrażanie systemów IT ze 100 szpitali publicznych i prywatnych, http://www.sarota.pl/pl/fortinet/1099-informatyzacja-sluzby-zdrowia-a-d-2014-nie-wszystkie-szpitale-gotowe-na-cyfryzacje-danych; 25.03.2014.

[22] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2011 nr 113 poz. 657).

nych), pozwoli na zdobycie przez pracowników stosownego doświadczenia, co zwiększy ich skuteczność w niwelowaniu uchybień w procesie ochrony informacji dotyczących pacjentów.

Podsumowując podkreślić należy, iż ochrona danych osobowych, włącznie z informacjami medycznymi, niezależenie od metod oraz form ich przechowywania i przetwarzania, ma podstawowe znaczenie dla korzystania przez osobę z prawa do poszanowania jej życia prywatnego i rodzinnego, gwarantowanego przez art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności[23]. Nienaruszalność poufności danych dotyczących stanu zdrowia jest ważną zasadą w systemach prawnych wszystkich Sygnatariuszy Konwencji. Ujawnienie takich danych może poważnie wpłynąć na życie prywatne i rodzinne jednostki, jak i na jej położenie społeczne i sytuację zawodową, narażając tę osobę na potępienie i ostracyzm. Poszanowanie poufności danych dotyczących stanu zdrowia ma kluczowe znaczenie nie tylko dla prywatności pacjenta, lecz także dla utrzymania zaufania tej osoby do zawodu lekarza oraz do opieki medycznej w ogólności. Bez takiej ochrony osoby potrzebujące opieki medycznej mogą żywić obawy i zrezygnować z poszukiwania odpowiedniego leczenia, ryzykując tym samym własnym zdrowiem[24].

Bibliografia

Dyrektywa 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pl:NOT; 25.02.2014.

http://www.giodo.gov.pl/317/id_art/974/j/pl/ 23.02.2014 r.

Huk A. (2001), *Tajemnica zawodowa lekarza*, Prokuratura i Prawo 2001, nr 6

Jackowski M. (2011), *Ochrona danych medycznych,* Wolters Kluwer Polska.

Kodeks Etyki Lekarskiej

Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dn. 28 stycznia 1981 r. (Ogłoszona D.n. 85-1203, 15 list. 1985.- JO 20 list. 1985. Weszła w życie 1.10.1985) http://www.giodo.gov.pl/plik/id_p/343/j/pl/ 25.02.2014 r.

[23] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2. (Dz. U. z 1993 r., nr 61 poz. 284).

[24] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 6 czerwca 2013 r. nr 1585/09.

Krzymowski W., Glosa do wyroku Sądu Okręgowego w Lublinie dn. 2.06.2010 r. (II Ca 349/10; niepubl.), http://www.legeartis.wpia.uw.edu.pl/wp-content/uploads/2013/06/Glosa-do-wyroku-SO-w-Lublinie-II-Ca-349.10-W.-Krzymowski.pdf 07.03.2014.

https://p1.csioz.gov.pl/38 25.03.2014.

http://www2.mz.gov.pl/wwwmz/index?mr=m17&ms=796&ml=pl&mi=796&mx=0&mt=&my=796&ma=032667 25.03.2014.

http://www.sarota.pl/pl/fortinet/1099-informatyzacja-sluzby-zdrowia-a-d-2014-nie-wszystkie-szpitale-gotowe-na-cyfryzacje-danych 25.03.2014.

http://www.infodent24.pl/lexdentpost/lekarz-dentysta-w-roli-spowiednika,5970_0.html 25.02.2014.

http://statystyka.policja.pl/ 13.02.2014.

http://www.polscy-lekarze.net/edytor4/protes02.html 25.02.2014.

Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania.

Safjan M. (1999), *Ochrona danych osobowych – granice autonomii informacji,* [w:] M. Wyrzykowski, (red.), *Ochrona danych osobowych*, Warszawa.

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012.

Ustawa z dnia 30 sierpnia 1991 r. o zakładach opieki zdrowotnej (Dz. U. 1991 Nr 91 poz. 408).

Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty Dz. U. 2008 nr 136 poz. 857).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926, z późn. zm.).

Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2009 r., nr 52, poz. 417).

Prawne aspekty ochrony przedsiębiorstw w przestrzeni wirtualnej

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 221-232

Paweł Sydor
University of Social Sciences

Legal Protection of Virtual Reality. An Attempt at the Practical Recognition of Software Ownership in Local Conditions

Abstract: Legislation protecting intellectual property constitutes a distinct field of law, differently governing institutions associated with the ownership of copyright, types of authors' rights and possibility of their transfer. In the opinion of the author, that area, through its different regulation of institutions whose manners of protection and understanding seem to have long been established (such as ownership), requires special attention of entrepreneurs. That is due to the fact that, under the copyright law, the transfer is possible solely for the author's economic rights, whereas the author's moral rights shall always remain with the author as his or her subjective rights. Moreover, the author may demand a remuneration increase when a contract has already been performed, and, finally, the sufferer has a much greater possibility to pursue his or her claims (in terms of their value). In the opinion of the author, all those elements discussed on the example of the case study presented in the text indicate the "self-sufficiency" and efficacy of copyright law institutions in the assessment of socio-economic relations occurring in virtual reality and relating, in particular, to local communities with their essential intensity of interpersonal relations.

Key words: virtual reality, intellectual property, contract, autor`s fee, legal clair.

Preface

From the point of view of the property law, *i.e.* that area of the civil law which deals with rights to things, including ownership, intellectual property is an extraordinary phenomenon [Rudnicki, 1999, p. 33]. The object of ownership in that approach is an intellectual creation, which is *de facto* some abstract of thought, necessarily only stored on specific carriers or fixed in another form. That concerns, in particular, computer software, obviously recorded on electronic carriers. It is, however, a computer program that is the object of intellectual property not the carrier itself, which is a tangible item.

The virtual reality of software ownership means that issues related to the scope of protection of that ownership may appear to be less clear. In my opinion, it can particularly affect economic activity in local communities [Bukraba-Rylska, 2007, p. 481] in which, perforce, the principle of greater flexibility of workers applies in the absence of the economic basis for narrow specialization and more broadly developed discourse culture based on local community links. It is obvious that those phenomena are absolutely positive as social interactions allow for maintaining local ties. With respect to virtual reality, however, they may cause some disturbances in the discussed area, *i.e.* the limits of protection of intellectual property. The purpose of this article is to present legal institutions serving to protect property rights, taking into account a specific social context: the local community and small entrepreneur. In the author's opinion, applicable legal regulations enable to protect intellectual property and pursue claims in the event of infringement. For the proper presentation of the issue and implementation of the practical dimension of conference assumptions, the article starts with a presentation of the tenor of an actual legal dispute, simplified to allow exemplification, *ceteris paribus*, of the relationships of interest [Milewski, Kwiatkowski, 2013]. The example allows to outline the institution of intellectual property and its protection, whereas conclusions attempt to develop modes of conduct in that respect.

Infringement of intellectual property – A Case Study

In a small town, company A carried out service-type activity involving the provision of other companies, media providers, with services consisting in doing research into consumer needs of individual households and businesses and sending the data to companies that have outsourced those services. In order to render the services, company A commissioned computer programmer B to develop a computer program whose value was estimated at PLN 10,000. The programmer sold the author's economic rights to company A. Company A was hiring several employees, including employee Z, within the framework of streamlining projects to improve the operation of company A. Employee Z made a few appropriate changes to the program without informing the programmer.

The town was chosen by leading companies exploring market needs for econometric reasons because consumer needs of the local community were consistent with those of the global community. Employee Z, due to, in his opinion, inadequate remuneration for the streamlining projects, left the

company and, after a few months, set up a rival company utilizing a computer program based on similar system assumptions, becoming a competitor for the company which he had left. When company A submitted a query to person Z concerning the legality of the software use, he pointed out that the possible convergence of system assumptions was coincidental and, what is more, the program itself had been consulted with programmer B. Programmer B confirmed that fact arguing that his salary had been unjustly low and, therefore, he requested company A to pay an extra remuneration of PLN 10,000.

Intellectual Property – Basic Legal Concepts

Pursuant to Article 1 of the Act of 4 February 1994 on Copyright and Related Rights (consolidated text: Journal of Laws [Dz.U.] of 2006, No. 90, item 631, as amended), the work shall be a manifestation of creative activity of individual character, established in any form, regardless of the value, purpose and manner of expression. In particular, as the legislator indicates in the Act, the object of copyright shall include:

1) works expressed in words, mathematical symbols, graphic signs (literary, journalistic, scientific and cartographic works and computer programs);
2) artistic works;
3) photographs;
4) string musical instruments;
5) industrial designs;
6) architectural, architectural and urban planning as well as urban planning works;
7) musical as well as musical and lyrical works;
8) theatrical, theatrical and musical as well as choreographic and pantomime works;
9) audiovisual works (including films).

According to the basic principles of the copyright law, the object of protection may only be a form of expression; protection does not apply to discoveries, ideas, procedures, methods and principles of operation and mathematical concepts.

Thus, we can see that copyright focuses on the work, while protection of the author of the work stems from the existence of the work rather than any special powers or abilities held by the author. On account of creation of the work, the author has certain rights at two levels:

1) the author's moral rights;
2) the author's economic rights.

The subject of the article primarily requires to put emphasis on the author's economic rights, since those, as their mere name suggest, can be the object of transactions due to being transferable. However, the description of their characteristics requires their dialectical description based on comparisons [Czub, 2012, pp. 20–40]. Thus, the author's moral rights, pursuant to the cited provisions of the Act (Article 16), protect the link between the author and his or her work, which is unlimited in time and independent of any waiver or transfer. Those rights include, in particular: the authorship of the work; the right to sign the work with the author's name or pseudonym or to make it available to the public anonymously; the right to have the contents and form of the work inviolable and properly used; the right to decide on making the work available to the public for the first time and control the manner of using the work. We see, therefore, that the author's moral rights protect the author; the author may not (regardless of the needs of the moment) waive the authorship of works, both journalistic and literary or computer programs, to name just a few. Due to the creation of the work, the author shall have the author's economic rights that protect (Article 17) the exclusive right to use the work and to manage its use in all fields of exploitation, and to receive remuneration for the use of the work. In contrast to the author's moral rights, the author's economic rights are transferable; hence, they have a certain value, constituting, pursuant to Article 55 (1) of the Act of 23 April 1964 – the Civil Code (consolidated text: Journal of Laws [Dz. U.] of 2014, item 121), part of the enterprise in its objective supposition, being understood as a set of tangible and intangible assets.

So, how can the author's economic rights be transferred? The author's economic rights may pass on to others through inheritance or under an agreement on the transfer of the author's economic rights (free of charge or against remuneration) or an agreement on the use of the work hereinafter referred to as the "licence", covering fields of exploitation expressly mentioned therein [Czajkowska-Dąbrowska, 1998, pp. 34–35]. At the conclusion of an agreement on the transfer of the author's economic rights, the rights pass to the buyer. Upon granting a licence, the author's economic rights remain with the author, although the latter is limited in his or her right to manage the use of the rights depending on the provisions of the licence agreement [Bart, Markiewicz, 2011]. The copyright applies civil law institutions (agreements, licences *etc.*), thereby moving the discussion on the analysis of specific issues concerning rights occurring on the background of its

norms to the area of the civil law. One of the basic principles of the civil law is the principle that *pacta sund servanda* (agreements must be kept) [Bieniek, 1999]. Copyright violates that principle in favour of the author. Pursuant to Article 44 of the cited Act on Copyright and Related Rights, the author may request the court for a due increase in his or her remuneration in the case of gross discrepancy between the remuneration of the author and the benefits of the acquirer [see: Judgment of the Court of Appeal in Poznań of 12 August 2009, IACa 502/09, unpublished].

Notwithstanding the above remarks on the ownership of software under the copyright law, it should be kept in mind that, assuming that the software can be used in industry, it may be protected under provisions of the industrial property law[1] (Act of 30 June 2000, consolidated text: Journal of Laws [Dz. U.] of 2013, item 1410). On the basis of the industrial property law, the work is understood similarly to its understanding under the copyright law as a manifestation of creative activity of individual character which may have industrial importance. By the way, it can be added that streamlining projects are also protected under the industrial property law. The author of a streamlining project enjoys, within the enterprise and in accordance with the rules governing it, protection as the author in terms of both moral rights (for example, no one can claim to be the author of the project) and economic rights. The author of the project shall have a claim for compensation related to the protection of rights at both levels according to comments provided below.

Legal Consequences of the Infringement of Intellectual Property

Compared to other areas of the law, including, in particular, rights *in rem* within the framework of the civil law in its broad sense, the specificity of copyright offers, regardless of protection under the criminal law, two kinds of claims related to the infringement of the author's moral and economic rights.

Copyright Protection under the Civil Law

The infringement of the author's moral rights results in the rightholder's claim (pursuant to Article 78 of the cited Act) for *such an action to be ceased. In the event the infringement has been committed, the author may also request the person who has committed the infringement to perform all the actions necessary for the elimination of its effects and, in particular, to make a public statement of an appropriate form and contents. If the infringement was culpable, the court may award the author an appropriate*

[1] Widely understood - as all activities connected with the production and the organization of the production process, pursuant to article 27 of the Act of 30 June 2000 on Industrial Property Law;

amount of money to repair the suffered damage or – at the request of the author – oblige the perpetrator to pay a relevant amount of money for a social cause as indicated by the author. According to the case-law: liability for the infringement of the author's moral rights is objective one, independent of the good or bad faith of the person who has infringed the interests. In Article 78 of the Act on Copyright and Related Rights, the legislator has made provision for a situation where the infringement has been culpable, resulting in the award to the author of a certain amount to repair the suffered damage. The basic criterion is the dimension and intensity of the suffered damage (as assessed with objectified measures), the degree of negative consequences for the sufferer resulting from the infringement of his or her personal interests, including those financially unmeasurable. One of the major premises of the evaluation is the degree of culpability on the part of the offender. A criterion in the form of the financial situation of the liable person is also indicated. That criterion may be, however, of the auxiliary nature, and not decisive in determining the amount of compensation. In some cases, the court may abandon the award of compensation. That particularly applies to a case where, based on the assessment of all circumstances, it can be decided that the non-financial measures of protection of personal interests already applied (apology, making a statement, taking other actions to eliminate effects of the infringement) are sufficient for the protection of interests of the sufferer ... [Judgment of the Court of Appeal in Poznań of 15 July 2013, IACa 387/13, unpublished]. The intangible nature of the author's moral rights determines the model of protection that implements, first and foremost, issues related to a certain moral satisfaction of the author [Kolczyński, 2010, pp. 36–43], which is also associated with the terminology itself (compensation and not damages).

The infringement of the author's economic rights leads to the author's entitlement, pursuant to Article 79 of the Act, to request the person who has infringed them to:

1) cease the infringement;
2) eliminate the consequences of the infringement;
3) repair the inflicted damage:
    a) on general terms or
    b) by payment of double or, where the infringement is culpable, triple the amount of respective remuneration, which would have been due at the time of claiming it in exchange for the rightholder's consent to the use of the work;
4) render the acquired benefits.

Regardless of the claims referred to in paragraph 1, the rightholder may demand:

1) a single or multiple announcement of a press statement having the appropriate wording and form, or communicating to the public a part of or entire court ruling issued in the examined case, in the manner and to the extent defined by the court;
2) the payment by the person who has infringed the author's economic rights of an appropriate amount of at least twice the probable value of benefit obtained by the perpetrator of the infringement in favour of the Fund for the Promotion of Creative Activity, if the infringement has been culpable and made in the course of business activity carried out on behalf of a third party or in the offender's own name, even if on account of a third party.

Protection of the Author's Moral Rights Under the Criminal Law

Pursuant to Article 115 of the Law on Copyright and Related Rights: *whoever usurps the authorship or misleads as to the authorship of the whole or part of another person's work or artistic performance shall be subject to a fine, restriction of freedom or imprisonment for up to 3 years*. Further criminal provisions penalize the infringement of the author's economic rights through *e.g.* the dissemination of works without permission or purchasing copies obtained in breach of the law. In addition to the criminal provisions of the Act on Copyright and Related Rights, the provisions of the Penal Code – Article 278 §2 of the Penal Code – stipulate the penalty of imprisonment for a person who, without the consent of an authorized person, obtains another person's computer program in order to gain financial benefit.

The liability under the criminal law is based on the principle of guilt understood as a personally chargeable commission of a prohibited act [Góral, 1997, pp. 19–22]. Thus, in order to assume liability, along with the establishment of infringement, it must be proved that the infringement was not accidental but deliberate, because such a state of consciousness of the offender is required by the legislator to assume the criminal liability of the perpetrator [Judgment of the Administrative Court in Warsaw of 8 April 2009, I SA/WA 986/08, unpublished]. The perpetrator of plagiarism must, therefore, know that he or she is committing a prohibited act and want to commit it (direct intention) or, knowing that he or she may commit a prohibited act, accept such a possibility (possible intention). Plagiarism may be the so called obvious plagiarism (concerning virtually the entire work from its contents to its form)

and hidden plagiarism, in which essential elements of the work are convergent, which is very important, taking into account the above case study.

Operation of Legal Institutions Governing Intellectual Property on the Example of the Described Case

In the described example, an infringement of intellectual property rights undoubtedly occurred. Company A entered into an agreement to transfer the author's economic rights with the programmer, thus gaining the right to manage the use of the work in the agreed areas of exploitation. The programmer remained the author of the program because, pursuant to the above-mentioned provisions, the author's moral rights, including authorship, are non-transferable. When copying software owned by company A, employee Z infringed *de facto* and *de iure* the author's economic rights. The fact that the works are only similar rather than identical may not rule out the possibility that it was plagiarism. According to court rulings on issues related to the assessment of the similarity of works, taking into account their diversity, and based only on the similarity or even identity of institutions of their protection, it can be stated *that an industrial design refers to the form of the product, hence its external observable characteristics; the product cannot be deemed separate solely due to the fact that the material used to reach the final effect applied to be registered as an industrial design is different from that originally used or that methods employed to make the product according to a registered design have changed. External elements that are not sufficiently visible cannot also determine a different, individual character of an industrial design* ... [Judgment of the Supreme Administrative Court in Warsaw of 19 October 2010, IIGSK 932/09, unpublished]. To apply that view to the matter at hand, we can emphasize that the fact whether the work has been copied will be determined based on the convergence of essential characteristics.

What remains to be considered is the question of infringement of the rights of person Z and the programmer by company A. Person Z advanced an argument that he had not received sufficient remuneration for changes in the computer program, which were to have the form of streamlining projects. In turn, the programmer raised a claim concerning possible inconsistence of the received amount of remuneration for the transferred author's economic rights. Thus, a question can be asked about the possibility to pursue claims through interference in the sphere of the author's economic rights of company A. That question must be answered in the negative. The filing of claims by person Z and the programmer does not make them *per se* enforceable and subject to a possible deduction. For both the persons, it

would have to lead to the view that it is possible for the sufferers to pursue their claims in every possible manner, including the misappropriation of economic rights. It can seem controversial from the point of view of infringement of the author's moral rights of the programmer to interfere with the content of the work created by him, as part of its improvement. So, could company A, interfering with the content of the work (a computer program developed by the specified programmer) within the framework of streamlining projects, infringe the author's moral rights? According to the described facts of the case, such a claim was not formulated, which, however, does not prevent an attempt to reflect on that issue. The answer will depend on the legal relationship between the programmer and company A and the extent of the interference. If, therefore, he did not assume a duty to service the program and changes introduced into the program by company A aimed to improve it, such a conduct does not seem to constitute an infringement of the author's moral rights as defined above. In the case, however, where the changes were actually aimed at reconfiguring the program in a way being far from the author's intentions, an infringement of the programmer's rights could be established independently of the fact that he sold the author's economic rights to his work, which is the specificity of intellectual property. Nevertheless, it should be kept in mind that computer programs are regulated differently under the copyright law [Barta, Markiewicz, 2001, p. 81] in the very scope of possible interference in the program. Thus, pursuant to Article 74 and 75 of the quoted Act [Judgment of the Supreme Administrative Court in Białystok of 25 June 2002, SA/Bk 1232/01], the author's economic rights to the computer program include the right to do:

1) the permanent or temporary reproduction of a computer program, in its whole or part, by any means and in any form; where it is necessary to reproduce a computer program for its loading, displaying, running, transmitting and storing, the consent of the rightholder shall be required to such acts;
2) the translation, adaptation, arrangement or any other changes in the computer program, providing for the rights of the person who made those changes.

Such changes do not require the consent of the author. As for workers' claims concerning the possible lack of financial settlement of submitted streamlining projects – pursuant to provisions of the industrial property law (the Act of 30 June 2000, consolidated text: Journal of Laws [Dz. U.] of 2013, item 1410, as amended) – that requires the presence of a streamlining

programme in a given work establishment [Judgment of the Voivodship Administrative Court in Wrocław of 12 January 2010, I SA/Wr 1602/09].

Therefore, if we assume that there was an infringement of rights of company A, it can pursue a claim, within the framework of civil law liability, for the cessation of infringement, damages (in one of the two specified forms) and, finally, the release of obtained benefits (benefits in a sense broader than mere income). In turn, under the criminal law, it can be assumed that person Z committed an offence against Article 278 of the Penal Code. The programmer may be held liable as well, regardless of the possible merits of his claims for higher remuneration.

By Way of Summary

The protection of intellectual property includes a wide range of legal institutions related to innovative activities. The specificity of that field of law stems from the fact that the object of regulation is intangible items, particularly in the sphere of virtual reality which undoubtedly includes the reality of computer software. From the practical point of view, it ought to be especially emphasized that issues connected with intellectual property are exhaustively regulated in the Act on Copyright and Related Rights and the Act on the Industrial Property Law. The self-sufficiency of those regulations means that entrepreneurs do not need to resort to other legal acts, including those forming the basis of civil law relationships. That also entails a certain risk due to the different, as compared to the civil law, regulation of issues concerning performance of duties and possibility to request an increase in remuneration after performance of duties[2] and a certain "double nature" of rights – in the scope of economic and moral rights, and – in the scope of the latter – the right to require the performance of a work in accordance with its intended purpose (with the above-mentioned restrictions related to computer programs) [Czachórski, 1994, p. 210]. In addition, the different regulation of the range of possible compensation claims means that, in the event of establishing such an infringement by an entrepreneur using an illegal (illegally acquired) software, compensation claims may become a much greater

[2] Although the provisions of the Civil Code 357 (1) provides for the possibility of "conversion" commitment, but this is the special situation, referred to clause *rebus sic stantibus* - an extraordinary change in circumstances, the same applies to the possibility provided for in Art. 358 - the so-called *ius moderandi*, in the event of a material change in the purchasing power of money. In the sphere of authors rights - only necessary condition for such an occurrence is much higher than the expected profit of the work.

burden than a compensation under the provisions of the Civil Code, not to mention the criminal procedure. In my opinion, those aspects should certainly be taken into account in estimating the actual costs of virtual products, while the quoted case shows that disputes concerning virtual property are themselves anything but virtual.

Bibliography

Barta J., Markiewicz R., (2009), *Antologie i wypisy* (Anthologies and extracts), nr 2, ZNUJ 2009.

Barta J., Markiewicz R., (2001) *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz* (The Law on Copyright and Related Rights. Comment), Dom Wydawniczy ABC, Warszawa.

Bieniek G. (red), (1999), *Komentarz do kodeksu cywilnego. Księga trzecia – zobowiązania* (Commentary on the Civil Code. The Third Book – Obligations), Wydawnictwo Prawnicze, Warszawa.

Bukraba-Rylska I. (2007), *Kultura w Polsce lokalnej – w mikroskopie i przez lunetę [w:] Oswajanie wielkiej zmiany. Instytut Socjologii Uniwersytetu Warszawskiego o polskiej transformacji (*Culture in Poland the Local-in a Microscope and Telescope [in] Taming the Great Change. Institute of Sociology of the University of Warsaw about the Polish Transformation*,* Krzemiński I, Raciborski J. (red.), Wydawnictwo UW, Warszawa.

Czachórski W. (1994), *Zobowiązania. Zarys wykładu*, (Obligations. The Outline of Speech), PWN, Warszawa.

Czajkowska-Dąbrowska M., (1998), *Merchandising – czyli komercjalizacja popularnych symboli* (Merchandising – Commeralization of Popular Symbols), PPH 1998/10.

Czub K. (2012), *O konstrukcji intelektualnych dóbr osobistych (*The Construction of Autor`s Moral Rights), ZNUJ nr 1, 2012 r;

Góral R.(1997), *Kodeks karny. Komentarz Praktyczny*, (Penal Code. A Pracitical Commentary), Wydawnictwo Zrzeszenia Prawników Polskich, Warszawa.

Kolczyński J. (2010), *W sprawie niektórych autorskich praw osobistych pracownika do programu komputerowego oraz uzyskania autorskich praw majątkowych on – line, (*On Employee`s Certain Moral Rights to Computer Program Copyright and Property Rights on-line), PPH nr 1, s. 36–43.

Milewski R., Kwiatkowski E. (2013), *Podstawy ekonomii (*The Basis of Economics), PWN, Warszawa.

Rudnicki S., (1999), *Komentarz do kodeksu cywilnego, Księga druga, własność i inne prawa rzeczowe*, (Commentary on the Civil Code, The Second Book, Ownership and Other Rights in Rem, Wydawnictwo Prawnicze, Warszawa.

Judgments:

Judgment of the Supreme Court z 3 grudnia 2008 r, VCNP 82/08.

Judgment of ten Voivodship Administrative Court w Warszawie z dnia 8 kwietnia 2009 roku, I SA/WA 986/08.

Judgment of the Supreme Administrative Court w Warszawie z 19 października 2010 roku, IIGSK 932/09.

Judgment of the Supreme Administrative Court w Białymstoku z 25 czerwca 2002 roku, SA/Bk 1232/01.

Judgment of the Court of Appeal w Poznaniu z 12 sierpnia 2009 roku, iaca 502/09.

Judgment of the Voivodship Administrative Court we Wroclawiu z 12 stycznia 2010 roku, I SA/Wr 1602/09.

Judgment of the Court of Appeal w Poznaniu z 15 lipca 2013 roku, IACa 387/13.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 233-246

Justyna Trippner-Hrabi
Społeczna Akademia Nauk
Mark Hrabi
Government Policy Advisor Department for Transport – London

Organizacje wirtualne w nowoczesnym zarządzaniu przedsiębiorstwem

Virtual Organizations in management of modern company

Abstract: Companies in 21st centuries are changing and evaluating all the time. In present economic situation the information, products, services etc. can be transfer very fast. Managers leading firms must know new theoretical and practical business models that help them to manage them in virtual and international environment. The main objective of the paper is to describe chosen aspects of virtual organizations. That factors can be the chances and also the threats for them.

Key words: virtualization, organization, management.

Wstęp

Gospodarka XXI wieku charakteryzuje się między innymi tym, że dla pomyślnego funkcjonowania i rozwoju dominującą rolę odgrywa dopływ do jej struktur wiarygodnych informacji. Mają one charakter strategiczny [Hansen 2009, s. 103]. Koncepcja organizacji wirtualnej jest w powszechnej opinii uważana za tą, która w dużym stopniu odzwierciedla dokonujące się przemiany społeczno-technologiczne, zwłaszcza rozwój technologii informacyjnej i związane z nim procesy globalizacji działalności gospodarczej. Jako swoista metafora organizacyjna podmioty wirtualne są pochodną ery społeczeństwa informacyjnego, a przede wszystkim sektora komputerowego, skąd hasło „wirtualny" trafiło do nauki o organizacji i zarządzaniu. Pojęcie społeczeństwa informacyjnego zostało użyte pierwszy raz przez T. Umesao w artykule na temat teorii ewolucji społeczeństwa opartego na technologiach informatycznych [Hassan 2008, s. 37]. Termin ten określa społeczeństwo postindustrialne, którego podstawową cechą jest szerokie korzystanie

z technologii teleinformatycznych w różnych aspektach życia takich jak: praca, kultura, czas wolny. Zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności organizacji działających w różnych branżach.

Celem artykułu jest opisania wybranych aspektów organizacji wirtualnych, które mogą stanowić zarówno szanse jak i zagrożenia dla ich działalności rynkowej. Publikacja została napisana w oparciu o przegląd i analizę literatury krajowej oraz międzynarodowej.

Wirtualizacja podmiotów gospodarczych

Wirtualność staje się uznanym paradygmatem w naukach o zarządzaniu. Jest ona odpowiedzią na megatrendy, dotyczące [Grudzewski, Hejduk, Sankowska, Wańtuchowicz 2007, s. 157–158]:

- nieustających przemian w otoczeniu bliższym i dalszym przedsiębiorstwa, które narzucają stosowanie przez nie strategii opartych na trzech głównych elementach: wysokiej jakości, niskich kosztach oraz szybkiej reakcji na potrzeby klientów;
- internetowych i innych nowoczesnych środków przekazu informacji określających trendy prowadzenia biznesu, umożliwiające m.in. pracę na odległość;
- globalizacji powodującej wchodzenie przez firmy na rynki światowe, na których mogą one oferować swoje produkty szerokiej gamie nabywców, mając możliwość kooperowania z mnogością organizacji, a także przeciwstawiając się wielonarodowej konkurencji;
- dóbr typu: szkolenia, kursy, które są oparte na informacji i procesach zarządzania wiedzą i mogą być tworzone, rozpowszechniane i sprzedawane za pomocą przekazu cyfrowego;
- kooperacji przedsiębiorstw przyjmującej postać określaną mianem sieci, która stała się powszechnym sposobem ich współpracy, zapewniającej efektywne wykorzystanie zasobów oraz dużą elastyczność i szybkość reakcji na zmiany;
- współpracy międzynarodowych zespołów zadaniowych, które tworząc nowe rozwiąznia posługują się narzędziami teleinformatycznymi w swojej pracy.

Pierwotnym źródłem rozwoju wirtualności była informatyka, która przyczyniła się do budowania większych, pojemniejszych pamięci, mających zastosowanie w mikroprocesorach, systemach sieciowych i multimedialnych.

Następnie została stworzona tzw. wirtualna rzeczywistość, gdzie możliwe stało się jej, oddziaływanie w wymiarach prawie realnych na ludzkie zmysły tj.: smak, dotyk, węch, słuch, wzrok [Zimniewicz 2009, s. 118].

Przedsiębiorstwa, aby minimalizować np. koszty, straty oraz błędy u osób uczących się i doszkalających, wykorzystują wirtualną rzeczywistość np. w medycynie (symulowanie operacji, współuczestniczenie w operacjach „na odległość"), budownictwie i architekturze (wizualizacja budynków, mostów), nauki pilotażu (samoloty, statki, samochody). Wirtualizacja jest jedną z determinant prowadzenia wirtualnych uczelni, w których studenci mają szansę podnieść kwalifikację poprzez przyswajanie wiedzy skodyfikowanej i nieformalnej w wybranych placówkach. Standardem stała się wirtualizacja świadczenia usług i dostarczania produktów. Biura turystyczne, wydawnictwa, banki, sklepy z powodzeniem wykorzystują sieć komputerową do prowadzenia działalności [Bernais, Ingram, Kraśnicka 2007, s. 121]. Bazę ofertową skierowaną do klientów, partnerów oraz obecnych i przyszłych pracowników przedstawiają one, (oprócz stron internetowych i tradycyjnych form komunikacyjnych), na wirtualnych targach, które funkcjonują w cyberprzestrzeni. Przedsiębiorstwa mają tam swoje stoiska i pokoje branżowe, gdzie prezentowana jest ich oferta handlowa, oraz mają możliwość wymiany poglądów, odpowiedzi na pytania, oraz obserwowania częstotliwości odwiedzin ich firmy przez inne podmioty. Do tego typu form funkcjonowania można zaliczyć m.in. Wirtualne Targi Pracy, Międzynarodowe Wirtualne Targi Budownictwa, Wirtualne Targi Nieruchomości, Wirtualne Targi Ekologiczne, Euro-regionalne Targi Turystyczne [www.targikarpaty.pl, www.targi.pracuj.pl, www.mwtb.pl, www.etargi.nowyadres.pl].

Najnowszymi projektami podmiotów, które posługują się wirtualnością by dotrzeć do klientów i ułatwiać im załatwianie niezbędnych procedur jest stworzenie wirtualnego sądu E-sąd (województwo lubelskie) czy powołanie Polskiej Partii Internetowej.

Wyżej wymienione organizacje stają się pośrednikami w dostarczaniu produktów i usług wirtualnych, które zaspokajają specyficzne potrzeby klientów. Dzięki wirtualizacji przedsiębiorstwa mogą być bardziej elastyczne, innowacyjne i dostosowywać swoją strukturę, np. zatrudnienia czy ofertową do istniejącego popytu. Elementy te powodują, iż firmy stają się bardziej konkurencyjne, co ma relewantny wpływ na ich pozycje na rynkach lokalnych oraz globalnym. Obecnie szczytowym punktem rozwoju koncepcji wirtualności jest organizacja wirtualna.

Przykładem firmy, która dostosowała się do wymogów prowadzenia działalności gospodarczej w wirtualnym świecie jest przedsiębiorstwo

LOVEFILM. Jest to organizacja specjalizująca się w wypożyczaniu płyt (kiedyś kaset) z filmami i grami. Aby sprostać dzisiejszym wymaganiom popytu, klienci mogą otrzymać zamawiany towar na tradycyjnych nośnikach zapisu (płyta DVD) lub w postaci pliku multimedialnego i oglądać dany tytuł onlinе. Cała procedura zamawiania, rezerwacji, płacenia i korzystania z produktu odbywa się bez „wychodzenia z domu" i jest możliwa poprzez wykorzystanie Internetu. Firma ta również wirtualnie poszukuje dostawców, odbiorców, negocjuje warunki współpracy, składa zamówienia, bada satysfakcje klientów, informuje o nowych produktach czy stosuje tracing przesyłek – czyli śledzi aktualne miejsce pobytu wysłanego lub oczekiwanego zamówienia.

Środkiem niezbędnym do sprawnego funkcjonowania w wirtualnym świecie jest korzystanie z nowych i ciągle ulepszanych form zapisu, przechowywania i przekazywania informacji oraz nieustanne doskonalenie i pozyskiwanie nowych umiejętności przez społeczeństwo.

Szybki rozwój Internetu i masowe korzystanie z niego przez podmioty gospodarcze oraz społeczeństwa, można upatrywać w tym, iż massmedium to daje ogromne pokłady korzyści miedzy innymi takie jak: możliwość przekazu (dokumenty, animacje, muzyka itp.), rzetelność informacji, skrócone kanały komunikacyjne, globalny zasięg, standaryzacja form zapisu, możliwość aktualizacji, interaktywność, relatywnie niskie koszty, łatwość obsługi, eliminacje barier czasowo-przestrzennych. Podkreśla się jednak również zagrożenia, jakie niesie ze sobą nowoczesna technologia a mianowicie: utrata bezpieczeństwa przekazywanych danych oraz różny poziom zaufania pomiędzy partnerami[1]. Spowolniona szybkość transmisji informacji – spowodowana awarią urządzeń, obecnością wirusów – jest również negatywnym aspektem tego typu form zarządzania. Jak podaje Sikorska K., 40% przedsiębiorstw rocznie traci dane w środowisku wirtualnym. Zaznaczyć trzeba, że tylko, jednej trzeciej z nich udaje się odzyskać utracone informacje. [Sikorska 2013, s. 3]. Coraz więcej podmiotów gospodarujących przenosi pliki z danymi do środowiska wirtualnego. Należy pamiętać o właściwym zabezpieczeniu ich treści w celu zminimalizowania utraty strategicznych informacji. Pogląd, że cyber środowisko jest bezpieczniejszą formą przechowywania i magazynowania danych niż inne ich typy zapisu jest błędne. Utrata lub wyciek informacji z wirtualnych urządzeń spowodowane może być np. uszkodzeniem systemu plików, awariami macierzy RAID czy uszkodzeniem serwerów danych. Szeroko nagłaśniane wycieki informacji, z dużych organi-

zacji państwowych i prywatnych, są jedynie wierzchołkiem góry lodowej. Głównie utrata danych dotyczy firm działających w skali mikro. Sytuacja ta może być następstwem np. zgubienia urządzeń IT, błędną obsługą narzędzi informatycznych czy niewłaściwym niszczeniem poufnych dokumentacji. Niezależnie od skali działania organizacji, wyciek strategicznych danych, powoduje ogromne szkody nie tylko finansowe jak również te o charakterze wizerunkowym. [http://www.web.gov.pl/aktualnosci/]. Przedsiębiorstwa w celu minimalizowania wyżej wspomnianych zdarzeń winny odpowiednio aplikować najnowocześniejsze programy i wiedzę dotyczące ochrony poufnych i cennych informacji. Powinny one również korzystać z produktów ubezpieczeniowych, które chronią firmę przed konsekwencjami z tytułu utraty danych handlowych i osobowych oraz roszczeń osób trzecich np., poszkodowanych kooperantów czy klientów.

Ujęcia definicyjne organizacji wirtualnych

Pośród definiujących organizację wirtualną można wyodrębnić dwie grupy autorów reprezentujących nieco odmienne stanowiska. U jednych przy próbach opisania organizacji uwypuklone zostaje ujęcie procesowe, u drugich strukturalne zwane również instytucjonalnym [Charlesworth 2007, s. 9].

W ujęciu procesowym zakłada się, że organizacja wirtualna jest ogniwem absorbującym i wykorzystującym zmianę płynącą z otoczenia zadaniowego i ogólnego. Podmiot staje się aktywnym elementem projektowania dalszych procesów organizacyjnych opartych na zaistniałych okolicznościach. Oznacza to, że firma jest ciągle otwarta na stałe przeprojektowanie, którego celem jest dostosowane jej struktur do otoczenia i zaistniałego procesu a nie zbudowanie jakieś trwałej i nieelastycznej instytucji. Cechą charakterystyczną organizacji wirtualnej są bardzo częste zmiany jej zainteresowań dotyczące współpracy z innymi podmiotami, rynkami zbytu i zaopatrzenia, które są zależne od istniejącego popytu. W ujęciu procesowym podmiot wirtualny nieustannie ewoluuje, dostosowując się do coraz to nowych celów biznesowych, korzystając z sieci komputerowych i sprzedając swoje wyroby zarówno na realnym jak i wirtualnym rynku.

Istotna część obowiązków w tej organizacji jest powierzana telepracownikom, którzy swoje zadania mogą wykonywać w miejscach oddalonych od siedziby firmy np. w domu, podczas podróży czy w specjalnych centrach. Dlatego też firmy mogą łatwiej pozyskiwać właściwe osoby do zespołów zadaniowych, ponieważ mają możliwość współdziałania z pracownikami pochodzącymi z różnych krajów. Sytuacja taka jest możliwa dzięki biegłemu

posługiwaniu się przez nich nowoczesnymi urządzeniami informatycznymi oraz tym, że mogą oni korzystać z banków informacyjnych różnych podmiotów. Pracownicy „stacjonarni" jak i telepraconicy są bardzo ważnym zasobem organizacyjnym, ponieważ transformują wiedzę w procesy generowania wartości dodanej w przestrzeni rynkowej. Dzięki czemu tego typu organizacja opiera się na wiedzy oraz zależy od kapitału niematerialnego. Nasuwa się jednak wątpliwość czy określenie telepracownik jest tym najbardziej słusznym? Nazwa ta sugeruje, iż zatrudnieni korzystają jedynie z telefonów czy wideotelefonów, a przecież obecnie głównymi narzędziami ich pracy są również: Internet, komputery, PDA (BlackBerry, Palm Treo) oraz platformy komunikacyjne. Bardziej celowe byłoby przypisywać im nazwę: pracowników wirtualnych, pracujących na odległość, niestacjonarnych lub cyberpracowników. A analogicznie pracę, jaką wykonuję mianem: wirtualnej, na odległość, niestacjonarnej lub cyberpracą.

Opisywany typ przedsiębiorstwa w bardzo dużym zakresie korzysta z outsourcingu, powierzając wykonywanie wielu czynności firmom zewnętrznym. Tworzy się wtedy sieć, która składa się z poszczególnym podmiotów, współprzyczyniających się do powstania finalnego produktu czy usługi.

Podejście strukturalne uwypukla elementy składowe organizacji wirtualnej, ich cechy charakterystyczne oraz powiązania i zależności występujące pomiędzy poszczególnymi podmiotami gry rynkowej (dostawcy, odbiorcy, konkurencja), jak i interakcje z otoczeniem dalszym. Poszczególne części składowe organizacji przyczyniają się do powodzenia całości, a jej sukces determinuje funkcjonowanie poszczególnych jednostek w tym zbiorze. Przy tym ujęciu podkreśla się także czasowość organizacji wirtualnej oraz jej elementów składowych, jakimi są niezależne przedsiębiorstwa pozostające w stałej gotowości do natychmiastowego, wspólnego działania w momencie pojawienia się impulsów rynkowych. Każdy z partnerów tej współpracy wnosi unikatowe kompetencje, wiedzę, doświadczenie oraz inne zasoby potrzebne do osiągnięcia zakładanego celu. Gdy popyt na dane wyroby zostaje zaspokojony, organizacja wirtualna ulega rozwiązaniu a poszczególne firmy nawiązują nowe współpracę tworząc kolejne sieci z innymi przedsiębiorstwami. Podstawowym narzędziem działania takiej organizacji jest technologia informatyczna, którą wykorzystują w swojej pracy zatrudnieni „stacjonarnie" jak i cyberpracownicy.

Cechą charakterystyczną obydwu podejść jest to, że organizacje te posiadają w swoich strukturach międzynarodowe zespoły wirtualne. W ich skład wchodzą osoby o bardzo odmiennym pochodzeniu, kulturze, wieku, upodobaniach,

sprawności itd. Grupy te są kreatorami wielu nowoczesnych rozwiązań i nośnikami wiedzy, które odpowiednio aplikowane do zaistniałej sytuacji mogą stać się przyczynkiem sukcesu i powodzenia danego przedsięwzięcia. Różnorodność pracowników staje się atutem firmy, gdyż jest ona źródłem mnogości pomysłów, które w lepszym stopniu zaspokajają oczekiwania różnych grup klientów. Przedsiębiorstwa, zatrudniające międzynarodowych pracowników muszą również liczyć się możliwością wystąpienia konfliktów, które przy użyciu odpowiednich narzędzi można skutecznie niwelować.

Inna definicja ukazuje, że organizacja wirtualna to tymczasowa albo stała koalicja geograficznie rozprzestrzenionych jednostek lub grup podmiotów, które korzystając z różnych zasobów, możliwości i okazji dążą do osiągnięcia wspólnego celu [Dimitrakos, Golby, Kearney 2004, s. 4]. Uwypuklona została tutaj cecha organizacji wirtualnej, która zakłada, że podmioty współdziałające często zlokalizowane są w odrębnych przestrzeniach geograficznych a współpraca pomiędzy nimi jest możliwa dzięki osiągnięciom teleinformatycznym. W innych ujęciach organizacji wirtualnej podkreślono, że głównym wyznacznikiem jest jej tymczasowość tzn. z założenia ma ona określony cykl życia zapewniający jedynie wykonanie jakiegoś projektu [Radoiu 2008, s. 55]. Śledząc zaproponowaną przez C. Garton i K. Wegryn definicję zauważyć można, iż określają oni organizacje wirtualną, jako podmiot w którym przynajmniej jeden z członków zespołu pracuje na odległość [Gartton, Wegryn 2006, s. 4]. Nasuwa się jednak pewna wątpliwość, łącząca się z nieprzyjętym w definicji kryterium odległości pracy osoby zatrudnionej jako cyberpracownika od centrali. Co w sytuacji, gdy jeden z pracowników jest zlokalizowany np. tylko 1 km od głównej siedziby? Czy mamy wówczas do czynienia z organizacją wirtualną czy w tylko w pewnym stopniu zwirtualizowaną? Problem jak dotąd nie znalazł w literaturze przedmiotu wyjaśnienia. Należałoby wprowadzić odpowiednie mierniki (jakościowe i ilościowe) oraz wzory wyliczające procentowy udział wirtualności w danej organizacji. Jednakże kwalifikacja kryteriów poziomu wirtualności jest rzeczą trudną.

Dokonując reasumpcji należy zauważyć, iż obligatoryjnie występującymi elementami w organizacji wirtualnych krajowych, monokulturowych jest to, że:

- są to przedsiębiorstwa lub grupy jednostek, (które połączone są ze sobą na zasadzie sieci) realizujących określony projekt;
- długość ich istnienia może być tymczasowa lub długookresowa przechodząca we współpracę o charakterze strategicznym (np. Allegro, PAO, m-Bank);
- zatrudnieni w tych przedsiębiorstwach biegłe posługują się rozległą i zróżnicowaną infrastrukturą informatyczną;

- ich najważniejszym zasobem są ludzie, będącymi dostawcami nowych pomysłów i wiedzy;
- są to podmioty cechujące się różnym stopieniem wirtualizacji;
- są to podmioty hybrydowe, ponieważ w większym lub mniejszym zakresie kompilują w sobie elementy charakterystyczne dla tradycyjnych jak i wirtualnych form organizacyjnych;
- wykazują elastyczność w reagowaniu na zmiany w potrzebach i uwarunkowaniach płynących z rynków;
- podmioty wchodzące w ich skład koncentrują się na kluczowych kompetencjach;
- bazują one na zaufaniu, jako podstawowym narzędziu koordynacyjno-kontrolnym.

Elementami uzupełniającymi jest to, że:

- przedsiębiorstwa w dużej mierze korzystają z usług telepracowników (cyberpracowników),
- zatrudnieni nie są na stałe związani z jedną organizacją,
- współpraca przedsiębiorstw odbywa się częściej na zasadach partnerskich niż powiązaniach ściśle hierarchicznych,
- duży nacisk kładzie się na innowacyjność i doskonalenie,
- wdrażane są w nich programy zarządzania wiedzą i talentami.

Dodatkowymi elementami charakterystycznymi dla międzynarodowych organizacji wirtualnych jest to, że:

- jednostki takie posiadają multidyscyplinarne, międzynarodowe, zespoły zadaniowe, których praca podlega zasadom komplementarności;
- w ich skład wchodzą międzynarodowe zespoły wiedzy;
- przedsiębiorstwa realizujące założone cele wywodzą się z różnych obszarów geograficznych;
- posiadają zdywersyfikowane międzynarodowe źródła finansowania;
- korzystają z międzynarodowych zasobów materialnych i niematerialnych;
- tworzą międzynarodowe struktury organizacyjne, wyodrębniając spółki matki i córki;
- szybciej zwiększają zasięg działania, mają możliwość działania globalnego;
- posiadają rozmytą tożsamość, czyli nie ma jasno wyznaczonych granic (z punktu widzenia klienta) pomiędzy daną organizacją a jej kooperantami.

Konfiguracje organizacji wirtualnych

W literaturze przedmiotu wyróżnia się dwa ujęcia powstawania i wyłaniania organizacji wirtualnej [Lichtarski, Moroz 2002 oraz Katzy, Loh, Hang 2005, s. 29-45]. Pierwsze wskazuje na wyłonienie się jej z tradycyjnie zhierarchizowanej, zarządzanej i funkcjonującej firmy, która ulega dezagregacji na mniejsze struktury połączone wspólnym celem przy zachowaniu dużego stopnia niezależności przy jego osiąganiu. Spora część czynności pomocniczych zlecana jest podmiotom zewnętrznym na zasadach outsourcingu. W drugim podkreśla się rolę podmiotu integrującego wirtualność działań w rezultacie pojawienia się biznesowej szansy rynkowej. W skład przedsiębiorstwa wchodzą różne niezależne jednostki tworzące sieć, której byt rynkowy uzależniony jest od wielkości popytu i jego trwania w czasie. Podmiot integrujący może w różny sposób przewodzić tym rodzajem współpracy i jednocześnie przybierać następujące nazwy: nazwy:

- przedsiębiorstwo rdzeń (*core firm*) – jeden z uczestników, który wyróżnia się na tle innych pod względem wielkości, zamożności, potencjału, „dyktujący" zasady współpracy i często będący łącznikiem z otoczeniem;
- broker (integrator, moderator) – podmiot, który inicjuje i poszukuje uczestników do wirtualnej platformy współpracy a następnie koordynuje i pośredniczy w dalszych etapach działania;
- komitet sterujący (*steering committee*) – zespół (przeważnie kadra kierownicza) składający się z przedstawicieli poszczególnych jednostek wchodzących w skład organizacji wirtualnej;
- menadżer wirtualny – osoba pracująca w otoczeniu wirtualnym charakteryzująca się wysokim poziomem kompetencji w zakresie komunikacji, negocjacji i koordynacji pracy rozproszonych jednostek [Brzozowski 2010, s. 130–132].

Organizacja wirtualna może przyjmować różnorodne konfiguracje. Poniżej zostały scharakteryzowane najpopularniejsze jej formy określane w literaturze także mianem modeli [Brzozowski 2003, s. 48–54; Lethbridge 2001, s. 19–22; Malthotr 2007, s. 36–39]. Model wirtualnego wizerunku polega na dodaniu przez tradycyjnie zarządzane przedsiębiorstwo nowego kanału komunikacyjnego jakim jest strona WWW. Może ona służyć jedynie, jako źródło dodatkowej informacji o ofercie firmy, albo umożliwiać również zakup dóbr producenta online. Przedsiębiorstwo takie jest przede wszystkim postrzegane, jako wirtualne przez konsumentów korzystających z możliwości nabycia dobra w sieci a nie przez tych kupujących jej produkty w bardziej

konwencjonalny sposób. Jednocześnie twórcą i operatorem stron WWW jest podmiot zewnętrzny.

Kolejna postacią organizacji jest sieć zrównoważona (model zrównoważonej kooperacji), która jest skompilowana z niezależnych podmiotów. Ich wkład materialnych i niematerialnych zasobów jest porównywalny, a także w podobnym stopniu partycypują one w zarządzaniu założonymi celami. Wirtualna współpraca ma charakter komplementarny i pozwala osiągnąć efekt synergii przy jednoczesnym rozłożeniu ryzyka i kosztów realizowanej inwestycji pomiędzy organizacjami. Działanie takie jest często efektem zaciśnięcia wcześniejszych związków kooperacyjnych miedzy stronami. Dość powszechna jest sytuacja, gdzie jeden lub paru członków aliansu chcą wybić się na pozycję lidera i odgrywać dominują rolę w sieci, pozostałym przedsiębiorstwom przypisując role satelickie w zakresie decyzyjnego podporządkowania. Może to prowadzić do zachwiania równowagi współpracy, zaufania, komunikacji między partnerami a w rezultacie do gorszych efektów finalnych.

Wyróżnia się także sieć zdominowaną (model aliansu gwiaździstego), w której główną rolę odgrywa jedno przedsiębiorstwo dysponujące najbardziej relewantnymi kompetencjami, zasobami wiedzy, finansów, informacji. Jest ono głównym decydentem współpracy tworząc koncepcję prowadzonego biznesu, integrując działalność, dobierając partnerów (firmy satelickie), kreując kulturę organizacyjną, opracowując strategię w tym kanały komunikacyjne z klientami i poszczególnymi partnerami. Wizerunek takiej firmy, która jest nośnikiem logo lidera aliansu gwiaździstego, jest bezpośrednio zauważany przez finalnych odbiorów. Produkt tworzy wizerunek lidera odbierany i oceniany na rynku. Tego nie można odnieść do firm satelickich, które w sieci zdominowanej z rynkiem finalnym mają jedynie pośredni kontakt. Z tego typu aliansu wynikać mogą niebezpieczne tendencję w zarządzaniu, polegające niekiedy na spotykanych próbach lidera do przechodzenia w stosunku do partnerów na pozycję wiodąca, scentralizowaną, prowadzącą do autokratycznych sposobów kierowania siecią.

Kolejną z omawianych postaci organizacji jest model łańcucha wartości, w którym punktem wyjścia jest identyfikacja kluczowego procesu lub procesów, w najwyższym stopniu wymagających sprawnej koordynacji przepływów informacyjnych. Następnie na podstawie tego procesu, kształtowana jest konfiguracja organizacji, której cechą jest sekwencyjne wykorzystanie kompetencji poszczególnych uczestników. Podmiotem odpowiadającym za kontakty z klientem jest uczestnik obsługujący ostatnie ogniwo w łańcuchu tworzenia wartości.

Immanentnymi zasobami organizacji wirtualnej krajowej i międzynarodowej są zespoły zadaniowe, kooperanci klienci, którzy tworzą kapitał ludzki w tej strukturze. Tożsamość (…) zbiorowa należy do ważniejszych koncepcji wykorzystywanych we współczesnych naukach społecznych i humanistycznych [Sułkowski 2012, s. 214]. Są one cennym zasobami i akceleratorami kreującym oraz koordynującym nową wiedzę, dzięki której współpraca może przebiegać bez większych zakłóceń. Dzięki kapitałowi ludzkiemu organizacja ta jest oparta na wiedzy, będącej źródłem nowych pomysłów i rozwiązań niezbędnych do prawidłowego rozwoju i osiągania satysfakcjonującego poziomu konkurencyjności. Właściwa konfiguracja zatrudnionych rozpoczyna się już na etapie rekrutacji i selekcji do przedsiębiorstwa. Firmy posiadające wielonarodowych pracowników muszą wymagać od nich nie tylko standartowych umiejętności organizatorskich, właściwego gospodarowania czasem, ale również umiejętności technicznych, administracyjnych, językowych, wysokiego poziomu samodyscypliny, oraz umiejętności pracy w różnych miejscach (np. samolot, dom, biblioteka). Jak z tego wynika poziom oczekiwań firmy na satysfakcjonujące ją szeroko rozumiane kwalifikacje pracowników jest w firmie wirtualnej znacznie wyższy niż w tradycyjnej. Wyżej wymienione umiejętności powinny być weryfikowane na etapie rekrutacji.

Pracownicy wirtualni często kooperują z wieloma podmiotami wykonując różnorodne projekty, dlatego tradycyjna ścieżka kariery, przypisana jednej osobie w tej samej firmie, traci na znaczeniu. Zatrudnieni wytyczają swój rozwój poprzez współpracę z wieloma organizacjami skupiając się na najbardziej interesujących ich ofertach. Z punktu widzenia pracodawców sytuacja taka może być korzysta, ponieważ dopasowują oni strukturę zatrudnienia w swoim przedsiębiorstwie do aktualnego zapotrzebowania. Niemniej jednak pracowników najzdolniejszych, najefektywniejszych powinno się pozyskiwać i zatrzymywać do dłuższej współpracy, ponieważ to przecież oni są najcenniejszym zasobem tworzącym wiedzę i czyniącym daną organizację bardziej konkurencyjną.

Osoby czy zespoły pracujące na odległość nie mogą być „zapominane" przez menadżerów w kwestiach takich jak: komunikacja, zebrania, aktualizacja informacji dotyczące danego zadania, szkolenia itp. Taka sytuacja może stać się bardzo demotywująca dla zatrudnionych szczególnie, gdy będą oni wiedzieli, iż pracownicy stacjonarni nie są pomijani w wyżej wymienionych kwestiach. Czyli takie same reguły współpracy muszą obowiązywać cyberpracowników i osoby pracujące w siedzibie firmy.

Analiza SWOT

Przedstawiając pozytywne i negatywne aspekty organizacji wirtualnej posłużono się metodą analizy strategicznej SWOT, w której oprócz mocnych i słabych stron podmiotu zaproponować można hipotetyczne, generalne szanse i zagrożenia dla tego typu formy organizacyjnej.

Tabela 1. Analiza SWOT dla organizacji wirtualnej

Mocne strony	**Słabe strony**
• duża elastyczność i innowacyjność w działaniu, • obniżenie kosztów (zmniejszenie zapotrzebowania na powierzchnię biurową), • możliwość pozyskania tańszych i bardziej dostępnych zasobów materialnych oraz niematerialnych, • możliwość optymalnego doboru pracowników z uwagi na cele firmy, • różnorodność i swoboda w zakresie doboru komplementarnych kooperantów, która przyczynia się do zaistnienia efektu synergii, • łatwość komunikowania się, • większe audytorium potencjalnych klientów – globalny zasięg, • szybsza reakcja działania w zakresie funkcjonowania i rozwoju firmy, • możliwość outsourcingu czynności pomocniczych, • dzielenie poziomu kosztów i ryzyka między współpracującymi podmiotami, • efektywne wykorzystanie zasobów, • stosowanie nowoczesnych rozwiązań z zakresu organizacji i zarządzania, • zwiększenie satysfakcji pracowników z wykonywanej pracy poprzez bodźce materialne i niematerialne.	• rozmyta tożsamość, • konieczność inwestowania w nowoczesną niejednokrotnie drogą infrastrukturę informatyczną, • możliwość negatywnego oddziaływania czynnika „zaufanie" stanowiącego kluczowy element sukcesu, • brak precyzyjnej kontroli nad pracą zatrudnionych i współkooperantów, • negatywna opinia o przedsiębiorstwie docierająca do globalnych klientów, • słabsze zabezpieczenie danych o podstawowych celach firmy jej strategiach oraz dysponowanych przez nią zasobach.
Szanse	**Zagrożenie**
• szeroki dostęp zasobów informacyjnych, • łatwość w stosowaniu benchmarkingu konkurencyjnego i funkcjonalnego,	• obniżenie poziomu szybkości, sprawności oraz awarie urządzeń informatycznych,

• międzynarodowa współpraca, w której łatwiej pokonane są bariery czasu, przestrzeni, prawne, • możliwość pozyskiwania pracowników odmiennych kulturowo przy jednoczesnym niwelowaniu barier geograficznych, • możliwość pozyskania pracowników z tzw. słabszych grup ludności: niepełnosprawni, kobiety w ciąży, emeryci,	• różnorodność pracowników źródłem konfliktów i nieporozumień, • brak dostępu do Internetu w niektórych regionach kraju i świata, • brak zaufania przez niektórych konsumentów do organizacji wirtualnych i jej produktów, • nieuczciwe organizacje wirtualne wewnątrz sieci, • trudności koordynacyjne dotyczące współpracy w sieci, • trudności ze znalezieniem lub niewłaściwy dobór firm współpracujących, • hakerzy.

Źródło: opracowanie własne na podstawie [Mikuła, Mikuła 2006, s. 86].

Zakończenie

W podsumowaniu artykułu należy zauważyć, że sukces organizacji wirtualnej zależy od paru czynników. Po pierwsze, jakości kapitału ludzkiego wspartego dalszą chęcią podnoszenia we własnym zakresie poziomu kwalifikacji indywidualnych i zespołowych. Jak również możliwości pozyskiwania międzynarodowych ekspertów tworzących zespoły wiedzy. Należy również kłaść nacisk na nieustające działania motywujące wspierające owe wysiłki ze strony pracodawców. Otwartość społeczeństwa na korzystanie z produkcji dóbr i usług dostarczanych przez te organizacje, ma też wpływ na powodzenie opisywanych podmiotów. Kolejnym czynnikiem winno być wyzwolenie przez organizacje wirtualne w rezultacie działań marketingowych impulsów pozytywnych na rynku. Ważnym elementem jest dbanie o należytą rangę w relacjach wewnątrz organizacyjnych, międzyorganizacyjnych i z rynkiem odbiorców czynnika określanego mianem zaufanie. Kolejnym aspektem jest właściwe zabezpieczenie danych o charakterze osobowym i handlowym w celu zminimalizowania ich utraty. Przedostanie się poufnych, strategicznych informacji w ręce osób i firm niepowołanych, skutkować będzie poważnymi konsekwencjami finansowymi oraz utratą imagu i pozycji wizerunkowej przedsiębiorstwa. Ostatnim punktem jest odpowiedni poziom liberalizacji przepisów państwowych i międzykontynentalnych ułatwiających nawiązywanie współpracy i kooperacji.

Bibliografia

Bernais J., Ingram J., Kraśnicka T. (2007), *ABC Współczesnych koncepcji i metod zarządzania.*, WAE, Katowice.

Brzozowski M. (2003), *Wybrane Modele Organizacji Wirtualnej,* [w] Zeszyty Naukowe AE Poznań z. 3, Poznań.

Brzozowski M. (2010)*, Organizacja wirtualna*, PWE, Warszawa.

Camison C., Devece C., Garrigos F., Palacios D. (2008), *Connectivity and Knowledge Management in Virtual Organizations: Networking and Developing Interactive Communications*, ISF, London.

Charlesworth A. (2007), *Internet Marketing: A Practical Approach, A Butterworth-Heinemann*, Oxford.

Davidow W., Malone M. (1992), *The virtual Corporation*: *Structuring and Revitalizing the Corporation for the 21st Century*, HarperBusiness, New York.

Dimitrakos T., Golby D., Kearney P. (2004), *Towards a trust and Contract Management Framework for Dynamic Virtual Organizations*, British Telecom, UK.

Gartton C., Wegryn K. (2006), *Managing without Walls, maximize success with virtual, global, and cross-culture teams*, MC Press, Lewisville.

Grudzewski M., Hejduk I., Sankowska A., Wańtuchowicz M. (2007), *Zarządzanie zaufaniem w organizacjach wirtualnych*, Difin, Warszawa.

Hansen M. (2009), Collaboration. *How leaders avoid the traps, create unity, and reap big results*, HBP, Boston.

Hassan R. (2008), *The Information Society: Cyber Dreams and Digital Nightmares*, Polity Press, Cambridge.

Katzy B., Loh H., Hang Ch. (2005), *Modelling for virtual organization,* [in:] *Virtual Organization – System and Practice* (Eds.) Afsarmanesh H., Camarinha-Matos L., Ollus M., Springer, New York.

Lethbridge N. (2001), An I-Based *Taxonomy of Virtual Organizations and the Implications for Effective Management,* [in:] *Developing Effective Organizations*, Vol 4, No 1.

Lichtarski J., Moroz M. (2002), *Koordynacja w organizacji wirtualnej*, [w] *Stan i perspektywa rozwoju teorii i praktyki zarządzania na progu XXI wieku*, (red.) Lichtarski J., Pace Naukowe AE we Wrocławiu.

Malhotra Y. (2007), *Knowledge Management and Virtual Organizations*, IGI Global, Hershey, USA.

Mikula B. (2006), *Organizacje oparte na wiedzy*, WAEK, Kraków.

Radoiu D. (2008), *Virtual Organization – Conceptual Modelling*, Studia Univ. Babes-Bolyai, Informatica, Volume III, Nr 1.

Sikorska K.(2013), *Utrata danych a środowiska wirtualne*, eGospodarka, 2013 [w:] www.egospodarka.pl

Stallings W. (2009), *Network Security Essential. Application and Standards*, Pearson, New Jersey.

Sułkowski Ł. (2012), *Kulturowe procesy zarządzania*, Difin, Warszawa.

Wilson F. (1999), *Cultural control within the Visual Organization*, Sociological Review 1999.

www.etargi.nowyadres.pl dn.,18.08.2013

www.targi.pracuj.pl, dn., 26.09.2013

www.targikarpaty.pl, dn., 12.09.2010

www.web.gov.pl/aktualnosci dn., 22.01.2014

Zimniewicz K. (2009), *Współczesne koncepcje zarządzania*, PWE, Warszawa.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 247-261

Józef Paszkowski
Społeczna Akademia Nauk

Polityka bezpieczeństwa przedsiębiorstw w świetle zmian technologii telekomunikacyjnych i rynku elektronicznego

The security policy of enterprises in the light of changes in the t elecommunications technologies and the electronic market

Abstract: This article presents the organizational and legal situation of telecomputer safety in enterprises on the electronic and mobile technology market. The author discusses the basic methods of the security system structure in small and medium enterprises which face increasing threats to the security of data processing. A draft of the security system structure as well as the procedure of designing the security policy in enterprises on the electronic and logistic chains structure markets have been presented. Guaranteeing the required security of the computer systems in the heterogenic processing is possible through telecomputer security outsourcing and the coordination of the enterprises' collaboration.

Key words: telecomputer safety, e-business, security policy, the enterprises collaboration, outsourcing.

Wprowadzenie

Od komputerów uzależniona jest cała nasza współczesna cywilizacja. Od samego zarania informatyka odgrywa szczególną rolę w przedsiębiorstwach, a z chwilą powstania Internetu, również w całym ich biznesowym otoczeniu. Integracja informacyjna przedsiębiorstw i powstanie technologii internetowych, stworzyły szeroką perspektywę ich rozwoju. Technologie informacyjne (ang. *Information Technology*, IT) otworzyły wręcz nieograniczony dostęp do informacji, „łamiąc" dotychczasowe bariery przestrzeni i wymiany informacji. Przedsiębiorstwa i powstały rynek elektroniczny stały się najważniejszym z punktu widzenia gospodarczego rozwoju, kierunkiem zastosowań informatyki. Trzeba też dodać, że technologie informacyjne wkroczyły w kolejną fazę rozwoju, nazwaną „trzecią platformą", w której podstawową rolę zaczynają odgrywać rozwiązania mobilne [Sobczak, Kulisiewicz, 2013, s. 10].

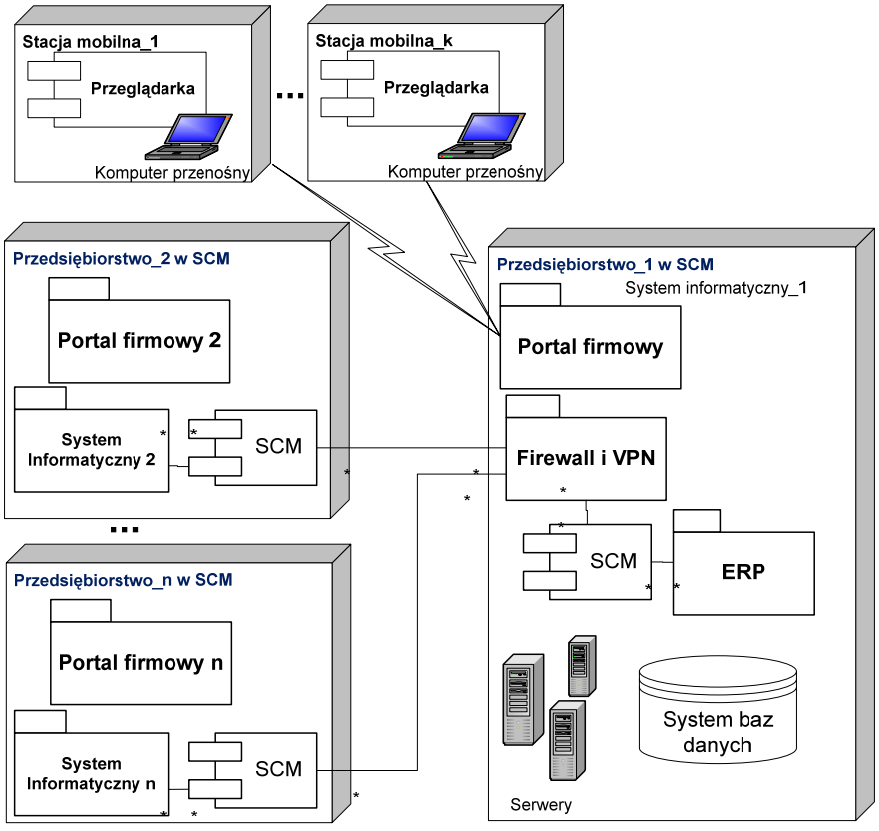
Jednak te cechy, które stały się motorem rozwoju i zastosowań technologii teleinformatycznych, w tym możliwości integracji systemów i niegraniczonego dostępu do danych, stały się przyczyną różnych problemów i zagrożeń. Właśnie te czynniki mające wpływ na bezpieczeństwo danych, stanowią genezę poniższych rozważań. Szczególnym zainteresowaniem objęte zostały procesy zapewnienia bezpieczeństwa teleinformatycznego w przedsiębiorstwach. Celem niniejszego artykułu jest przedstawienie skali zagrożeń wynikających z rozwoju technologii telekomunikacyjnych, uwarunkowań technologicznych rynku elektronicznego oraz przedsięwzięć, jakie powinny podejmować przedsiębiorstwa w zaistniałej sytuacji.

System teleinformatyczny przedsiębiorstwa w kontekście bezpieczeństwa teleinformatycznego

Aktualnie systemy informatyczne przedsiębiorstw oparte są na architekturze systemów klasy MRP/ERP [Adamczewski 2000, s. 45–64]. Powstanie technologii internetowych przekształciło architekturę systemu przedsiębiorstwa do postaci ERP II, w którym nastąpiło swoiste wyjście przetwarzania danych poza granice przedsiębiorstw, łącząc je z systemami kooperujących przedsiębiorstw [Paszkowski, Sowa 2009, s. 89–92]. Podstawę technologiczną zmian stworzyły takie rozwiązania jak EDI (ang. *Electronic Data Interchange*) – elektroniczna wymiana danych i SCM (ang. *Supply Chain Management*) – zarządzanie łańcuchem dostaw. Umożliwiają one łączenie w sieci systemów informatycznych współpracujących przedsiębiorstw [Paszkowski i in. 2012, s. 111–119], tworząc rozbudowane technologicznie i informacyjnie heterogeniczne systemy teleinformatyczne. Współdziałanie przedsiębiorstw, szczególnie integracja przepływów informacji między ich systemami informatycznymi, rodzi szereg problemów z integracją danych i ich bezpieczeństwem. Z kolei rozwój technologii radiowych, upowszechnienie urządzeń mobilnych typu smartfony i tablety otworzyły kolejny „worek z problemami". Jednym z nich jest Bring Your Own Device, tj. włączanie do firmowych sieci prywatnych, niedostatecznie chronionych, urządzeń pracowników. Jest to tzw. Shadow IT, polegający na samowolnym, wykorzystywaniu przez pracowników niedozwolonych rozwiązań (programów z nieautoryzowanych źródeł, tworzenie nieautoryzowanych kopii plików), używanie prywatnych urządzeń jak smartfony, laptopy, tablety czy aplikacji działających w chmurze [Pietruszyński 2014]. Kolejnym obszarem zagrożeń są zasoby programowo-sprzętowe, które dotychczas były izolowane od Internetu, uważane za bezpieczne i często pozbawione ochrony. Jednym z takich

miejsc potencjalnie narażonych na ataki, są systemy sterowania technologicznymi procesami produkcji, SCADA (ang. *Supervisory Control And Data Acquisition*). Pracownicy włączają doraźnie swoje komputery mobilne do sieci SCADA, albo łączą się przez Internet z portalem producenta lub serwisu. Zalecane jest odseparowanie systemów SCADA od reszty firmowej architektury IT, by nie było możliwości przejęcia kontroli nad systemem produkcji poprzez któryś z elementów jej struktury, np. zainfekowaną stację roboczą. Przykładem takiej potencjalnie zagrożonej hybrydy systemów teleinformatycznych przedsiębiorstw z miniami pracowników i klientów, jest architektura systemów przedsiębiorstw w łańcuchu dostaw, przedstawiona na rysunku 1.

Rysunek 1. Architektura hybrydowego systemu przedsiębiorstwa pracującego w łańcuchu dostaw



Źródło: opracowanie własne.

Taka różnorodność poszczególnych składników sieci, zarówno pod względem systemów operacyjnych jak i wykorzystywanych aplikacji oraz połączenie sieci współpracujących przedsiębiorstw, komplikuje problem budowy systemu bezpieczeństwa. Występuje tu efekt skali, stanowiący, że prawdopodobieństwo wystąpienia zagrożenia[1] jest wprost proporcjonalne do złożoności systemu. Analizując zagrożenia przenoszone przez sieć Internet, trzeba zwrócić uwagę na ewolucję złośliwego oprogramowanie tzw. malware (ang. malicious software). Malware wykorzystuje podatności[2] w aplikacjach bądź usługach i za pomocą nośnika tzw. exploita, czyli kodu, może rozprzestrzeniać się w sieci zarówno przez robaki internetowe (ang. *Internet worms*) – samo propagujące się w sieci złośliwe aplikacje, jak i złośliwe strony internetowe czy wykorzystywane pliki PDF. Celem zorganizowanych grup przestępczych stają się botnety – sieci przejętych komputerów, które pozwalają w wybranym przez przestępców momencie wykonać zaplanowany atak przeciw wybranym organizacjom, firmom czy obiektom [Grudziecki 2012, s. 11–12]. Oczywiście oprócz zagrożeń atakami przy pomocy złośliwego oprogramowania czy wirusów, istnieją inne zagrożenia jak ataki terrorystyczne na infrastrukturę, klęski żywiołowe, pożary, awarie sprzętu i zasilania czy działania destrukcyjne człowieka, zarówno te niezamierzone jak i celowe. W niniejszych rozważaniach zostaną wymienione jedynie w kontekście proponowanych zabezpieczeń w dalszej części artykułu. Ich opisy można znaleźć w literaturze, m.in. w pracach Białasa [2007] i Lidermana [2003].

Warunkiem wstępnym analizy takiej struktury jest ustalenie stanu formalnoprawnego: zdefiniowanie pojęć oraz wymagań bezpieczeństwa informacji oraz obowiązujących w tym zakresie prawa.

Bezpieczeństwo danych i systemów informatycznych – definicje i podstawy prawne

Dla poniższych rozważań przyjęto rozpatrywanie bezpieczeństwa w zakresie całego systemu teleinformatycznego. Pod tym pojęciem należy rozumieć synergiczne połączenie systemu informatycznego z wszystkimi używa-

[1] Zagrożenie (ang. threat), to – potencjalne naruszenie zabezpieczeń systemu informatycznego (punkt 3.1.115 w PN-I-02000:1998)

[2] Podatność nazywana także luką w oprogramowaniu (ang. *vulnerability*), może istnieć zarówno w samym systemie operacyjnym (np. w implementacji stosu TCP/IP), jak i w aplikacji świadczącej usługi serwerowe, np. serwer MS SQL). Pozwala ona w sposób nieautoryzowany ominąć zabezpieczenia systemu [Grudziecki 2012, s. 11].

nymi przez niego systemami telekomunikacyjnymi, w tym m.in. takimi jak sieć Internet i technologie mobilne. W literaturze można spotkać dwa kierunki rozważań: bezpieczeństwo danych i bezpieczeństwo systemów informatycznych. Pierwsza kategoria wynika z tego, że w przedsiębiorstwach przechowuje się i przetwarza olbrzymie ilości danych. Dane te odgrywają priorytetową rolę w funkcjonowaniu współczesnych, zinformatyzowanych przedsiębiorstw, stanowiąc jeden z najważniejszych ich zasobów. Zapewnienie „bezpieczeństwa danych" należy rozumieć jako ich ochronę, „czyli zabezpieczenia przed nieupoważnionym lub nieprawidłowym, przypadkowym bądź umyślnym ujawnieniem, modyfikacją lub zniszczeniem" [Stokłosa i in. 2001]. Można też mówić o bezpieczeństwie informacji, dodatkowo obejmującym: przetwarzanie, przechowywanie dokumentów i ich nośników, wszystkie kanały przesyłania informacji, również poza systemami informatycznymi oraz przechowywane tradycyjnie w postaci dokumentów drukowanych. W znacznym stopniu dane są przetwarzane przy pomocy systemów informatycznych i bezpieczeństwo danych obejmuje specyficzną dziedzinę problemową. Rozpatrywane zagadnienia bezpieczeństwa ulegają poszerzeniu o problemy wynikające z komputerowego przetwarzania, zagadnienia niezawodności urządzeń systemów komputerowych i błędów oprogramowania, a także związane z użyciem technologii komunikacyjnych. Najkrócej stan bezpieczeństwa systemów komputerowych oddaje definicja podana przez Garfinkela [2003] „System komputerowy jest bezpieczny, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją". Polska norma PN-I- 13335-1: 999 definiuje „bezpieczeństwo systemu informatycznego, jako wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności" [Paszkowski 2006, s. 32].

Poniżej (tab. 1) zostały przedstawione określenia podstawowych atrybutów, używanych do oceny bezpieczeństwa danych i przetwarzających je systemów. Formalnym punktem odniesienia oceny stanu i wymagań bezpieczeństwa są regulacje prawne, zarówno międzynarodowe jak i krajowe. Należy przede wszystkim wymienić podstawowe normy międzynarodowe ISO (ang. International Organization for Standardization) i odpowiadające im polskie normy PN, określające wymagania dotyczące bezpieczeństwa informacji. Najważniejsze z nich to [Normy 2014]:

- ISO/IEC 27001:2005 - międzynarodowy standard budowy Systemów Zarządzania Bezpieczeństwem Informacji, w Polsce opublikowano 4.01.2007 r. jako normę PN-ISO/IEC 27001:2007.

- ISO/IEC 17799:2005, a w Polsce ogłoszona jako PN-ISO/IEC 17779) – szczegółowe zalecenia dla procesu wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji w organizacji.
- ISO/IEC 13335:2000 (PN-I-13335) – zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych.

Tabela 1. Charakterystyka bezpieczeństwa systemu informatycznego i jego atrybuty

Nazwa atrybutu	Opis
Poufność (ang. *confidentiality*)	właściwość systemu przetwarzania danych, zapewniająca, że treść danych tj. zawarta w nich informacja jest udostępniana lub ujawniana tylko uprawnionym, autoryzowanym osobom, podmiotom lub procesom.
Dostępność, (ang. *availability*)	Oznacza czas bezawaryjnego działania usługi w stosunku do całości czasu, w którym usługa ta powinna być klientom świadczona. Dostępność 90% oznacza, że na 100 jednostek czasu w 90 system działał bezawaryjnie. Dostępność usługi dotyczyć może kogoś lub czegoś, kto lub co ma do tego prawo
Integralność danych, spójność (ang. *data integrity*)	właściwość przetwarzanych danych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób.
Rozliczalność (ang. *accountability*)	Właściwość systemu lub procesu przetwarzania danych, zapewniająca, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi. Stan ten najczęściej jest osiągany za pomocą różnych form rejestrowania zdarzeń np. logowania, w połączeniu z ochroną integralności, niezaprzeczalności oraz autentyczności zapisów w rejestrze.
Niezawodność (ang. *reliability*)	własność obiektu określająca poprawną jego pracę (gdy wykonuje wszystkie powierzone mu funkcje i czynności) przez wymagany czas i w określonych warunkach eksploatacji (przy określonych czynnikach wymuszających).
Uwierzytelnianie (ang. *authenticity*)	Funkcja lub proces sprawdzenia i potwierdzenia zadeklarowanej tożsamości podmiotu biorącego udział w procesie komunikacji [PN-ISO/IEC 27000:2009] Uwierzytelnienie ma zapewnić określony poziom pewności, że dany podmiot jest w rzeczywistości tym, za który się podaje. Dotyczy użytkowników, procesów, systemów lub instytucji.

Źródło: Opracowanie własne na podstawie PN-13335-1, [Białas 2006, Normy 2014].

Ponadto obszar bezpieczeństwa informacji i danych regulują także takie ustawy jak [Ustawy 2014]:

- Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.,

- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie … przetwarzania danych osobowych,
- Ustawa o ochronie informacji niejawnych, z dnia 22 stycznia 1999 r.
- Ustawa o ochronie baz danych z dnia 27 lipca 2001 r.
- Ustawa o świadczeniu usług drogą elektroniczną, z dnia 18 lipca 2002 r.
- Ustawa o podpisie elektronicznym, z dnia 18 września 2001 r.
- Ustawa o elektronicznych instrumentach płatniczych, z dnia 18 września 2001 r.
- Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z dnia 20 lipca 2011 r.,
- Ustawa o rachunkowości z dnia 29 września 1994 r.

W normie PN-ISO/IEC 17779 określono zasady analizy bezpieczeństwa SI i definicje poziomów bezpieczeństwa informacji. Określa ona zasady polityki bezpieczeństwa, organizację systemu bezpieczeństwa, i metody klasyfikacji zasobów informacyjnych. Projekt systemu bezpieczeństwa teleinformatycznego przedsiębiorstwa wymaga wykonania następujących zadań [Paszkowski 2006, s. 32-36]:

- ustalenie celów, strategii i opracowanie polityki bezpieczeństwa;
- określenie wymagań bezpieczeństwa dla użytkowanego systemu informatycznego (SI);
- dokonanie identyfikacji i analizy zagrożeń dla zasobów SI;
- identyfikowanie zagrożeń dla zasobów wrażliwych[3] oraz analizę ryzyka;
- wybór i wyspecyfikowanie zabezpieczeń minimalizujących zagrożenia przy przyjętym poziomie ryzyka;
- wdrożenie i monitorowanie zabezpieczeń w czasie eksploatacji, dla założonego poziomu ochrony informacji;
- opracowanie i wdrożenie programu szkolenia użytkowników SI w zakresie bezpieczeństwa systemów;
- wdrożenie narzędzi wykrywanie naruszeń bezpieczeństwa i opracowanie procedur reagowanie na incydenty[4].

[3] Wrażliwość informacji (*information sensibility*) jest miarą ważności przypisaną informacji dla danego podmiotu w celu wskazania konieczności jej ochrony. Informacje wrażliwe mogą zostać wykorzystane przeciwko temu podmiotowi poprzez ujawnienie, uniedostępnienie oraz zmanipulowanie jawne lub skryte.

Najważniejszym zadaniem jest opracowanie Polityki Bezpieczeństwa, dokumentu ustalającego ramy systemu bezpieczeństwa firmy.

Budowa polityki bezpieczeństwa

Polityka bezpieczeństwa (ang. *security policy*) „jest zbiorem spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne" [Wikipedia 2014]. Określa ona, „w jaki aktywa informatyczne obejmujące informacje wrażliwe są zarządzane, chronione i rozpowszechniane wewnątrz organizacji, która je wykorzystują" [PN-I-02000:2002].

Punktem wyjścia opracowania jest ustalenie, co powinno być chronione z ustaleniem priorytetów, jakie są zagrożenia z ustaleniem poziomów ryzyka i jakie są oszacowania możliwych strat. W trakcie analizy należy odpowiedzieć na szereg pytań, m.in. [Paszkowski 2006, s. 31]:

1. Jakie dane są wrażliwe i mają krytyczne znaczenie dla organizacji?
2. Jakie straty poniesie przedsiębiorstwo w wypadku ich utraty, nieuprawnionego ujawnienia czy zmiany treści?
3. Jakie będą koszty odtworzenia danych lub uruchomienia SI po awarii/incydencie?
4. Jakie będą koszty ograniczeń i utrudnień stosowania środków bezpieczeństwa?
5. Jakie jest ryzyko[5] wystąpienia poszczególnych zagrożeń?

Istotne jest ustalenie obszarów, które powinny być szczególnie chronione i nadanie im odpowiednich priorytetów ochrony, np. danych dotyczących prac badawczo – rozwojowych (ang. Research and Design, R&D), polityki inwestycyjnej, umów handlowych, informacji o kontrahentach, wynikach sprzedaży, sytuacji finansowej. Oprócz zabezpieczeń technologicznych niezbędne są właściwie ustalone zasady polityki bezpieczeństwa oraz środki

[4] Incydent bezpieczeństwa (*security incident*), to niekorzystne zdarzenie związane z systemem teleinformatycznym, które według obowiązujących reguł lub zaleceń może być uznane za awarię, faktyczne lub domniemane naruszenie zasad ochrony informacji lub prawa własności.

[5] Ryzyko (risk) to prawdopodobieństwo albo możliwość tego, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować naruszenie lub zniszczenie zasobów.

prewencyjne adekwatne do potencjalnych zagrożeń. Np. jak cytuje Pietruszyński [2014] „Pracownicy HP mający dostęp do najwyższego poziomu tajności informacji wewnętrznych, np. z R&D, nie mają prawa korzystać z rozwiązań mobilnych".

Polityka bezpieczeństwa powinna m.in. określać następujące zasady [Paszkowski 2006, s. 33]:

- opracowania, wdrażania i aktualizacji dokonywanych zmian Polityki Bezpieczeństwa, w tym regulaminów użytkowników i procedur bezpieczeństwa;
- korzystania z komputerowych stanowisk pracy, aplikacji systemu informatycznego, baz danych i kontroli dostępu do nich;
- komunikacji w postaci wymiany danych i dokumentów;
- ochrony antywirusowej;
- zachowania w sytuacjach kryzysowych poprzez identyfikację incydentu naruszenia bezpieczeństwa i realizacji procedur obronnych;
- prowadzenia audytów i monitoringu procesów wdrożeniowych i eksploatacyjnych systemu informatycznego;
- zapewnienie zgodności polityki bezpieczeństwa z obowiązującymi regulacjami prawnymi z zakresu bezpieczeństwa teleinformatycznego poprzez śledzenie zmian prawa i adekwatną aktualizację systemu).

Opracowane zasady powinny objąć cały proces udostępniania informacji, niezależnie od sposobu jej gromadzenia i przetwarzania. Analizie podatności i ryzyka powinny być poddane wszystkie zasoby teleinformatyczne przedsiębiorstwa, w tym takie jak: sprzęt komputerowy, oprogramowanie, dane przechowywane na nośnikach i w czasie przesyłania w sieci, zasoby osobowe (użytkownicy i administratorzy), dokumentacja IT i elementy infrastruktury, m.in. pomieszczenia, sieć energetyczna, itp. W szczególności w dokumentacji polityki bezpieczeństwa powinny znaleźć następujące treści:

- Definicje podstawowych pojęć;
- Zakres odpowiedzialności;
- Zasady tworzenia kont użytkowników w systemie, procedura obsługi konta po zwolnieniu pracownika;
- Wymagania dotyczące tworzenia, zmiany i ewidencji haseł;
- Zasady korzystania z sieci Internet i udostępniania informacji (treści);

- Regulaminy użytkowników;
- Zasady korzystania z połączeń modemowych i mobilnych;
- Metody ochrony danych strategicznych, krytycznych dla firmy i ich klasyfikacji (np. projekty badawczo-rozwojowych, finanse, dane osobowe), kopie zapasowe;
- Metody ochrony przed wirusami komputerowymi i szkodliwym oprogramowaniem;
- Audyty bezpieczeństwa, monitorowanie i zapis historii pracy systemu;
- Zasady zarządzania zmianami, w tym aktualizacji oprogramowania;
- Usługi outsourcingowe, np. zapasowe centra przetwarzania;
- Zasady zapewnienia ciągłości działania systemu informatycznego, w tym sprawności urządzeń IT, usługi serwisowe, procedury odtworzenia systemu po awarii.

Opracowana Polityka Bezpieczeństwa powinna mieć postać zredagowanego dokumentu, autoryzowanego przez autorów i zatwierdzonego przez Zarząd oraz powinno być ustalone kto odpowiada za wdrożenie, nadzór i okresową aktualizację np. Administrator Bezpieczeństwa Informacji. Przykładowy opis zawartości dokumentu Polityki Bezpieczeństwa można znaleźć w opracowaniu pod redakcją Darowskiej [2000].

Podstawą do opracowania Polityki bezpieczeństwa w przedsiębiorstwie, powinny być wyniki analizy stanu bezpieczeństwa danych i systemu informatycznego, uzyskane z audytu bezpieczeństwa [Wolska 2012, s. 81]. Audyt może być przeprowadzony przez firmę, która ma kompetencje, do tego rodzaju przedsięwzięć i można wtedy mówić o audycie zewnętrznym lub w ramach własnej komórki organizacyjnej i wtedy jest to audyt wewnętrzny.

Audyt bezpieczeństwa i wybrane metody i narzędzia budowy bezpieczeństwa systemu informatycznego

Audyt bezpieczeństwa informacji to porównanie do standardów, w tym zasad Polityki bezpieczeństwa. Jest podstawą analizy i modyfikowania mechanizmów ochrony informacji. Stosowanych w audytach może być kilka standardów, m.in.:

- COBIT (ang. *Control Objectives for Information and related Technology*) – opracowany przez organizację audytorów ISACA (ang. *Information Systems*

Audit and Control Association, www.isaca.org), zawiera m.in. listę trzystu dwu wymagań dotyczących trzydziestu czterech procesów;

- TCSEC (ang. *Trusted Computer System Evaluation Criteria*) opracowany został przez Agencję Bezpieczeństwa Narodowego Departamentu Obrony USA i Narodowe Biuro Standaryzacji – jako Orange Book;
- BS 7799, opracowany przez Brytyjski Instytut Standaryzacyjny, m.in. listę 127 wymagań.

Audyt zawsze musi odnosić się do założonych kryteriów oceny przyjętych przez przedsiębiorstwo w zakresie bezpieczeństwa informacji, np. [Wolska, 2012 s.82]; m.in. zobowiązania wynikające z zawartych umów, obowiązujących przepisów prawa, polityki bezpieczeństwa oraz norm, np. ISO/IEC 27001. Opis wykonania audytu można znaleźć m.in. w pracach Wolskiej [2012, ss. 83-92] oraz Lidermana [2003].

Do badania bezpieczeństwa systemu informatycznego stosuje się też różne narzędzia, np. jednym z nich jest pakiet Sysinternals Suite dla platformy Windows [2014]. Składa się z ponad 60 programów, dedykowanych głównie administratorom, m.in.:

1) DiskMon: umożliwia monitorowanie akcji przeprowadzanych na pamięciach dyskowych przez uruchomione programy;
2) Handle: wyświetla informacje plikach i folderach aktualnie używanych przez wybrany program lub wszystkie uruchomione aplikacje;
3) PsLoggedOn: pozwala sprawdzić jacy użytkownicy są zalogowani na komputerze lokalnym lub zdalnym;
4) PsLogList: tworzy raport zdarzeń (*Event Log*) na lokalnym lub zdalnym komputerze;
5) PsShutdown: pozwala wyłączyć lokalny lub zdalny komputer, wylogować użytkownika, zablokować system lub przerwać rozpoczęte wyłączanie;
6) RootkitRevealer: zaawansowane narzędzie do wykrywania złośliwego oprogramowania.

Przedstawione programy prezentują zakres i niektóre możliwości testowania systemów informatycznych pod kątem bezpieczeństwa. Przedsiębiorstwo potrzebuje specjalistów, oprogramowania i aktualnej wiedzy z zakresu bezpieczeństwa. Projektowanie i bieżące utrzymanie takiego systemu staje się coraz bardziej złożone. Skala zagrożeń, w tym działania przestępcze w sieci, np. sabotaż czy kradzież danych z zakresu know-how, ciągły rozwój zaawansowania technologii, m.in. cloud computing, czy technologii mobilnych, powodują, że zarządzanie bezpieczeństwem firmowych systemów IT jest coraz

bardziej wymagające. Utrzymanie niezbędnej infrastruktury spełniającej wymagania, zakup oprogramowania i zatrudnianie dedykowanych do ich obsługi specjalistów ds. bezpieczeństwa i analityków jest dla przedsiębiorstw, szczególnie MSP, nieosiągalne, a na pewno nieopłacalne. Coraz większym problemem staje się zabezpieczenie wymaganej dostępności usług systemu informatycznego. Przykładowo godzina przestoju oznacza czasami trudne do wyliczenia straty, na pewno utrata wiarygodności i często klientów. Dobrym rozwiązanie jest outsourcing IT, a szczególnie w zakresie usług zapewnienia bezpieczeństwa teleinformatycznego.

Outsourcing bezpieczeństwa teleinformatycznego

Outsourcing polega on na przekazania części działalności przedsiębiorstwa firmie zewnętrznej. Obecnie outsourcing jest stosowany, jako metoda optymalizacji wykorzystania zasobów i środków przedsiębiorstwa, polegający na przeniesieniu realizacji niektórych realizowanych własnych funkcji i procesów do firm zewnętrznych. Korzyści osiągane z outsourcingu są osiągane głównie przez:

1) Zmniejszenie kosztów własnych, poprzez eliminowanie tych funkcji przedsiębiorstwa, dla których koszty utrzymania są większe, niż koszty usług w outsourcingu, tj. gdy prace są wykonywane okresowo lub incydentalnie np. prace specjalistów bezpieczeństwa różnych dziedzin czy usuwanie skutków awarii.
2) Dostęp do nowoczesnych technologii z zakresu know – how i zasobów, np. specjalistycznego oprogramowania, zespołu specjalistów, infrastruktury centrów komputerowych, firmy outsourcingowej, która specjalizuje się w swojej dziedzinie.

Zakres outsourcingu bezpieczeństwa SI może objąć, m.in. usługi [Paszkowski 2006, s. 44-45]:

- Zarządzanie bezpieczeństwem i polityką bezpieczeństwa;
- Monitoring systemów i sieci;
- Prowadzenie zapasowych centrów przetwarzania dla systemów przedsiębiorstwa;
- Ochrona przed oprogramowaniem typu Malware;

- Zapewnienie ochrony przed atakami typu DDoS (ang. *Distributed Denial of Service*[6]*;*
- Kolokacja, tj udostępnianie powierzchni w centrum przetwarzania danych (Data Center);
- Hosting, tj. udostępnianie serwerów,
- Aplication System Provider lub Provisioning (ASP), tj. udostępnianie oprogramowania np. systemu informatycznego;
- Udostępnienie systemów zarządzania wiedzą i szkolenia elektroniczne (e-learning);
- Odtwarzanie po awarii i wykonywanie kopii danych – *Disaster Recovery.*

Outsourcing bezpieczeństwa informatycznego oferuje szereg firm, m.in.:

- firma ATM S.A. - www.atm.com.pl usługi w trzech centrach danych; ATMAN i Thinx Poland w Warszawie ATMAN Katowice.
- AVET Information and Network Security Sp. z o.o. (AVET INS) http://www.avet.com.pl/

W perspektywie rozwoju integracji systemów informatycznych współpracujących przedsiębiorstw, Outsourcing bezpieczeństwa teleinformatycznego jest jednym z najlepiej rokujących rozwiązań systemu bezpieczeństwa IT.

Podsumowanie

Ryzyko jest silnie związane z rozwojem IT. Im szerzej informatyka obejmuje i monopolizuje procesy przedsiębiorstwa, tym większy jest zasięg i wielkość potencjalnych strat w wyniku awarii lub naruszeń bezpieczeństwa teleinformatycznego. Zagrożenia bezpieczeństwa SI są nie do uniknięcia, tak długo jak długo będzie zawodna technologia, człowiek oraz jak daleko od idealnej będzie jego natura. Polityka bezpieczeństwa pozwala uzyskać minimalizację dopuszczalnego ryzyka i uzyskanie wymaganego poziomu pewności funkcjonowania SI. Zapewnia wyważenie wymagań bezpieczeństwa z podejmowanymi działaniami i nakładami. Na podstawie analizy ryzyka zagrożeń i oceny własnych zasobów IT, ustalany jest dopuszczalny poziom bezpieczeństwa i niezbędne do jego osiągnięcia środki. Niezwykle ważne jest to

[6] DDoS – rozproszona odmowa usługi – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów [Wikipedia, 2014].

też dla współpracy przedsiębiorstw na rynku elektronicznym i reputacji firmy. Polityka bezpieczeństwa w przedsiębiorstwach tworzy podstawę wymiany wymagań i standardów organizacyjnych dla budowanych systemów bezpieczeństwa w sieci współpracujących przedsiębiorstw i integracji ich SI. Pozwala uzgadniać zakres wymaganych przedsięwzięć, zwiększać wzajemne zaufanie i pewność ciągłości przetwarzania danych. Uzyskanie i wymiana wiedzy o istniejących zagrożeniach, umożliwia opracowanie odpowiednich scenariuszy i procedur reagowania na zaistniałe naruszenia, minimalizację strat i maksymalnie szybkie doprowadzenie systemu do stanu przed awarią. Przygotowanie się przedsiębiorstwa do realnych zagrożeń czy minimalizacja skutków katastrof i zbudowanie odpowiednich zabezpieczeń oraz procedur awaryjnych, jest tylko możliwe, gdy w przedsiębiorstwie jest wdrożona i realizowana dobra Polityka Bezpieczeństwa.

Zapewnienie bezpieczeństwa systemu informatycznego i danych, jest w aktualnej sytuacji warunkiem koniecznym ciągłości funkcjonowania przedsiębiorstwa.

Bibliografia

Adamczewski P.(2000), *Zintegrowane systemy informatyczne w praktyce*, Wyd. MIKON, Warszawa, 2000.

Białas A. (2007), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa.

Darowska M. (2000), *Strategia rozwoju systemu informacyjno-informatycznego resortu środowiska - ŚRODOWISKO 2000*, Proj Antares, Wyd. Ministerstwa Środowiska, Warszawa.

Garfinke S. (2003), *Practical Unix and Internet Security*, II ed., O'Reilly.

Grudziecki T. (2012), *Współczesne zagrożenia w sieci Internet oraz sposoby walki z nimi przy pomocy systemów-pułapek*, Zeszyty Naukowe WSI, Zeszyt 7, ss. 11–27, Warszawa, [onlinel], http://zeszyty-naukowe.wwsi.edu.pl/zeszyty/zeszyt7/Audyt_Zgodnosci_Z _Norma_ Iso-_Iec_27001-_2005.pdf, 27.05.2014.

Liderman K. (2003), *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Mikom, Warszawa.

Normy (2014) - wersja polska [online], http://sklep.pkn.pl/, 28.04.2014.

Paszkowski J. (2006): *Projektowanie, wdrażanie i eksploatacja systemu informatycznego*. Moduł 4, [w:] Systemy informatyczne, Polski Uniwersytet Wirtualny, Łódź, Lublin.

Paszkowski J., Sowa G. (2009), *Technologie informacyjne w logistyce zewnętrznej przedsiębiorstw. Analiza stanu i kierunki rozwoju*. w: Wybrane problemy zastosowania platformy elektronicznej red. Niedźwiedziński M., Lange-Sadzińska K., Marian Niedźwiedziński Consulting Łódź.

Paszkowski J., Filutowicz. Z., Sowa G. i inn.(2012), *Propozycja zmian w systemie zarządzania łańcuchem dostaw*, Studia i materiały Polskiego Stowarzyszenia Zarządzania Wiedzą", nr 62.

Pietruszyński P. (2014), *Infrastruktura IT w obliczu rosnących zagrożeń*, Computerworld, 3/2014.

PRZEDSIĘBIORCZOŚĆ i ZARZĄDZANIE
Wydawnictwo SAN – ISSN 1733-2486
Tom XV – Zeszyt 9 cz. 1 – 2014 – ss. 263-272

Jędrzej Dzikowski
Sędzia Sądu Rejonowego dla Łodzi-Śródmieścia w Łodzi

Prawne aspekty transakcji cywilnych dokonywanych przez Internet

Legal aspects of civil transactions online

Abstract: The objective of the article is to present new regulations of May 2014 which concern transactions online. The author discusses the principles of concluding contracts through declarations in an electronic form. He presents the consequences of the changes in the definition of a consumer and burdening the businessman with additional obligations in trade with a consumer.

Key words: Virtual reality, contract, consumer, terms of sale, withdrawal from a contract.

Wprowadzenie

Celem niniejszego artykułu będzie naświetlenie prawnych aspektów zawierania transakcji handlowych w wirtualnej przestrzeni oraz zasygnalizowanie zagrożeń z tym związanych.

Cyberprzestrzeń staje się coraz bardziej popularnym miejscem obrotu gospodarczego. Aktywność internautów ujawnia się nie tylko na powszechnie znanych portalach sprzedażowych, ale dotyczy również rozliczeń finansowych, w tym zakupu walut. Symptomem rewolucji wirtualnej jest np. posługiwanie się tzw., bitcoinami, czyli internetowymi walutami niebędącymi powszechnym środkiem płatniczym. O stopniu skomplikowania tego ostatniego aspektu świadczy to, iż taką transakcję można zdefiniować, jako dwie niezależne od siebie umowy sprzedaży, z których jedna dotyczy nabycia waluty internetowej, a druga kupna właściwego przedmiotu sprzedaży. Wykonanie każdej z nich może rodzić problemy związane, np. ze składaniem elektronicznych oświadczeń woli (o czym będzie mowa niżej) lub z niewłaściwym wykonaniem umowy.

W szybko zmieniającym się cyfrowym świecie, odrębnym problemem staje się przestrzeganie standardów dotyczących ochrony własności intelek-

tualnej, oraz ochrony danych osobowych związanych z posługiwaniem się bazami danych.

W orzecznictwie sądowym dostrzega się również konieczność szerszego uregulowania tzw. prawa do zapomnienia, czyli uprawnienia do żądania usunięcia z cyberprzestrzeni określonych informacji dotyczących danej osoby fizycznej, bądź prawnej np. informacji o wcześniej przeprowadzonych licytacjach, niekorzystnych doniesieniach prasowych czy zamieszczeniu w rejestrze dłużników. Prawo do zapomnienia powinno dotyczyć również tzw. personalizacji internetowej. Mianowicie, odwiedzając portale internauta godzi się na korzystanie z plików cookies. Dzięki temu właściciel portalu zbiera informacje o naszych zainteresowaniach. Traktuje nas jak potencjalnych odbiorców innych usług czy produktów. Informacje te są później wykorzystywane w kampaniach promocyjnych. Problem polega na tym, iż pełne korzystnie z danych zamieszczonych na stronie wymaga bezwarunkowej akceptacji strategii plików cookies. Konsument jest zatem postawiony przed, w gruncie rzeczy niedopuszczalnym, wyborem – albo ochrona prywatności albo niepełne korzystanie z dobrodziejstw strony.

Skoro Internet jest medium, w którym na szeroką skalę dochodzi do publikacji różnego rodzaju treści, to należy rozważyć odpowiednie stosowanie regulacji prawa prasowego. W zakresie zgody na publikację, zezwolenie można cofnąć przed opublikowaniem danej treści. Uwaga ta ma bardzo istotne znaczenie, gdyż zgodnie z brzmieniem art. 3a ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2002, nr 101, poz. 926) w prawie prasowym po publikacji danej treści nie stosuje się ochrony danych osobowych. Konkludując, każda – choćby dorozumiana – zgoda na publikację danych osobowych internauty wyklucza dochodzenie roszczeń związanych z ochroną danych osobowych.

Zawieranie umów poprzez oświadczenia elektroniczne

Przesłanki skuteczności poszczególnych umów – sprzedaży, zamiany, przekazu – są uregulowane w KC. Tamże znajdują się również przepisy dotyczące składania oświadczeń woli na odległość – w tym w postaci elektronicznej – oraz przesłanki uchylania się od skutków czynności prawnych (z powołaniem na wady oświadczeń woli). Każda umowa wymaga dwóch zgodnych oświadczeń woli. W wirtualnej rzeczywistości są one składane z chwilą wprowadzenia do komputera lub innego urządzenia w taki sposób, żeby odbiorca mógł zapoznać się z ich treścią. W zależności od sytuacji oświadczenie może być potraktowane, jako oferta albo odpowiedź na ofertę.

Oferta złożona w formie elektronicznej wiąże składającego, jeżeli druga strona niezwłocznie potwierdzi jej otrzymanie. Jeżeli nadawca nie wyznaczył terminu na odpowiedź to zaproponowane warunki przestają wiązać, gdy nie zostaną przyjęte niezwłocznie (o ile chodzi o bezpośrednią rozmowę). Może też być tak, iż oferta przestaje wiązać z upływem czasu, w którym oferent nie otrzymał odpowiedzi w takim czasie, jaki jest zwykle, zwyczajowo przyjęty (o ile chodzi o ofertę wysłaną za pośrednictwem urządzenia elektronicznego). Judykatura wypracowała zasadę, iż w przypadku relacji pomiędzy osobami fizycznymi odpowiedź na maila z taką ofertą powinna być udzielona w ciągu jednego, najpóźniej dwóch dni. Reasumując, w każdym przypadku brak odpowiedzi poczytuje się za brak zgody na zaproponowane warunki. Zmiana stanowiska strony inicjującej negocjacje albo w nich uczestniczącej jest możliwa, gdy oświadczenie zmieniające dociera najpóźniej z chwilą oświadczenia początkowego albo wcześniej.

Gdy transakcje są dokonywane pomiędzy przedsiębiorcami to oferta może być odwołana przed zawarciem umowy, jeżeli to oświadczenie zostało złożone drugiej stronie przed wysłaniem przez nią akceptacji oferty.

Skutek błędów generowanych podczas składania oświadczeń.

W tym miejscu należy się odnieść do błędów, które mogą być wygenerowane podczas emisji oświadczeń. Należy tu zastosować reguły wynikające z ogólnych zasad odpowiedzialności cywilnej. Przesłanką podstawową jest ustalenie winy w wygenerowaniu błędu.

W praktyce zdarzają się również takie sytuacje, iż osoby trzecie – za zgodą lub bez zgody posiadacza konta internetowego związanego z numerem IP – uczestniczą w różnego rodzaju aukcjach, dokonują transakcji albo prowadzą negocjacje. Należy tu wyróżnić kilka sytuacji. Po pierwsze, strona transakcji, która została wygenerowana na cudzym komputerze odmawia później wypełnienia wynegocjowanych warunków. W takim przypadku to posiadacz danego konta jest zobowiązany wobec kontrahenta. Oczywiście ma on później roszczenie regresowe wobec sprawcy szkody. Po drugie, może być i tak, iż strona transakcji samowolnie skorzystała z cudzego konta. W takim przypadku odpowiedzialność ponosi bezpośredni uczestnik transakcji.

W obu tych przypadkach może dodatkowo zaistnieć problem z akceptacją transakcji płatniczych dokonanych własną albo cudzą kartą Tutaj również przyjmuje się, że to nominalny a nie faktyczny posiadacz karty ponosi odpowiedzialność za obciążenie rachunku o ile niezwłocznie nie wszczął procedury *cashback*. W ewentualnym procesie reklamacyjnym posiadacz karty

będzie musiał wykazać, że bezpośrednio po powzięciu widomości o nieuprawnionym użyciu karty podjął działania zmierzające do zablokowania transakcji albo odwrócenia jej skutków.

Definicja konsumenta

Dotychczas podstawowe regulacje dotyczące umów zawieranych na odległość były zawarte ustawie z dnia 2 marca 2000 roku o ochronie niektórych praw konsumentów oraz odpowiedzialności za produkt niebezpieczny (t.j. Dz. U. z 2012 r., poz. 1225) oraz w ustawie z dnia 27 lipca 2002 r. o szczególnych warunkach sprzedaży konsumenckiej oraz o zmianie Kodeksu cywilnego (Dz. U. Nr 141, poz. 1176, z późn. zm.9).

Te dwa akty prawne zostały uchylone ustawą z dnia 30 maja 2014 roku o prawach konsumenta (Dz. U. z 2014 r, poz. 827), która implementuje Dyrektywę 2011/83/UE z dnia 25 października 2011 roku. Ustawa została opublikowana w dniu 24 czerwca 2014 roku i wejdzie w życie po upływie 6 miesięcy od dnia ogłoszenia, czyli 25 grudnia tego roku. Należy pamiętać, iż zgodnie z treścią art. 51 do umów zawartych przed dniem wejścia w życie tej ustawy stosuje się przepisy dotychczasowe, czyli regulacje obu uchylonych aktów prawnych.

W nowym akcie prawnym inaczej został uregulowany status konsumenta oraz przedsiębiorcy dokonujących transakcji za pośrednictwem Internetu, co czyni transakcje dokonywane przez tego pierwszego dużo bardziej bezpiecznymi. Ustawa o prawach konsumenta zmienia definicję konsumenta zawartą w art. 22 zn.1 KC. Dotychczas, za konsumenta uważano osobę fizyczną dokonującą czynności prawnej niezwiązanej bezpośrednio z jej działalnością gospodarczą lub zawodową.

Omawiana ustawa, określiła konsumenta, jako osobę fizyczną, która dokonując czynności związanej z prowadzoną działalnością gospodarczą lub zawodową, działa także w celu niezwiązanym z tą działalnością i cel ten przeważa. Cel handlowy przedsiębiorcy nie może być dominujący. Oczywistym wydaje się, że taki zapis zrodzi liczne problemy interpretacyjne w przypadku różnego typu umów o charakterze mieszanym.

Nowa definicja konsumenta może rodzić problemy natury fiskalnej. Pamiętać trzeba o tym, iż organy skarbowe mogą weryfikować jedynie działania związane z prowadzoną działalnością, a nie z życiem prywatnym. Powstaje zatem pytanie, jak ustalić, czy nabyty laptop był wykorzystywany tylko do celów prywatnych w miejscu zamieszkania przedsiębiorcy. W takich sytuacjach konieczna będzie kontrola odwiedzanych stron, czy wykonywanych przele-

wów. Takie postępowanie naruszałoby prawo przedsiębiorcy do prywatności. Byłoby również sprzeczne z fundamentalną zasadą postępowania podatkowego zakazującą nakładania na podatnika obowiązku dostarczania – na etapie postępowania wyjaśniającego czy kontrolnego – dowodów mających potwierdzić wstępne założenia organu kontrolującego. Dowody te mogłyby być następnie wykorzystane przeciwko podatnikowi już we właściwym postępowaniu opartym o przepisy karno-skarbowe. Reasumując niedopuszczalne jest postępowanie na zasadzie: „przedsiębiorco udostępnij swój prywatny laptop, to może uda nam się ustalić niekorzystne dla ciebie fakty podatkowe".

W mojej ocenie organy podatkowe powinny działać w ramach kultury oświadczeń, a nie zaświadczeń. Decydować powinno oświadczenie przedsiębiorcy, iż kupił sprzęt dla celów prywatnych. Organy muszą w takiej sytuacji zaniechać jakichkolwiek czynności sprawdzających.

Obowiązki przedsiębiorcy w relacjach z konsumentem.

Ustawa o prawach konsumenta w art. 12 wprowadza obowiązek szerokiego informowania konsumenta o istotnych elementach transakcji, ale już nie w formie papierowej lecz z wykorzystaniem „trwałego nośnika" czyli również mailowo. Zgodnie z treścią art. 7 konsument nie może zrzec się praw przyznanych ustawą, a postanowienia umów mniej korzystne nie obowiązują danej strony. Informacje, o których mowa w art. 12 stanowią integralną część umowy i mogą być zmienione jedynie za wyraźnym porozumieniem stron. Zgodnie z treścią art. 26, w przypadku sprzeczności pomiędzy przepisami art. 12–23, a przepisami ustawy z dnia 4 marca 2010 r. o świadczeniu usług na terytorium Rzeczypospolitej Polskiej (Dz. U. nr 47, poz. 278, z późn. zm.) oraz ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422) stosuje się przepisy ustawy o prawach konsumenta. Dotychczas przedsiębiorca miał obowiązek potwierdzić informacje przewidziane w art. 12 w tradycyjnej formie pisemnej, co często nie było dochowywane. Obecnie za zgodą konsumenta może przesłać je w formie elektronicznej.

W każdym przypadku jednostronnego redagowania obowiązków umownych istnieje ryzyko, że regulaminy mogą zawierać tzw. klauzule niedozwolone. Przykładowo w 2012 roku prezes UOKiK nakazał wpisanie do rejestru 1398 takich postanowień. Liczba wpisów dotyczących usług wynosiła 277, w tym z branży internetowej 257. Według aktualnych danych, aż 1045 klauzul z rejestru dotyczy handlu w sieci [Kuligowski 2014]. Zjawisko to świad-

czy to ewidentnie o dużym potencjalnym ryzyku nieprawidłowego konstruowania relacji handlowych w wirtualnej rzeczywistości.

Zawsze jednak, ujemne skutki wadliwie opracowanych ogólnych warunków sprzedaży, polegające na możliwości dowolnej ich interpretacji, będą obciążać zbywcę, jako profesjonalistę i autora tych warunków. W tym zakresie można sięgnąć do bogatego orzecznictwa związanego z takimi dokumentami opracowywanymi przez ubezpieczycieli komunikacyjnych. W takim wypadku odpowiedzialność – mimo określonych zapisów zawartych w warunkach – może być w praktyce znacznie szersza niż to zakładał przedsiębiorca (per analogia wyrok Sądu Apelacyjnego w Łodzi z dnia 28 lutego 1996 r., wydany w sprawie o sygnaturze IACr 37/96, opublikowany w OSA z 1996 r., nr 9, poz. 43). W razie sformułowania ich treści w sposób nasuwający wątpliwości, skutki tego obciążają zbywcę (per analogia wyrok Sądu Apelacyjnego w Warszawie z dnia 8 lipca 1997 roku wydany w sprawie o sygnaturze IACa181/97, opublikowany w Prawie Gospodarczym. z 1998 r., nr 5, poz. 41). Należy zatem przyjąć, iż w razie niejasności lub wątpliwości w sformułowaniu treści ogólnych warunków sprzedaży, należy je interpretować na korzyść ubezpieczającego. Wielokrotnie orzecznictwo odwoływało się nawet do tzw. zasad współżycia społecznego – czyli powszechnie akceptowanych w społeczeństwie norm postępowania. (np. per analogia orzeczenie Sądu Najwyższego z dnia 24 lipca 1959 r., wydane w sprawie o sygnaturze 4CR1027/58, opublikowane w OSPIKA z 1961 r., poz. 32, a także wyrok Sadu Najwyższego z dnia 18 marca 2003 r., wydany w sprawie o sygnaturze VCKN1858/00, niepubl., LEX nr 78897).

Ważne regulacje zawiera art. 10 ustawy o prawach konsumenta. Mianowicie, najpóźniej w chwili wyrażenia przez konsumenta woli związania się umową przedsiębiorca ma obowiązek uzyskać wyraźną zgodę konsumenta na każdą dodatkową płatność wykraczającą poza uzgodnione wynagrodzenie. Jeżeli przedsiębiorca zastosował domyślne opcje, które konsument musi odrzucić w celu uniknięcia dodatkowej płatności, konsument ma prawo do zwrotu uiszczonej płatności dodatkowej. Regulacja ta sprowadza się do tego, iż konsument akceptując płatności musi „klikać" w wyraźnie wyodrębnione elementy strony zawierające precyzyjnie określoną kwotę oraz słowo „ZAMÓWIENIE Z OBOWIĄZKIEM ZAPŁATY" – art. 17 – lub innych równoznacznym np. „AKCEPTUJĘ" „PŁACĘ". Jeżeli w celu kontaktu przedsiębiorca podał numer telefonu, to opłata za połączenie nie może być wyższa od opłaty za zwykłe połączenie przewidzianej przez operatora.

Zgodnie z treścią art. 21 przedsiębiorca ma obowiązek przekazać konsumentowi potwierdzenie zawarcia umowy na odległość na trwałym nośniku

w rozsądnym czasie po jej zawarciu, najpóźniej w chwili dostarczenia rzeczy lub przed rozpoczęciem świadczenia usługi.

Odstąpienie od umowy

Załącznik do ustawy zawiera ustandaryzowany wzór oświadczenia o odstąpieniu od umowy. We wszystkich państwach UE termin na dokonanie takiej czynności został wydłużony z 10 do 14 dni. Zgodnie z art. 28 bieg terminu do odstąpienia od umowy rozpoczyna się:

1) dla umowy, w wykonaniu której przedsiębiorca wydaje rzecz, będąc zobowiązany do przeniesienia jej własności – od objęcia rzeczy w posiadanie przez konsumenta lub wskazaną przez niego osobę trzecią inną niż przewoźnik, a w przypadku umowy, która:
   a) obejmuje wiele rzeczy, które są dostarczane osobno, partiami lub w częściach – od objęcia w posiadanie ostatniej rzeczy, partii lub części;
   b) polega na regularnym dostarczaniu rzeczy przez czas oznaczony – od objęcia w posiadanie pierwszej z rzeczy;
2) dla pozostałych umów – od dnia zawarcia umowy.

Zaniechanie poinformowania o prawie do odstąpienia ma ten skutek, że takie uprawnienie konsumenta wygasa dopiero po upływie 12 miesięcy od zakończenia wyżej przewidzianych terminów- o czym stanowi art. 29. Jeżeli oświadczenie o odstąpieniu zostało wysłane w formie elektronicznej przedsiębiorca zawsze musi przesłać konsumentowi potwierdzenie jego otrzymania. Ważne jest to, iż nawet wtedy gdy sprzedawca dopuszcza złożenie oświadczenia w formie wirtualnej, to nabywca może i tak skorzystać z tradycyjnego oświadczenia, albo złożyć je na stronie internetowej sklepu.

Istotna zmiana dotyczy tego, iż konsumentowi nie przysługuje już prawo do odstąpienia od umowy o dostarczanie treści cyfrowych nie zapisanych na nośniku materialnym, czyli np. przesyłanych przez Internet (dotychczas to prawo było ograniczone do nośników materialnych, np. płyt z muzyką), jeżeli spełnianie świadczenia rozpoczęło się za wyraźną zgodą konsumenta przed upływem terminu do odstąpienia od umowy i po poinformowaniu go przez przedsiębiorcę o utracie prawa odstąpienia od umowy. W przypadku odstąpienia od umowy sprzedaży klienci mogą zwrócić towar nawet bez opakowania, z tym że sprzedawcy nie zawsze chcą go przyjąć. Tego typu postanowienia zawarte w regulaminach wielokrotnie kwestionował Sąd Ochrony Konkurencji i Konsumentów. Również niezgodne z prawem jest potrącanie przez przedsiębiorców kosztów naprawy otwartego lub uszkodzonego opakowania. Konsument jest wówczas pozbawiony informacji

o kwocie owego potrącenia. Taka praktyka jest możliwa, gdy konsument nie zastosował się do instrukcji rozpakowywania i opakowanie nie nadaje się do dalszego wykorzystania [Kuligowski 2014].

W przypadku usług prawo odstąpienia jest możliwe po zakończeniu wykonywania usługi (obecnie wystarczy samo rozpoczęcie świadczenia). W trakcie biegu terminu na odstąpienie konsument może korzystać z rzeczy w sposób konieczny do stwierdzenia jej charakteru, cech i funkcjonowania. Preambuła do DYREKTYWY wskazuje, iż nabywca powinien obchodzić się z rzeczą w taki sposób, jak w przypadku nabycia towaru w sklepie – np. może przymierzyć odzież, ale nie powinien jej nosić. Trzeba pamiętać, iż przedsiębiorcy, na zasadach ogólnych, przysługuje prawo do dochodzenia odszkodowania za zbyt intensywne korzystanie z rzeczy.

W przypadku odstąpienia od umowy przez konsumenta sprzedawca musi – najpóźniej w terminie 14 dni – zwrócić cenę oraz koszty dostarczenia do konsumenta (jeżeli ten wybierze droższy sposób dostawy, przedsiębiorca nie musi zwracać różnicy w porównaniu z najtańszym). Co do zasady, zwrot kosztów transakcji powinien nastąpić przy użyciu takiego samego sposobu zapłaty, jakiego użył nabywca, chyba że konsument wyraźnie zgodził się na inny sposób zwrotu, który nie wiąże się dla niego z żadnymi kosztami. Jednakże bezpośrednie koszty odesłania towaru poniesie nabywca, o ile wybrał sposób dostarczenia rzeczy inny niż najtańszy zwykły sposób dostarczenia oferowany przez przedsiębiorcę. Ważne jest to, że jeżeli umowę zawarto poza lokalem przedsiębiorstwa a rzecz dostarczono konsumentowi do miejsca jego zamieszkania, przedsiębiorca jest zobowiązany do odebrania rzeczy na swój koszt, gdy ze względu na charakter rzeczy nie można jej odesłać w zwykły sposób pocztą.

Bardzo istotną nowością jest zlikwidowanie zakazu przedpłaty. Dotychczas sposobem ominięcia tej restrykcji było korzystanie przez przedsiębiorców z płatności za pobraniem. Według nowych regulacji sprzedawca będzie mógł zaliczkować transakcję.

Wystawianie faktur VAT

W orzecznictwie przyjmuje się, iż jeżeli sprzedawca wystawia fakturę VAT pomimo tego iż nie był do tego uprawniony, to kontrahent takiego podmiotu, czyli nabywca, ponosi odpowiedzialność podatkową o ile na podstawie całokształtu okoliczności sprawy mógł się zorientować, że transakcja będzie służyła popełnieniu przestępstwa karno-skarbowego.

Pamiętać należy o tym, iż stawka podatku VAT jest obliczana według prawa obowiązującego w miejscu wykonania usługi. Np. gdy serwer był zarejestrowany w Luxemburgu to transakcja jest opodatkowana tamtejszą stawką. W orzecznictwie przyjmuje się, aby w transakcjach z elementem transgranicznym zwracać się do polskich placówek handlowych i dyplomatycznych w celu uzyskania pomocy w zweryfikowaniu kontrahenta zagranicznego.

W tym miejscu należy odnieść się do problemów związanych z księgowaniem przychodów i wydatków uzyskanych dzięki transakcjom w internecie. Wymogi formalne związane z dokonywaniem wpisów w podatkowej księdze przychodów i rozchodów uregulowane są w §12 ust. 3 pkt. 2 Rozporządzeniu MF z dnia 23 sierpnia 2003 roku w sprawie prowadzenia podatkowej księgi przychodów i rozchodów (pkpir) (Dz. U. nr 152, poz. 1475 z poźn. zm.). Przewiduje on, iż podstawą zapisów w księdze są dowody księgowe, w tym m.in.: inne dowody, wymienione w §13 i 14, stwierdzające fakt dokonania operacji gospodarczej zgodnie z jej rzeczywistym przebiegiem i zawierające co najmniej:

a) wiarygodne określenie wystawcy lub wskazanie stron (nazwę i adresy) uczestniczących w operacji gospodarczej, której dowód dotyczy;
b) datę wystawienia dowodu oraz datę lub okres dokonania operacji gospodarczej, której dowód dotyczy, z tym że jeżeli data dokonania operacji gospodarczej odpowiada dacie wystawienia dowodu, wystarcza podanie jednej daty;
c) przedmiot operacji gospodarczej i jego wartość oraz ilościowe określenie, jeżeli przedmiot operacji jest wymierny w jednostkach naturalnych;
d) podpisy osób uprawnionych do prawidłowego udokumentowania operacji gospodarczych – oznaczone numerem lub w inny sposób umożliwiający powiązanie dowodu z zapisami księgowymi dokonanymi na jego podstawie.

Podczas wydawania jednej z interpretacji podatkowych, uznano, iż pomimo dokonywania zakupów przez internet – na aukcji – od osób fizycznych, przedsiębiorca nie mógł wpisać wydatku do podatkowej księgi przychodów i rozchodów). To praktyczne zagadnienie pojawiło się na kanwie kupowania za jednym razem kilkudziesięciu telefonów komórkowych. W tym przypadku nabywca miał dane osobowe zbywcy, dane sprzętu i kwotę należną. Od firmy pośredniczącej w przekazaniu pieniędzy dostał również dokładne potwierdzenie, jakiej transakcji dotyczyła zapłata (kartę płatności z podaniem godziny, minuty i sekundy). Organ podatkowy zakwestionował te dowody z uwagi na brak podpisu zbywcy. Z przedstawionych przez podatnika dokumentów nie wynikało bowiem który konkretnie przedmiot został nabyty za konkretną cenę. Organ powziął wątpliwość, czy była to jedna transakcja, czy też kilka równoczesnych, co utrudniało mu weryfikację kwot. Należy zatem

unikać zbiorczego płacenia za kilkanaście zakupionych przedmiotów. Warto poprosić sprzedawcę o przesłanie podpisanej umowy [Maj 2014].

W mojej ocenie, taka interpretacja organów podatkowych rodzi uzasadnione wątpliwości. Umowa elektroniczna nie musi być przecież podpisana przez obie strony, gdyż nie dochodzi do bezpośredniego kontaktu stron.

Wnioski

Wprowadzone zmiany legislacyjne należy ocenić pozytywnie. Dotychczasowe dwie ustawy zostały zastąpione jednym aktem prawnym, co z pewnością usprawni poruszanie się przez konsumentów w zawiłej tematyce prawnej. Tym samym przyczyni się do poniesienia świadomości prawnej nabywców i ograniczy niepożądane praktyki przedsiębiorców. Nowe regulacje praw konsumentów nie powinny rodzić większych problemów jurydycznych, gdyż stanowią one rozwinięcie i uproszczenie już istniejących przepisów, które były stosowane przez ponad dekadę. Niewątpliwą zaletą jest ujednolicenie uprawnień konsumenta na całym obszarze wspólnego rynku. Nabywcy towarów i usług zyskali taką samą, i w dodatku silną, pozycję prawną we wszystkich państwach, co przyczyni się do uproszczenia dochodzenia roszczeń. Usprawni to postępowania sądowe, ułatwi zatem wydawanie europejskich nakazów zapłaty i nadawanie europejskich klauzul wykonalności. Będzie to miało o tyle istotne znaczenie, że wiele transakcji internetowych już obecnie zawiera elementy transgraniczne.

Bibliografia

Brodniewicz W. (1998), *Postępowanie cywilne z zarysie,* Wydawnictwa Prawnicze PWN.

Chytła K. (2005), *Ochrona niektórych praw konsumentów oraz odpowiedzialność za szkodę wyrządzoną przez produkt niebezpieczny. Komentarz do zmian wprowadzonych ustawą z dnia 6 maja 2005 r. o zmianie ustawy o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny*, LEX.

Kidyba A. (2010), *Kodeks cywilny. Komentarz.* Tom III. Zobowiązania – część szczególna, LEX.

Kuligowski Ł. (2014), *Pralkę i zabawkę można zwrócić bez pudełka,*, Rzeczpospolita z 2.09.2014.

Maj M. (2014), *Zakup przez Internet, ale fiskus żąda podpisu*, Rzeczpospolita z 3.06.2014.

Rogoń D. (2005), *Ochrona niektórych praw konsumentów oraz odpowiedzialność za szkodę wyrządzoną przez produkt niebezpieczny*, LEX.

Ustawa z dnia 4 marca 2010 r. o świadczeniu usług na terytorium Rzeczypospolitej Polskiej (Dz. U. nr 47, poz. 278, z późn. zm.).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422).

PN-I-02000:2002 – *Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia*, [online] http://sklep.pkn.pl/,28.05.2014.

PN-ISO/IEC 17799:2005 – *Technika informatyczna – Techniki Bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.* [online] http://sklep.pkn.pl/, 28.05.2014.

PN-ISO/IEC 27001:2007 *Technika informatyczna –- Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, [online] http://sklep.pkn.pl/, 28.05.2014.

Sobczak A., Kulisiewicz T. (2013), *Jak zacząć? Analiza rozwiązań technologicznych pomocnych przy budowie Otwartego Rządu i ponownym wykorzystaniu informacji publicznej, Ośrodek Studiów nad Cyfrowym Państwem*, Wyd. 1, Łódź, [online], http://www.andrzejsobczak.net/sites /default/files/analiza_rozwiazan_technologicznych.pdf, 29.04.2014.

Stokłosa J., Bilski T., Pankowski T. (2001), *Bezpieczeństwo danych w systemach informatycznych*. Wydawnictwo Naukowe PWN. Warszawa – Poznań.

Sysinternals [2014] *Opis narzędzi*, [online] http://vurmil.blogspot.com/2012/10/ sysinternals-suite-opis-narzedzi.html, Wer.instal.: http://download.sysinternals.com /files/SysinternalsSuite.zip, 28.05.2014.

Ustawy (2014), *Teksty ustaw i rozporządzeń*, [online], isap.sejm.gov.pl.

Wikipedia (2014), [online], http://pl.wikipedia.org/wiki/, 27.05.2014.

Wolska E. (2012), *Audyt zgodności z normą ISO/IEC 27001: 2005*, Zeszyty Naukowe WSI, Zeszyt 7, s. 79–93, Warszawa, [omlinel, http://zeszyty-naukowe.wwsi.edu.pl/ zeszyty/zeszyt7/Audyt_Zgodnosci_Z_Norma_Iso-_Iec_27001-_2005.pdf, 27.05.2014

O powiecie Brodnickim

Herbem powiatu brodnickiego jest czerwony jeleń w skoku. W myśl tradycji historycznych odczytywany jest jako czynnik integrujący społeczność lokalną pełniący również istotną rolę w budowaniu pomyślnej przyszłości wszystkich obywateli tej ziemi.

Powiat brodnicki położony jest w północno-wschodniej części województwa kujawsko-pomorskiego. Od północy i wschodu graniczy z woj. warmińsko-mazurskim a od południowego wschodu z woj. mazowieckim. Obszar powiatu brodnickiego rozciąga się w dorzeczu Wisły i jej prawobrzeżnych dopływów Skrwy, Drwęcy i Osy. Osią hydrograficzną obszaru jest Drwęca – najdłuższy prawobrzeżny dopływ dolnej Wisły.

Centralnym ośrodkiem powiatu brodnickiego jest miasto Brodnica. Jako stolica powiatu jest siedzibą instytucji powiatowych, służb i straży, zapewniających mieszkańcom i istniejącym tu podmiotom gospodarczym bezpieczeństwo i niezbędne usługi socjalne, zdrowotne i kulturalne na bardzo wysokim poziomie.

Miasta i gminy powiatu brodnickiego wchodzą w skład Obszaru Funkcjonalnego „Zielone Płuca Polski". Podstawowym atutem powiatu brodnickiego są jego walory turystyczne, które wpływają na jego rozwój. Na terenie powiatu znajdują się regiony wyjątkowo atrakcyjne turystycznie, wśród nich: Brodnicki Park Krajobrazowy, będący częścią Pojezierza Brodnickiego, Górznieńsko-Lidzbarski Park Krajobrazowy oraz Dolina Drwęcy – jedna z najczystszych polskich rzek, stanowiąca w całości ichtiologiczny rezerwat przyrody. Ze względu na te wyżej wymienione walory krajobrazowo-przyrodnicze, ważną gałęzią gospodarki powiatu brodnickiego jest turystyka.

Siedziba Starostwa Powiatowego w Brodnicy.

Jezioro Ciche w gminie Zbiczno.

Bogactwo lasów i jezior, dobrze rozwinięta baza noclegowa oraz liczne gospodarstwa agroturystyczne przyciągają turystów z różnych zakątków kraju i zagranicy. Od paru lat w powiecie brodnickim intensywnie rozwija się agro-

turystyka. Większość gospodarstw zrzeszonych jest w Agroturystycznym Stowarzyszeniu Pojezierza Brodnickiego. Gospodarstwa agroturystyczne zapewniają szeroki wachlarz ciekawych i interesujących sposobów spędzania wolnego czasu. Polecane są m.in. wczasy w siodle, przejażdżki bryczką, żeglowanie, spływy kajakowe, wypożyczanie sprzętu sportowego i turystycznego, ognisko, grill, możliwość spożywania świeżych owoców i warzyw oraz przetworów pochodzących z gospodarstwa.

Na terenie powiatu brodnickiego, w ciągu całego roku odbywa się szereg interesujących imprez, które uprzyjemniają pobyt mieszkańcom oraz przybyłym turystom. W wielu gminach w okresie wiosenno-letnim odbywają się różne interesujące imprezy rekreacyjno-kulturalno-sportowe, często połączone z występami popularnych zespołów muzycznych, przeplatane różnorodnymi konkursami i zabawami dla dzieci i dorosłych. Miłośnicy sportów z kolei mogą brać udział w organizowanych w wielu gminach biegach, rajdach rowerowych czy zawodach sportowych.

Wizualizacja szpitala po modernizacji (projekt)

Godna podkreślenia jest działalność Szpitala Brodnickiego. Szpital miał swoje wzloty i upadki. Teraz jest stabilny finansowo, ma coraz więcej pacjentów, realizowana jest modernizacja szpitala i wyposażenie w sprzęt zakładu

radiologii. Planowane zakończenie modernizacji szpitala to koniec roku 2015. Funkcjonują w nim liczne poradnie specjalistyczne, oddział neonatologiczny szpitala, który wyposażony jest w najnowszy specjalistyczny sprzęt, a w szpitalnej pracowni endoskopowej wykonuje się badania w oparciu o wyposażenie nowej generacji. Ważnym atutem Szpitala jest przyszpitalne lądowisko umożliwiające lądowanie śmigłowcom ratunkowym.

Wybierając się w podróż drogami łatwo zauważyć liczne kilometry wyremontowanych dróg powiatowych oraz przebudowane mosty. W realizacji inwestycji wspieraliśmy się środkami z Regionalnego Programu Operacyjnego (RPO), Narodowego Programu Przebudowy Dróg (NPPD), Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA), a także z Ministerstwa Infrastruktury. Niemałe znaczenie miały też finanse z samorządów gminnych, bowiem wiele chodników i dróg powstało dzięki współpracy Powiatu z Miastem Brodnicą, gminami: Brodnica, Bobrowo, Bartniczka, Jabłonowo Pomorskie, Osiek, Świedziebnia i Zbiczno.

Most na rzece Księtówka w gminie Świedziebnia

Wartym podkreślenia jest rozwój brodnickiej oświaty, dobrze zorganizowanej na każdym szczeblu nauczania. W szkołach prowadzone są termomodernizacje, buduje się sale gimnastyczne i tworzy zaplecza boisk piłkarskich

z nowatorsko rozwiązanym systemem wentylacji i ogrzewania, ale także sale fitness, siłownie i nowoczesną infrastrukturę sanitarną.

Nowa hala sportowa przy I Liceum Ogólnokształcącym w Brodnicy

Inwestując w szkolnictwo wychodzimy na wprost oczekiwaniom młodzieży, kierując się ofertami zdobycia „zawodu na dobrą przyszłość". Efekty powyższego przekładają się na systematycznie zmniejszające się bezrobociu na terenie powiatu brodnickiego.

Powiat Brodnicki może też pochwalić się uruchomieniem Geoportalu Powiatu Brodnickiego. To strony internetowe, na których dostępne dla wszystkich są mapy i inne dane geodezyjne z obszaru powiatu. Strony są wygodne dla inwestorów, wykonawców i tych, którzy wydają potrzebne do inwestowania dokumenty, ale także np. wtedy, gdy zwykły użytkownik Internetu szuka konkretnego miejsca w terenie. Po drogach na terenie powiatu można przemieszczać się, śledząc teren z punktu widzenia pieszego lub jadącego drogą.

Gospodarzami, którzy dbają o rozwój i przyszłość Powiatu Brodnickiego w latach 2010–2014 są: Piotr Boiński – Starosta Brodnicki (*z prawej strony)* i Jędrzej Tomella – Wicestarosta (z lewej strony).

Zapraszamy więc i zachęcamy do odwiedzania naszego Powiatu z bogatą historią, atrakcyjnym zapleczem turystycznym, ale też z nowatorskimi rozwiązaniami, które wkomponowane w całościowy program działalności stanowią ciekawą lekturę. Zapraszamy również do inwestowania w naszym powiecie, gdzie znajdziecie wyjątkowo przychylną atmosferę do efektywnego prowadzenia biznesu. Czasami żartujemy, że sprawy niemożliwe rozwiązujemy od ręki a trudne w siedem dni.

Do zobaczenia w Powiecie Brodnickim, gdzie dobrze się wypoczywa i inwestuje pieniądze.

Starosta
Piotr Boiński

Wicestarosta
Jędrzej Tomella