Folia Iuridica Universitatis Wratislaviensis
2017, vol. 6 (1), 107–118

Maciej Błażewski
Uniwersytet Wrocławski

Zasada zapewnienia bezpieczeństwa w e-administracji

The principle of security in e-government

Streszczenie

Zasada zapewnienia bezpieczeństwa w e-administracji jest zasadą prawa, która służy stanowieniu i stosowaniu przepisów prawa w związku z administrowaniem i użytkowaniem systemów teleinformatycznych i środków komunikacji elektronicznej. Celem zapewnienia bezpieczeństwa w e-administracji jest ochrona przechowywanych i przekazywanych informacji. Zasada ta pozwala ujednolicić wykładnię przepisów prawa regulujących e-administrację, które są znacznie zróżnicowane.

Słowa kluczowe

środek komunikacji elektronicznej, e-administracja, system teleinformatyczny, bezpieczeństwo informacji

Abstract

The principle of security of e-government is the principle of law, which serves lawmaking and exercise of law in connection with the administration and use of ICT systems and means of electronic communication. The objective of ensuring safety of e-government is the protection of stored and transmitted information. This principle allows unifying the interpretation of laws regulating e-government, which are significantly varied.

Keywords

means of electronic communication, e-government, ICT systems, safety of information

1. Wstęp

Rozwój e-administracji jest warunkowany stworzeniem i utrzymaniem poczucia zaufania wśród pracowników administracji publicznej, obywateli i przedsiębiorców względem używanej technologii informacyjno-komunikacyjnej (ICT – *Information and Communication Technologies*), w tym systemów teleinformatycznych i środków komunikacji elektronicznej[1]. E-administracja jest narzędziem komunikacji pomiędzy tymi podmiotami służącym poprawie jakości działań wykonywanych przez organy ad-

[1] Zob. A. Pawluczuk, P. Drożdżewicz, E. Grudzińska, K. Hołubowicz, *Strony internetowe urzędów gmin jako element wsparcia e-administracji w gminie*, „Samorząd Terytorialny" 2014, nr 5, s. 36–37. Bezpieczeństwo jest jednym z kryteriów wyboru technologii informacyjno-komunikacyjnej przez obywateli

ministracji publicznej[2]. Celem opracowania jest wykazanie, że zasada zapewnienia bezpieczeństwa w e-administracji, jako zasada prawa, ma na celu stosowanie wysokiej jakości warunków i wymagań technicznych i organizacyjnych dla sprawnej ochrony przekazywanych oraz przechowywanych informacji.

2. Zasada zapewnienia bezpieczeństwa w e-administracji jako zasada prawa

Zasada zapewnienia bezpieczeństwa w e-administracji jest zasadą prawa mającą wpływ na stanowienie i stosowanie prawa, w tym wykładnię przepisów regulujących administrowanie systemami teleinformatycznymi i środkami komunikacji elektronicznej oraz ich użytkowanie. Zasada zapewnienia bezpieczeństwa w e-administracji jest zasadą prawa o opisowym charakterze[3], ponieważ jej treść można wyprowadzić z szeregu norm prawnych zawartych m.in. w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne[4], ustawie o ochronie danych osobowych[5], w innych ustawach oraz wielu rozporządzeniach[6]. Zgodnie z tą zasadą administratorzy i użytkownicy systemów teleinformatycznych i środków komunikacji elektronicznej powinni wykonywać czynności o charakterze technicznym i organizacyjnym, w celu ochrony informacji publicznej oraz prywatnej[7]. Przepisy prawne dotyczące tych systemów oraz środków komunikacji powinny zatem być stanowione oraz interpretowane w sposób zapewniający bezpieczeństwo tych informacji[8]. Zasada ta nie ma absolutnego charakteru,

oraz przedsiębiorców. Zob. K. Kościński, *Podatnik jako użytkownik i współtwórca usług elektronicznej administracji podatkowej*, „Przegląd Prawa Publicznego" 2010, nr 10, s. 55–56.

[2] M. Stachowicz, Sz. Mamrot, *Standaryzacja jako czynnik optymalizacji usług świadczonych przez administrację publiczną*, „Samorząd Terytorialny" 2015, nr 5, s. 67.

[3] Problematykę zasad prawa o charakterze opisowym przedstawiła S. Wronkowska, *System prawny a porządek prawny i ład społeczny*, [w:] S. Wronkowska, Z. Ziembiński (red.), *Zarys teorii prawa*, Ars boni et aequi, Poznań 1997, s. 187.

[4] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2014 r., poz. 1114 ze zm.).

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922), dalej u.o.d.o.

[6] Przepisy prawne, z których wywiedziono zasadę zapewnienia bezpieczeństwa w e-administracji, są wyrażone m.in. w aktach prawnych powołanych w kolejnych przypisach tego opracowania.

[7] Nauka prawa administracyjnego podkreśla duże znaczenie bezpieczeństwa informacji przechowywanych w systemach teleinformatycznych lub przekazywanych za pośrednictwem środków komunikacji elektronicznej. Zob. B. Michalak, *Bezpieczeństwo informacji w rejestrach medycznych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2010, z. 2, s. 145–146.

[8] Problematykę znaczenia zasad prawa dla procesu stanowienia oraz stosowania prawa przedstawiła S. Wronkowska, *System prawny…*, s. 188.

ponieważ zabezpieczenie informacji nie może uniemożliwiać lub znacznie utrudniać do nich dostępu lub ich modyfikacji przez osoby uprawnione[9].

3. Sfery bezpieczeństwa informacji w e-administracji

Zapewnienie bezpieczeństwa w e-administracji obejmuje dwie sfery: przekazywanie i przechowywanie informacji. Bezpieczeństwo przekazania informacji jest gwarantowane przez warunki i wymagania techniczne dotyczące środków komunikacji elektronicznej, które związane są z trzema kierunkami komunikacji: do pracowników administracji publicznej (G2G – *government to government*), do obywateli (G2C – *government to citizen*) oraz do przedsiębiorców (G2B – *government to business*)[10]. Bezpieczeństwo przechowywania informacji jest związane m.in. z wymaganiami technicznymi dla rejestrów publicznych[11]. Podmiotami zabezpieczającymi przechowywanie informacji są administratorzy systemów teleinformatycznych, którymi są organy administracji publicznej oraz inne podmioty wykonujące zadania publiczne[12].

---

[9] M. Błażewski, *Wartości w e-administracji i ich wyważenie*, [w:] J. Zimmermann, *Aksjologia prawa administracyjnego*, Wolters Kluwer, Warszawa 2017, s. 205-206. Autor przedstawia problematykę wyważenia powszechności i bezpieczeństwa elektronicznej administracji.

[10] B. Kasprzyk, *Aspekty funkcjonowania e-administracji dla jakości życia obywateli*, [w:] M.G. Woźniak, *Nierówności społeczne a wzrost gospodarczy. Społeczeństwo informacyjne – regionalne aspekty rozwoju*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2011, s. 343–344; E. Ziemba, T. Papaj, J. Będkowski, *Egzemplifikacja e-government w Polsce – analiza porównawcza SEKAP i ePUAP*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29, s. 430.

[11] Wymagania techniczne mające zapewnić bezpieczeństwo przechowania informacji na rejestrach publicznych prowadzonych z wykorzystaniem systemów teleinformatycznych zostały przedstawione w przypisach do dwóch fragmentów tego opracowania, to jest: 1. bezpieczeństwo informacji przekazywanej za pośrednictwem systemów teleinformatycznych oraz 2. środki zapewnienia bezpieczeństwa informacji.

[12] W świetle art. 3 ust. 1 i art. 3 ust. 2 pkt 1 w zw. z art. 7 pkt 4 u.o.d.o. administratorem danych może być organ państwowy, organ samorządu terytorialnego, państwowa lub komunalna jednostka organizacyjna oraz podmiot niepubliczny realizujący zadania publiczne. Zgodnie z wykładnią celowościową art. 7 pkt 2a u.o.d.o. przetwarzanie danych przez ich administratora może odbywać się w systemie teleinformatycznym. Na takie rozumienie tych przepisów wskazuje nauka prawa. Zdaniem A. Drozda na podmioty odpowiedzialne za zapewnienie bezpieczeństwa informacji został nałożony także obowiązek ochrony danych osobowych w prowadzonych przez nie systemach teleinformatycznych. Na zapewnienie bezpieczeństwa danych w tych systemach składa się m.in. stosowanie środków technicznych i organizacyjnych uniemożliwiających nieuprawnione przetwarzanie danych. Zob. A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisów*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2007, s. 19–20, 65. Jak wskazuje I. Zgoliński, aktualne przepisy ustawy o ochronie danych odnoszą się do pojęcia systemu teleinformatycznego w znaczeniu ścisłym, czyli związanym z przetwarzaniem danych w drodze elektronicznej. Zob. I. Zgoliński, *Komentarz do art. 7*, [w:] I. Zgoliński, I. Zduński (red.), *Praktyczny komentarz do ustawy o ochronie danych osobowych*, Wydawnictwo Kujawsko-Pomorskiej Szkoły Wyższej, Bydgoszcz 2013, s. 44. Zdaniem M. Ganczar ochrona danych przez organy administracji publicznej odnosi się m.in. do rejestrów publicznych, które są prowadzone przez te organy. Szczególna potrzeba ochrony danych ma miejsce w odniesieniu do systemów teleinformatycznych, w przypadku których istnieje znaczne potencjalne niebezpieczeństwo nieprawidłowego wyprowadzenia tych danych ze zbioru znajdującego się w tych systemach. Zob. M. Ganczar, *Obowiązki administracji publicznej w za-*

Przepisy prawa określają jedynie szczegółowe cele i ramy dla warunków i wymagań organizacyjnych i technicznych dla środków komunikacji elektronicznej oraz systemów teleinformatycznych.

Warunki organizacyjno-techniczne pobierania i gromadzenia danych są określone przez przepisy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[13]. Przepisy szczególne odwołują się także, w sytuacjach nieuregulowanych przez powyższe wymagania, do norm pozaprawnych, w tym do norm ISO[14]. Administrator systemu teleinformatycznego posiada częściową swobodę określania ram ochrony systemu teleinformatycznego. Może on dookreślać regulacje prawne m.in. za pomocą systemu bezpieczeństwa informacji[15].

Przepisy prawa oraz normy pozaprawne mają na celu zapewnienie wysokiego standardu przesyłania oraz przechowywania informacji, w tym zapewnienie ich rzetelności,

kresie ochrony danych osobowych, [w:] G. Szpor (red.), *Ochrona danych osobowych. Skuteczność regulacji*, Municipium, Warszawa 2009, s. 114, 115.

Także inne przepisy prawne wskazują, że część systemów teleinformatycznych administrowanych przez podmioty prywatne służy wykonywaniu zadań publicznych. Systemy te pozwalają prowadzić m.in. przez lekarza weterynarii rejestru psów zaszczepionych przeciwko wściekliźnie (rozporządzenie Ministra Rolnictwa i Rozwoju Wsi z dnia 28 czerwca 2004 r. w sprawie wzoru i szczegółowego sposobu prowadzenia rejestru psów zaszczepionych przeciwko wściekliźnie oraz wzoru zaświadczenia o szczepieniu psa przeciwko wściekliźnie, Dz. U. Nr 160, poz. 1672).

[13] Zgodnie z § 4 ust. 5 rozporządzenia Ministra Zdrowia z dnia 6 czerwca 2013 r. w sprawie Systemu Ewidencji Zasobów Ochrony Zdrowia (Dz. U., poz. 671), dalej r.z.o.z., System Ewidencji Zasobów Ochrony Zdrowia, w zakresie warunków organizacyjno-technicznych gromadzenia i pobierania danych, powinien być zgodny z warunkami określonymi w przepisach ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. W świetle § 4 ust. 2 rozporządzenia Ministra Zdrowia z dnia 7 marca 2016 r. w sprawie Rejestru Medycznie Wspomaganej Prokreacji (Dz. U., poz. 316), dalej r.r.m.w.p., Minister Zdrowia, prowadząc Rejestr Medycznie Wspomaganej Prokreacji, opracowuje, wdraża, nadzoruje, utrzymuje oraz modyfikuje system zarządzania bezpieczeństwem informacji zgodnie z przepisami ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

[14] § 4 ust. 5 r.z.o.z.; § 4 ust. 2 rozporządzenia Ministra Zdrowia z dnia 19 kwietnia 2013 r. w sprawie Systemu Rejestru Usług Medycznych Narodowego Funduszu Zdrowia (Dz. U., poz. 514).

[15] § 4 ust. 2 r.r.m.w.p.; § 5 ust. 2 rozporządzenia Ministra Zdrowia z dnia 29 sierpnia 2016 r. w sprawie Polskiego Rejestru Wrodzonych Wad Rozwojowych (Dz. U., poz. 1383); § 4 ust. 2 rozporządzenia Ministra Zdrowia z dnia 4 marca 2016 r. w sprawie Ogólnopolskiego Rejestru Ostrych Zespołów Wieńcowych (Dz. U., poz. 320); § 4 ust. 2 rozporządzenia Ministra Zdrowia z dnia 23 marca 2016 r. w sprawie Rejestru Nowotworów Niezłośliwych Dużych Gruczołów Ślinowych (Dz. U., poz. 404), dalej r.r.n.n. Nauka prawa, w części dotyczącej ochrony danych osobowych, wskazuje, że celem zapewnienia bezpieczeństwa danych osobowych przetwarzanych za pomocą systemów teleinformatycznych jest zapewnienie optymalnego poziomu bezpieczeństwa całości danych w organizacji, w tym wypełnienie dyspozycji ustawowych oraz przeprowadzenie kontroli przetwarzania tych danych. Zob. T.A.J. Banyś, J. Łuczak, *Zabezpieczenie danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak (red.), *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, Difin, Warszawa 2016, s. 139.

kompletności[16], integralności[17] oraz aktualności[18], jak również ochrony informacji poufnych[19] i prywatnych przed ich nieupoważnionym udostępnieniem[20].

Określenie w przepisach prawa celów i ram dla warunków i wymagań organizacyjnych i technicznych pozwala podmiotom odpowiedzialnym za zapewnienie bezpieczeństwa dostosowanie się do zmiennych uwarunkowań społecznych oraz rozwoju technologii, dzięki czemu możliwe jest zachowanie wysokich standardów bezpieczeństwa, czyli takich, które odpowiadają w sposób optymalny aktualnym zagrożeniom.

4. Bezpieczeństwo informacji przekazywanej i przechowywanej za pośrednictwem systemów teleinformatycznych

Zasada zapewnienia bezpieczeństwa w e-administracji obejmuje ciągłą ochronę procesu przekazywania i przechowywania informacji za pośrednictwem systemów teleinformatycznych i środków komunikacji elektronicznej[21]. Ingerencja w proces przeka-

[16] Zgodnie z art. 34 ust. 1 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t.j. Dz. U. z 2016 r., poz. 963 ze zm.) Zakład Ubezpieczeń Społecznych ma obowiązek zapewnić rzetelność i kompletność informacji zgromadzonych na kontach ubezpieczeniowych i na kontach płatników składek.

[17] Przepisy prawa częściowo określają obowiązek zapewnienia integralności przechowywanych danych. Zgodnie z § 4 ust. 2 rozporządzenia Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. Nr 205, poz. 1692 ze zm.), dalej r.u.r.p., podmiot, któremu udostępniono dane zgromadzone w rejestrze publicznym, odpowiada m.in. za integralność zgromadzonych danych.

[18] Przepisy prawa częściowo nakładają na administratorów systemów teleinformatycznych obowiązek aktualizacji przechowywanych informacji. Zgodnie z § 3 ust. 3 rozporządzenia Ministra Zdrowia z dnia 25 kwietnia 2006 r. w sprawie prowadzenia krajowego rejestru przeszczepień (Dz. U. Nr 76, poz. 542), dalej r.k.r.p., krajowy rejestr przeszczepień powinien umożliwić aktualizację danych, identyfikując czas i osobę dokonującą aktualizacji oraz określanie danych sprzed aktualizacji. W świetle § 5 ust. 2 pkt 1 rozporządzenia Ministra Środowiska z dnia 20 grudnia 2012 r. w sprawie sposobu prowadzenia przez marszałka województwa rejestru wyrobów zawierających azbest (Dz. U., poz. 25), dalej r.r.w.a., system teleinformatyczny zapewniający prowadzenie rejestru wyrobów zawierających azbest powinien umożliwiać aktualizację informacji dotyczących województw, powiatów, gmin, miejscowości i ulic zgodnie z rejestrem TERYT.

[19] Zgodnie z § 2 ust. 3 rozporządzenia Ministra Zdrowia z dnia 5 kwietnia 2012 r. w sprawie rejestru lekarzy odbywających szkolenie specjalizacyjne (Dz. U., poz. 415), dalej r.r.l., przekazanie danych do rejestru lekarzy odbywających szkolenie specjalizacyjne powinno gwarantować ich poufność. W świetle § 7 rozporządzenia Ministra Zdrowia z dnia 20 października 2015 r. w sprawie rejestru dawców komórek rozrodczych i zarodków (Dz. U., poz. 1745), dalej r.r.d.k., przekazanie drogą elektroniczną danych do rejestru dawców komórek rozrodczych i zarodków powinno nastąpić za pomocą połączenia gwarantującego poufność przekazanych danych.

[20] W świetle § 6 ust. 4 rozporządzania Rady Ministrów z dnia 17 stycznia 2013 r. w sprawie zintegrowanego systemu informacji o nieruchomościach (Dz. U., poz. 249), przechowanie danych osobowych w zintegrowanym systemie informacji o nieruchomościach odbywa się zgodnie z zasadami określonymi w przepisach szczególnych dotyczącymi wysokiego poziomu bezpieczeństwa. Zgodnie z § 4 r.k.r.p. dane gromadzone w krajowym rejestrze przeszczepień powinny być przechowywane w sposób zapewniający ochronę danych osobowych biorcy przed osobami nieuprawnionymi.

[21] Jak słusznie wskazał A. Drozd, odnosząc się do problematyki ochrony danych, zapewnienie bezpieczeństwa powinno mieć dynamiczny charakter, czyli powinno być właściwe co do zmieniających się zagrożeń. Zob. A. Drozd, *Ustawa o ochronie danych…,* s. 249. Podobnie uważa I. Zduński, który wskazuje, że systemy teleinformatyczne służące ochronie danych powinny być ciągle udoskonalane. Zob. I. Zduński, *Ko-*

zywania oraz przechowywania informacji może być związana z czynnikami przypadkowymi lub umyślnie wywołanymi przez użytkowników lub osoby trzecie[22]. Organy administracji publicznej oraz inne podmioty wykonujące zadania publiczne, które zarządzają systemami teleinformatycznymi i środkami komunikacji elektronicznej, powinny zapewnić ochronę przekazywanych i przechowywanych informacji przed: utratą[23], usunięciem[24], zniszczeniem[25], uszkodzeniem[26], zatarciem[27], zniekształceniem[28], nieuprawnioną zmianą[29] oraz wykorzystaniem niezgodnie z celem[30]. Zabezpieczenie systemu teleinformatycznego dotyczy także ochrony przed nieuprawnioną ingerencją osób trzecich obejmującej uniemożliwienie m.in. dostępu do nich przez osoby nieupoważnione[31], w tym kradzieży danych[32] oraz dokonanie wpisu przez osoby nieuprawnione do rejestru publicznego prowadzonego elektronicznie[33].

5. Środki zapewnienia bezpieczeństwa informacji

Przepisy prawa wprowadzają szereg środków zapewnienia bezpieczeństwa informacji przekazywanej lub przechowywanej za pomocą systemów teleinformatycznych

mentarz do art. 36, [w:] I. Zgoliński, I. Zduński (red.), *Praktyczny komentarz…*, s. 155. Na potrzebę ciągłego podejmowania czynności zapewniających bezpieczeństwo ochrony danych, m.in. w systemach teleinformatycznych, wskazują także T.A.J. Banyś oraz J. Łuczak, *Zabezpieczenie danych osobowych…*, s. 140.

[22] Zgodnie z § 6 pkt 2 r.r.d.k. ochrona danych zawartych w rejestrze dawców komórek rozrodczych i zarodków powinna być chroniona przed przypadkowym lub nieuprawnionym zniszczeniem.

[23] Art. 6 ustawy z dnia 18 grudnia 2003 r. o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności (t.j. Dz. U. z 2015 r., poz. 807 ze zm.), dalej u.k.s.e.p.; § 4 ust. 1 pkt 1 rozporządzenia Ministra Gospodarki z dnia 10 maja 2013 r. w sprawie ewidencji obrotu towarami o znaczeniu strategicznym (Dz. U., poz. 619), dalej r.e.o.t.; art. 36 ust. 1 u.o.d.o.

[24] § 4 ust. 3 rozporządzenia Ministra Zdrowia z dnia 25 kwietnia 2006 r. w sprawie centralnego rejestru niespokrewnionych dawców szpiku i krwi pępowinowej (Dz. U. Nr 79, poz. 557 ze zm.), dalej r.c.r.d.s.; § 4 rozporządzenia Ministra Środowiska z dnia 23 lipca 2009 r. w sprawie sposobu prowadzenia przez marszałka województwa rejestru dotyczącego PCB (Dz. U. Nr 124, poz. 1034), dalej r.p.c.b.; § 5 ust. 2 pkt 4 r.r.w.a.

[25] § 4 ust. 1 pkt 2 r.e.o.t.; § 6 pkt 2 r.r.d.k.; art. 36 ust. 1 u.o.d.o.

[26] § 4 ust. 1 pkt 2 r.e.o.t.; art. 36 ust. 1 u.o.d.o.

[27] § 4 r.p.c.b.

[28] § 4 r.p.c.b.; § 5 ust. 2 pkt 4 r.r.w.a.; art. 36 ust. 1 u.o.d.o.

[29] § 4 ust. 1 r.u.r.p.

[30] § 4 ust. 1 pkt 3 r.e.o.t.

[31] § 3 ust. 7 r.r.l.; § 7 ust. 2 rozporządzenia Ministra Sprawiedliwości z dnia 19 grudnia 2016 r. w sprawie rejestru funduszy inwestycyjnych (Dz. U., poz. 2188); § 6 pkt 1 r.r.d.k.; § 3 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych z dnia 24 grudnia 2014 r. w sprawie trybu i terminów przekazywania danych pomiędzy rejestrem PESEL a rejestrami centralnymi (Dz. U., poz. 1942); § 4 ust. 1 r.r.n.n.; § 5 r.c.r.d.s.; § 2 ust. 2 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 28 czerwca 2001 r. w sprawie określenia wzorów ewidencji i rejestrów prowadzonych w postępowaniu w sprawie repatriacji oraz sposobu przetwarzania danych zawartych w tych ewidencjach i rejestrach (Dz. U. Nr 73, poz. 778 ze zm.); § 4 ust. 1 pkt 4 r.e.o.t.; art. 6 u.k.s.e.p.; art. 36 ust. 1 u.o.d.o.

[32] § 4 ust. 1 pkt 3 r.e.o.t.; art. 36 ust. 1 u.o.d.o.

[33] § 2 rozporządzenia Ministra Kultury i Dziedzictwa Narodowego z dnia 26 stycznia 2012 r. w sprawie sposobu prowadzenia i udostępniania rejestru instytucji kultury (Dz. U., poz. 189).

oraz środków komunikacji elektronicznej. Środki te są zróżnicowane ze względu na rodzaj chronionej informacji. Prawodawca, stanowiąc prawo, powinien uwzględnić zasadę zapewnienia bezpieczeństwa w e-administracji poprzez wprowadzenie unormowań przewidujących stosowanie odpowiednich środków. Środkami zapewnienia bezpieczeństwa informacji są m.in. potwierdzenie tożsamości, weryfikowanie, monitoring systemów teleinformatycznych, szyfrowanie, zapewnienie kopii zapasowej oraz równorzędnych sposobów przekazywania danych.

Przekazanie danych organowi administracji publicznej wymaga potwierdzenia tożsamości podmiotu wysyłającego te dane. Przepisy prawa wprowadzają szeroki katalog środków potwierdzających tożsamość, zróżnicowany w zależności od rodzaju systemu teleinformatycznego oraz przekazywanych danych. Środkami potwierdzającymi tożsamość są: kwalifikowany podpis elektroniczny[34] oraz podpis potwierdzony profilem zaufanym ePUAP[35], jak również inny środek zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej[36]. Część systemów teleinformatycznych zakłada także możliwość przekazywania informacji poprzez nadanie użytkownikom tych systemów identyfikatora lub loginu oraz możliwości

[34] Kwalifikowany podpis elektroniczny jest wymagany np. w postępowaniu administracyjnym w kierunkach komunikacji G2B oraz G2C, w tym przy: przekazaniu pełnomocnictwa w formie elektronicznej (art. 33 § 2a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, t.j. Dz. U. z 2016 r., poz. 23 ze zm., dalej k.p.a.), uwierzytelnieniu odpisu pełnomocnictwa oraz odpisów innych dokumentów sporządzonych w formie dokumentu elektronicznego (art. 33 § 3a k.p.a.), składaniu wezwania dokonywanym w formie dokumentu elektronicznego (art. 54 § 2 k.p.a.), składaniu podania wniesionego w formie dokumentu elektronicznego (art. 63 § 3a pkt 1 k.p.a.), poświadczaniu zgodności z oryginałem odpisu dokumentu sporządzonego w formie dokumentu elektronicznego (art. 76a § 2a k.p.a.), wydaniu decyzji administracyjnej wydanej w formie dokumentu elektronicznego (art. 107 § 1 zd. 1 k.p.a.), wydaniu postanowienia sporządzonego w formie dokumentu elektronicznego (art. 124 § 1 k.p.a.), wydaniu zaświadczenia w formie dokumentu elektronicznego (art. 217 § 4 k.p.a.), sporządzeniu zawiadomienia w formie dokumentu elektronicznego (art. 238 § 1 k.p.a.). Kwalifikowany podpis elektroniczny jest wymagany także w związku z przekazaniem informacji w kierunku komunikacji G2G, w tym przy: składaniu przez wojewodę zgłoszenia do ministra właściwego do spraw administracji publicznej w celu dokonania wpisu do rejestru związków międzygminnych (art. 68 ust. 1d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, t.j. Dz. U. z 2016 r., poz. 446 ze zm.).

[35] Podpis potwierdzony profilem zaufanym ePUAP jest wymagany w kierunku komunikacji G2B oraz G2C, np. w postępowaniu administracyjnym oraz procedurach związanych z partycypacją społeczną, w tym: przekazaniu pełnomocnictwa w formie elektronicznej (art. 33 § 2a k.p.a.), uwierzytelnieniu odpisu pełnomocnictwa oraz odpisów innych dokumentów sporządzonych w formie dokumentu elektronicznego (art. 33 § 3a k.p.a.), składaniu podania wniesionego w formie dokumentu elektronicznego (art. 63 § 3a pkt 1 k.p.a.), poświadczaniu zgodności z oryginałem odpisu dokumentu sporządzonego w formie dokumentu elektronicznego (art. 76a § 2a k.p.a.), wnoszeniu uwag do projektu miejscowego planu zagospodarowania przestrzennego (art. 18 ust. 3 pkt 2 ustawy z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, t.j. Dz. U. z 2016 r., poz. 778 ze zm.). Zob. też I. Adamska, *Czy nowelizacja ustawy o informatyzacji i KPA zrewolucjonizuje e-administrację?*, „Czas Informatyzacji" 2010, nr 1, s. 6–7; S.P. Zalipski, *Są nowe akty wykonawcze do informatyzacji, czyli ePUAP-ką po łapkach*, „Czas Informatyzacji" 2011, nr 2, s. 75.

[36] Zgodnie z art. 63 § 3a pkt 1 k.p.a. podanie, które zostało wniesione w formie dokumentu elektronicznego, powinno być uwierzytelniane w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej.

wygenerowania hasła[37]. Przekazanie informacji jest wówczas warunkowane podaniem prawidłowego identyfikatora lub loginu i hasła przez osoby upoważnione przez użytkownika systemu teleinformatycznego[38].

Podmioty wykonujące zadania publiczne, które przechowują informacje w systemach teleinformatycznych, powinny umożliwić ich weryfikację z dokumentami będącymi podstawą wpisania tych informacji[39]. Organ administracji publicznej ma także obowiązek weryfikacji danych przechowywanych przez inny organ[40].

Część systemów teleinformatycznych monitoruje czynności związane z przekazywaniem oraz przechowywaniem danych. Monitoring obejmuje m.in. logowania, próby logowania, rejestrację czynności wykonywanych przez użytkowników[41] oraz wdrożone zabezpieczenia[42].

Dane przekazywane za pośrednictwem środków komunikacji elektronicznej są częściowo szyfrowane, jeżeli wymagają ochrony przed ujawnieniem względem osób trzecich. Organ administracji publicznej w tym celu wykorzystuje np. szyfrowany kanał komunikacyjny[43] lub przekazuje zaszyfrowane dane[44].

Regulacje dotyczące e-administracji nakładają na organy administracji publicznej oraz inne podmioty wykonujące zadania publiczne obowiązek stworzenia kopii zapasowej

[37] § 4 ust. 1 rozporządzenia Ministra Finansów z dnia 30 września 2014 r. w sprawie wniosków o wpis do rejestru agentów ubezpieczeniowych (Dz. U., poz. 1376); § 4 ust. 4 rozporządzenia Ministra Środowiska z dnia 8 stycznia 2016 r. w sprawie Centralnego Rejestru Operatorów Urządzeń i Systemów Ochrony Przeciwpożarowej (Dz. U., poz. 56), dalej r.c.r.s.o.p.

[38] § 4 ust. 3 r.r.l.

[39] § 3 ust. 3 r.e.o.t.

[40] Art. 14 ust. 2 pkt 2 ustawy z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (t.j . Dz. U. z 2016 r., poz. 476 ze zm.).

[41] § 8 pkt 1 rozporządzenia Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (Dz. U., poz. 1001 ze zm.). Zgodnie z art. 38 u.o.d.o. kontrolę nad ochroną danych osobowych w systemach teleinformatycznych prowadzi administrator danych. Zdaniem A. Drozda administrator danych ma swobodę w wyborze środka kontroli nad wprowadzeniem i przekazaniem danych. Środkiem takim może być rejestr udostępnień oraz właściwy dobór osób upoważnionych do przetwarzania danych. Zob. A. Drozd, *Ustawa o ochronie danych*…, s. 368. Podobnie uważa I. Zduński, który wskazuje, że kontrola nad przetwarzaniem danych m.in. w systemach teleinformatycznych polega głównie na badaniu poprawności przekazywania danych z i do zbioru. Zob. I. Zduński, *Komentarz do art. 38*, [w:] I. Zgoliński, I. Zduński (red*.), Praktyczny komentarz…*, s. 163. Takie samo zdanie przedstawia L. Kępa, który wskazuje, że kontrola dostępu do systemu teleinformatycznego obejmuje identyfikację użytkownika poprzez wymóg podania loginu oraz uwierzytelnienie użytkownika poprzez podanie hasła. Zob. L. Kępa, *Ochrona danych osobowych w praktyce*, Difin, Warszawa 2014, s. 244–251.

[42] § 3 pkt 2 r.c.r.s.o.p.

[43] § 2 pkt 8 rozporządzenia Ministra Zdrowia z dnia 3 października 2012 r. w sprawie opisu systemu teleinformatycznego, w którym jest prowadzony Rejestr Zezwoleń na Prowadzenie Hurtowni Farmaceutycznej (Dz. U., poz. 1118); § 10 ust. 1 rozporządzenia Ministra Finansów z dnia 18 września 2006 r. w sprawie prowadzenia rejestru pośredników ubezpieczeniowych oraz sposobu udostępniania informacji z tego rejestru (Dz. U. Nr 178, poz. 1316).

[44] § 2 ust. 3 r.r.l.

dla części informacji publikowanych w elektronicznych rejestrach publicznych[45]. Prawodawca wprowadza szerokie zróżnicowanie wymagań technicznych dla tej kopii. Kopia zapasowa może być zapisana na informatycznym nośniku danych[46], który będzie chronił informacje przed zatarciem[47], utratą[48], usunięciem[49] lub zniekształceniem[50]. Kopią zapasową mogą być także wydruki części danych przechowywane w postaci papierowej[51].

Przepisy prawa przewidują także możliwość przekazywania części danych z pominięciem elektronicznych środków komunikacji, gdy ich transfer jest niezbędny w krótkim terminie. Dane te mogą być przekazane m.in. za pośrednictwem telefaksu[52].

6. Zakończenie

Przepisy prawa regulujące przekazywanie i przechowywanie informacji za pośrednictwem systemów teleinformatycznych oraz środków komunikacji elektronicznej powinny być stanowione i stosowane, w tym interpretowane, zgodnie z zasadą zapewnienia bezpieczeństwa w e-administracji. Zasada ta ma duże znaczenie dla prawidłowego administrowania i użytkowania tych systemów i środków komunikacji ze względu ze znaczną liczbę aktów prawnych regulujących ten aspekt działania administracji publicznej. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne jedynie częściowo reguluje warunki i wymagania dla systemów teleinformatycznych i środków komunikacji elektronicznej. Znaczna część regulacji jest wyrażona w innych ustawach i rozporządzeniach, czego skutkiem jest m.in. zróżnicowanie szczegółowych celów ochrony informacji oraz środków zapewnienia bezpieczeństwa informacji. Pomimo tego zróżnicowania regulacje te pozwalają na zachowanie wysokiej jakości wymagań i warunków technicznych oraz organizacyjnych gwarantujących w sposób optymalny bezpieczeństwo w e-administracji.

---

[45] § 3 ust. 2 rozporządzenia Ministra Gospodarki z dnia 22 sierpnia 2012 r., w sprawie sposobu ewidencjonowania wprowadzonych do obrotu materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym (Dz. U., poz. 1008); § 3 ust. 3 r.e.o.t.; § 2 ust. 2 pkt 2 rozporządzenia Ministra Spraw Wewnętrznych z dnia 18 czerwca 2014 r. w sprawie centralnej ewidencji pojazdów (Dz. U., poz. 816); § 9 ust. 3 rozporządzenia Ministra Rozwoju i Finansów z dnia 21 grudnia 2016 r. w sprawie ewidencji i innych dokumentacji dotyczących wyrobów akcyzowych i znaków akcyzy (Dz. U., poz. 2257), dalej r.e.w.a.

[46] § 5 r.p.c.b.

[47] § 5 r.p.c.b.

[48] § 9 ust. 3 r.e.w.a.

[49] § 5 r.p.c.b.

[50] § 5 r.p.c.b.; § 9 ust. 3 r.e.w.a.

[51] § 2 ust. 2 r.c.r.d.s.; § 2 ust. 1 pkt 1 lit. d rozporządzenia Ministra Rolnictwa i Rozwoju Wsi z dnia 28 kwietnia 2008 r. w sprawie dodatkowych wymagań, jakie powinny spełniać związki hodowców lub inne podmioty ubiegające się o prowadzenie rejestrów zwierząt gospodarskich innych niż świnie (Dz. U. Nr 84, poz. 513).

[52] Art. 202b ust. 3 ustawy z dnia 3 lipca 2002 r. Prawo lotnicze (t.j. Dz. U. z 2016 r., poz. 605 ze zm.).

Bibliografia

Wykaz źródeł prawa

Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2016 r., poz. 23 ze zm.).

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2016 r., poz. 446 ze zm.).

Ustawa z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (t.j. Dz. U. z 2016 r., poz. 476 ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r., poz. 922).

Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (t.j. Dz. U. z 2016 r., poz. 963 ze zm.).

Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (t.j. Dz. U. z 2016 r., poz. 605 ze zm.).

Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (t.j. Dz. U. z 2016 r., poz. 778 ze zm.).

Ustawa z dnia 18 grudnia 2003 r. o krajowym systemie ewidencji producentów, ewidencji gospodarstw rolnych oraz ewidencji wniosków o przyznanie płatności (t.j. Dz. U. z 2015 r., poz. 807 ze zm.).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2014 r., poz. 1114 ze zm.).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 28 czerwca 2001 r. w sprawie określenia wzorów ewidencji i rejestrów prowadzonych w postępowaniu w sprawie repatriacji oraz sposobu przetwarzania danych zawartych w tych ewidencjach i rejestrach (Dz. U. Nr 73, poz. 778 ze zm.).

Rozporządzenie Ministra Rolnictwa i Rozwoju Wsi z dnia 28 czerwca 2004 r. w sprawie wzoru i szczegółowego sposobu prowadzenia rejestru psów zaszczepionych przeciwko wściekliźnie oraz wzoru zaświadczenia o szczepieniu psa przeciwko wściekliźnie (Dz. U. Nr 160, poz. 1672).

Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz. U. Nr 205, poz. 1692 ze zm.).

Rozporządzenie Ministra Zdrowia z dnia 25 kwietnia 2006 r. w sprawie prowadzenia krajowego rejestru przeszczepień (Dz. U. Nr 76, poz. 542).

Rozporządzenie Ministra Zdrowia z dnia 25 kwietnia 2006 r. w sprawie centralnego rejestru niespokrewnionych dawców szpiku i krwi pępowinowej (Dz. U. Nr 79, poz. 557 ze zm.).

Rozporządzenie Ministra Finansów z dnia 18 września 2006 r. w sprawie prowadzenia rejestru pośredników ubezpieczeniowych oraz sposobu udostępniania informacji z tego rejestru (Dz. U. Nr 178, poz. 1316).

Rozporządzenie Ministra Rolnictwa i Rozwoju Wsi z dnia 28 kwietnia 2008 r. w sprawie dodatkowych wymagań, jakie powinny spełniać związki hodowców lub inne podmioty ubiegające się o prowadzenie rejestrów zwierząt gospodarskich innych niż świnie (Dz. U. Nr 84, poz. 513).

Rozporządzenie Ministra Środowiska z dnia 23 lipca 2009 r. w sprawie sposobu prowadzenia przez marszałka województwa rejestru dotyczącego PCB (Dz. U. Nr 124, poz. 1034).

Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 26 stycznia 2012 r. w sprawie sposobu prowadzenia i udostępniania rejestru instytucji kultury (Dz. U., poz. 189).

Rozporządzenie Ministra Zdrowia z dnia 5 kwietnia 2012 r. w sprawie rejestru lekarzy odbywających szkolenie specjalizacyjne (Dz. U., poz. 415).

Rozporządzenie Ministra Gospodarki z dnia 22 sierpnia 2012 r., w sprawie sposobu ewidencjonowania wprowadzonych do obrotu materiałów wybuchowych, broni, amunicji oraz wyrobów i technologii o przeznaczeniu wojskowym lub policyjnym (Dz.U., poz. 1008).

Rozporządzenie Ministra Zdrowia z dnia 3 października 2012 r. w sprawie opisu systemu teleinformatycznego, w którym jest prowadzony Rejestr Zezwoleń na Prowadzenie Hurtowni Farmaceutycznej (Dz. U., poz. 1118).

Rozporządzenie Ministra Środowiska z dnia 20 grudnia 2012 r. w sprawie sposobu prowadzenia przez marszałka województwa rejestru wyrobów zawierających azbest (Dz. U., poz. 25).

Rozporządzanie Rady Ministrów z dnia 17 stycznia 2013 r. w sprawie zintegrowanego systemu informacji o nieruchomościach (Dz. U., poz. 249).

Rozporządzenie Ministra Zdrowia z dnia 19 kwietnia 2013 r. w sprawie Systemu Rejestru Usług Medycznych Narodowego Funduszu Zdrowia (Dz. U., poz. 514).

Rozporządzenie Ministra Gospodarki z dnia 10 maja 2013 r. w sprawie ewidencji obrotu towarami o znaczeniu strategicznym (Dz. U., poz. 619).

Rozporządzenie Ministra Zdrowia z dnia 6 czerwca 2013 r. w sprawie Systemu Ewidencji Zasobów Ochrony Zdrowia (Dz. U., poz. 671).

Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie opisu, minimalnej funkcjonalności oraz warunków organizacyjno-technicznych funkcjonowania Platformy Udostępniania On-Line Usług i Zasobów Cyfrowych Rejestrów Medycznych oraz Elektronicznej Platformy Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (Dz. U., poz. 1001 ze zm.).

Rozporządzenie Ministra Spraw Wewnętrznych z dnia 18 czerwca 2014 r. w sprawie centralnej ewidencji pojazdów (Dz. U., poz. 816).

Rozporządzenie Ministra Finansów z dnia 30 września 2014 r. w sprawie wniosków o wpis do rejestru agentów ubezpieczeniowych (Dz. U., poz. 1376).

Rozporządzenie Ministra Spraw Wewnętrznych z dnia 24 grudnia 2014 r. w sprawie trybu i terminów przekazywania danych pomiędzy rejestrem PESEL a rejestrami centralnymi (Dz. U., poz. 1942).

Rozporządzenie Ministra Zdrowia z dnia 20 października 2015 r. w sprawie rejestru dawców komórek rozrodczych i zarodków (Dz. U., poz. 1745).

Rozporządzenie Ministra Środowiska z dnia 8 stycznia 2016 r. w sprawie Centralnego Rejestru Operatorów Urządzeń i Systemów Ochrony Przeciwpożarowej (Dz. U., poz. 56).

Rozporządzenie Ministra Zdrowia z dnia 4 marca 2016 r. w sprawie Ogólnopolskiego Rejestru Ostrych Zespołów Wieńcowych (Dz. U., poz. 320).

Rozporządzenie Ministra Zdrowia z dnia 7 marca 2016 r. w sprawie Rejestru Medycznie Wspomaganej Prokreacji (Dz. U., poz. 316).

Rozporządzenie Ministra Zdrowia z dnia 23 marca 2016 r. w sprawie Rejestru Nowotworów Niezłośliwych Dużych Gruczołów Ślinowych (Dz. U., poz. 404).

Rozporządzenie Ministra Zdrowia z dnia 29 sierpnia 2016 r. w sprawie Polskiego Rejestru Wrodzonych Wad Rozwojowych (Dz. U., poz. 1383).

Rozporządzenie Ministra Sprawiedliwości z dnia 19 grudnia 2016 r. w sprawie rejestru funduszy inwestycyjnych (Dz. U., poz. 2188).

Rozporządzenie Ministra Rozwoju i Finansów z dnia 21 grudnia 2016 r. w sprawie ewidencji i innych dokumentacji dotyczących wyrobów akcyzowych i znaków akcyzy (Dz. U., poz. 2257).

Literatura

Adamska I., *Czy nowelizacja ustawy o informatyzacji i KPA zrewolucjonizuje e-administrację?*, „Czas Informatyzacji" 2010, nr 1.

Banyś T.A.J., Łuczak J., *Zabezpieczenie danych osobowych*, [w:] T.A.J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak (red.), *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, Difin, Warszawa 2016.

Błażewski M., *Wartości w e-administracji i ich wyważenie*, [w:] J. Zimmermann, *Aksjologia prawa administracyjnego*, Wolters Kluwer, Warszawa 2017.

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisów*, Wydawnictwo Prawnicze LexisNexis, Warszawa 2007.

Ganczar M., *Obowiązki administracji publicznej w zakresie ochrony danych osobowych*, [w:] G. Szpor (red.), *Ochrona danych osobowych. Skuteczność regulacji*, Municipium, Warszawa 2009.

Kasprzyk B., *Aspekty funkcjonowania e-administracji dla jakości życia obywateli*, [w:] M.G. Woźniak, *Nierówności społeczne a wzrost gospodarczy. Społeczeństwo informacyjne – regionalne aspekty rozwoju*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2011.

Kępa L., *Ochrona danych osobowych w praktyce*, Difin, Warszawa 2014.

Kościński K., *Podatnik jako użytkownik i współtwórca usług elektronicznej administracji podatkowej*, „Przegląd Prawa Publicznego" 2010, nr 10.

Michalak B., *Bezpieczeństwo informacji w rejestrach medycznych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2010, z. 2.

Pawluczuk A., Drożdżewicz P., Grudzińska E., Hołubowicz K., *Strony internetowe urzędów gmin jako element wsparcia e-administracji w gminie*, „Samorząd Terytorialny" 2014, nr 5.

Stachowicz M., Mamrot Sz., *Standaryzacja jako czynnik optymalizacji usług świadczonych przez administrację publiczną*, „Samorząd Terytorialny" 2015, nr 5.

Wronkowska S., *System prawny a porządek prawny i ład społeczny*, [w:] S. Wronkowska, Z. Ziembiński (red.), *Zarys teorii prawa*, Ars boni et aequi, Poznań 1997.

Zalipski S.P., *Są nowe akty wykonawcze do informatyzacji, czyli ePUAP-ką po łapkach*, „Czas Informatyzacji" 2011, nr 2.

Zgoliński I., Zduński I. (red.), *Praktyczny komentarz do ustawy o ochronie danych osobowych*, Wydawnictwo Kujawsko-Pomorskiej Szkoły Wyższej, Bydgoszcz 2013.

Ziemba E., Papaj T., Będkowski J., *Egzemplifikacja e-government w Polsce – analiza porównawcza SEKAP i ePUAP*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29.