Czas informacji
Prawo nowych technologii • Informacja w administracji i gospodarce
ISSN 2081-6189
kwartalnik 2/3(11)/2012

Dystrybucja oprogramowania – modele, szanse i zagrożenia

Prawna regulacja dostępu do internetu a bezpieczeństwo polityczne
Agnieszka Jarzewicz

Elektroniczne dowody osobiste w Polsce – co dalej z projektem PL.ID
Mieczysław T. Starkowski

Wpływ e-usług na administrację publiczną
Ewa Modzelewska

Studium wykonalności projektu informatycznego w administracji
Dariusz Bogucki

Koncepcja rozwoju i modyfikacji ePUAP
Piotr Walesiak

Nowa unijna regulacja w zakresie danych osobowych
Damian Karwala

cpi
centrum promocji informatyki
www.cpi.com.pl

NAUKA

4 **Prawna regulacja dostępu do Internetu a bezpieczeństwo polityczne. O dylemacie dyktatora z perspektywy polityki medialnej na Kubie**
Agnieszka Jarzewicz

21 **Metoda wartości wypracowanej (Earned Value)**
Dariusz Bogucki

30 **Uwagi o właściwości miejscowej sądu penitencjarnego w przedmiocie udzielenia zezwolenia na zastosowanie dozoru elektronicznego**
Agnieszka Zdanowska

36 **Wpływ e-usług na funkcjonowanie administracji publicznej**
Ewa Modzelewska

44 **Technologie komputerowe w perspektywie etycznej. Moralność w e-rzeczywistości - część II**
Mariusz Szynkiewicz

PUBLICYSTYKA I PRAKTYKA

56 **Elektroniczne dowody osobiste w Polsce – co dalej z projektem PL.ID**
Mieczysław T. Starkowski

63 **Trochę historii informatyzacji w kraju i na świecie – dlaczego wybuchła „wielka rewolucja" SOA**
Piotr Kociński

70 **O czym mówiono na imprezach ŚDSI 2012**

72 **Studium wykonalności projektu informatycznego w administracji - część I refleksji redaktora**
Dariusz Bogucki

80 **Koncepcja rozwoju i modyfikacji ePUAP**
Piotr Walesiak

85 **XVIII Forum Teleinformatyki 27-28 września br., Warszawa-Międzylesie**

87 **Wirtualne zakupy - czyli jak kupować w sklepach i na aukcjach internetowych?**
Katarzyna Czajkowska-Matosiuk

PRAWO

104 **Dystrybucja oprogramowania – modele, szanse i zagrożenia**
Marcin Maruta

109 **Podpis elektroniczny – nowa regulacje europejskie**
Michal Tabor

112 **Nowa unijna regulacja w zakresie danych osobowych – uwagi na temat projektu rozporządzenia z dnia 25 stycznia 2012 r. - część II**
Damian Karwala

121 **Wdrożenie systemów informatycznych w orzecznictwie Sądu Najwyższego**
Bohdan Widła

126 **Wymiana plików w sieciach P2P od strony prawnej**
Katarzyna Czajkowska-Matosiuk

STAŁE RUBRYKI

136 **Rewolucja technologiczna a dane osobowe**
Tomasz Soczyński

143 **Korzyści płynące ze stosowania strategii zarządzania komunikacją w projekcie**
Ewa Szczepańska

150 **Glosa do wyroku KIO z dnia 23 marca 2012 r., sygn. akt: KIO 467/12 oraz KIO 483/12**
Wojciech Kaliński

154 **Paradoks realnego rynku**
Edwin Bendyk

W kolejnym numerze:

- „*SMART CITIES AND COMMUNITIES*" *- ważna inicjatywa Komisji Europejskiej* - Dariusz Bogucki
- Metodologia projektowania e-usług publicznych - Ewa Modzelewska
- SEKAP - wywiad z osobą wdrażającą e-usługę - Ewa Modzelewska
- Innowacyjność procesowa e-usług publicznych - Ewa Modzelewska
- Epistemologiczne aspekty koncepcji Smogu informacyjnego (idea prof. Tadeusiewicza) - Mariusz Szynkiewicz
- Studium wykonalności projektu informatycznego w administracji – część II - Dariusz Bogucki
- Bezpieczny stadion - Mieczysław T. Starkowski
- Dokument elektroniczny. Czym jest, do czego służy i jakie są jego rodzaje - Katarzyna Czajkowska-Matosiuk
- Zakładanie działalności gospodarczej przez przedsiębiorców internetowych - Katarzyna Czajkowska-Matosiuk
- Zakładanie serwisu firmowego w Internecie - Katarzyna Czajkowska-Matosiuk
- Nowa unijna regulacja w zakresie danych osobowych – uwagi na temat projektu rozporządzenia z dnia 25 stycznia 2012 r. - część III - Damian Karwala
- Ochrona danych osobowych na gruncie Konstytucji RP - Robert Owerczuk

Wiesław Paluszyński redaktor naczelny
wieslaw.paluszynski@czasinformacji.pl

Kolejny zeszyt naszego czasopisma dociera do Państwa rąk po dość długiej przerwie. Jest to z tego względu łączony numer 2 i 3 z tego roku. Niestety i nas nie omijają objawy kryzysu. Kondycja finansowa naszych prenumeratorów spowodowała, że musieliśmy szukać dodatkowych partnerów, aby utrzymać Czas Informacji „na powierzchni". Dzięki wsparciu Polskiej Izby Informatyki i Telekomunikacji to przedsięwzięcie jest na dobrej drodze do stabilności. Jest to bezsprzecznie efekt wsparcia sektora firm teleinformatycznych, które rozumieją, że informacja jest podstawą do trafnych decyzji w informatyzacji sektora publicznego. Postanowiły wiec nośnik tej informacji, jakim jest nasze czasopismo wesprzeć. Co najważniejsze, wesprzeć nie z pozycji komunikacji marketingowej, ale wesprzeć, jako narzędzie umożliwiające dystrybucję do sektora publicznego informacji o charakterze naukowym, inżynierskim, prawnym i praktycznym. Dla nas to zobowiązanie, aby wykorzystać ten czas wsparcia na zbudowanie nowego kanału komunikacyjnego z naszymi czytelnikami, wykorzystującego e-narzędzia i niewielką odpłatność za elektroniczny dostęp do czasopisma. Mam nadzieję, że uda nam się to zrobić od nowego roku. W tym roku zaś planujemy jeszcze wydanie w czwartym kwartale tradycyjnego 4 numeru. Szczególnie serdecznie dziękujemy za okazaną pomoc i objęcie naszego czasopisma partnerstwem przez PIIT jej Prezesowi, dr inż. Wacławowi Iszkowskiemu.

Szkoda tylko, że wsparciem takiej platformy jaką jest Czas Informacji, nie jest w żadnej formie zainteresowana większość sektora publicznego, nawet w formie prenumeraty, czy kupna czasopisma, bo o innych nie śmiemy marzyć. To, że nasze czasopismo jest potrzebne, pokazuje zaś obecna sytuacja na rynku, gdzie ciągle królują prawdy obiegowe oparte na braku wiedzy. Ciągłe decyzje dotyczące informatyki, podejmowane są przez osoby mające w zakresie stosowania technik teleinformatycznych wiedzę ograniczoną lub żadną. Za to efekty ich decyzji, niosą dla wdrożeń technik informacyjnych niewyobrażalne straty, zarówno finansowe, jak i wizerunkowe. A przede wszystkim cofają nasz sektor publiczny cywilizacyjnie, szkodząc niejako przy okazji polskim firmom teleinformatycznym na rynku unijnym.

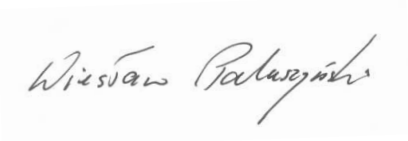
Aby przełamać tę kwadraturę koła i dostarczyć rzetelną wiedzę dotyczącą zasad korzystania z oprogramowania (co było spowodowane szeregiem publikacji prasowych wskazujących na całkowity brak wiedzy w tym zakresie) w czerwcu br. PIIT zorganizowała specjalną konferencję dotyczącą modeli dystrybucji oprogramowania. Konferencja przeznaczona była dla sektora publicznego, a także dla organów kontrolnych, które oceniając prawidłowość zakupu oprogramowania, powinny dysponować wiedzą w tym zakresie. Była to pierwsza z cyklu takich edukacyjnych konferencji zapowiedzianych przez Izbę. Podstawowe tezy dotyczące tej problematyk, będące efektem konferencji, omawia w tym numerze czasopisma mecenas Marcin Maruta.

We wrześniu jesteśmy partnerem kolejnego Forum Teleinformatyki. Dla jego uczestników polecamy szczególnie publikację Piotra Kocińskiego kończącą jego cykl o e-administracji, artykuł o koncepcji rozwoju i modyfikacji e-PUAP Piotra Walesiaka, czy bardzo ciekawe artykuły o charakterze ponad czasowym Piotra Szynkiewicza o etyce w informatyce II cześć i Agnieszki Jarzewicz o prawnych regulacjach dostępu do internetu w kontekście bezpieczeństwa politycznego (to taka szersza analiza po ACTA).

Mamy też nowe zapowiedzi regulacji prawnych ze strony UE. I tak - Michał Tabor omawia założenia nowych regulacji w zakresie identyfikacji i podpisu elektronicznego, a Damian Karwala nowe regulacje w zakresie ochrony danych osobowych.

Ponieważ jednym z powodów niewydolności wdrożeń projektów informatycznych jest złe planowanie, to odpowiedzialnym za to polecam publikację Dariusza Boguckiego o tym, jak poprawnie zrobić studium wykonalności projektu w administracji publicznej (i nie tylko). Szczególnie zaś dla realizujących projekty, polecam artykuł Ewy Szczepańskiej o korzyściach z właściwego zarządzania komunikacją w projekcie.

Poza tym trochę życia, więc Mieczysław Starkowski podążył tropem unieważnionego postępowania na blankiety elektronicznego dowodu osobistego i doszedł do… ściany. Ciekawym polecam, bo dowiedzą się, gdzie ta ściana się znajduje. Poza tym, jak zawsze stałe rubryki: o orzecznictwie w zamówieniach publicznych, ochronie danych osobowych i projektach informatycznych. Na zakończenie zeszytu Edwin Bendyk, narzekający na usługi i paradoksy realnego rynku. Warto poczytać, jak zawsze…



Prawne regulacje dostępu do Internetu a bezpieczeństwo polityczne. O dylemacie dyktatora z perspektywy polityki medialnej na Kubie

Agnieszka Jarzewicz

Artykuł wprowadza w dyskusję nad promocją legislacyjnej tendencji gwarantowania dostępu do Internetu w systemie praw człowieka. Głównym celem podjętych rozważań jest dookreślenie funkcji aksjotwórczej kluczowego osiągnięcia rewolucji informacyjnej, jakim jest Internet. Proponowana argumentacja stanowi wyraz potrzeby interdyscyplinarnego ujęcia opozycji determinizmu i instrumentalizm technologicznego. Egzemplifikacji empirycznej dostarcza polityka w dziedzinie mass mediów na Kubie. Analiza materiału badawczego zorientowana jest na wskazanie politycznego wymiaru efektu synergicznego, jaki do komunikacji masowej wnosi maszyna uchodząca za egalitarną platformę wolności informacji i wolności ekspresji. Przemyślenie politycznej funkcji informacji oraz informacyjnego aspektu bezpieczeństwa politycznego posłuży do zasygnalizowania potrzeby doprecyzowania bezpieczeństwa prawnego ze względu na holistycznie ujęte prawa człowieka.

Internet stanowi bezprecedensowy środek komunikacji społecznej nie tylko ze względu na istotne usprawnienia tego procesu pod względem zasięgu, szybkości i sprawności przekazu informacji, a także możliwości integrowania i stanowienia przekaźnika dla wszelkich innych mediów. To medium wyjątkowe ze względu na stopień interaktywności społecznej, którą umożliwia i oddziaływania synergiczne, które wprowadza do procesu komunikacji. Interakcyjny potencjał Internetu prowadzi do radykalnego przeformułowania roli uczestnika komunikacji masowej, ponieważ intensyfikuje przemienność ról komunikacyjnych. Uczestnik tego procesu przekształca się z pasywnego odbiorcy komunikatów, nadawanych tradycyjnymi kanałami jednokierunkowego przekazu, w aktywnego twórcę treści wymienianych za pomocą narzędzia komunikacji zdecentralizowanej. Intensyfikacja sprzężenia zwrotnego w relacji między nadawcą a odbiorcą w komunikacji masowej zapośredniczonej komputerowo jest czynnikiem wpływającym na treści i rezultaty komunikowania. Synergia charakteryzuje w najwyższym stopniu relację komunikacyjną opartą na sieciowych połączeniach maszyn dialektycznych, jakimi ze względu na sprzężenie zwrotne są komputery, w skali globalnej[1]. Efekt synergiczny komunikacji odbywającej się dzięki dostępowi do globalnej sieci komputerowej zachodzi w dwóch wymiarach: technologicznym i społecznym. Komunikacja w Internecie obejmuje przy tym synergię maszyny z maszyną, synergię człowieka z maszyną i synergię człowieka z człowiekiem.

Zwielokrotnione oddziaływania synergiczne medium cyfrowego wnoszą do komunikacji i badań nad tym procesem nową jakość. Doniosłość komunikacji zapośredniczonej komputerowo w skali globalnej wiąże się z modelem rozproszonej mocy obliczeniowej i jego wpływem na przebieg interakcji ludzkich, zarządzanie informacją i przemiany formacji społeczno-ekonomicznych[2]. Jednym z aspektów synergii jest

1 M. Szynkiewicz,*Rozwój technologii komputerowych w świetle filozoficznej refleksji nad nauką i techniką*, w: Czas informacji 3(8)/2011, s. 6 – 10.

2 J. Papińska-Kacperek, (red.), *Społeczeństwo*

polityczny wymiar nowych mediów jako część zasobów komunikacyjnych środowiska obliczeniowego. Uważa się dość powszechnie, że społeczno-polityczny wymiar efektu synergicznego komunikacji masowej o przebiegu sieciowym przyczynia się do rozwoju demokratyzacji i globalnego społeczeństwa informacyjnego. Oddziaływania synergiczne nabierają szczególnego znaczenia w roli źródła danych dla cybernetyki w związku z rozwojem Web 2.0. Skoro nowe media społeczne są areną uprawiania wolności słowa, ta zaś jest kluczowa dla demokracji i społeczeństwa informacyjnego, a Internet dostarcza potencjalnie egalitarnej platformy komunikacyjnej, to efektem komunikacji w Internecie, jak się twierdzi, jest liberalizacja sfery publicznej. Czy oznacza to, że demokratyczny potencjał rewolucji informacyjnej tkwi w technologii i przyczynia się do demokracji poprzez komunikacyjne wspieranie rozwoju społeczeństwa otwartego? Do jakiego stopnia przemiany ustrojowe mogą zależeć od rozwoju technologii informacyjno-komunikacyjnych?

Czy dostęp do Internetu powinien być prawem człowieka?

Gdy w 2011 r. Polska obchodziła dwudziestolecie nawiązania połączenia z Internetem, przedmiotem ożywionych dyskusji gremiów międzynarodowych stało się zagadnienie, czy dostęp do globalnego medium powinien być gwarantowany prawami człowieka. Wznowienie zagadnienia było reakcją na opublikowane w tamtym czasie dwa raporty poświęcone wolności słowa w Internecie. Jeden z nich, *Raport o promocji i ochronie prawa do wolności opinii i ekspresji*, wydany został w imieniu Rady Praw Człowieka Organizacji Narodów Zjednoczonych[3]. Jego autor, Frank La Rue wyraził przekonanie, że Internet przyczynia się do postępu społecznego, ponieważ ułatwia poszukiwanie informacji obiektywnych, przez co służy odkrywaniu prawdy. Internet cieszy się, w myśl raportu, największym uznaniem spośród mediów dzięki skuteczności w upowszechnianiu ideałów demokracji, zwiększaniu przejrzystości mechanizmów władzy i wspieraniu społeczeństwa obywatelskiego. W licznych komentarzach do tego raportu argumentuje się na rzecz uznania powszechnego dostępu do Internetu w kategoriach prawo-człowieczych. Żaden z paragrafów raportu nie zawiera explicite deklaracji, jakoby dostęp do Internetu, jak postulują jedni, czy wręcz sam Internet, jak chcą inni, należeć miał do systemu praw podstawowych. Frank La Rue odnotowuje przy tym fakt rozpoznania Internetu jako prawa podstawowego przez rządy niektórych z państw członkowskich ONZ, takich jak Estonia, Francja, Finlandia, a także Costa Rica. Ze swojej strony daje on wielokrotnie wyraz przekonaniu, że Internet stał się niezbędnym narzędziem realizacji prawa do wolności opinii i ekspresji, eo ipso korzystania z wielu innych wolności gwarantowanych systemem praw człowieka. Cyfrowe supermedium stanowi niejako *katalizator wolności*, dlatego La Rue postuluje traktowanie powszechnego dostępu do globalnej sieci komputerowej – zarówno w wymiarze infrastruktury technologicznej, jak i w sferze treści – jako priorytetu polityki rozwojowej. Omawiany raport promuje aktywność zorientowaną na wdrażanie Milenijnych Celów Rozwoju w zakresie światowego partnerstwa na rzecz transferu technologii informacyjnych i komunikacyjnych. Powszechność dostępu do Internetu zalecana jest przez wzgląd na korzyści społeczne, ekonomiczne i polityczne państw rozwijających się, jak też korzyści dla rozwoju ogólnoludzkiego.

3 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Przykładu radykalizacji promocji dostępu do Internetu w roli uniwersalnego standardu, który należy wdrażać w ramach prognozowania kierunków i realizowania rozwoju społeczeństwa informacyjnego dostarcza drugi ze wspomnianych raportów, zatytułowany *Wolność ekspresji w Internecie*. Dotyczy on regulacji prawnych w zakresie dostępu do Internetu na obszarze państw należących do Organizacji Bezpieczeństwa i Współpracy w Europie. Sporządzony został na zlecenie Dunji Mijatović, przewodniczącej OBWE ds. wolności mediów. Podczas oficjalnej prezentacji raportu, Mijatović podkreśliła, że ujęcie dostępu do Internetu w terminologii prawo-człowieczej powinno stać się kluczową tendencją legislacyjną w działaniach na rzecz wolności mediów w XXI wieku[4]. Autor raportu, Yaman Akdeniz, zawarł w tym zakresie wyraźne sformułowania normatywne: *Dostęp do Internetu powinien być uznany za prawo człowieka i rozpoznany jako implicytny względem prawa do wolności ekspresji i wolności informacji*[5]. *Każdy powinien mieć prawo do uczestniczenia w społeczeństwie informacyjnym, a do odpowiedzialności spoczywającej na państwach powinno należeć gwarantowanie obywatelom dostępu do Internetu*[6]. W myśl przedstawionej argumentacji, dostęp do Internetu daje się wywnioskować jako najważniejsza przesłanka dla lokalnego i globalnego rozwoju społeczeństwa informacyjnego, stanowiąc współcześnie niezbędny warunek korzystania z wolności uświęconych w Artykule 19 Powszechnej Deklaracji Praw Człowieka.

Tymczasem na łamach *The New York Times* Vinton Cerf, jeden z twórców Internetu oraz usług sieciowych, jak też współzałożyciel międzynarodowego ruchu obywatelskiego Internet Society, kontestuje nadawanie statusu prawo-człowieczego jakiejkolwiek technologii[7]. Tendencja taka jest według niego pomyłką, ponieważ technologie posiadają zastosowanie w historycznie i społecznie określonych kontekstach rozwoju cywilizacyjnego, pewne z nich wychodzą z użytku i zastępowane są innymi, natomiast prawa człowieka są z założenia prawami uniwersalnymi. Skoro wolność słowa i prawo do informacji są możliwe do osiągnięcia przy zastosowaniu różnorodnych mediów i technologii, to pomimo unikatowych własności Internetu, gwarantowanie powszechności dostępu do tego medium mocą prawa naturalnego, byłoby nadużyciem. Mocniejszymi argumentami dysponują, zdaniem Cerfa, zwolennicy traktowania dostępu do Internetu w kategoriach systemu praw obywatelskich. Na rzecz takiego podejścia przemawia fakt, że zapewnienie dostępu do globalnej sieci stanowi przedmiot polityki rządowej poszczególnych państw. O ile prawa obywatelskie przyznawane są jednostce ludzkiej ze względu na relację istniejącą między jednostką a państwem, o tyle prawa człowieka, argumentuje Cerf, przysługują jej w sposób nieodłączny od ludzkiej natury. Przyjmując postawę krytyczną wobec stosowania narracji prawo-człowieczej do samej możliwości korzystania z sieci komputerowych, podkreśla zarazem rolę informatyki i inżynierii komputerowej we wspieraniu praw człowieka poprzez ze względu bezpieczeństwo Internauty. Obok tworzenia technologicznych rozwiązań zwiększających

4 http://www.osce.org/fom/80735
Tendencje te odzwierciedlają wyniki sondażu BBC z marca 2010 roku, na który powołuje się raport *Wolność ekspresji w Internecie.* Zgodnie z sondażem, na ponad 270 tys. respondentów z 26 krajów co czwarty na pięciu respondentów uważa dostęp do Internetu za prawo podstawowe. http://news.bbc.co.uk/2/hi/8548190.stm

5 http://www.osce.org/fom/80723 s. 34.

6 Ibid. s. 47.

7 http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html

bezpieczeństwo informatyczne wskazuje także na potrzebę uświadamiania praw, którymi dysponują Internauci[8].

Niewątpliwie zagadnienie relacji, w jakiej pozostają względem siebie prawa człowieka i prawa obywatelskie, jest złożone i niejednoznaczne. Stanowisko Vintona Cerfa w tej kwestii reprezentuje klasyfikacyjną tendencję wyraźnego rozgraniczania między pierwszymi z nich jako prawami naturalnymi a drugimi jako przynależnymi do praw stanowionych. Źródło tych pierwszych upatrywane jest w godności istoty ludzkiej, czyli wartości, co do której przyjmuje się pierwotność względem państwa, dzięki czemu odnośnym prawom nadaje się status przyrodzony. Inna tendencja wyraża się w przekonaniu, że prawa obywatelskie stanowią integralną część praw człowieka, ponieważ w przeważającej mierze są one instrumentalnie podporządkowane realizacji wartości, jakie przysługują jednostce ludzkiej niezależnie od stanu posiadania obywatelstwa i w tym sensie wykraczają poza relację między obywatelem a państwem, a zdefiniowane są na gruncie systemu praw naturalnych i jako takie są prawami powszechnymi[9].

Samo założenie o uniwersalnym zasięgu systemu praw człowieka, które miałoby implikować autonomię systemu i niezależności należących do niego praw poszczególnych od kontekstów społeczno-kulturowych, nie jest przyjmowane bezdyskusyjnie. Rezultat sceptycyzmu wobec zasady powszechności praw człowieka nie jest obojętny dla koncepcji prawa naturalnego. Przedstawiciele radykalnego multikulturalizmu zarzucają prawom człowieka retorykę indywidualistyczną i zlaicyzowaną – nieprzystającą do rzeczywistości wspólnotowej. Uważają, że to dyskurs uwięziony w oświeceniowej utopii, która stanowi produkt modernizmu niekompatybilnego z etosem wspólnotowym kultur opartych na plemiennej strukturze społecznej albo kolektywnie zarządzanych. Komunitarianie twierdzą, że zindywidualizowany dyskurs prawo-człowieczy jest przeszkodą we właściwym rozpoznaniu praw grupowych i zapewnieniu określonym grupom odpowiedniej ochrony przed dyskryminacją. Skrajni przeciwnicy praw człowieka formułują zarzut, że system prawa wyrażonego w języku o aspiracji do aksjologicznej uniwersalności jest narzędziem, za pomocą którego Zachód uprawia kulturowy imperializm[10]. Z tej perspektywy nadanie Internetowi prawo-człowieczego statusu implikuje podejrzenia o komputerowo zapośredniczoną kolonizację[11].

Historyczno-kulturowej niejednorodności sposobów interpretowania podstaw aksjologicznych prawa oraz różnicom światopoglądowym w odniesieniu do źródła pochodzenia ius naturale towarzyszy zróżnicowanie sposobów rozumienia samego pojęcia natury ludzkiej. Skrajny sceptycyzm czy wręcz sprzeciw wobec systemu praw człowieka podlega krytyce między innymi z perspektywy, która stroni od esencjalizmu w ujmowaniu natury ludzkiej. Konstruktywizm w rozumieniu pojęcia natury ludzkiej prowadzi do złagodzenia różnic

8 http://www.internetsociety.org/internet-everyone

9 Zob. Altman A., *Civil Rights*, w: *The Stanford Encyclopedia of Philosophy* (Summer 2009 Edition), Edward N. Zalta (ed.), URL = http://plato.stanford.edu/archives/sum2009/entries/civil-rights/

10 R Howard-Hassman, J Donnelly, *Liberalism and Human Rights: a Necessary Connection*, w: *The Human Rights Reader. Major Political Essays, Speeches and Documents from Ancient Times to the Present*, M R Ishay (ed.), Routledge, New York, 2007, s. 405-410.

11 Zob. Ch. Ess , *Culture in Collision: Philosophical Lessons from Computer-mediated Communication,* w: J. H. Moor, T. W. Bynum (red.), *Cyberphilsophy. The Intersection of Computing and Philosophy*, s. 218-242.

konceptualnych między tezami komunitarian i liberałów. Zamiast traktować prawa człowieka jakby dotyczyły one prawd moralnych niezależnie od tych praw istniejących – prawd moralnych, które należy uprzednio odkryć – wskazuje się z tego punktu widzenia na niepodzielność systemu praw człowieka i zależność między jednostką a społeczeństwem w samej już możliwości formalnej korzystania z tych praw[12]. Osłabienie opozycji między narracją, jaką stosują komunitarianie i liberałowie w opisach relacji między jednostką a wspólnotą prowadzi do wniosku, że niesłusznie zarzuca się prawom człowieka, jakoby traktowały one istotę ludzką niczym metafizycznie wyizolowaną ze społeczeństwa jednostkę, skoro będąc animal symbolicum staje się ona podmiotem praw człowieka wraz z innymi osobami w danym układzie społecznym. Ponadto próba osłabienia radykalnie formułowanych tez w odniesieniu do istoty ludzkiej i wspólnoty pozwala zauważyć, że podważanie systemu praw człowieka z pozycji radykalnego multikulturalizmu jest wewnętrznie sprzeczne. Z jednej strony zwolennicy tego skrajnego stanowiska co do wielokulturowości negują możliwość bezstronnej oceny kultur, z drugiej natomiast głoszą ideał nieograniczonej tolerancji, który jest tylko kolejną próbą uchwycenia *widoku Znikąd*. Adwersarze twierdzą w przypływach śmiałości posądzanej o etnocentryzm, że sprzeciw wobec systemu praw człowieka służy forsowaniu dyktatorskich praktyk legislacyjnych.

Jeżeli druga z wymieniona wyżej tendencji w ujmowaniu relacji między prawami człowieka i prawami obywatelskimi wyzbyta jest esencjalizmu w charakteryzowaniu natury ludzkiej, a w zamian orientuje się na holistyczne uzasadnianie systemu praw człowieka, to różnice między prawami podstawowymi i obywatelskimi tracą na znaczeniu. Holistycznie ujęte prawa człowieka tworzą system, na który składają się współzależne i nierozłączne prawa podstawowe, obywatelskie i polityczne, ekonomiczne, społeczne i kulturalne. Holistyczne ujęcie zyskuje rosnące poparcie wraz z rozwojem jurysdykcji, która umożliwia ochronę praw człowieka na poziomie ponad-narodowym. Z tej perspektywy wydaje się, że pomimo utrzymującej się wieloznaczności w sposobach posługiwania się terminologią prawniczą, różnica między stanowiskiem promowanym przez Dunję Mijatović i Yamana Akdeniza, zgodnie z którym dostęp ten powinien być gwarantowany prawami człowieka, a argumentacją Vintona Cerfa skłonnego co najwyżej zaakceptować regulację zagadnienia za pomocą praw obywatelskich, nie odgrywa większego znaczenia. Z drugiej strony podejście Cerfa jest bliższe stanowisku Franka La Rue, ponieważ obaj wyraźnie ujmują Internet w roli narzędzia uprawiania wolności opinii i ekspresji oraz realizowania licznych innych praw człowieka. O ile zatem autorzy obu raportów oraz Vinton Cerf, promują Internet w roli niezbędnego współcześnie narzędzia korzystania z prawa do wolności ekspresji i wolności informacji, o tyle Mijativić oraz Akdeniz wyczytują z tego prawa, że również dostęp do globalnego medium powinien być potraktowany w kategorii prawo-człowieczej. Tymczasem La Rue oraz Vinton Cerf poprzestają na skonstatowaniu instrumentalnego charakteru medium cyfrowego wobec praw człowieka i promowaniu gwarancji dostępu do medium na poziomie rządowej polityki medialnej, nieodłącznej od polityki rozwojowej państwa. Kierunki tej ostatniej dookreślają Millenijne Cele Rozwojowe.

Dylemat dyktatora

W dyskusji nad prawo-człowieczym statusem Internetu dadzą się wyróżnić przekonania rozpoznane na gruncie filozofii

12 Zob. J Habermas, *The Postnational Constellation. Political Essays*, MIT Press, Cambridge, Massachusetts, 2001, s. 125-126.

i socjologii technologii jako determinizm i instrumentalizm technologiczny[13]. Poglądy te opierają się na przeciwstawnych względem siebie twierdzeniach przedmiotowych na temat relacji między nowymi technologiami informacyjnymi i komunikacyjnymi a sferą wartości społecznych oraz idei i doktryn politycznych. Według determinizmu technologicznego, otwarta architektura sieci komputerowej skutkuje zdecentralizowanym typem komunikacji społecznej, dzięki czemu służy politycznej emancypacji społeczeństw, upowszechnia i stabilizuje demokrację. Instrumentalizm natomiast wiąże technologię z aksjologią ze względu na sposób użycia i cele, do których technologia jest stosowana. O ile determinizm ujmuje aksjologię w terminach atrybutu systemu teleinformatycznego, o tyle instrumentaliści przyjmują, że sieć to tylko narzędzie. Według tych drugich, aksjologia jest implikacją celów i sposobów użycia medium w roli narzędzia. Pierwsi zakładają, że status aksjotwórczy jest sprawą wewnętrzną technologii. Konkludują, że wystarczy zadbać o dystrybucję i dostęp do technologii sieciowej, aby wpłynąć na preferencje i zachowania komunikacyjne oraz systemy wartości użytkowników. Oznacza to, że technologii przysługuje autonomia w oddziaływaniu na kulturowo-polityczne formy życia społecznego: technologia determinuje sposoby użycia, a wraz z nimi preferencje i zachowania komunikacyjne, wreszcie systemy polityczne. Tymczasem instrumentaliści przypisują technologii aksjologiczną neutralność. Twierdzą, że z opisu związków między narzędziem a wartościami należy dokonać w języku docelowym kontekstu użycia, czyli z uwagi na to, do czego i w jaki sposób narzędzie jest stosowane. Użycie narzędzia w różnych warunkach społeczno-politycznych i kulturowych nie implikuje, według nich, zunifikowanych efektów końcowych.

Wymownej egzemplifikacji determinizmu technologicznego dostarcza tzw. dylemat dyktatora, sformułowany w połowie lat 80. przez George'a P. Shultza, sekretarza stanu w administracji Ronalda Reagana. Otóż przed dylematem dyktatora stać mają społeczeństwa totalitarne w obliczu wyzwań rewolucji informacyjnej. Aby mianowicie utrzymać polityczne status quo, dyktatura musiałaby stłumić rozwój technologii informacyjno-komunikacyjnych; jeśli natomiast społeczeństwo totalitarne wejdzie na drogę rozwoju ekonomicznego, co wymaga trzymania tempa postępu technologicznego, wówczas niechybnie przyczyni się do erozji totalitaryzmu. Shultz uznał, że dyktatura de facto nie jest stanie powstrzymać rozwoju technologicznego, musi ugiąć się przed erą informacji[14]. Oznacza to, że technologiczny potencjał swobody w przepływie informacji prowadzić ma do przezwyciężenia politycznego zniewolenia wraz ze wszelkimi tego konsekwencjami społecznymi, ekonomicznymi i kulturowymi.

Krytycy determinizmu wyrażonego w dylemacie dyktatora zwracają uwagę na pierwotnie militarny cel Internetu jako produktu technologicznego zaprojektowanego w USA na potrzeby strategii zimnowojennej. Zdecentralizowana struktura nowego medium, do której odwołują się piewcy determinizmu, służyć miała w zamyśle konstruktorów do przekazu informacji – utopijnego z uwagi na aspekt materialny – w warunkach wybuchu nuklearnego. Zogniskowanie uwagi na militarnej funkcji nowej technologii informacyjno-komunikacyjnej zmienia kapitalnie perspektywę analizy. Rewolucyjne medium masowe oparte na technologii komunikacyjnego wdrażania, jak chcą determiniści, w demokrację wywodzi się z dwubiegunowej konfrontacji politycznej napędzającej wyścig

13 Zob. Ch. Ess, ibid.
14 http://www.rand.org/pubs/rgs_dissertations/RGSD127/sec2.html

zbrojeń. Historia Zimnej Wojny jest zapleczem ideologicznym, od którego nie można odizolować trwającej do dziś promocji Internetu – twierdzi Evgeny Morozov w wydanej w 2011 r. książce *The Net Delusion: The Dark Side of Internet Freedom*[15]. Polemizując najpierw z determinizmem tłumaczy, że wiara w emancypacyjny wpływ Internetu jest przejawem cyberutopizmu. W odniesieniu do przekonania głoszącego, że Internet służy represjonowanym, nie zaś represjonującym, używa też określenia „doktryna Google". Binarny ideologicznie, jak argumentuje, wydźwięk dylematu dyktatora, jest przejawem gloryfikacji strategicznej potęgi Stanów Zjednoczonych, a zarazem świadczy o naiwności, która znajduje wyraz w niedocenianiu paradoksalnej natury sowietyzmu W paradoksy obfituje rzeczywistość polityczno-ekonomiczna na białoruskim froncie Web 2.0, gdzie wojna o niezależność mediów jest znakomitym poligonem dla polityczno-mafijnej cenzury, propagandy i łamania praw człowieka.

Morozov śledzi ambiwalencję jaką na fali entuzjazmu wzbudziła sekwencja wydarzeń politycznych związanych z rolą nowych mediów społecznych w przemianach politycznych na Bliskim Wschodzie i w Północnej Afryce. Niedługo po tym jak pomysł nominacji Twittera do Pokojowej Nagrody Nobla zataczał kręgi poparcia, rozpoczęły się czystki polityczne z wykorzystaniem cyfrowych technologii. Irańskie media publikowały wizerunki osób utrwalonych na umieszczanych w Internecie zdjęciach lub filmach z pro-demokratycznego poruszenia, zwracając się do ludności o pomoc w zidentyfikowaniu rewolucjonistów. Renesans utopii towarzyszący Wiośnie Arabskiej to reiteracja etnocentryzmu łudząco podobna, zauważa Morozov, do nieostrożnego optymizmu Francisa Fukuyamy głoszącego koniec historii wraz z triumfem liberalnej demokracji i gospodarki wolnorynkowej. Czy utopią jest sądzić, że społeczeństwo zamknięte i cenzura z jednej strony, z drugiej zaś społeczeństwo informacyjne, rozwój ekonomiczny i globalizacja wzajemnie się wykluczają? Czyżby piewcy *doktryny Google* nie przewidzieli, że Internet może służyć w roli użytecznego narzędzia propagandy, instrumentu logistycznej sublimacji cenzury? Zdaniem autora nie doceniono funkcji usług pośrednictwa w transmisji danych.

Media masowe na służbie masowej partii

Spór pomiędzy entuzjastami determinizmu i zwolennikami instrumentalizmu technologicznego warto przemyśleć na przykładzie kubańskiej polityki w dziedzinie mediów cyfrowych. Karaibska wyspa oddalona o 90 mil od wybrzeży Stanów Zjednoczonych i objęta z początkiem lat 60. embargiem handlowym uzyskała dostęp do Internetu najpóźniej spośród krajów Ameryki Łacińskiej. Stanowisko rządu kubańskiego jest bez wątpienia kontynuacją dwubiegunowej konfrontacji politycznej. W konsekwencji konstytucyjnie usankcjonowanego systemu monopartyjnego polityka medialna Kuby opiera się na mechanizmach ścisłej monopolizacji i kontroli państwowej. Artykuł 53 Konstytucji Kubańskiej, zawarty w rozdziale dotyczącym podstawowych praw, obowiązków i gwarancji, przyznaje obywatelom *wolność słowa i prasy w wypełnianiu zadań społeczeństwa socjalistycznego*, oraz stanowi, że *media masowe są własnością państwa lub społeczeństwa*. Artykuł ten explicite wyklucza możliwość objęcia mediów własnością prywatną. Artykuł 62 ogranicza wszelkie wolności obywatelskie, gdy ich uprawianie *kłóci się z istnieniem i celami państwa socjalistycznego lub decyzją Kubańskiego ludu o budowaniu socjalizmu*

15 E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs, New York, 2011.

i komunizmu[16]. Bert Hoffman w pracy *The Politics of the Internet in Third World Development* podkreśla, że ścisły monopol i kontrola państwowa w dziedzinie mediów masowych stanowi główny filar systemu politycznego na Kubie i promowany jest jako konieczna i skuteczna forma obrony tego, co określa się mianem kubańskiej niezależności medialnej[17]. Z perspektywy czasu pozwalającego zestawić rewolucję kubańską z rewolucją informacyjną zyskuje na wymowie argumentacja Zbigniewa Brzezińskiego i Carla Joahima Friedricha z 1956 r., w myśl której monopol aparatu państwowego na mass media jest jednym z podstawowych czynników charakteryzujących reżim totalitarny[18].

Do fundamentalnych założeń socjalistyczno-komunistycznego ustroju politycznego Kuby należy doktrynalne utożsamienie pojęcia państwa z pojęciem społeczeństwa, co do którego zakłada się z kolei, że definiuje ono ex essentia egzystencję indywidualną. Gwarantowana konstytucyjnie państwowa własność mediów stanowić ma legalną podstawę realizacji rzekomej wolności słowa i prasy w społeczeństwie, którego interesy są doktrynalnie nieodróżnialne od interesów klasy rządzącej. Przez pół wieku od czasu, gdy Fidel Castro objął stanowisko premiera, interesy społeczeństwa zorganizowanego w partię masową wyrażane były głosem dyktatora, który emitowano w częstotliwościach kultu jednostki. Pomimo pewnych przemian w oficjalnej narracji polityki Raula Castro, stan prawny na Kubie niezmiennie legitymizuje monopol partii komunistycznej na mass media. Oznacza to podtrzymywanie – charakterystycznego dla dyktatur typu sowieckiego – ograniczenia praw indywidualnych ze względu na polityczne cele i działalność państwa[19]. Pojęcie wolności formalnej, istniejącej w sferze polityki, ulega w warunkach totalitarnych semantycznej inflacji do tego stopnia, że służy do oznaczania treści sprzecznych ze źródłowym znaczeniem tego słowa – ulega zafałszowaniu. Totalitaryzm nie dopuszcza bowiem, jak objaśnia Leszek Kołakowski w tekście *Istota i istnienie w pojęciu wolności*, antagonizmu między podmiotem zbiorowym a indywidualnym. Wolność jednostki jest postrzegana jako proste przełożenie swobód partii. Władza, jaką państwo posiada nad podmiotem poszczególnym, legitymizuje tym samym zwyrodnienie swobód partyjnych w autorytaryzm i zniewolenie jednostki[20].

W ramach procesu ucyfrowienia wyspy, początkowo, od 1992 r., połączenie sieciowe Kuby zapośredniczone było w Kanadzie, a w 1996 r. wyspa oficjalnie nawiązała połączenie bezpośrednie z USA. Stało się to możliwe z powodu zwrotu, jaki nastąpił w historii embarga przeciw Kubie. Na mocy słynnej ustawy Torricellego (Cuban Democracy Act) z 1992 r., podpisanej przez George'a H. W. Busha, a wprowadzonej w życie za prezydentury Billa Clintona, doszło do wyłączenia z embarga środków komunikacji społecznej. Ustawa ta należy do jednej z najbardziej kontrowersyjnych strategii w polityce zagranicznej USA. Z jednej strony dramatycznie zaostrzyła uprzednie ograniczenia zakazując wysyłania na wyspę towarów spożywczych i lekarstw, za wyjątkiem pomocy humanitarnej. Z drugiej strony ustawa torowała drogę do rozwoju łączności w celu animacji

16 http://www.cubanet.org/ref/dis/const_92_e.htm
17 B. Hoffman, *The Politics of the Internet in Third World Development. Challenges in Contrasting Regimes with Case Studies of Costa Rica and Cuba*, Routledge, New York, 2004, s. 200-214.
18 Z. Brzeziński, C. J. Friedrich, *Totalitarian Dictatorship and Autocracy*, New York, 1956, s. 52-53.
19 Zob. R. Aron , *Esej o* wolnościach, Aletheia, Warszawa 1997, s. 131.
20 L. Kołakowski, *Światopogląd i życie codzienne*, PIW, Warszawa, 1997, s. 115-121.

społeczeństwa obywatelskiego na Kubie. Na zlecenie Departamentu Obrony Stanów Zjednoczonych amerykański think tank RAND wykonał projekt polityki informacyjno-komunikacyjnej, który objął strategie ucyfrowienia wyspy.

Bert Hoffman, wnikliwie śledząc proces decyzyjny w sprawie cyfryzacji po stronie kubańskiej, pokazuje, że niemałe znaczenie odegrały w tym procesie konsultacje z Chinami. Chińska Republika Ludowa od 1987 r. korzystała w łączności cyfrowej z pośrednictwa Niemiec, a sześć lat później uzyskała dostęp bezpośredni. Wbrew hurraoptymizmowi dla deterministycznej wizji upadku komunizmu, doświadczenie chińskie, inaczej niż radzieckie, bynajmniej nie przemawiało za utratą partyjnej kontroli nad mass mediami. Gdy w 1996 r. Kuba nawiązała połączenie bezpośrednie, kubański rynek medialny został uregulowany na mocy rządowego rozporządzenia *Dostęp Republiki Kuby do sieci informacyjnych globalnego zasięgu*. Zalegalizowana forma pośrednictwa w udostępnianiu sieci globalnej na wyspie explicite wykluczyła kapitał prywatny w nabywaniu kompetencji administracyjnych – te ograniczono do instytucji i przedsiębiorstw państwowych. Co istotne, uprawnienia do pośrednictwa w usługach dostawczych przysługują w pierwszej kolejności osobom prawnym i instytucjom zasłużonym w życiu i rozwoju narodu. Państwową politykę medialną opartą na wykluczeniu jednostki dyktuje wzgląd na bezpieczeństwo narodowe Kuby. Politbiuro opracowało instrukcje realizacji ścisłego monopolu państwowego na dostęp do Internetu adekwatnie do linii argumentacji, którą Raul Castro posłużył się w potępieniu tendencji analogicznych do polityki głasnosti w Związku Radzieckim. Według tej argumentacji, reforma mediów rozpoczęta przez Michaiła Gorbaczowa w połowie lat 80., pozbawiła aparat władzy kontroli nad mass mediami, co doprowadziło do upadku socjalistycznego supermocarstwa[21].

Kontrola mass mediów w erze informacji uzyskała rangę priorytetu w polityce bezpieczeństwa narodowego Kuby. Oficjalne komunikaty formułowane w reakcji na dociekania w sprawie medialnej polityki wykluczenia informacyjnego na Kubie nie prześcigają się w analizowaniu politycznych funkcji i skutków monopolu państwowego na Internet. Mniemana niezależność medialna w rzeczywistości społecznej, w której wolność jednostki jest ideologicznie zrównana z wolnością partii rządzącej, to swoboda, jaką dysponuje aparat władzy w stosowaniu propagandy. Nomenklatura stała się areną ćwiczeń ze strategii propagandowych, instrumentalnie podporządkowanych wartości najwyższej, jaką jest bezpieczeństwo narodowe Kuby Castrowskiej. Użycie nowego medium masowego nie może de facto zagrażać bezpieczeństwu partyjnego aparatu władzy. Zamiast wygłaszać tyrady o zagrożeniach pluralizmu, jakie narzędzie *wrogiego wpływu imperialnego* przysparza komunikacji masowej, obarczano oficjalnie Stany Zjednoczone odpowiedzialnością za reglamentację cyberprzestrzeni. Wykluczenie informacyjne miało być postrzegane jako rezultat warunków technicznych i finansowych, na jakich Kubie udostępniają sieć Stany Zjednoczone. Za twierdzeniem, że koszty satelitarnej transmisji danych oraz przepustowość niewystarczająca dla użytku prywatnego stoi de facto polityka wewnętrzna Kuby. Gdy państwowy monopol na media zaczął stopniowo przekształcać się poprzez dopuszczenie spółek o kapitale mieszanym pochodzenia zagranicznego i Kuba porozumiała się z Wenezuelą o doprowadzenie światłowodu, zarzut pod adresem USA o informacyjnej blokadzie mieszkańców wyspy stracił na sile oddziaływania. Wbrew

21 B. Hoffman, ibid. s. 132-162.

nadziejom, jakie wiązano z technologiczną innowacją łączności cyfrowej, jaka oficjalnie nastąpiła z początkiem 2011 r., kubańscy Internauci do dziś muszą polegać na transmisji satelitarnej. Jednocześnie wenezuelski Minister Nauki i Technologii zapewnił, że usługa została wykonana i połączenie jest aktywne, natomiast decyzja w sprawie użycia należy do rządu Raula Castro. Milczenie rządu w tej kwestii utwierdza w domysłach o kontynuacji wewnętrznej selektywnej polityki medialnej. Yoanni Sanchez, znakomita pisarka i najsłynniejsza kubańska bloggerka, umieściła w sieci komentarz zatytułowany *Kabel czy marchewka*, w którym skonstatowała używanie Internetu przez rząd kubański w roli pola walki: światłowód jest tylko kolejną bronią w trwającej *wojnie mediów*[22].

Kubański Internauta na froncie wojny mediów

Partycypacja Kubańczyków w globalnej cyberprzestrzeni nie przekracza jak dotąd trzech procent populacji pomimo pewnych ustępstw prawnych ze strony rządu Raula Castro[23]. *Ustawa o bezpieczeństwie informacji* podtrzymuje zakaz łączności cyfrowej z mieszkaniami prywatnymi, ale od Internet zaczął być stopniowo dostępny na użytek prywatny w miejscach publicznych[24]. Stopniowo rząd zezwolił na stworzenie punktów dostępu w urzędach pocztowych, na uniwersytetach, w hotelach, gdzie zaczęto umieszczać kafejki internetowe; zaczęły powstawać młodzieżowe centra komputerowe. Zwiększeniu się punktów publicznego dostępu do sieci nie towarzyszy bynajmniej liberalizacja kontroli zachowań, przeciwnie, zaostrzyła się adekwatnie do wzrostu ryzyka, jakie dla państwa socjalistycznego potencjalnie wiąże się z aktywnością indywidualną użytkownika mediów. Partia komunistyczna będąc *najwyższą siłą przewodnią społeczeństwa i państwa* czuwa nad Internautą za pomocą rozbudowanego aparatu kontroli, który obejmuje cenzurę i propagandę w kolektywistycznym modelu zarządzania informacją. Do strategii kubańskiej reglamentacji cyberprzestrzeni należy ograniczanie dostępu do sieci, filtrowanie i blokowanie treści, monitorowanie zachowań w sieci.

Aby przyłączyć się w okrojonym politycznie środowisku cyfrowym, Kubańczycy zobligowani są do złożenia wniosku o akredytację i podpisać zobowiązanie do nieużywania Internetu w celu poszukiwania lub otrzymywania treści anty-kubańskich. Komitet Obrony Rewolucji opiniuje wniosek i decyduje o przyznaniu, nieprzyznaniu lub cofnięciu akredytacji. Mechanizmy represji działają już na poziomie procedur rejestracji Internauty, obejmują też kontrolę efektów regularnej identyfikacji zachowań w sieci udostępnianej w poszczególnych punktach. Instytucje udostępniające Internet zatrudniają osoby odpowiedzialne za informatyczny oraz informacyjny wymiar bezpieczeństwa narodowego. Zapewnianie bezpieczeństwa informatycznego wymaga kompetencji technicznych w zakresie ochrony systemów teleinformatycznych przed potencjalnym i zaistniałym zagrożeniem, jakim są wirusy lub ataki hackerów. Kompetencje te obejmują znajomość komputerowego sprzętu i oprogramowania. Bezpieczeństwo informacyjne dotyczy sfery symbolicznej zatem wymaga umiejętności interpretowania – nie tylko informacji, ale też związków między informacją a uczestnikiem komunikacji. Struktury administracyjne i policyjne oraz społeczne otoczenie Internauty są zaangażowane w kontrolę jego zachowań związanych

22 http://www.desdecuba.com/generationy/?p=3000&cp=all
23 http://www.rsf.org/IMG/pdf/rapport_gb_md_1.pdf
24 B. Hoffman, ibid.

z nadawaniem i odbieraniem komunikatów, tworzeniem i przetwarzaniem informacji. Policja jest alarmowana za pomocą odpowiedniego oprogramowania o wywrotowej aktywności Internauty. Nieposłuszny posiadacz akredytacji sieciowej może ją wnet stracić, podobnie jak i zatrudnienie w dotychczasowym miejscu pracy, także szanse na znalezienie innego zatrudnienia. Będąc oskarżony o łamanie prawa narodowego, o co wcale nietrudno na wewnętrznym froncie totalitarnym, podlega karze utraty wolności przez osadzenie w więzieniu.

Zabiegom wzmożonej kontroli mającej na celu eliminację zagrożeń informacyjnych podlegają kubańscy dysydenci, niezależni dziennikarze, organizacje pozarządowe. W zależności od stopnia jawności krytycznego charakteru aktywności dysydenci podlegali całkowitej lub częściowej blokadzie łączności i politycznego monitoringu. Wypracowali w tych okolicznościach kanały informowania świata zewnętrznego w oparciu o współdziałanie nowych technologii ze starymi i pomoc emigrantów. Informacje nadawane drogą telefoniczną lub tradycyjną pocztą z wyspy trafiają do emigrantów, by ukazać się na stronach www. Komunikaty niewygodne dla dyktatury docierają do publiczności międzynarodowej, omijając skrzętnie mieszkańców wyspy. Środowiska dysydenckie, kubańska diaspora, organizacje pozarządowe i humanitarne takie jak Amnesty International czy Reporterzy bez Granic od lat alarmują światową opinię publiczną doniesieniami o drastycznym łamaniu praw człowieka przez dyktaturę braci Castro, ujawniając zarazem zatrważającą zależność, jaka istnieje pomiędzy obywatelską aktywnością na rzecz uświadamiania praw człowieka, a penalizacją tego rodzaju aktywności w imię utrzymania tzw. porządku społecznego w państwie socjalistyczno-komunistycznym.

O tym, jakie konkretnie działania stanowią potencjalnie kontr-rewolucyjną aktywność, aparat państwowy rozstrzyga w sposób autorytarny. Usankcjonowanie dyktatury w ustawie zasadniczej znajduje konsekwencje w zapisach prawa karnego. Artykuł 103 Kubańskiego Kodeksu Karnego stanowi, że na każdego, kto agituje za działalnością wywrotową poprzez uprawianie propagandy w formie ustnej lub pisemnej, sporządza, upowszechnia lub posiada materiały propagandowe, czy też w jakikolwiek inny sposób, podburza przeciwko państwu komunistycznemu, porządkowi społecznemu lub międzynarodowej solidarności, nakłada się karę pozbawienia wolności od roku do lat dziewięciu. Osoba, która rozpowszechnia fałszywe lub szkodliwe treści wywołujące społeczny niepokój lub niezgodę, ma podlegać uwięzieniu na okres od roku do lat czterech. Za użycie środków komunikacji masowej do prowadzenia wskazanej aktywności wywrotowej, nakłada się karę pozbawienia wolności od lat siedmiu do piętnastu. Każdy natomiast, kto zezwala na stosowanie środków komunikacji masowej do prowadzenia rzeczonej działalności, podlega uwięzieniu od roku do lat czterech[25].

W warunkach totalitarnych każda forma krytyki, oporu i niezadowolenia z rzeczywistości politycznej, społecznej i ekonomicznej może być zinterpretowana w terminach aktywności anty-państwowej. Metody egzekwowania prawa na Kubie implikuje w praktyce systematyczne prześladowanie, internowanie i osadzanie dysydentów w więzieniach, poddawanie więźniów politycznych torturom, na które składa się przemoc fizyczna i stosowanie technik psychiatrii represyjnej. Obywatel zaznajomiony z konsekwencjami anty-kubańskich czynów waży ryzyko decyzji. Samo-dyscyplinuje się mając na uwadze w szczególności *Ustawę*

25 http://www2.fiu.edu/~fcf/IACHR.html#II

o ochronie niezależności narodowej i ekonomicznej Kuby. Ustawa ta weszła w życie w 1999 r., a na jej podstawie za przekazanie USA komunikatów, których skutkiem może być zaostrzenie anty-kubańskiej polityki kara osadzenia w więzieniu wydłuża się do lat piętnastu, a nawet dwudziestu[26].

Na Kubie oba typy bezpieczeństwa – informatyczne, oparte na kompetencjach technicznych, oraz informacyjne, wymagające urzędowo-społecznej ingerencji w kontrolowanie Internauty – są podporządkowane wartości ostatecznej, jaką jest bezpieczeństwo narodowe. Kubański Internauta nie jest chroniony zobligowanym do organizowania i kontrolowania wszelkich zasobów komunikacyjnych na rzecz realizowania celów państwa. Pomimo braku przejrzystości w negocjacjach z USA, zainicjowanie działań zapowiadających zdjęcie embarga handlowego, co nastąpiło w lipcu 2012 r. wraz ze statkiem, który wypłynął z Miami do Hawany z żywnością, lekarstwami i przedmiotami codziennego użytku, zapowiada obiecujące zmiany. Jak długo jednak potencjalny nabywca komputera, modemu lub innych akcesoriów teleinformatycznych, skazany będzie na transakcję czarnorynkową, przekraczającą zazwyczaj jego zdolność finansową do wykonania takiej transakcji, i podlegał penalizacji w imię prawa wewnętrznego, rażąco łamiącego prawa człowieka, tak długo społeczeństwo otwarte ery informacji pozostanie mrzonką na Kubie.

Powolna infekcja wolnościowa przeciw cyfrowej auto-blokadzie

Dostęp monopartyjnej Kuby do Internetu nie doprowadził jak dotąd do istotnych przemian politycznych i rozwojowych. Nadzieje wyrażane w metaforach kolejnych prezydentów USA o szerzeniu się demokracji wraz z modemem i telefonem komórkowym lub za pomocą bloga są o tyle płonne, że technologiczne *zarażenie wirusem wolności* nie przynosi efektów natychmiastowych ani radykalnych. Czy ideologia, która przyjmuje, że Internet jest narzędziem automatycznej, zdeterminowanej aktywizacji społecznej prowadzącej do obalenia totalitaryzmu, mogłaby w ogóle uchodzić za liberalną? Czy wolność może oznaczać partycypację rozumianą jako podstawa społeczeństwa obywatelskiego w terminach przyczynowo-skutkowych?

Deterministyczna argumentacja na rzecz pluralizmu światopoglądowego nie uniknie sprzeczności wewnętrznej. Widać to wyraźniej, gdy uporządkuje się myślową relację, w jakiej prawo pozostaje względem wolności. Pomocna jest w tym względzie klarowność oksfordzkiego wykładu Isaiaha Berlina, utrwalonego w eseju *Dwie koncepcje wolności*. Istnieje różnica pojęciowa między wolnością, korzystaniem z wolności, wreszcie warunkami, w których z wolności można czynić użytek. Wolność stanowi możliwość dokonania wyboru, co oznacza, że bycie wolnym polega na dysponowaniu opcją, w ogólnym rozumieniu. Wolność nie ogranicza się jedynie do tego, co dane, zakłada także tworzenie tego, co nowe. Przybiera dwie formy: negatywną i pozytywną. Wolność negatywna polega na nieingerencji w sferę podmiotową, pozytywna zaś na samosterowności podmiotu. Aby istota ludzka mogła cieszyć się wolnością w obu jej postaciach, muszą zaistnieć odpowiednie ku temu warunki. Brak warunków do korzystania z wolności sprawia, że chociaż formalnie jednostka dysponuje opcją, to jednak przysługująca jej na mocy prawa możliwość wyboru nie znajduje praktycznej realizacji. Na przykład, brak elementarnej wiedzy o tym, jak

26 http://www.cubaverdad.net/crime_under_law_88.htm

posłużyć się medium, nie reguluje wolności do komunikowania za jego pomocą, lecz sprawia, że wolność ta jest bezużyteczna.

Prawo do wolności w cyberprzestrzeni jest elementem heterogenicznych systemów dookreślających warunki korzystania z całego szeregu swobód. Funkcjonuje w rzeczywistości społecznej synergicznie zwielokrotnionej w splocie świata symbolicznego z technologią. Warunki do korzystania z wolności dookreślone są holistycznie. Czy Internet stanowi warunek konieczny wolności informacji i wolności ekspresji? Rozproszona moc obliczeniowa i szybkość sieci mogą prowadzić do opłakanych efektów społecznych. Demokratyczny potencjał nowych technologii nie jest warunkiem wystarczającym dla zaistnienia transformacji ustrojowej. Technologie nie stanowią jedynego źródła zagrożeń politycznych, trudno więc oczekiwać, aby jedynie użycie technologii miało usunąć zaistniałe zagrożenia. Wystarczy, że media cyfrowe, które uchodzą za arenę uprawiania wolności ekspresji staną się sferą oddziaływań instytucji takiej, jaką jest kubański Komitet Obrony Rewolucji, aby blokować fenomen komunikacyjny, który w sposób niezafałszowany określa się mianem mediów niezależnych. Oddziaływanie Internetu nie jest samorzutne, lecz zależy od polityki w dziedzinie mass mediów, a ta może służyć wzmacnianiu ochrony praw człowieka, albo przeciwnie, ich rażącemu łamaniu. Zamiast otwierać i poszerzać, Internet może kurczyć i zamykać domenę publiczną, gdy użyty zostanie w roli instrumentu kryminalizacji obywatelskiej postawy krytycznej.

Isaiah Berlin śledził wyradzanie się wolności pozytywnej na „pokrzywionym drzewie człowieczeństwa" w autorytaryzm. Jeżeli dostęp do Internetu na Kubie ujmiemy w kategorii wolności pozytywnej, staje się jasne, że wyrodziła się ona w wolność autorytarnej oligarchii. Cenzura, propaganda i blokowanie aktywizmu politycznego w cyberprzestrzeni mogą iść w parze z zabezpieczaniem pewnych korzyści ekonomicznych. Internet stając się elementem wewnętrznych planów rozwojowych w warunkach totalitarnych, nie zagraża reżimowi automatycznie, natychmiastowo. Co więcej, pomimo oczywistej presji ekonomicznej, do pewnego stopnia społeczeństwo totalitarne staje się beneficjentem systemów teleinformatycznych. Kubański program informatyzacji służby zdrowia oraz edukacji stały się priorytetami-wewnętrznej polityki rozwojowej[27]. Przykład kubańskiej polityki medialnej uczy zatem, że chociaż rewolucja informacyjna stanowi wyzwanie dla dyktatury, nie musi być wyzwaniem skrajnym. Internet może równie skutecznie służyć upowszechnianiu demokracji, co i uprawianiu propagandy wzmacniającej reżim.

Czy wobec tego dylemat dyktatora nie jest za wąski do opisu konfrontacji dyktatury z technologią cyfrową? Czy z faktu, że rewolucja informacyjna nie zdołała dotychczas wyprzeć rewolucji kubańskiej, należy wnioskować, że nie stanie się tak w przyszłości? Czy racja nie leży jednak po stronie determinizmu w utrzymywaniu, że Internet przyniesie konieczne zmiany polityczne wówczas jedynie, gdy będzie powszechnie dostępny i używany adekwatnie do zdecentralizowanej struktury sieci? Swoboda przepływu informacji nie podlega redukcji do warunków technologicznych komunikacji. Medium zaprojektowane do zdecentralizowanej komunikacji stosowane być może z pewnym powodzeniem w sposób uregulowany za pomocą modelu wysoce scentralizowanej kontroli politycznej. Jeżeli jednak na demokratyczny potencjał

27 B. Hoffman, ibid. s. 188, 190.

medium cyfrowego spojrzy się w perspektywie długofalowego oddziaływania, to społeczeństwo otwarte okazuje się projektem, którego realizacja możliwa jest, o ile dojdzie najpierw do swoistej politycznej infekcji wewnętrznej. Narodziny kultury hackerskiej wraz z rozkwitem czarnych rynków teleinformatycznych, w tym rynku kont e-mailowych, to symptomy wirusa wolności w cyberprzestrzeni. Rozpoczyna on swoje działanie w środowisku dywersji informacyjnej skierowanej przeciw dyktaturze.

Pożądane dla rozważań nad technologicznym determinizmem i instrumentalizmem jest zaadaptowanie aparatu pojęciowego wypracowanego dla nauk o komunikacji w szkole poznańskiej przy zastosowaniu społeczno-regulacyjnej teorii kultury Jerzego Kmity. Zabieg taki pozwala zauważyć, że wybór pomiędzy tymi dwoma poglądami dostarcza racji dla opisywania i wyjaśniania oddziaływań zachodzących między sferą materialną kultury, czyli cywilizacją, a sferą symboliczną, tj. kulturą w wąskim rozumieniu, określaną tradycyjnie mianem duchowej. Zasadniczym korpusem tej ostatniej jest proces komunikacji społecznej, który jest procesem zapośredniczonym interpretacyjnie. Teleinformatyczne zapośredniczenie interakcji ludzkich potwierdza dualizm procesów komunikacji – ich duchowo-materialny charakter.

Główny przedmiot sporu między zwolennikami determinizmu i instrumentalizmu technologicznego to replika zagadnień, których konceptualizacja w XIX wieku wpłynęła na rozwój humanistyki i nauk społecznych. Niemieckie szkoły neokantyzmu dopełniły wówczas przewrót kopernikański, jakiego Kant dokonał w XVIII-wiecznej epistemologii zorientowanej na poznanie natury, o rozwiązania humanistyczne. Ukształtowała się metodologicznie pojęta opozycja poglądów nazwanych w stuleciu następnym przez Karla Poppera terminami „naturalizm" i „antynaturalizm". Niemieckie szkoły neokantyzmu rozwinęły świadomość metodologiczną humanistyki poprzez konceptualizację konstruktywizmu wiedzy zależnej od świadomości ludzkiej. Według Heinricha Rickerta fakty historyczne oraz powiązania między nimi nie były przedmiotem nauk idiograficznych, które bazują na kategorii faktu jednostkowego, nie zaś prawa przyczynowo-skutkowego[28]. Instrumentalizm antynaturalistyczny byłby podstawą metodologiczną do ujmowania nauk o rozwoju społecznym związanym z upowszechnianiem technologii cyfrowej inaczej niż nakazują rygory metodologiczne nauk nomotetycznych.

Maszyny dialektyczne komplikują pole badawcze w naukach o komunikacji i wymagają interdyscyplinarnej współpracy uwzględniającej *współczynnik humanistyczny* w komunikacji cyfrowej. Pojęcie tego współczynnika wprowadzone do humanistyki przez Floriana Znanieckiego uzyskało eksplikację w terminach komunikacji społecznej w ujęciu społeczno-regulacyjnym Jerzego Kmity[29]. Odróżnienie dwóch typów uwarunkowania czynności – funkcjonalnego i subiektywnoracjonalnego – pozwala uzasadnić twierdzenie o instrumentalnym podporządkowaniu narzędzia komunikacji wobec celu legislacyjnego, jakim jest ochrona wolności w komunikacji. Z kulturowego punktu widzenia pożądane jest umiarkowane podejście do przedmiotu sporu między zwolennikami doktryn o radykalnej

28 A. Pałubicka, *Naturalizm i antynaturalizm*, w: Z. Cackowskki (red.), F*ilozofia a Nauka. Zarys encyklopedyczny*, Ossolineum, Wrocław, 1987, s. 403-412.

29 J. Kmita, *Kultura i poznanie*, PWN, Warszawa 1985; G. Banaszak, J. Kmita, Społeczno-regulacyjna koncepcja kultury, Instytut Kultury, Wasrszawa 1994.

wymowie. Medium i rzeczywistość stanowią ontologicznie różne struktury, ale funkcjonalnie od siebie zależne. Oddziaływania między technologią a kontekstami zastosowania, które obejmują preferencje i zachowania komunikacyjne użytkowników, żywione przez nich wartości oraz systemy polityczne, w których funkcjonują, nie dadzą się zredukować do jednego typu uwarunkowania. Dlatego informacja może w równym stopniu wyzwalać, co i służyć represji.

Internet a rozwój nauk o bezpieczeństwie

Niezależność mediów jako czynnik przeciwdziałający cenzurze jest testem na typ polityki, jaką państwo prowadzi w dziedzinie mass mediów. Kubańska polityka w dziedzinie mediów cyfrowych stanowi przykład teleinformatycznego kolektywizmu. Kolektywistyczna polityka określająca metody zarządzania mass mediami, w przeciwieństwie do medialnego pluralizmu, zakłada narodowo-państwowy model niezależności mediów. Niezależność medialna Kuby oznacza swobodę dyktatury w stosowaniu propagandy, odporność na kierowaną pod adresem dyktatury krytykę i dowolność w stosowaniu strategii kontrolowania Internauty, jak i pozostałych mediów masowych. Internet jest obwarowany murami prawa chroniącego dyktaturę przed zagrożeniami ze strony jednostki, nie zaś jednostkę przed zagrożeniami ze strony dyktatury. Prawo strzeże jednostkę w tym sensie, że uniemożliwia lub likwiduje zagrożenia, jakie dla jej uczestnictwa w realizacji społecznego powołania do budowy socjalizmu i komunizmu niesie, z założenia, wrogi imperializm. Beneficjentem komunikacji zapośredniczonej komputerowo, inaczej niż przyjmuje się na gruncie indywidualistycznej wizji Internetu, jest naród. Podmiot indywidualny ponosi dramatyczne koszty medialnego kolektywizmu, w które wpisana jest inter alia wolność słowa. Internet jest w takim układzie polem oddziaływania dyktatury i państwa policyjnego a prawo chroni bezpieczeństwo państwa będąc poprzez wykluczanie przejawów postawy krytycznej wobec status quo.

Zwolennicy umiarkowanego podejścia do przedmiotu sporu między determinizmem i instrumentalizmem technologicznym, jak Charles Ess, podkreślają, że dyskusji nad prawoczłowieczym uzasadnieniem ucyfrowienia sfery publicznej powinna towarzyszyć animacja świadomości społecznej i indywidualnej w zakresie prawa do wolności opinii i ekspresji. Niezbędna dla zaistnienia przemian demokratycznych komunikacyjna samosterowność Internautów nie ujawni się bez prawnego zagwarantowania ich wolności negatywnej. Wydzielenia takiej sfery w relacji między jednostką a państwem, w którą państwo nie ma prawa ingerować, wymaga radykalnego przeformułowania koncepcji bezpieczeństwa, na której państwo opiera politykę wewnętrzną i zagraniczną.

Internet jest medium o wyjątkowym znaczeniu dla rozważań nad politycznymi zależnościami między wolnością a bezpieczeństwem. Rozwój tego medium przebiegał równolegle do rozwoju w naukach o bezpieczeństwie. Pod względem genezy Internet jest technologicznym produktem Zimnej Wojny. Dzisiaj natomiast, mówiąc językiem Manuela Castellsa, wszyscy jesteśmy całkowicie zanurzeni w tym nowym technologicznym systemie[30]. W okresie dwubiegunowej konfrontacji supermocarstw bezpieczeństwo militarne było uprzywilejowanym przedmiotem studiów strategicznych i badań nad pokojem[31]. Koncepcja bezpieczeństwa

30 M. Castells, *Społeczeństwo sieci*, PWN, Warszawa 2008, s. 65.

31 B. Buzzan, L. Hansen, *The evolution of International Security Studies*, Cambridge University Press, 2009, s. 153.

ludzkiego wypracowana w szkole kopenhaskiej przełamała dominację państwo-centryczną orientacji nauk o bezpieczeństwie, poprzez przeorientowanie zakresu przedmiotowego pojęcia bezpieczeństwa na ochronę człowieka i wartości ludzkich[32]. Koncepcję bezpieczeństwa ludzkiego rozwinęła i upowszechniła na arenie międzynarodowej ONZ-owska agenda Program Narodów Zjednoczonych ds. Rozwoju w wydanym w 1994 r. Raporcie o Rozwoju Ludzkim. Dookreślono w nim bezpieczeństwo ludzkie w terminach uniwersalizmu i holizmu. Kompleksowa koncepcja bezpieczeństwa o uniwersalnym zasięgu, podkreśla funkcję prewencji w działaniach zorientowanych na zapewnianie bezpieczeństwa jednostkom i grupom.

Dla niniejszych rozważań istotne jest, że jedną z siedmiu podstawowych, najważniejszych kategorii bezpieczeństwa wymienionych w Raporcie Rozwoju Ludzkiego jest bezpieczeństwo polityczne, a jego aspektem jest niezależność jednostki i grupy w sferze idei oraz informacji. Bezpieczeństwo polityczne polega na honorowaniu aksjologii wyrażonej w prawach człowieka. Obok represji, jakie państwo stosuje wobec jednostki, państwowa kontrola idei oraz informacji może stanowi obszar nadużyć i zagrożeń świadczących o braku bezpieczeństwa politycznego. Kwestia jest tym bardziej paląca, że państwa wykorzystujące mechanizmy kontroli informacji do represjonowania jednostek i grup używają policji i sił zbrojnych do łamania praw człowieka[33]. Wobec stopniowo postępującego ucyfrowienia społeczeństw totalitarnych niezbywalnym czynnikiem przemian ustrojowych powinien stać się wzmożony wysiłek gremiów międzynarodowych w zagwarantowaniu bezpieczeństwa politycznego w dostępie do potencjalnie emancypacyjnego wpływu nowych technologii informacyjno-komunikacyjnych. Inaczej ani podmiot indywidualny, ani społeczeństwo nie staną się beneficjentem rewolucji informacyjnej. Wszędzie tam, gdzie prawa człowieka są łamane w komunikacji, który jest procesem niezbywalnym dla funkcjonowania każdej formy życia społecznego, łamane są także inne z jego praw podstawowych. Kompleksowy charakter bezpieczeństwa implikuje kumulację zagrożeń w reakcji na brak bezpieczeństwa w którymkolwiek z jego aspektów. Zagrożeniom w jednej z dziedzin życia społecznego towarzyszą zagrożenia w innych obszarach ludzkiej egzystencji. Monitoring bezpieczeństwa politycznego w aspekcie informacyjnym oraz metody egzekwowania tych praw w warunkach społeczeństwa *rażonego totalitaryzmem* i *logiką oblężenia* powinny stać się niecierpiącym zwłoki przedmiotem porozumień ponadnarodowych, zorientowanych na wypracowanie holistycznej koncepcji bezpieczeństwa prawnego. W 1934 r. Czesław Znamierowski pisząc o bezpieczeństwie prawnym stwierdził istnienie zależności funkcjonalnych między strukturami legislacyjnymi państwa i ochroną bezpieczeństwa jednostki i społeczeństwa a ładem publicznym. Prawna kontrola organów państwa została omówiona jako niezbędna wobec naruszeń interesów jednostki. Przejście z epoki regulacji prawnych systemu westfalskiego do ery informacji wymaga jakościowej transformacji prawa[34]. Aksjologia współczesnej geopolityki implikuje świadomość niezbywalności legislacyjnej inkluzji kategorii życia ludzkiego w związku z aktywnością jednostek i grup w rzeczywistości wirtualnej, stosownie do wyzwań humanitarnych epoki.

32 A. Urbanek, *Koncepcja human security a kształtowanie środowiska bezpieczeństwa społeczności lokalnych*, w G. Kędzierska, A. Pepłoński (red.), *Zarządzanie kryzysowe. Podstawowe problemy*, WNSP, Białystok 2012.
33 http://hdr.undp.org/en/media/hdr_1994_en_chap2.pdf , s. 32-33.
34 Cz. Znamierowski, *Wiadomości elementarne o państwie*, Warszawa 1934, s. 28-36.

O podmiotowej potrzebie bezpieczeństwa politycznego i prawnego w erze informacji świadczą oba raporty, które stały się punktem wyjścia dla niniejszych rozważań. Oba zostały opublikowane 16 lat po wydaniu Raportu Rozwoju Ludzkiego i w obu podkreśla się jako kluczową dla ochrony wolności słowa w środowisku cyfrowym konieczność prawnego opracowania definicji pojęć, które wiążą się z niepokojącym naruszaniem praw człowieka w imię wojny z terroryzmem ogłoszonej jako konflikt o zasięgu globalnym. Ponadnarodowe struktury społeczno-militarne terroryzmu, wymagają transformacji prawa międzynarodowego. Niejasność terminologiczna obejmuje cały szereg pojęć, które nie pozostają bez wpływu na bezpieczeństwo Internautów. Dunja Mijatović wymienia wśród nich terminy takie jak 'szkodliwość', 'ekstremizm', 'mowa nienawiści', 'propaganda terrorystyczna'. Efektem tej niejasności jest erozja praw obywatelskich w cyberprzestrzeni oraz poważne luki istniejące w systemie egzekwowania prawa humanitarnego. Oba raporty są apelem o legislacyjne przeciwdziałanie podatności terminologii prawnej na subiektywne interpretacje. Dla dokonania istotnego postępu w semantyce prawa ponad-narodowego dotyczącego mass-mediów, podobnie jak interpretacji pojęcia bezpieczeństwa prawnego, uważam za pożądane włączenie intelektualnych zdobyczy na polu cybernetyki, wiedzy logicznej, teorii państwa, teorii prawa oraz filozofii kultury.

Agnieszka Jarzewicz - absolwentka studiów magisterskich w Instytucie Kulturoznawstwa UAM w Poznaniu i studiów doktoranckich w Instytucie Filozofii UAM. Zajmuje się problematyką z zakresu filozofii kultury i nauk o komunikacji.

Zapraszamy do udziału

WARSZTATY

WYKONYWANIE FUNKCJI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

- poziom I

17 października 2012 r., Warszawa

Warsztat prowadzi:

Dr Grzegorz Sibiga (Instytut Nauk Prawnych PAN)

Do kogo skierowane są warsztaty:

Za nadzór nad przestrzeganiem zasad techniczno-organizacyjnej ochrony danych odpowiedzialni są administratorzy bezpieczeństwa informacji. Warsztaty są skierowane do wszystkich osób wykonujących funkcję ABI w niejednoznacznym stanie prawnym, w którym status i obowiązki ABI zostały uregulowane w sposób niezwykle lakoniczny.

Korzyści z uczestnictwa w warsztatach:

- właściwe stosowanie przepisów o ochronie danych osobowych,
- omówienie prawnych obowiązków administratora bezpieczeństwa informacji,
- przygotowanie do kontroli GIODO

W programie m.in.:

- Podstawy prawne działania administratora bezpieczeństwa informacji
- Obowiązki ABI w zakresie bezpieczeństwa techniczno-organizacyjnego
- Administrator bezpieczeństwa informacji - status i kompetencje
- Udział ABI w kontroli inspektorów oraz postępowaniu przed GIODO
- Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych

Więcej informacji: www.cpi.com.pl

Metoda wartości wypracowanej (Earned Value)

dr inż. Dariusz Bogucki

Każdy menedżer projektu marzy o obiektywnym sposobie oceny stanu w jakim znajduje się jego projekt. Wiadomo bowiem, że mechaniczne porównanie harmonogramu bazowego i aktualnego nie zawsze upoważnia do stwierdzenia, że projekt jest opóźniony. Podobnie wyliczenie różnicy pomiędzy kosztem planowanym i rzeczywiście poniesionym nie zawsze wystarcza do oceny zasadności poniesionych kosztów.

Dobrze wiedzieć, że istnieje metoda, która pozwala na wiarygodną ocenę stanu zaawansowania projektu i zasadności poniesionych kosztów. **Metoda wartości wypracowanej – EV (ang. Earned Value)** jest standardem stosowanym w projektach finansowanych przez agencje rządowe USA (m.in. NASA, Ministerstwo Obrony), Bank Światowy, NATO a także Komisję Europejską i wielkie korporacje jak IBM.

Krótka historia

Zacznijmy od tego, że metoda EV nie jest to nowość ostatnich lat. Jej początki sięgają przełomu XIX i XX wieku, kiedy to w ocenie wyników procesu produkcyjnego zastosowano porównywanie rzeczywistej wartości wykonanej pracy z wartością planowaną.

Natomiast sama metoda Wartości Uzyskanej (EV) powstała w latach 60-tych i została opisana w podręczniku z 1963 roku *„Guide to PERT/Cost”*, jako narzędzie oceny postępu dużych projektów armii USA i NASA. Pierwszym projektem, w którym zastosowano tę metodę, był projekt rakiet balistycznych Minuteman, ale prawdziwym poligonem doświadczalnym dla EV, był projekt Apollo.

W 1967 roku Ministerstwo Obrony Stanów Zjednoczonych wprowadziło standard C/SCSC (*Cost/Scheduling Control System Criteria*), który obejmował 35 kryteriów, które miały warunkować skuteczne i obiektywne monitorowanie realizacji projektów (częste i kosztowne porażki), a kluczem było EV. W 1996 roku liczbę kryteriów zredukowano do 32 i całkowicie przebudowano, w ten sposób powstała koncepcja Earned Value Management System (EVMS), która została opisana w dokumencie ANSI / EIA 748.

Warto dodać, że w polskiej literaturze można spotkać **różne tłumaczenia terminu** EV: Wartość Uzyskana, Wartość Wypracowana, Wartość Zarobiona / Nabyta czy Przerób. Wszystkie te nazwy definiują sposób mierzenia postępu realizacji projektu na podstawie stosunku faktycznego nakładu

Na czym to wszystko polega

Najprościej wytłumaczyć działanie metody EV na przykładzie: Wyobraźmy sobie, że w projekcie X realizowane są zadania A i B polegające na położeniu po 120 km kabla światłowodowego przy koszcie 1 km = 3 JF (jednostek finansowych) w ciągu 4 JT (jednostek czasu). Kontrola przeprowadzona dla T=1 JT (czyli w ¼ projektu) pokazuje taki stan:

- W obydwu projektach miało być położone 30 km kabla (2x90 JF = 2x 3*30 JF);
- W projekcie A położono 20 km kabla, ale przy koszcie 1 km = 4 JF (4*20 =80 JF);

- W projekcie B położono 40 km kabla, ale przy koszcie 1 km = 2 JF (2*40= 80 JF);

W projektach A i B planowaliśmy zapłacić po 90 JF. W obydwu tak naprawdę zapłaciliśmy wykonawcom po 80 JF. Tak więc, w obydwu przypadkach różnica pomiędzy kosztem faktycznym i planowanym = +10 JF (zapłaciliśmy mniej, co niewątpliwie cieszy księgowych). Tyle, że ten wynik w jakikolwiek sposób nie pokazuje, że Projekt A jest realizowany drożej i wolniej a B – taniej i szybciej.

Taką wartością, która odwzorowuje wpływ opóźnienia zadania na koszty jest tzw. **Planowany Koszt Wykonanej Pracy (zwany Earned Value),** który obrazuje, ile planowaliśmy zapłacić za to, co rzeczywiście zrobiono:

- W przypadku A jest to: 20 x 3 JF = 60 JF (<90 JF)
- W przypadku B jest to: 40 x 3 JF = 120 JF (> 90 JF)

Wprowadźmy zatem następujące definicje:

1. **Planowany Koszt Planowanej Pracy:** Budgeted Cost of Work Scheduled (**BCWS**) / **Planned Value (PV)** – Suma planowanych kosztów realizacji zadań planowanych do poniesienia w danym momencie czasu;
2. **Rzeczywisty Koszt Wykonanej Pracy:** Actual Cost of Work Performed (**ACWP**) / **Actual Cost (AC)** – Suma rzeczywistych kosztów realizacji zadań faktycznie zrealizowanych w danym momencie czasu.
3. **Planowany Koszt Wykonanej Pracy:** Budgeted Cost of Work Performed (**BCWP**) /**Earned Value (EV)** – Suma planowanych kosztów realizacji zadań faktycznie zrealizowanych w danym momencie czasu.

Wskaźnik BCWP ma interesującą interpretację: Z jednej strony BCWP pokazuje, ile **zgodnie z planem** zapłacono, by za **rzeczywiście wykonaną** pracę (podczas gdy ACWP mówi, ile faktycznie zapłacono za **rzeczywiście wykonaną** pracę). z drugiej zaś BCWP wyraża **ilość rzeczywiście wykonanej** pracy w języku kosztów planowanych (podczas gdy BCWS wyraża **ilość pracy planowanej** do danego dnia, w języku kosztów planowanych).

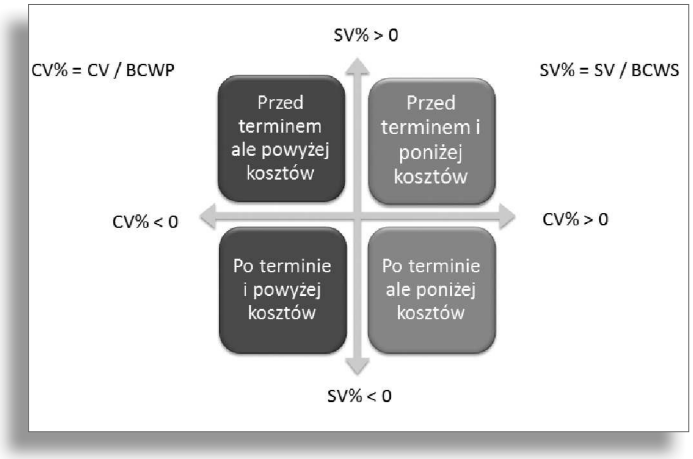
Wskaźniki podstawowe

Wprowadźmy następujące wskaźniki:

4. **Odchylenie Kosztu *CV = BCWP-ACWP*** (ang. Cost Variance - CV) pokazuje odchylenie od kwoty, którą powinno się zapłacić za rzeczywiście wykonaną pracę. Innymi słowy wskaźnik ten pokazuje, jaki jest wynik finansowy faktycznie wykonanych prac w stosunku do planu:
   - **CV < 0** wskazuje, że praca do tej pory była wykonywana drożej niż przewidywano (oszacowanie kosztu było zbyt optymistyczne).
   - **CV > 0** wskazuje na to, że pracę wykonuje się taniej.

Fakt opóźnienia lub przyśpieszenia wykonania zadania nie jest w CV w ogóle brany pod uwagę. Ponadto wskaźnik ma charakter lokalny: CV < 0 może wynikać z wykonania prac droższych, ale nie planowanych na ten okres lub z wykonania prac więcej niż planowano

2. **Odchylenie Harmonogramu *SV = BCWP-BCWS*** (ang. *Schedule Variance* - SV) pokazuje odchylenie od ilości pracy, która miała być (zgodnie z planem) wykonana do danego dnia, wycenione w kosztach planowanych (budżetowanych). SV pokazuje zatem postęp w czasie prac faktycznie wykonanych, a więc opóźnienia i przyspieszenia realizacji zadań:



Rysunek 1: *Interpretacja parametrów CV i SV*

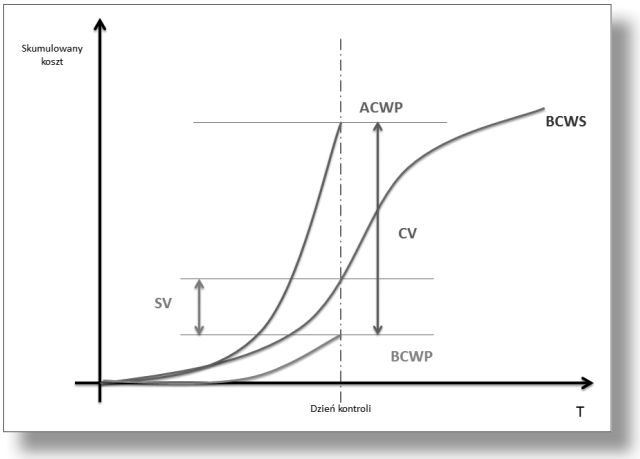
- **SV < 0** wskazuje, że praca do tej pory była wykonywana dłużej niż przewidywano (oszacowanie harmonogramu było zbyt optymistyczne).
- **SV > 0** wskazuje na to, że pracę wykonuje się szybciej.

Wymiarem SV nie są jednostki czasu a finansowe! Wskaźnik ten podobnie jak CV ma charakter lokalny: SV < 0 może wynikać z wykonania prac dodatkowych, ale nieplanowanych na ten okres lub z wykonania prac więcej niż planowano.

Wskaźniki SV i CV analizowane wspólnie, pozwalają ocenić sytuację ewentualnego braku pieniędzy w budżecie lub ich nadwyżki w danym momencie, co obrazuje poniższy diagram, na którym wartości CV i SV znormalizowano zgodnie z regułami ***CV% = CV / BCWP i SV% = SV / BCWS:***

Ich interpretacja jest prosta i czytelna:

CV%	SV%	Interpretacja
>0	>0	Projekt przeszacowany, założono za duże marginesy czasu i finansowe na realizacje zadań. Należy zmodyfikować plan projektu.
>0	<0	W projekcie wystąpiły opóźnienia w realizacji zadań i w wydatkowaniu środków (sytuacja dość typowa dla projektów w administracji np. w wyniku problemów z zamówieniami publicznymi)
<0	>0	W projekcie przyśpieszono realizację zadań kosztem dodatkowych środków (sytuacja dla projektów biznesowych realizowanych w obliczu konkurencji).
<0	<0	Projekt niedoszacowany, założono za małe rezerwy na czas i środki. Należy zmodyfikować plan projektu.
=0	=0	Projekt realizowany idealnie zgodnie z planem. Niestety, najczęściej to tylko teoria.



Rysunek 2: *Interpretacja podstawowych parametrów metody EV*

Powyższy rysunek obrazuje sposób wyliczenia wskaźników podstawowych na tle przebiegu krzywych BCWS, BCWP i ACWP:

Oprócz opisanych wyżej odchyleń różnicowych, metoda *Earned Value* stosuje **dwa wskaźniki wydajności**:

- **Wskaźnik Wydajności Kosztu** (Cost Performance Index) **CPI = BCWP/ACWP**
- **Wskaźnik Wydajności Harmonogramu** (Schedule Performance Index) **SPI = BCWP/BCWS**

Systematyczne śledzenie CPI i SPI dostarcza skumulowanych informacji na temat dotychczasowego przebiegu realizacji projektu:

CPI pokazuje, jak kształtowały się (dotychczas) rzeczywiste koszty jednostkowe w stosunku do planowanych. Na przykład CPI = 0,92 oznacza, że za <u>każdą wydaną złotówkę</u> wykonano pracę o wartości 0,92 zł.

SPI z kolei ilustruje, jaka część planowanej pracy została faktycznie wykonana. Dla przykładu SPI = 0,7 oznacza, że <u>z każdej złotówki planowanej pracy</u> wykonano jedynie pracę o wartości 0,70 zł.

CPI < 1 oznacza, że koszt wykonanej pracy jest wyższy niż planowano, natomiast CPI > 1 - koszt wykonanej pracy jest niższy niż planowano (co nie musi być dobre). Z kolei SPI > 1 oznacza, że praca wykonywana jest przed czasem, a SPI < 1 oznacza wystąpienie opóźnienia w projekcie.

Wyznaczanie EV

Istota metody polega na śledzeniu stanu zaawansowania wykonywanych prac i obliczeniu wartości tych prac według założeń budżetowych (zaakceptowanego kosztorysu). W danej chwili dla każdego zadania określa się trzy wielkości związane z zasadnością poniesionych kosztów. Metodyczne podejście do zastosowania Earned Value wymaga:

1. Zbudowania możliwie najbardziej szczegółowego harmonogramu projektu / programu z pełną strukturą podziału pracy (WBS);
2. Zbudowania na tej podstawie Bazowego Harmonogramu Rzeczowo-Finansowego – podstawa do wyznaczenia PV;
3. Zdefiniowania reguł „tworzenia wartości uzyskanej" – metryk, reguł i wskaźników umożliwiających ocenę stopnia zaawansowania prac;
4. Monitorowania postępu wykonywanej pracy zgodnie z przyjętymi założeniami (aktualny HRF) i wyznaczania w ten sposób AC oraz EV;

Kluczowe (ale i najtrudniejsze) w tym algorytmie jest właściwe wyznaczanie *Wartości Uzyskanej (EV) poszczególnych zadań.* Im dokładniej będzie ona wyznaczona, tym lepszą ocenę prac uzyskamy. Definicyjnie EV jest to **suma planowanych budżetów wykonanych zadań**, którą można obliczyć korzystając ze wzoru:

$$BCWP = BZ * \%WZ ,$$

gdzie:

BZ – Budżet zadania (planowany),

%WZ – Procent wykonania zadania <=1 i to stwarza problem,

Głównym zadaniem w wyznaczaniu EV jest dobranie takiej reguły / metryki, aby możliwie dobrze ilustrowała nie tyle „harmonogramowe" postępy prac, ile stan zaawansowania produktów projektu – to istota EVMS. Jest to zarazem główny problem omawianej metody, bowiem nie ma jednej reguły, która da się zastosować we wszystkich przypadkach.

Poniższa tabela ilustruje najczęściej stosowane reguły wyznaczania EV:

Metoda	Opis	Uwagi
Metoda 0/100	• Najprostsza metoda, polegająca na przydzieleniu wartości uzyskanej w wysokości 100% planowanych kosztów dopiero po całkowitym wykonaniu zadania. • Do momentu zakończenia zadania jest określone, jako niewykonane.	Metoda odpowiednia dla krótkotrwałych projektów z małą liczba zadań. Jest także stosowana do oceny zewnętrznej projektu, gdy brak jest bliższych danych o nim.
Metoda 50/50	• Metoda podobna do poprzedniej, ale po rozpoczęciu zadania uzyskuje ona 50% planowanego budżetu. • Kolejne 50% przydzielane jest dopiero po ukończeniu zadania.	Przy dużej liczbie takich zadań, statystyczny rozkład ich rozpoczęć i zakończeń powoduje, że krzywa wartości uzyskanych dobrze odpowiada rzeczywistości.
Metoda 0/30/70/90/100 (przedziałowa)	Wartości procentowe są środkami przedziałów, zatem w tej metodzie przyporządkowujemy kolejne części budżetu w następujący sposób: • 0% – od rozpoczęcia zadania do 15% jego wykonania. • 30% – gdy zadanie jest w fazie 15% do 50% realizacji. • 90% – dla zadania wykonanego w 80% do 95%. • 100% – od 95% do 100% wykonania zadania.	Metoda ta jest oparta na ocenie eksperta, który na podstawie swojej wiedzy o zakresie i realizacji zadania, klasyfikuje je do odpowiednich przedziałów. Funkcjonuje w kilku wariantach wartości progowych przedziałów. Stosowana przez Komisję Europejską do oceny postępu projektów B+R.

Metoda	Opis	Uwagi
Metoda subiektywnej oceny	• Metoda ta również opiera się na ocenie eksperta, z tą jednak różnicą, że nie klasyfikuje on zadania do jednej z kilku „przegródek" a po prostu ocenia postęp zadania. • Wartość uzyskaną przydzielamy zgodnie z tą oceną.	Wadą tej metody są zwykle zbyt optymistyczne oceny eksperta, szczególnie, gdy ocenia on samego siebie. W tej sytuacji oceny szybko sięgają pułapu 90%, a potem długo nie mogą osiągnąć 100%.
Metoda w oparciu o doświadczenie	Metoda ta bazuje na podobieństwie aktualnego zadania (projektu, etapu) do zadań (projektów, etapów) wykonywanych w przeszłości. Na podstawie informacji o wykonaniu w obecnym projekcie.	Metoda ta jest stosowana głównie w budownictwie.
Według wag kamieni milowych	Wartość uzyskaną przypisujemy na podstawie wag odpowiadających kamieniom milowym projektu, najczęściej na bazie kwot w harmonogramie finansowym projektu.	Wariantem tej metody jest uwzględnianie również procentu wykonania zadania. Stosowana przez Komisję Europejską do oceny postępu projektów B+R.
Metoda wskaźników obiektywnych	Stosowana początkowo w ocenie postępu prac budowlanych. Kontrolerzy obmierzali postęp prac i na tej podstawie przydzielano wartość uzyskaną.	Rozważana przez Komisję Europejską do oceny realizacji projektów inwestycyjnych.

Prognozowanie przyszłości projektu

Metoda Earned Value pozwala nie tylko ocenić obecny stan realizacji projektu, ale z dobrym przybliżeniem przewidzieć jego przyszłość i uprzedzić o grożących nam problemach. Służy do tego pięć parametrów:

- **BAC** *(Budget At Completion)* — **aktualna wartość budżetu końcowego**.

  Jest to taki budżet projektu (zadania, grupy zadań), jaki według dzisiejszej wiedzy będzie obowiązywał na końcu projektu. Z BAC można porównywać prognozowane koszty. Jeśli nie zostały podjęte decyzje dotyczące zmiany BAC, to BAC będzie zawsze budżetem początkowym.
  Zawsze obowiązuje wzór: **BAC = Budżet początkowy + zaakceptowane modyfikacje.**

- **EAC** (Estimate at Completion) **- szacowany koszt końcowy:**
  Jest to przewidywany koszt całkowity realizacji całego projektu, całego zadania, bądź całej grupy zadań według stanu wiedzy na dzisiaj. Innymi słowy jest to poprawiona estymacja kosztu sprzed rozpoczęcia realizacji.
  EAC wyliczany jest wg. liniowej aproksymacji AC (ACWS):

$$EAC = AC + \frac{BAC - EV}{CPI} = BAC/CPI$$

- **ETC (Estimate to Complete) - szacowany koszt pozostały**, czyli ile jeszcze przewiduje się wydać na dane zadanie czy projekt, wg stanu wiedzy na dzień dzisiejszy. Zachodzi równość: **EAC = AC+ ETC** (wydaliśmy już AC)

- **VAC (Variance At Completion) - prognozowane odchylenie od kosztów,** po zakończeniu projektu (zadania, grupy zadań), które oblicza się za pomocą następującego wzoru:

VAC = BAC – EAC

Interpretacja VAC jest kluczowa dla losów projektu: Jeśli VAC > 0, to projekt zmieści się w planowanym budżecie jeśli jednak VAC < 0, to mamy problem, bo projekt nie zmieści się w budżecie.

- **EOR/ ETR (Estimate of Realization / Estimated Time of realization) Szacowany Czas Realizacji,** jest to wskaźnik, który pokazuje, jaki będzie końcowy czas realizacji projektu. Jest on wyrażony w jednostkach czasu (nie w pieniądzach) i liczony wg wzoru:

EOR = ETR = czas_planowany / SPI

Poniższy wykres ilustruje sposób wyliczenia wspomnianych parametrów.

Na koniec należy wspomnieć o dwóch tzw. **Wymaganych Wskaźnikach Wydajności**, przydatnych do monitorowania pozostałego do wykonania zakresu prac w projekcie. Są to:

- **Wymagany Wskaźnik Wydajności Kosztu (*TCPI*):**

TCPI =(BAC-BCWP)/(BAC-ACWP)

Wskaźnik ten pokazuje, z jaką wydajnością trzeba by realizować pozostały do wykonania zakres projektu, aby zmieścić się w dysponowanym funduszu projektu. Dla przykładu TCPI = 1,10 oznacza, że każda wydana złotówka powinna przynieść pracę o wartości 1,10 zł.

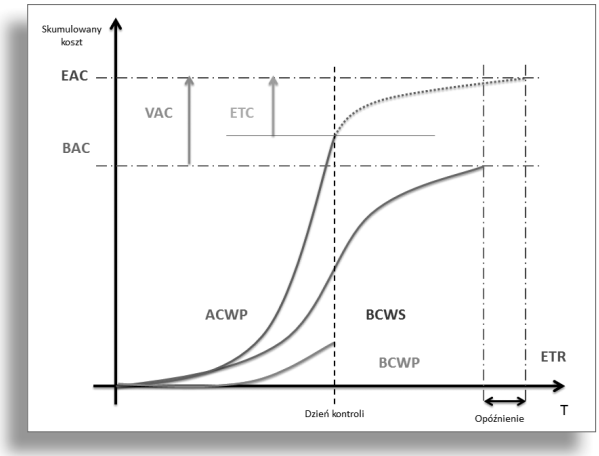
- **Wymagany Wskaźnik Wydajności Harmonogramu (*TCSI*):**

TCSI =(BAC-BCWP)/(BAC-BCWS)

Ten z kolei parametr pokazuje, z jaką wydajnością trzeba realizować pozostały zakres prac, aby zakończyć projekt planowo. Dla przykładu TCPI = 1,50 oznacza, że każda wydana złotówka na pozostałe prace powinna przynieść pracę, dotąd realizowaną za 1,50 zł.

Zalety i wady metody EV

W 1997 roku przeprowadzono badania ponad 700 dużych amerykańskich przedsięwzięć, które pokazało jej wysoka użyteczność:



Rysunek 3: *Interpretacja parametrów prognostycznych metody EV*

- Zastosowanie Earned Value już przy **15–20 %** zaawansowania projektu daje możliwość trafnego przewidzenia wyniku końcowego z dużą dokładnością i to niezależnie od typu programu, projektu, usługi.
- Po wykonaniu 15 % projektu można przyjąć, że ostateczne przekroczenie budżetu będzie nie mniejsze niż bieżące szacunki.
- Dla 20 % wykonania projektu, wskaźnik CPI jest już stabilny. Jego zmiany wahają się w granicach ±10%, co daje możliwość oszacowania końcowego kosztu projektu z dużym prawdopodobieństwem.

Konstrukcja metody powoduje jednak, że jest nieodporna na kłamstwa: opiera się na rzetelności osób, które podają dane podlegające kontroli i jakości bazowego i aktualnego harmonogramu rzeczowo-finansowego realizacji przedsięwzięcia. Wymaga ponadto dość szczegółowej kwantyfikacji planu projektu, jest zatem często postrzegana jako nie przystająca do projektów realizowanych zgodnie z metodykami zwinnymi (Agile) – co nie jest do końca prawdą.

EV nie posiada ponadto narzędzia pomiaru, jakości projektu, więc możliwe jest, że wskaźniki pokazują, że projekt mieści się w ramach budżetu i jest przed terminem, ale klienci są niezadowoleni z zakresu i jakości produktów.

Tradycyjne podejście od metody EV ma kłopoty z uwzględnieniem „pracy ciągłej" w projekcie (LOE – Level of Effort), której nie da się prosto skwantyfikować wydatkami.

Wadą metody EV jest nieintuicyjny SV (wyrażony w pieniądzu) i „samouzupełniajacy się" do 1 na koniec projektu wskaźnik SPI. W rezultacie szacowanie opóźnienia projektu blisko jego końca jest mało wiarygodne. Rozwiązaniem usuwającym ten problem jest rozwinięcie oryginalnej metody tzw. wariant **Earned Schedule**, który „przelicza" SV i SPI „na język czasu" poprzez wprowadzenie pomiaru odchylenia czasowego „w osi horyzontalnej". Odbywa się to zgodnie z regułami:

$$SV(t) = AT - ES;$$

$$SPI(t) = AT / ES,$$

Gdzie **AT** (Actual Time) – to czas przeprowadzania kontroli, a **ES** (Earned Schedule) - czas, w jakim BCWS osiągnie taką wartość, jaką BCWP osiągnęło w dniu kontroli, czyli **BCWS (ES) = BCWP (AT).**

Oczywiście precyzyjne wyznaczanie ES na podstawie dyskretnych wartości BCWS i BCWP nie jest proste, ale zdecydowanie poprawia prognozę czasu zakończenia projektu wg reguły:

$$ETR(t) = czas_planowany / SPI(t)$$

Podsumowując

Metoda wartości wypracowanej (EV) jest ważnym i użytecznym narzędziem menedżera projektu. Jest stosunkowo prosta w realizacji, oparta na jasnych i dobrze określonych regułach. Jest standardem *de facto* oceny zaawansowania projektu:

- Technika EV integruje ocenę zakresu, harmonogramu i koszt projektu przy pomocy prostych, jednoznacznych wskaźników;
- Metoda ta pozwala w jasny sposób odpowiedzieć na wiele pytań interesariuszy projektu. Może być stosowana do oceny przeszłych wyników projektu, aktualnego stanu jego realizacji, jak i do prognozowania przyszłych wyników projektu przez wykorzystanie technik statystycznych;
- Dobre planowanie projektu w połączeniu z efektywnym wykorzystaniem techniki EV zmniejsza liczbę problemów wynikających z przekroczenia harmonogramu i kosztów projektu.

Warto się zatem nią zainteresować nie tylko dlatego, że Komisja Europejska przymierza się do wdrożenia jej, jako standardu oceny postępów wszystkich projektów współfinansowanych ze środków UE, w nowej perspektywie finansowej na lata 2013-2020.

Dr inż. Dariusz Bogucki - dyrektor ds. Sektora Publicznego w EFICOM SA, wykładowca na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

Zapraszamy do udziału

FORUM

XIX FORUM INFORMATYKI W ADMINISTRACJI

18-19 października 2012 r.

Hotel Holiday Inn ****, ul. Telimeny 1, 05-410 Józefów k. Warszawy

19. edycja Forum Informatyki w Administracji, zgodnie z tradycja tej imprezy, ma dwa podstawowe nurty tematyczne. Pierwszy wątek to przegląd aktualnych problemów informatycznych administracji publicznej i propozycji ich rozwiązań (w tym także oferta, wiodących w tym zakresie firm teleinformatycznych). Drugi nurt to wykłady dyskusje wykraczające poza bezpośredni profesjonalizm i wprowadzenie treści uniwersalnych. Wykład Redaktora Jacka Żakowskiego na temat społecznych uwarunkowań wykluczenia cyfrowego oraz Profesora Andrzeja Markowskiego o poprawności języka urzędowego - to najlepsze przykłady humanistycznych akcentów w programie Forum. A poza tym - możliwości ciekawych rozmów i dyskusji kuluarowych, jak również konsultacji w stoiskach firmowych. Miłej i komfortowej atmosferze przebiegu Forum będzie sprzyjać lokalizacja imprezy w hotelu Holiday Inn Warszawa-Józefów.

W programie m.in.:

- Społeczne uwarunkowania wykluczenia cyfrowego
- Projekt ustawy o wykonywaniu zadań publicznych drogą elektroniczną w kontekście cech nowoczesnej administracji publicznej
- Rozporządzenie Rady Ministrów z dnia 12/04/2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych - dostosowanie systemów informatycznych podmiotów realizujących zadania publiczne do wymagań określonych w/w Rozporządzeniem w maksymalnym terminie 3 lat od wejścia w życie Rozporządzenia
- Rozwój kompetencji cyfrowych w administracji publicznej
- Bezpieczeństwo i dostępność danych w systemach IT (Rozwiązania NetApp)
- Kierunki rozwoju ePUAP
- Co trzeba zmienić aby przeciwdziałać niepowodzeniom przy realizacji centralnych projektów teleinformatycznych
- Prywatne czy publiczne - prawo autorskie a administracja
- Pułapki prawa autorskiego w zamówieniach publicznych, realizowanych przez jednostki administracji publicznej
- Język urzędowy - normy poprawności i komunikatywność przekazu
- Czy telefon komórkowy (smartfon) może służyć jako narzędzie elektronicznej administracji
- Perspektywy infrastruktury szerokopasmowej w kontekście zadań administracji publicznej. Inwentaryzacja infrastruktury, prowadzona przez UKE oraz dostępność danych i ich wykorzystanie

Więcej informacji: www.cpi-sk.pl

Uwagi o właściwości miejscowej sądu penitencjarnego w przedmiocie udzielenia zezwolenia na zastosowanie dozoru elektronicznego

Agnieszka Zdanowska

Zagadnienie wykonywania kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego wydaje się budzić od samego początku obowiązywania ustawy z dnia 7 września 2007 roku[1] liczne wątpliwości interpretacyjne, które zdają się nie maleć nawet w miarę coraz częstszego stosowania owej instytucji w praktyce sądów penitencjarnych. Wątpliwości, skutkujące niespójnością orzecznictwa, pojawiają się nie tylko w rozstrzygnięciach sądów penitencjarnych, orzekających w przedmiocie dozoru elektronicznego, ale także w orzecznictwie sądów apelacyjnych, rozstrzygających tak podstawowe kwestie jak – częste znamiennie – spory o właściwość pomiędzy sądami penitencjarnymi[2]. Ponadto na wskazane powyżej wątpliwości interpretacyjne, nakłada się – uzasadniony jeszcze jednak „nowością" instytucji dozoru elektronicznego – brak dorobku orzecznictwa i doktryny w tym zakresie, a także – jako problem „najnowszy" - proponowana w rządowym projekcie ustawy o zmianie ustawy o dozorze elektronicznym[3] nowa funkcja dozoru elektronicznego, jako instrumentu realizacji proponowanego przedmiotowym projektem tzw. aresztu domowego, stosowanego jako – równorzędny z tymczasowym aresztowaniem - środek zapobiegawczy.

Mając na uwadze specyfikę procesu orzekania w przedmiocie zezwolenia przez sąd penitencjarny na odbycie przez skazanego orzeczonej wobec niego kary pozbawienia wolności w systemie dozoru elektronicznego, polegającą – poza warunkami wskazanymi w art. 6 ustawy o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego (dalej w skrócie: DozElektrU) – między innymi na ustaleniu przez sąd, poprzez zwrócenie się o nadesłanie informacji od tzw. upoważnionego podmiotu dozorującego, czy na przeszkodzie w udzieleniu wyżej wymienionego zezwolenia nie stoją warunki techniczne, wskazać należy na zagadnienie właściwości miejscowej sądu penitencjarnego orzekającego w przedmiocie zastosowania dozoru elektronicznego.

Istotny z punktu widzenia omawianego zagadnienia, przepis art. 38 DozElektrU, wskazujący właściwość miejscową sądu penitencjarnego orzekającego w przedmiocie udzielenia zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego, pomimo krótkiego czasu obowiązywania ustawy, był już przedmiotem istotnej nowelizacji obowiązującej od 25 czerwca 2010 roku[4], która zmieniając

1 Ustawa z dnia 7 września 2007 roku o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego, tekst jedn. Dz. U. z 2010 r. Nr 142, poz. 960, z późn. zm.

2 Por. np. postanowienie Sądu Apelacyjnego w Katowicach z dnia 10 listopada 2009 r., sygn. II AKo 219/09, KZS 2010, nr 1, poz. 78; postanowienie Sądu Apelacyjnego w Warszawie dnia 2 lutego 2010 r., sygn. II AKo 3/10, Lex nr 677997; postanowienie Sądu Apelacyjnego w Warszawie dnia 31 marca 2010 r., sygn. II AKo 38/10, Lex nr 678002.

3 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego oraz niektórych innych ustaw (Druk sejmowy Nr 4602).

4 Ustawa z dnia 21 maja 2010 r. o zmianie ustawy o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego, Dz. U. z 2010 r. Nr 101, poz. 647.

brzmienie tegoż przepisu *in fine* stała się podstawą licznych wątpliwości interpretacyjnych. Przepis art. 38 DozElektrU w swoim pierwotnym brzmieniu stanowił bowiem, iż „orzekanie w sprawach dotyczących wykonania kary pozbawienia wolności w systemie dozoru elektronicznego należy do sądu penitencjarnego, w którego okręgu kara jest lub ma być wykonywana”[5].

Jednocześnie przytoczone powyżej brzmienie art. 38 DozElektrU pozostawało w ścisłym związku z – kluczowym dla przedmiotowej ustawy w brzmieniu sprzed nowelizacji z dnia 21 maja 2010 roku – art. 6, którego ust. 2 miał zastosowanie w przypadku skazanych już odbywających orzeczoną karę pozbawienia wolności w zakładzie karnym, a chcących skorzystać z dozoru, tj. w tzw. schemacie następczym (*back door)*[6]. Mając na uwadze fundamentalny – dla całego systemu wykonywania kary pozbawienia wolności w systemie dozoru elektronicznego – art. 6 DozElektrU, na marginesie niniejszych rozważań, wskazać należy na kształtowanie się jego treści w toku kolejnych nowelizacji.

Przedmiotowy przepis w pierwotnym brzmieniu stanowił, iż sąd penitencjarny może udzielić zezwolenia na odbycie kary pozbawienia wolności nieprzekraczającej 6 miesięcy w systemie dozoru elektronicznego skazanemu na taką karę (…), przy czym możliwość zastosowania dozoru elektronicznego istniała również wobec skazanych, którym – zgodnie z art. 6 ust. 2 – wymierzono karę nieprzekraczającą roku, przy czym czas pozostały do odbycia tej kary nie przekracza 6 miesięcy. Takie brzmienie ustawy stwarzało możliwość odbywania kary pozbawienia wolności w systemie dozoru elektronicznego nie tylko wobec skazanych, którym nie zarządzono jeszcze wykonania kary, ale także w stosunku do skazanych już odbywających karę pozbawienia wolności.

Nowelizacją z 21 maja 2010 roku podwyższono przedmiotowe kryterium wysokości orzeczonej kary pozbawienia wolności, która może być wykonywana w systemie dozoru elektronicznego, do wymiaru 1 roku. Znowelizowany przepis wskazuje nadto, iż wskazane powyżej kryterium 1 roku ma również zastosowanie do skazanego, któremu wymierzono dwie lub więcej niepodlegających łączeniu kar pozbawienia wolności, które skazany ma odbyć kolejno. Takie działanie ustawodawcy uzasadniane było usprawnieniem procedur związanych ze stosowaniem instytucji wykonywania kary pozbawienia wolności w systemie dozoru elektronicznego w krajowym porządku prawnym[7], poprzez racjonalizację i usprawnienie systemu udzielania zezwoleń na odbywanie kary pozbawienia wolności w systemie dozoru elektronicznego przez wskazane sądy penitencjarne[8].

Wskazane wyżej pierwotne brzmienie art. 38 DozElektrU pozwoliło wypracować jednolite w tym zakresie stanowisko doktryny, które jednoznacznie wskazywało, w kontekście kryterium właściwości miejscowej, iż zamiarem [ustawodawcy] było wskazanie jako właściwego sądu, w którego okręgu kara jest wykonywana, a drugi człon alternatywy, tj. sąd, w którego okręgu kara ma być wykonywana, pojawił się dla potrzeb rozpoznania wniosku o zastosowanie dozoru

5 Dz. U. z 2007 r. Nr 191, poz. 1366.
6 Zob. np. W. Kotowski, B. Kurzępa, Dozór elektroniczny. Komentarz praktyczny, Warszawa 2009, s. 32-38.
7 A. Kiełtyka, A. Ważny, Ustawa o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego. Komentarz, Warszawa 2011, s. 78.
8 Ibidem, s. 78.

elektronicznego, na (…) etapie [kiedy] dozór elektroniczny jeszcze nie jest wykonywany; jak się wydaje, pierwszeństwo winno mieć kryterium miejsca aktualnego wykonywania kary, a kryterium miejsca przyszłego wykonywania należy stosować tylko wtedy, gdy kara nie jest jeszcze wykonywana[9].

Ponadto w świetle obowiązującej wówczas ustawy, w kontekście dozorowania w tzw. schemacie następczym zadawano pytanie, czy ustawodawcy chodziło o sąd penitencjarny miejsca wykonywania kary pozbawienia wolności w systemie dozoru elektronicznego czy miejsca wykonywania kary pozbawienia wolności w ogóle[10], jednocześnie stawiając tezę, iż chodzi raczej o miejsce wykonywania kary w systemie dozoru elektronicznego, gdyż do takiego wniosku prowadzi wykładnia funkcjonalna, a także sugestia wynikająca z redakcji końcowej części art. 38 – karą, która „ma być wykonywana", jest z pewnością kara w systemie dozoru elektronicznego, a ustawodawca ujmuje ją w tej normie łącznie z karą, która „jest wykonywana"[11].

Jednocześnie w piśmiennictwie podnoszono[12], iż w przypadku orzekania o dozorze *back door* (art. 6 ust. 2 DozElektrU), jeśli zakład karny, w którym skazany przebywa i przyszłe miejsce dozorowania leżą w okręgu różnych sądów penitencjarnych, należy przyjąć, że właściwy jest sąd miejsca przyszłego dozorowania. Przy czym sądem wykonującym karę pozbawienia wolności w systemie dozoru elektronicznego powinien być sąd właściwy dla miejsca wykonywania tej kary. Co więcej, sąd ten powinien przeprowadzić posiedzenie w zakładzie karnym, w którym przebywa skazany (art. 41 ust.1 DozElekrU), co oznacza przeprowadzenie posiedzenia w zakładzie leżącym w okręgu innego sądu penitencjarnego. We wskazanym kontekście nadto postulowano rozważenie „rozdzielenia kompetencji do decydowania o zastosowaniu dozoru elektronicznego od kompetencji do jego wykonywania"[13].

Wspomnianą nowelizacją z 21 maja 2010 roku ustawodawca, zmieniając treść art. 38 DozElektrU, określił kryterium właściwości miejscowej sądu penitencjarnego orzekającego w przedmiocie udzielenia zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego wskazując na sąd penitencjarny, w którego okręgu skazany przebywa. Taka zmiana redakcyjna brzmienia przepisu skutkuje wątpliwościami interpretacyjnymi w zakresie określenia właściwości miejscowej sądu penitencjarnego właściwego do udzielenia dozoru elektronicznego.

Jednocześnie znamienne jest, że przez wprowadzenie nowej zasady zakładało się znaczne usprawnienie procesu orzekania w sprawach stosowania systemu dozoru elektronicznego[14]. W uzasadnieniu przedmiotowej nowelizacji wskazano jedynie, że „nowe brzmienie art. 38 (…) doprecyzowuje właściwość sądu, co do samej kwestii udzielenia zezwolenia"[15].

Rozważając założenia uzasadnienia nowelizacji trzeba przypomnieć treść art. 41 ust 1 DozElektrU, który stanowi, że jeżeli wniosek

9 M. Rusinek, Ustawa o dozorze elektronicznym. Komentarz., Warszawa 2010, s. 158 i n.
10 Ibidem, s. 158-160
11 Ibidem, s. 158-160
12 Ibidem, s. 158-160
13 Ibidem, s. 158-160.
14 A. Kiełtyka, A. Ważny, Ustawa o wykonywaniu …, s. 80.
15 Uzasadnienie do projektu ustawy o zmianie ustawy o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego (Druk sejmowy Nr 2855).

o udzielenie skazanemu zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego, dotyczy skazanego, który odbywa już karę pozbawienia wolności w zakładzie karnym, posiedzenie sądu penitencjarnego powinno odbyć się w tym zakładzie, w którym skazany przebywa. W uzasadnieniu do projektu nowelizacji art. 38 DozElektrU[16] wskazywano, że „dotychczasowe brzmienie przepisu sprawiałoby ogromne trudności w świetle art. 41, gdy skazany odbywał karę np. w Suwałkach, a kara w systemie dozoru elektronicznego miałaby być wykonywana we Wrocławiu z uwagi na miejsce stałego pobytu, to sąd z Wrocławia, będąc właściwy, musiałby odbyć posiedzenie w zakładzie karnym w Suwałkach lub skorzystać z pomocy prawnej, co w sposób oczywisty przedłużałoby postępowanie i zwiększało jego koszty". Jednocześnie można domniemywać, iż ujęcie właściwości miejscowej sądu penitencjarnego właśnie poprzez zapis „okręg, w którym skazany przebywa" mogło mieć na celu dostosowanie treści art. 38 DozElektrU do generalnej zasady właściwości miejscowej sądu penitencjarnego, ujętej w art. 3 § 2 k.k.w., który stanowi, że kompetencje należące do sądu penitencjarnego w postępowaniu wykonawczym realizuje sąd penitencjarny, w którego okręgu przebywa skazany, chyba że ustawa stanowi inaczej. Jednak i takie uzasadnienie wydaje się być niecelowe, bowiem bezpośrednie zastosowanie ogólnej regulacji w zakresie właściwości miejscowej na zasadach kodeksu karnego wykonawczego w odniesieniu do dozoru elektronicznego możliwe jest poprzez sięgnięcie do art. 5 DozElektrU.

Bezspornym jest, iż przepis art. 38 DozElektrU określa właściwość miejscową sądu penitencjarnego do orzekania w przedmiocie udzielenia zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego, zarówno skazanym pozbawionym wolności, jak też skazanym pozostającym na wolności i oczekującym na wprowadzenie tej kary do wykonania. W przypadku skazanego pozostającego na wolności, oczekującego na wprowadzenia orzeczonej kary do wykonania zagadnienie właściwości miejscowej sądu penitencjarnego orzekającego o dozorze elektronicznym nie budzi wątpliwości, jest to bowiem Sąd penitencjarny, w okręgu którego skazany przebywa, a uściślając miejsca jego zamieszkania, gdzie dozór będzie wykonywany.

Wątpliwości interpretacyjne pojawiają się w przypadku skazanego pozbawionego wolności. Można sobie bowiem wyobrazić sytuację, w której skazany kończy odbywanie kary pozbawienia wolności w zakładzie karnym właśnie np. w Suwałkach, jednocześnie w tym czasie zapada prawomocny wyrok w innej jego sprawie, gdzie wymiar kary pozwala złożyć wniosek o jej wykonanie w systemie dozoru elektronicznego w miejscu zamieszkania skazanego znajdującym się w okręgu np. Sądu Okręgowego dla Warszawy – Pragi. Czy w takim przypadku sądem właściwym miejscowo będzie sąd, w okręgu którego skazany odbywa karę pozbawienia wolności, czy też sąd, w okręgu którego dozór miałby być wykonywany.

Zgodnie z regulacją ogólną – zawartą w art. 3 § 2 k.k.w. – kompetencje należące do sądu penitencjarnego w postępowaniu wykonawczym realizuje sąd penitencjarny, w którego okręgu przebywa skazany, chyba że ustawa stanowi inaczej[17]. Literalna wykładnia treści przepisu art. 38 DozElektrU w połączeniu z treścią art. 3 § 2 k.k.w., nakazywałaby przyjąć, że w powyższym przypadku sądem

16 Zob. cyt. wyżej uzasadnianie do projektu.
17 M. Rusinek, Ustawa o dozorze …, s. 158.

właściwym będzie sąd penitencjarny, w którego okręgu skazany przebywa, a więc sąd penitencjarny w okręgu, którego położony jest zakład karny, gdzie skazany obecnie przebywa, tj. Sąd Okręgowy w Suwałkach. Wskazać jednocześnie należy, iż w przedmiotowym przypadku nie ma zastosowania treść art. 41 ust 1 DozElektrU, bowiem jak trafnie podniesiono w doktrynie[18] dyrektywa art. 41 ust. 1 dotyczy skazanego, który „odbywa już karę pozbawienia wolności w zakładzie karnym". Użycie słowa „już" sugeruje, że chodzi o odbywanie tej kary, która ma być przedmiotem wniosku o zastosowanie dozoru elektronicznego. Chodzi więc przede wszystkim o dozór w schemacie następczym (*back door*) z art. 6 ust. 2 DozElekrU. Jednocześnie przepis nie odnosi się do sytuacji orzekania względem skazanego pozbawionego wolności w ramach innego środka, bądź analogicznie pozbawionego wolności, w ramach wykonywania innego, niż mający być objęty dozorem wyroku. W tych wypadkach zasadą jest sprowadzenie skazanego do sądu penitencjarnego (miejsca dozorowania) na posiedzenie w przedmiocie wniosku[19].

Dokonując analizy zarysowanej problematyki należy mieć na uwadze stanowisko sądów odwoławczych, orzekających w przedmiocie sporów o właściwość między sądami penitencjarnymi. Przedmiotowe orzecznictwo, ukształtowane pod rządami ustawy o dozorze elektronicznym sprzed nowelizacji z 21 maja 2010 roku, zdaje się jednak znajdować zastosowanie również we wskazanym zakresie.

I tak Sąd Apelacyjny w Katowicach w postanowieniu z 10 listopada 2009 roku[20] zauważył, iż „podstawową zasadą rządzącą kwestią właściwości sądu penitencjarnego jest zasada miejsca pobytu osoby skazanej – art. 3 § 2 k.k.w. – co wynika głównie z potrzeby zapewnienia uczestnictwa osoby skazanej w posiedzeniach sądu penitencjarnego. Tak rozumiana kwestia właściwości sądu penitencjarnego umożliwia jednolite ujęcie unormowań zawartych w przepisach art. 38 oraz 41 ustawy z dnia 7 września 2007 r. o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego. Skoro decyduje miejsce pobytu osoby skazanej, to wskazane normy bez pozornej sprzeczności spójnie i konsekwentnie rozstrzygają problem właściwości sądu do rozpoznania wniosku o udzielenie zezwolenia na odbycie przez skazanego kary pozbawienia wolności w systemie dozoru elektronicznego – jeśli skazany przebywa w zakładzie karnym winien to być sąd w okręgu, którego skazany odbywa karę pozbawienia wolności (art. 41 ust. ustawy z dnia 7 września 2007 r.), a jeśli skazany jest na wolności to sąd w okręgu, którego kara jest lub ma być wykonywana (art. 38 tejże ustawy)".

Jednocześnie orzecznictwo Sądu Apelacyjnego w Warszawie zdaje się podążać w kierunku przeciwnym do przyjętego w powyższym orzeczeniu przez Sąd Apelacyjny w Katowicach. W postanowieniu z 31 marca 2010 roku Sąd Apelacyjny w Warszawie[21], rozstrzygając kwestię, czy sądem właściwym w przedmiocie zastosowania dozoru elektronicznego wobec skazanego odbywającego karę pozbawienia wolności w Areszcie Śledczym Warszawa - Białołęka, a mającego odbywać karę pozbawienia wolności w systemie dozoru elektronicznego w miejscu stałego pobytu, a więc w miejscowości P.-Letnisko, znajdującej się w obszarze

18 Ibidem, s. 165-166.
19 Ibidem, s. 165-166.
20 Postanowienie SA w Katowicach z dnia 10 listopada 2009 r., sygn. II AKo 219/09, KZS 2010, nr 1, poz. 78
21 Postanowienie SA w Warszawie z dnia 31 marca 2010 r., sygn. II AKo 23/10, LEX nr 678002.

właściwości miejscowej Sądu Okręgowego w O. będzie Sąd Okręgowy w Warszawie czy też Sąd Okręgowy w O. – wskazał na następujące stanowisko: „Właściwy miejscowo do orzekania w przedmiocie udzielenia zezwolenia jest (…) sąd penitencjarny, w okręgu którego kara pozbawienia wolności w systemie dozoru elektronicznego ma być wykonywana, a więc właściwy dla miejsca stałego pobytu skazanego lub innego wskazanego miejsca" a „mając na względzie fakt, iż wskazane we wniosku o udzieleniu zezwolenia miejsce stałego pobytu skazanego znajduje się w obszarze właściwości miejscowej Sądu Okręgowego w O., Sąd Apelacyjny postanowił rozstrzygnąć spór w ten sposób, że właściwym do rozpoznania niniejszej sprawy uznać Sąd Okręgowy w O."

W kontekście przedstawionej problematyki warto zwrócić uwagę na inne orzeczenie Sądu Apelacyjnego w Warszawie[22], którego postanowienie może prowadzić do przyjęcia postulatu zmiany brzmienia treści art. 38 DozElektrU, skutkującego uściśleniem właściwości sądu penitencjarnego właściwego do zastosowania dozoru elektronicznego, poprzez wskazanie, iż „orzekanie w przedmiocie udzielenia zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego należy do sądu penitencjarnego, w którego okręgu ma nastąpić wykonanie kary pozbawienia wolności w systemie dozoru elektronicznego".

Wymienione powyżej – nieliczne z uwagi na krótki czas obowiązywania ustawy – orzeczenia sądów apelacyjnych, pomimo, że wydawane w odniesieniu do brzmienia art. 38 DozElektrU sprzed nowelizacji z 21 maja 2010 roku, pozostają aktualne, co do istoty rozważanego w nich problemu dotyczącego właściwości miejscowej sądów penitencjarnych stosujących dozór elektroniczny. Przedmiotowa nowelizacja ustawy o dozorze elektronicznym w zakresie brzmienia art. 38, chociaż po części usprawiedliwiona towarzyszącą jej, jak wskazano wyżej, zmianą w art. 6 DozElektrU, to jednak zdaje się stanowić – wobec wskazanych okoliczności – ciągle jeszcze płaszczyznę wątpliwości interpretacyjnych.

Agnieszka Zdanowska - Powinno być: Kierownik Zespołu Biura ds. Kształcenia i Spraw Studenckich Uniwersytetu Warmińsko – Mazurskiego w Olsztynie.

22 Zob. postanowienie SA w Warszawie z dnia 2 lutego 2010 r., sygn. II AKo 3/10, LEX nr 677997.

Zapraszamy do udziału

SEMINARIUM
SYSTEMÓW INFORMATYCZNYCH Z PRAWEM. COMPLIANCE W PRAKTYCE
23 października 2012 r., Warszawa

W programie m.in.:
- Wpływ prawa na systemy informatyczne
- Zakres uprawnień i obowiązków menedżera (specjalisty) do spraw Compliance. Sposoby zapewnienia zgodności praktyk biznesowych z ładem prawnym
- Zgodność systemów informatycznych z obowiązującym prawem finansowym (w tym z prawem podatkowym)
- Odpowiedzialność za zgodność systemów informatycznych z wymogami prawa
- Korzyści płynące z wdrożenia normy ISO 27001
- Systemy kontroli wewnętrznej w zakresie IT. Wdrożenie zintegrowanych systemów zapewnienia zgodności systemów informatycznych z obowiązującymi przepisami

Więcej informacji: www.cpi.com.pl

Wpływ e-usług na funkcjonowanie administracji publicznej

Magister Ewa Modzelewska

E-usługi a service design

E-usługi, czyli usługi świadczone w sposób zautomatyzowany przy użyciu technologii informacyjnych, za pomocą systemów teleinformatycznych w publicznych sieciach telekomunikacyjnych, na indywidualne żądanie usługobiorcy, bez jednoczesnej obecności stron w tej samej lokalizacji oparte na spójnej i dojrzałej metodologii service design przyczyniają się do usprawnienia funkcjonowania struktur państwowych.

Przejście od sposobu produkcji industrialnej do post-industrialnej okazuje się równie trudne dla nas, jak niegdyś przejście od sposobu rzemieślniczego do industrialnego. Żeby przekroczyć ten próg i stać się uczestnikiem nowoczesnej ery, musimy nauczyć się korzystać z beneficjów jakie w dzisiejszych czasach oferują nam nowoczesne technologie. Jak na ironię, ten wymóg stosowania algorytmów innowacyjności praktycznie do wszystkiego, wrzeczywistości, może być przyczyną umniejszającą nasze uznanie dla złożoności usług i w ten sposób, skomplikowanych struktur rynkowych oraz procedur administracyjnych, po których się poruszamy.

Na podstawie badań przeprowadzonych przez niemiecki Frauenhofer Institut AO zajmujący się propagowaniem nowoczesnych metod rozwoju nowych usług, stwierdzono, iż w 32% przedsiębiorstw rozwój nowych usług opiera się na przypadkowych działaniach oraz na metodzie prób i błędów, w 37% opiera się na wcześniejszych doświadczeniach ale bez zastosowania ustalonego trybu postępowania, w 22% stosowane są opracowane wcześniej wzorce postępowania, a tylko w 10% przedsiębiorstw istnieją i stosowane są zdefiniowane wzorcowe procesy rozwoju nowych usług[1].

W artykule zatytułowanym *'How to design a service'* („Jak zaprojektować usługę") z 1982 r. G. Lynn Schostack stwierdził, że usługi, jako proces, można przedstawić w postaci systemu „molekularnego" składającego się z elementów, powiązań i potwierdzeń w postaci schematów, harmonogramu, analizy PERT itd. Te narzędzia stanowią pomoc nie tylko w rozumieniu usług ex ante i lepszym projektowaniu, ale także w modelowaniu, testowaniu i ich replikowaniu. Koncepcja systemu włączonego do sieci w naturalny sposób wprowadza nas w dziedzinę „projektowania społecznego" zwanego także „projektowaniem publicznym" lub „projektowaniem dla społeczności".

Definicja w ujęciu metodycznym brzmi: projektowanie usług to projektowanie pozytywnego doświadczenia klienta funkcjonującego w obrębie sieci interakcji łączącej poszczególne punkty styku z usługodawcą, zaspokajającej potrzeby obydwu stron. A mówiąc wprost, usługa jest niematerialną chwilą interakcji, dlatego łatwo znaleźć szereg analogii między związkiem klienta z usługą lub marką a cechami, jakich ludzie szukają w relacjach osobistych. Tym poszukiwanym

1 T. Meinen, E. Heinen, *Erfolg mit neuen Dienstleistungen*, Frauenhofer Institut AO 2010.

dobrem jest satysfakcja, pozytywna emocja, jakiej doznajemy podczas zaspokajania naszej potrzeby poprzez korzystanie z usługi, czyli doświadczenie użytkownika (*user experience*).

Najważniejszy jest obywatel

„Najważniejsze to przewidzieć, w jakim kierunku podążają konsumenci i podążać tam przed nimi" – słusznie zauważył Philip Kotler, guru marketingu. Czy można to odnieść do funkcjonowania państwa i zachowań obywateli? Jeszcze do niedawna uznawano, że trendy i typologie (segmentacje) konsumenckie są aktualne przez 5 lat. Obecnie okres trwałości tych opracowań to 2 lata.

XXI wiek to era konceptualna, w której postępująca cyfryzacja i digitalizacja stwarza możliwość rozwoju postaw prosumenckich. Z koncepcji Tofflera wywodzi się nurt włączania konsumenta do procesu tworzenia dóbr oraz termin prosument. W świetle zmian zachodzących w przestrzeni cyfrowej, publicznej oraz społeczno-gospodarczej proces współtworzenia serwisów (*co-creation*) przez samych użytkowników zyskuje na sile. Dobudowując do istniejących produktów i usług zindywidualizowane, dodatkowe funkcjonalności oraz twórcze wspólnoty społecznościowe angażujemy użytkownika już na etapie projektowania. Takie podejście stosują przedsiębiorstwa. Zaczynają je również wdrażać instytucje publiczne. *Co-creation* sprawia, że urząd od początku procesu projektowego łączy wszystkie elementy: badania potrzeb obywateli, projektowanie, działania marketingowe.

Coraz więcej organizacji przekracza tradycyjne relacje urzędnik – klient, aby wspólnymi siłami tworzyć nową, wartościową usługę, m.in. fixmystreet zaprasza obywateli do pisania komunikatów o stanie dróg, ulic, niedziałającej sygnalizacji świetlnej, przestępczości, mających na celu usunięcie tych niedogodności.

Na fundamencie kreatywności, koncepcji otwartych innowacji, odkryć technologicznych oraz związków między ludźmi aktywizujemy użytkownika w działania kreacyjne. Istnieje różnorodność metod i narzędzi dla uzyskania prawdziwego obrazu. Biorąc pod uwagę różne profile, doświadczenia użytkowników organizacje komercyjne, jak również instytucje publiczne są w stanie stworzyć prototyp odpowiadający potrzebom jednostkowym, a następnie wdrożyć go w życie.

Co więcej, współtworzenie w procesie projektowania wpływa na harmonijne interakcje między partnerami na etapie rzeczywistego generowania usługi, co jest zasadnicze dla trwałej satysfakcji użytkownika i pracownika świadczącego usługi. Dzięki współtworzeniu obywatele mają okazję dodać wartość do usługi już na wczesnym etapie jej tworzenia. Im bardziej użytkownik angażuje się w proces kreacji usługi, tym bardziej jest prawdopodobne, że usługa wywoła poczucie współwłasności, co z kolei będzie owocowało długoterminowym systemem lojalnościowym.

Co–creation jest zbieżne z filozofią otwartego rozwoju. Zaproponowane pomysły i rozwiązania będą zawsze iteracyjnie filtrowane, tak żeby tylko najlepsze z nich były przetwarzane w nowe prototypy i innowacje. Sesje współtworzenia mają na celu zbadanie potencjalnych kierunków i gromadzenie różnych punktów widzenia w procesie. Wyniki podjętych działań staną się inspiracją dla zasadniczego zespołu projektowego, który będzie musiał je opracować i ulepszać w kolejnych etapach projektowania usługi. Dodatkowa korzyść ze współtworzenia polega na tym, że ułatwia przyszłą współpracę poprzez zintegrowanie interdyscyplinarnego zespołu projektowego.

Na podstawie przeprowadzonej w czerwcu 2009 r. przez McKinsey[2] wielopłaszczyznowej analizy w zakresie: badania potrzeb użytkowników, wykorzystania rozwiązań Web 2.0 oraz personalizacji produktów i usług uzyskano odpowiedzi na pytania dotyczące rezultatów osiąganych dzięki skutecznemu wdrażaniu koncepcji co-creation, przebiegu procesu projektowania usług. Wyniki badań wskazują, iż największe korzyści odnosiły się do redukcji kosztów marketingowych, wdrażania produktów lub usług na rynek, relacji z klientami.

Samo zaangażowanie obywateli w projektowanie usługi może skutkować wzrostem lojalności, współodpowiedzialności. Potencjalny użytkownik buduje z nią więź opartą na zaufaniu i relacji wymiany, która nie jest już tylko transakcją, ale aktywnym uczestniczeniem. To zwiększa prawdopodobieństwo pozytywnych opinii przekazywanych wśród użytkowników tzw. pocztą pantoflową, a w dobie Internetu za pomocą licznych forów internetowych, blogów oraz portali społecznościowych. Opinie o produkcie lub usłudze są transmitowane w bardzo szybkim tempie[3].

Można zauważyć istotną zmianę w rozwoju technologicznym. Użytkowników nie interesują najnowocześniejsze rozwiązania, ale takie narzędzia informatyczne, które umożliwią zaspokojenie jednostkowych potrzeb. Podstawowe zasady w zarządzaniu projektowaniem usług mają na celu zaimplementować do organizacji wiedzę zbiorową na etapie konstruowania założeń.

„Stosowanie metod angażujących użytkownika na etapie projektowania, kierowanie się jego potrzebami, oczekiwaniami i ograniczeniami wymaga (jeżeli celem jest opracowanie wysoce innowacyjnego rozwiązania) stosowania bardzo zaawansowanych technik z rodziny *design thinking* w celu ominięcia tendencji konsumentów do koncentrowania się na tym co znane i istniejące. Niezbędne jest uwzględnienie w procesie badawczym i projektowym wszystkich kategorii klientów"[4].

Koncepcja aktywności odnosi się do działań uczestników, ich inicjatywy i stylu współpracy oraz wkładu do wydarzeń projektowych. Role użytkowników mogą przybierać różny kształt, od aktywnego udziału w rozwiązaniu i określaniu wyzwań projektowych do pasywnej roli, w której projektanci interpretują dane użytkowników nie angażując ich bezpośrednio.

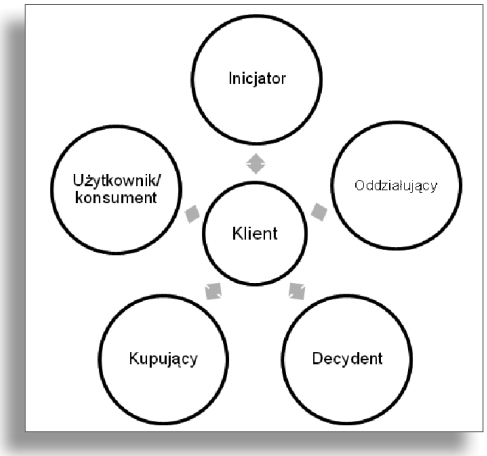
Opisując proces *service design* należy odwołać się do pięciu głównych zasad umożliwiających stworzenie ekosystemu usługi, sieci interakcji zachodzącej w przestrzeni cyfrowej pomiędzy usługodawcą oraz usługobiorcą:

1. NASTAWIENIE NA UŻYTKOWNIKA
2. **WSPÓŁTWORZENIE (wszyscy partnerzy powinni być włączeni w proces projektowania usług)**
3. SEKWENCJONOWANIE (usługa powinna być wizualizowana w postaci sekwencji wzajemnie powiązanych działań)

2 Na podstawie raportu firmy McKinsey z września 2009 roku: How companies are benefiting from web 2.0: McKinsey Global Survey Results http://www.mckinseyquarterly.com/Business_Technology/BT_Strategy/ [dostęp 26.06.2012]

3 http://www.teberia24.pl/?page_id=1210 [dostęp 27.06.2012]

4 Bochińska B., Palczewska I., *Raport wzornictwa e-usług. Analiza stanu wzornictwa usług świadczonych drogą elektroniczną i perspektywy ich rozwoju w Polsce*, Ministerstwo Gospodarki, Departament Gospodarki Elektronicznej, Warszawa 2011, s. 47.



Inicjator – inicjuje poszukiwanie rozwiązania problem konsumenta.

Oddziałujący – ma wpływ na decyzje o zakupie

Decydent – podejmuje decyzję, biorąc pod uwagę punkty widzenia inicjatora i oddziałującego, który produkt lub usługa ma być zakupiona

Kupujący – płaci za nabyty produkt lub usługę

Użytkownik – ostatecznie konsumuje produkt lub usługę

Rysunek 3 Kategorie klientów e-usług
źródło: *Bochińska B., Palczewska I., Raport wzornictwa e-usług. Analiza stanu wzornictwa usług świadczonych drogą elektroniczną i perspektywy ich rozwoju w Polsce, Ministerstwo Gospodarki, Departament Gospodarki Elektronicznej, Warszawa 2011, s. 48.*

4. POTWIERDZANIE (niewidoczne usługi należy wizualizować za pomocą artefaktu)
5. HOLISTYKA (należy brać pod uwagę całe otoczenie związane z usługą)[5].

Projektanci usług wizualizują, formułują i opracowują układy rozwiązań, które nie są jeszcze dostępne. Obserwują i interpretują potrzeby oraz zachowania, a następnie przekształcają je w potencjalne przyszłe usługi. W tym procesie stosują jednocześnie kilka podejść: eksploracyjne, generacyjne i ewaluacyjne. Tym działaniom nieustannie przyświeca skoncentrowanie się na użytkowniku (*human-centred design*).

Chcąc pokazać koncepcję *co - creation* jako nową wartość dla e-usług publicznych warto odnieść się do przykładu usługi publicznej („My Police"). Podczas *Social Innovation Camp* zrodziła się idea stworzenia e-usługi będącej internetowym narzędziem ułatwiającym komunikację pomiędzy obywatelami, a instytucjami sfery publicznej. Przed wdrożeniem projektu „MyPolice" przeprowadzono liczne badania ilościowe, etnograficzne, które umożliwiły rozpoznanie potrzeb przyszłych użytkowników oraz zrozumienie środowiska otaczającego usługę. Obywatele aktywizują się poprzez opisywanie swoich doświadczeń, wyrażanie opinii na temat działalności lokalnych organów policji. „Każde zgłoszenie jest łączone z datą i konkretnym miejscem (współpraca z Google Maps), dzięki czemu trafia właśnie do policjantów „obsługujących" dany rejon. Warto także zaznaczyć, że komentarze obywateli są kojarzone z określoną kategorią wykroczenia (np. „narkotyki", „alkohol", „kradzież", itp.), co pozwala np. sprawdzić, w jaki sposób policjanci obsługują obrabowanych w danym rejonie"[6].

Serwis „MyPolice" stanowi kompilację innowacyjności procesowej, marketingowej oraz produktowej, dostosowanej do szerokiej grupy odbiorców. Oddzielna platforma dla stróżów prawa pozwala zobaczyć, co dzieje

5 Stickdorn M., Schneider J., *This is service design thinking*, BIS Pulishers, Amsterdam, 2010.
6 Op. cit., Bochińska B., Palczewska I., *Raport wzornictwa e-usług. Analiza stanu wzornictwa usług..., s. 38.*

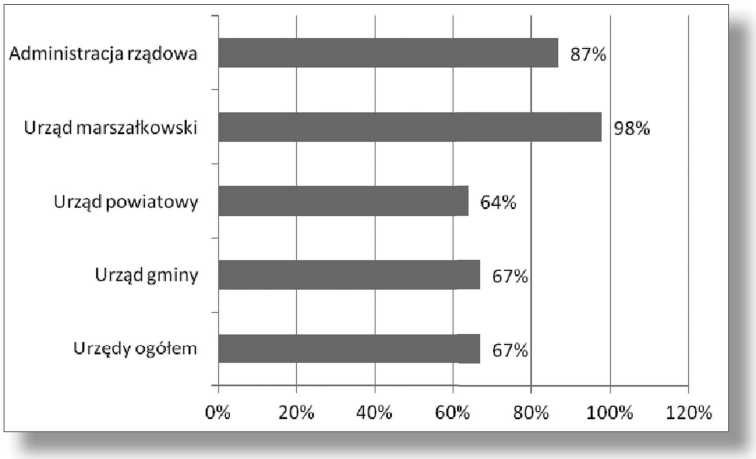


Tabela 1 Pracownicy urzędów posiadający dostęp do własnego służbowego konta poczty elektronicznej w 2011 r.
Źródło: Raport Ministerstwa Cyfryzacji i Administracji (Departament Społeczeństwa Informacyjnego) Społeczeństwo informacyjne w liczbach, Warszawa 2012, s. 35.

się w jego regionie. Przyspiesza czas reakcji odpowiedzi na zgłoszenia/komentarze obywateli. Syntetyczne spojrzenie na daną okolicę (mapa rejonów najbardziej niebezpiecznych), sprawdzenie korelacji między zmiennymi takimi jak: płeć, czas a miejsce, rodzaj popełnianych wykroczeń, jest możliwe dzięki rozbudowanej bazie danych wygenerowanych z serwisu.

Stan e-usług publicznych w Polsce

Na podstawie raportu z 2012 roku przygotowanego przez Ministerstwo Administracji i Cyfryzacji (Departament Społeczeństwa Obywatelskiego) w 2012 roku wynika, iż w Polsce prawie 4,6 mln gospodarstw domowych nie posiada dostępu do Internetu. W badaniu „Wpływ informatyzacji na działanie urzędów w Polsce" przeprowadzonym przez ARC Rynek i Opinia na zlecenie MSWiA w czerwcu i w lipcu 2011 roku wzięło udział 1601 urzędów. „Postępująca informatyzacja sprawia, że praca bez dostępu do Internetu będzie, a w wielu przypadkach już jest, niemożliwa. Konieczne zatem są zabezpieczenia na wypadek awarii sieci. Obecnie 28% urzędów posiada zapasowe łącze z Internetem na wypadek awarii łącza głównego, a jego przepustowość w prawie 70% przypadków przekracza 2 Mb/s. W łącze zapasowe częściej wyposażone są urzędy administracji rządowej (43%) niż samorządowej (28%). Sporą różnicę w tym zakresie daje się zauważyć w zależności od lokalizacji – w województwie kujawsko-pomorskim co drugi urząd posiada łącze zapasowe, natomiast w województwie podlaskim mniej niż co dziesiąty"[7].

Prawie 90% urzędów posiada elektroniczną skrzynkę podawczą. „Zróżnicowanie wyników ze względu na szczebel administracji jest niewielkie – elektroniczną skrzynkę podawczą najczęściej posiadają urzędy marszałkowskie (100%), urzędy powiatowe (94%), a najrzadziej instytucje administracji rządowej (86%). Wśród urzędów posiadających elektroniczną skrzynkę podawczą 87%

7 Raport Ministerstwa Cyfryzacji i Administracji (Departament Społeczeństwa Informacyjnego) Społeczeństwo informacyjne w liczbach, Warszawa 2012, s. 34.

udostępnia jej adres na swojej stronie BIP, natomiast w 69% przypadków jest ona umiejscowiona na platformie ePUAP”[8].

Z całą pewnością można rzec, iż Internet jest coraz powszechniej wykorzystywanym narzędziem pracy urzędników. Jednak jego zastosowanie służy przede wszystkim ułatwieniu pracy urzędnikom, niż dążeniu do poziomu transakcyjnego e-administracji. Niedostosowanie założeń programów e-usług do potrzeb społeczności lokalnej, brak zaangażowania urzędników w proces tworzenia serwisów publicznych sprawia, iż e-usługi są niedostosowane do potrzeb obywateli, nie spełniają ich oczekiwań zarówno na poziomie urzędów lokalnych, jak i centralnych.

Członkostwo Polski w Unii Europejskich implikuje szereg wyzwań w zakresie informatyzacji. Zwiększenie dostępności obywateli do usług publicznych, działanie na jak najwyższym poziomie, wykonywanie zadań publicznych mając na uwadze zadowolenie społeczeństwa, to główne zadania jednostek samorządu terytorialnego. Chcąc usprawnić tryb załatwiania spraw administracyjnych niezbędne jest wprowadzenie do praktyki administracyjnej swoistej architektury rozwiązań informatycznych oraz metod wdrożeniowych.

Reguły współpracy między organami administracji publicznej nie są przygotowane do korzystania z e-administracji i dokumentów elektronicznych. Brak jest współpracy i komunikacji między urzędami – urzędy działają wyspowo, silosowo, wykorzystując obywatela w roli biologicznego nośnika danych między urzędami”[9]. „2,5 mld zł miała kosztować informatyzacja polskiej administracji w latach 2007 – 2010. Plan nie został wykonany, a w nieskoordynowanych projektach utopiono setki milionów złotych. Teraz trzeba wydać kolejne 6 mld zł, by zadziałało to, co miało już funkcjonować”.

Większość stron internetowych instytucji publicznych nie funkcjonuje w formie e-Urzędu, w którym usługi świadczone są na poziomie transakcyjnym. Za pomocą dostępnych serwisów internetowych można najczęściej pobrać formularze, ale ich złożenie i uiszczenie opłat wymaga wizyty w urzędzie.

Informatyzacja administracji publicznej w Polsce przypomina bardziej bieg na 60 metrów niż maraton. Rzadko wdrażanie technologii informatyczno – komunikacyjnych przybiera postać zaplanowanego procesu z uporządkowanymi działaniami mającymi przynieść wymierne wskaźniki produktu i rezultatu. U podłoża tego zjawiska leży m.in. to, iż najczęstszym kryterium wyboru dostawców rozwiązań informatycznych jest cena. Kolejną przyczyną porażki w procesie informatyzacji samorządów jest słaba jakość tworzonych narzędzi informatycznych w sensie architektonicznym. Nie stworzono do tej pory na potrzeby e-administracji w Polsce koncepcji informatycznej umożliwiającej ujednolicenie modułów funkcjonalnych, standardów grup modułów składających się na dane aplikacje, ścieżki funkcjonalnej poszczególnych modułów, mapy relacji między modułami, dyspozycji dotyczących sterowania daną aplikacją, definicji interfejsów użytkownika, *touchpoints,* określenia narzędzi takich jak HCI, *user experience, interaction design*. Definiując w ten sposób rozwiązanie informatyczne możemy w pełni odpowiedzieć na potrzeby obywateli zachowując spójność wewnątrz systemową.

8 Ibidem, s. 35.
9 *Internet na wsi* http://www.internetnawsi.pl [data dostępu 30.05.2012]

E-administracja oznacza zmiany procesów wewnętrznych i zewnętrznych w strukturach administracyjnych, integrację rejestrów państwowych i baz danych dzięki wykorzystaniu technologii informacyjno - komunikacyjnych. Do najważniejszych korzyści informatyzacji usług publicznych należą:

- szybszy przepływ oraz dostępność informacji niezbędnych obywatelom;
- łatwiejszy dostęp do informacji na temat funkcjonowania organów administracji publicznej;
- krótszy czas oczekiwania na realizację danej usługi publicznej;
- eliminacja błędów, wzrost funkcjonalności świadczonych usług;
- e-urząd czynny 24 h na dobę przez 7 dni w tygodniu;
- oszczędność kapitału oraz racjonalizacja wydatków administracji publicznej związanych z jej informatyzacją;
- dialog społeczny (angażowanie użytkowników).

Bibliografia

Bochińska B., Palczewska I., *Raport wzornictwa e-usług. Analiza stanu wzornictwa usług świadczonych drogą elektroniczną i perspektywy ich rozwoju w Polsce*, Ministerstwo Gospodarki, Departament Gospodarki Elektronicznej, Warszawa 2011.

Dąbrowska A., Janoś – Kresło M., *Konsument na rynku e-usług w krajach Europy Środkowo – Wschodniej*, Wyd. Difin, Warszawa 2010.

Dąbrowska A., Janoś – Kresło M.,Wódkowski A., *e-usługi a społeczeństwo informacyjne*, Wyd. Difin, Warszawa 2009.

Gulda P., *Internet w stosunkach między władzą a obywatelami* [w:] Żak P. [red.] *Media i władza: demokracja, wolność przekazu i publiczna debata w warunkach globalizacji mediów*, Wyd. Naukowe Scholar, Warszawa 2006, s. 280 – 293.

Luterek M., *e-government. Systemy informacji publicznej*, Wyd. Akademickie i Profesjonalne, Warszawa 2010.

Meinen T., Heinen E., *Erfolg mit neuen Dienstleistungen*, Frauenhofer Institut AO 2010.

Materiały pokonferencyjne: 6th Borderlesse Government Services for Europeans, Poznań, 17-18 listopada 2011.

Moritz S., *Service design. Practical access to an evolving field*, Londyn 2005, tłumaczenie i redakcja naukowa: Instytut Wzornictwa Przemysłowego, Warszawa 2011.

Raport Ministerstwa Cyfryzacji i Admini stracji (Departament Społeczeństwa Informa cyjnego) Społeczeństwo informacyjne w liczbach, Warszawa 2012.

Stickdorn M., Schneider J., *This is service design thinking*, BIS Pulishers, Amsterdam, 2010.

Szopiński T., *E-konsument na rynku usług*, Wyd. Fachowe CeDeWu, Warszawa 2012.

Vilades X., *Design at your service. How to improve your business with the help of a designer*, Index Box S.I., Barcelona 2011.

Wójcik K., *e-Administracja w strategii rozwoju społeczeństwa informacyjnego Unii Europejskiej*, Urząd Komitetu Integracji Europejskiej.

Wielka kontrola NIK odkryła: system e-administracji padł, „Dziennik Gazeta Prawna", 13 grudnia 2011 r., nr 240 (3126 w2).

Źródła elektroniczne

http://tvp.info/informacje/technologie/niemcy-dowod-supernowoczesny/3190587

http://www.firmawczechach.pl/3,Urzedy_i_komunikacja.html

http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/online_availability_2006.pdf

http://www.mypolice.org/

http://www.samorzad.lex.pl/czytaj/-/artykul/boni-cyfryzacja-powinna-polepszyc-jakosc-uslug-publicznych

http://www.internetnawsi.pl

http://epuap.gov.pl/wps/portal/E2_OePUAP

http://biznes.gazetaprawna.pl/wywiady/24462,urzednicy_tworza_dla_urzedu_a_nie_dla_obywatela.html

http://eurzad.um.warszawa.pl/

https://www.sekap.pl/home.seam

http://www.e-uw.gov.pl/Strony/strona.html

http://www.fixmystreet.com/

http://www.gdansk.pl/nasze-miasto,512,18885.html

http://e-urzad.powiatwlodawski.pl/29

Ewa Modzelewska - doktorantka na Wydziale Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego (kierunek Nauki o polityce). Specjalista w Pionie Badań i Rozwoju Instytutu Wzornictwa Przemysłowego sp. z o.o.

Zapraszamy do udziału

FORUM

BIULETYN INFORMACJI PUBLICZNEJ (BIP) JAKO BROKER INFORMACJI - PROBLEMY PRAWNE UDOSTĘPNIANIA INFORMACJI PUBLICZNEJ

20 listopada 2012 r., Warszawa

Tegoroczne Forum powinno pomóc redaktorom BIP w znalezieniu odpowiedzi na pytanie jak zmierzyć się z tymi wyzwaniami. Oprócz przypomnienia najważniejszych zasad funkcjonowania tego trybu udostępniania informacji omówione zostaną zagadnienia dotyczące m.in. ochrony danych osobowych i zasad anonimizacji udostępnianych treści, teorii i praktyki ponownego wykorzystywania informacji publicznej, ograniczenia w dostępie oraz problemy prawe wynikające z prowadzenia BIP. Kolejne spotkanie w ramach Forum Administratorów, Koordynatorów i Redaktorów BIP powinno pomóc praktykom w znalezieniu rozwiązań problemów napotykanych przy codziennym zarządzaniu systemami informacji publicznej.

Więcej informacji: www.cpi.com.pl

Technologie komputerowe w perspektywie etycznej. Moralność w e-rzeczywistości - część II

Mariusz Szynkiewicz

Wstęp

Rozwój technologii komputerowych w coraz większym stopniu wpływa na kształt współczesnej refleksji nad moralnością. Zagadnienia etyczne w informatyce rozpatrywać możemy w dwóch zasadniczych kontekstach. Pierwszy z nich odnosi się do kwestii deontologicznych. Jego wyrazem są m.in. kodeksy zawodowe określające powinności przedstawicieli branży informatycznej. Regulują one stosunki wewnątrzśrodowiskowe: specjalista-specjalista, aspekty kompetencyjne oraz relacje o charakterze zewnętrznym: specjalista-użytkownicy, odbiorcy usług informatycznych. Z kolei druga z wyróżnianych płaszczyzn ma charakter praktyczny i dotyczy etycznych konsekwencji rozwoju technologii komputerowych [26, s. 51]. Obie perspektywy stanowią realizację zadań, jakie przed *etyką komputerową* (zwaną niekiedy *etyką informatyczną*) stawiali jej prekursorzy - Walter Maner i Norbert Wiener. Maner – twórca pojęcia etyki komputerowej – szczególną wagę przywiązywał do zagadnień deontologicznych. Jednocześnie wskazywał on na konieczność określenia podstawowych wartości i zasad wyznaczających kanon właściwego (etycznego) postępowania przedstawicieli zawodów informatycznych. Jak pisze Krystyna Górniak – Kocikowska: *Maner zakładał, że etyka komputerowa będzie obszarem dialogu głównie między filozofami a informatykami, zaś jej zasadniczym zadaniem będzie ochrona społeczeństwa (konsumentów) przed ewentualnymi negatywnymi skutkami wdrażania technologii komputerowych* [14]. Z kolei Wiener interesował się przede wszystkim praktycznym wymiarem rewolucji informatycznej. Jego analizy filozoficzne skupiały się na społecznych i kulturowych konsekwencjach funkcjonowania technologii komputerowych oraz potencjalnych zagrożeniach, które wynikać mogą z ich dynamicznego rozwoju [37, 38].

Współcześnie etyka komputerowa kojarzona jest powszechnie z rozważaniami natury deontologicznej, których praktycznym wyrazem są kodeksy etyki zawodowej (m.in. amerykański *ACM Code of Ethics and Professional Conduct* (1992) [19], kodeks etyczny niemieckiego stowarzyszenia *Gesellschaft für Informatik* (1994) [35] oraz uchwalony w roku 2011 polski *Kodeks Zawodowy Informatyka* (KZI) [21]). Wydaje się, że potrzeba formułowania podobnych dokumentów jest tym większa, im wyższy jest stopień znaczenia społecznego danej profesji. Wykładnia etyczna odnosi się w takich przypadkach do aksjologicznego i aplikacyjnego wymiaru opisywanych zawodów. Wspomniane regulacje dotyczą czterech zasadniczych kwestii i wyznaczają: a) ogólne zasady i wartości etyczne, b) relacje wewnątrzśrodowiskowe (specjalista-specjalista), c) stosunki zewnętrzne (specjalista –odbiorcy usług), d) tzw. zasady fachowości (np. obowiązek poszerzania wiedzy i umiejętności zawodowych) [10]. Pierwszą z wyróżnionych płaszczyzn rozpatrywać należy w aspekcie teoretycznym. Trzy dalsze mają charakter bardziej praktyczny.

Pytanie o zasadność formułowania kodeksu etycznego wzbudza w środowisku informatyków żywe dyskusje. Znajdujemy tu zarówno zwolenników podobnych dokumentów (np. W. M. Turski) [34], jak i osoby z rezerwą podchodzące do wszelkich tego typu

regulacji (J. Irlik) [17]. W kodeksach zawodowych normujących zasady etyczne szczególny nacisk kładzie się na instrumentalny charakter rozpatrywanych dziedzin aktywności zawodowej. Jest tak m.in. w przypadku KZI, który definiuje informatykę jako dziedzinę *służebną w stosunku do innych dyscyplin wiedzy i ich zastosowań* [21]. Kodeksy etyk zawodowych konstruuje się w kontekście obowiązującego prawa i są one niejako jego pozalegislacyjnym dopełnieniem. Karą za zachowania sprzeczne z przyjętymi kanonami etycznymi jest zazwyczaj ostracyzm lub, jak ma to miejsce w środowiskach hakerskich, wykluczenie ze społeczności. Współczesne kodeksy zawodowe zwyczajowo wzorowane są na Kodeksie Etyki Lekarskiej (KEL) [20]. W wielu z nich, np. we wspomnianych wykładniach medycznych oraz w kodeksie zawodu psychologa [11], pojawiają się zapisy dotyczące ochrony informacji. Właśnie ten, jakże często lekceważony aspekt deontologii, odgrywać zaczyna kluczową rolę w społecznym funkcjonowaniu zawodów informatycznych. Informacja stanowiąca podstawowy substrat ontologiczny informatyki jest bowiem w warunkach gospodarki opartej na wiedzy dobrem priorytetowym. Jej ochrona – np. w kontekście poufności danych – posiada nie tylko etyczny, ale i praktyczny wymiar.

Wybrane problemy etyki komputerowej

W swoim artykule zdecydowałem się przyjąć wienerowską perspektywę etyki komputerowej. Zagadnienia związane z funkcjonowaniem kodeksów etycznych w informatyce traktowane będą jedynie jako tło dla rozważań stanowiących główną treść teksu[1]. Pomijam również wątki metaetyczne nawiązujące do fenomenu etyki komputerowej, rozpatrywanej w kategoriach określonego działu nauk o moralności [5]. Jako użytkownik technologii komputerowych – typowy przedstawiciel gatunku *homoinformaticus* – skoncentruję się na tych problemach filozoficznych, które wynikają z aplikacyjnego charakteru informatyki. Postaram się wskazać i przeanalizować kilka - kluczowych moim zdaniem - zagadnień etycznych, związanych z rozwojem technologii komputerowych.

Dylematy natury prawnej

Jak podkreśla amerykańska etyczka Deborah G. Johnson, *(...) nowe technologie zmuszają nas do rozszerzenia przepisów prawnych tak, aby obejmowały nowe dziedziny (...) lub też do tworzenia nowych praw odnoszących się do nowych sytuacji wywołanych przez te technologie* [18, s. 107]. Zmiany jakie dokonały się za sprawą rewolucji informatycznej, wymusiły na legislatorach konieczność dostosowania obowiązujących przepisów do potrzeb nowej sytuacji społeczno-ekonomicznej. Rozwój technologii komputerowych i postępująca informatyzacja kolejnych obszarów życia społecznego zaowocowały wieloma dylematami, których rozstrzygnięcie wymaga użycia nowych - lub przynajmniej zmodyfikowanych - narzędzi prawnych. Większość z tych problemów wiąże się z elementarnymi zagadnieniami natury etycznej. W debacie publicznej szczególnie dużo miejsca poświęca się, medialnym z samej swej istoty, przykładom tzw. przestępczości komputerowej. Mianem tym określamy sytuacje, w których systemy komputerowe występować mogą w dwojakiej roli: a) obiektu nielegalnych działań, b) narzędzia wykorzystywanego do praktyk niezgodnych z prawem. Głównym przedmiotem tego typu

1 Bardzo często problem etyki w informatyce sprowadzany jest do poziomu etyki w biznesie IT. Należy jednak rozgraniczyć oba wskazane obszary tematyczne. Etyka informatyki koncentruje się przede wszystkim na zagadnieniach deontologicznych oraz moralnych konsekwencjach rozwoju nauk i technologii komputerowych. Jej aspekty biznesowe rozpatrujemy w kontekście bardziej ogólnej subdyscypliny etyki – etyki biznesu.

praktyk jest zaś informacja. Do najczęściej wymienianych przykładów przestępstw komputerowych należą: włamania do systemów, oszustwa, niszczenie danych, cyberterroryzm oraz przestępstwa gospodarcze. Problemy te są żywo dyskutowane przez środowiska prawnicze i zyskują coraz większe znaczenie społeczne, polityczne i gospodarcze. W niniejszym artykule skupię się na jednym wybranym wątku, łączącym zagadnienia informatyczne z rozważaniami prawnymi. Filozoficznym punktem wyjścia dla dalszych analiz będzie zaś, niezwykle ważna w naszej tradycji kulturowej, idea wolności. Zagadnienie wolności, rozpatrywane w świetle funkcjonowania technologii komputerowych, nabrało ogromnego znaczenia w trakcie wydarzeń związanych z pracami nad kontrowersyjną umową ACTA. W tym szczególnym przypadku spotykają się aż trzy, zasadnicze dla naszych rozważań, płaszczyzny problemowe: a) technologiczna – środowisko Internetu, b) filozoficzna – pojęcie wolności i c) prawna – problem własności[2].

Na wstępie należy więc zadać pytanie fundamentalne: czym w swej istocie jest wolność? Wolność rozumiana jest najczęściej jako stan, w którym dana jednostka posiada możliwość dokonywania swobodnych wyborów mając jednocześnie do dyspozycji rozmaite propozycje, rozwiązania czy poglądy. Ma więc ona charakter decyzyjny, zarówno w znaczeniu pozytywnym (wybiera określoną opcję), jak i negatywnym (wstrzymuję się od dokonania wyboru). Rzeczywista wolność realizuje się w warunkach braku szeroko rozumianego przymusu. Jest to oczywiście założenie idealizujące. Spór o istnienie tak pojmowanej wolności doprowadził do wyodrębnienia się w filozofii dwóch przeciwstawnych stanowisk: indeterminizmu, którego stronnicy wierzą w możliwość dokonywania wolnych wyborów i determinizmu, wskazującego na istnienie czynników warunkujących wszelkie podejmowane przez nas decyzje[3]. Zagadnienie wolności – jej charakteru, źródeł i zakresu - analizowali najwięksi myśliciele zachodu (m.in. Platon, Arystoteles, Kant, Hegel, Marks, Sartre, Berlin). Znalazło ono swoje miejsce także w rozważaniach związanych z technologiami komputerowymi. Jedną z jego najciekawszych postaci jest fenomen *etyki hackerskiej* i związanego z nią *ruchu wolnego oprogramowania*. Sygnalizowane kwestie odnoszą się bezpośrednio do dwóch powiązanych ze sobą pojęć: wolności i własności. Oba te problemy - istotne zarówno z filozoficznego, jak i prawnego punktu widzenia - odgrywają fundamentalną rolę w dyskusji nad regulacjami dotyczącymi własności oprogramowania.

Analizując zagadnienie własności oprogramowania należy określić istotę tego, co kryje się pod nazwą programu komputerowego. Według amerykańskiej ustawy *Copyright Act*, program komputerowy to *zestaw instrukcji stosowanych bezpośrednio lub pośrednio w komputerze w celu osiągnięcia określonego rezultatu* [8]. Klarowna definicja programu komputerowego okazuje się kluczowa przy pytaniu o to, jakiego typu prawa powinny chronić wytwory pracy programistów (prawo autorskie, prawo własności czy prawo patentowe). Niestety, skonstruowanie precyzyjnej definicji programu komputerowego nie jest zadaniem łatwym (ani dla informatyków, ani dla metodologów). Takiej – legalnej jak pisze Waglowski – definicji nie znajdziemy także w polskim prawodawstwie [36]. Jako podstawową przeszkodę na drodze do jej sformułowania wskazuje się najczęściej dynamiczny

2 Należy też zwrócić uwagę na filozoficzne konsekwencje problemu własności produktów informatycznych. Prawa te, dotyczą bowiem bytów o specyficznym statusie ontologicznym –‚bytów wirtualnych.

3 Oczywiście oba poglądy występują zazwyczaj w złagodzonych – mniej biegunowych – postaciach.

charakter rozwoju samej informatyki. Przyjmowane definicje mają więc charakter potoczny, a same programy komputerowe podlegają ochronie na zasadach podobnych do tych, które stosuje się w przypadku utworów literackich. Dzieje się tak mimo pewnych różnic występujących pomiędzy tymi dwoma rodzajami bytów. Niestety, proste przeniesienie tradycyjnych przepisów dotyczących obiektów materialnych na podmioty informatyki wydaje się jeszcze bardziej problematyczne[4]. Sytuacja ta rodzi więc nadal wiele poważnych problemów interpretacyjnych [Szerzej: 15].

Kwestia własności oprogramowania może być rozpatrywana w szerszym kontekście filozoficznym. W tym przypadku wiąże się ona, nie tylko z problemem prawa własności, ale także z pytaniem o prawo do wolności (jej znaczenie i dozwolony zakres). Cała dyskusja rozbija się na dwa bardziej szczegółowe zagadnienia: a) czy wolno chronić przepisami prawa (np. prawa patentowego lub prawa autorskiego) wytwory, które są nie tylko przedmiotami techniki, ale także obiektami nauki? b) czy programy, podlegające ochronie prawnej, traktować należy jako integralną całość, a ich pozyskiwanie, użytkowanie, modyfikowanie i udostępnianie interpretować według jednej zunifikowanej zasady prawnej? Czy też raczej powinniśmy uwzględnić złożoność samych programów komputerowych i za zasadne uznawać pytanie o to, czy wszystkie ich składowe (np. algorytm, kod maszynowy, kod wynikowy) mogą być chronione w ten sam sposób[5]? Pytanie pierwsze związane jest bezpośrednio z fenomenem etyki hackerskiej. Drugi z problemów koncentruje się na kwestiach definicyjnych i zagadnieniu złożoności programów (złożoności ich struktury).

Etyka hackerska stanowi ważną część szerszego pojęcia kultury hackerskiej, na którą składają się następujące wartości: wspólnotowość, specyficzny etos pracy, jej ukierunkowanie na cele poznawcze, a nie materialne, oraz takie elementy etyczne jak etos grupowy, specyficzne pojmowanie kwestii własności oraz silne przekonanie o tym, że działalność programistów jest rodzajem misji społecznej. Ważną cechą kultury hakerskiej jest również ideał perfekcjonistyczny, który polska etyczka Maria Ossowska uznawała za jedną z najważniejszych cnót obywatelskich [27]. Hakerzy, w przeciwieństwie do crakerów, rekrutują się spośród osób o wysokich kompetencjach zawodowych i ponadprzeciętnej wiedzy informatycznej. Co interesujące, jednym z powodów wykluczania ze środowiska hakerskiego wspomnianych już crakerów są właśnie ich pozaetyczne działania. Funkcję elementów integrujących społeczność hakerską pełnią normy i wartości wyznawane przez osoby identyfikujące się z tym nurtem. Kultura hackerska zaczęła się kształtować w latach 50 ub. wieku w wiodących ośrodkach informatycznych w USA (głównie MIT). Znaczenie terminu hakowanie (haker) zmieniało się na przestrzeni lat. Początkowo podobne działania identyfikowano z nieszkodliwymi, studenckimi żartami, które często traktowane były jako przejaw buntu wobec skostniałych struktur uniwersyteckich oraz symbol kreatywnego, nieszablonowego myślenia młodych programistów. Dekadę później hakowanie miało już zgoła inny wymiar. Hakerów kojarzono z elitą społeczności informatycznej. Przedstawiciele tych nieformalnych grup, stosując niestandardowe metody programowania, przyczyniali się do zwiększania efektywności i niezawodności narzędzi komputerowych. Określenie haker nabrało nobilitującego charakteru zarówno w merytorycznym, jak i etycznym znaczeniu [22]. Na początku lat 80 ub. wieku rozpoczął

4 Programy komputerowe chronione są w naszym kraju prawem autorskim. Szerzej: [36].
5 W systemie prawa polskiego prawem autorskim objęte są wszystkie postacie programu komputerowego.

się proces rozpadu społeczności hackerskiej. Wielu specjalistów, identyfikujących się z pierwotnymi założeniami ruchu, postanowiło wykorzystać swoje umiejętności w rodzącym się przemyśle IT. Niektórzy hakerzy przeszli na pozycje bardziej radykalne stając się crackerami. Jeszcze inni, jak Richard Stallman, postanowili walczyć o utrzymanie etosu nurtu hakerskiego. Symbolem tych starań stał się już wkrótce zainicjowany przez Stallmana projekt GNU [29, 31].

Mimo że hakerzy i crakerzy są przedstawicielami dwóch odrębnych środowisk (różni ich podejście do zagadnień etycznych, cel działalności i poziom wiedzy informatycznej)[6], często są ze sobą utożsamiani. Taka generalizacja jest bez wątpienia krzywdząca dla pierwszej z wymienionych grup. Podstawową dyrektywą światopoglądową spajającą środowisko hakerskie jest przywiązanie do ideału wolności. Zdaniem Castellsa hakerzy akcentują szczególnie trzy jej zasadnicze wymiary: a) wolność kreacyjną – tworzenie, przekształcanie, b) wolność poznawczą - wolny dostęp do wiedzy, c) wolność w dzieleniu się swoimi osiągnięciami. Wyrazem wyznawanych poglądów jest przywiązanie hakerów do ideałów głoszonych przez *ruch na rzecz wolnego oprogramowania*. Ten typ kultury określony został przez Castellsa mianem *kultury daru*. Obok pojęcia wolności, słusznie wyeksponowanego przez hiszpańskiego socjologa, należy zwrócić uwagę także na inny element systemu wartości funkcjonującego w społecznościach hakerskich. Mam tu na myśli jedną z ważnych idei etyki zachodniej – perfekcjonistykę (dążenie do doskonałości). W tym przypadku należy rozumieć ją bardziej praktycznie. Istotnym motywem pracy hakera jest dbałość o jak najwyższą jakość tworzonego oprogramowania. Praca nad udoskonalaniem oprogramowania uznawana jest za jedną z głównych powinności prawdziwego hackera. Innym aspektem funkcjonowania tej kultury, który rozpatrywać możemy w perspektywie etycznej, jest zespołowość. Hakerzy tworzą specyficzną społeczność, skupioną wokół określonych wartości, a jak wiadomo funkcjonowanie struktury społecznej wymaga istnienia wspólnej bazy przekonań moralnych.

Obecnie jedną z najważniejszych form etyki hakerskiej jest tzw. *filozofia GNU*, której filar stanowi przekonanie o wolności informacji. W koncepcji Stallmana wolność dotyczyć ma zarówno wymiaru osobowego działalności informatycznej (programista, użytkownik), jak i przedmiotowego (dane, programy). Program komputerowy nie jest tu traktowany jako produkt – przedmiot obrotu gospodarczego. Jest on w pewnym sensie wartością samą w sobie, a proces jego tworzenia, udoskonalania i upowszechniania, nie jest inspirowany przesłankami natury ekonomicznej. Należy jednak zaznaczyć, że kodeks wartości środowiska hakerskiego nie jest wymierzony przeciwko jakimkolwiek formom zarobkowania. Zwraca on jedynie uwagę na to, że kwestie finansowe nie mogą stanowić podstawowej motywacji, jaką kierują się w swojej pracy członkowie wspólnoty hackerskiej. Rolę tę pełnią natomiast takie wartości jak pasja i poczucie współuczestnictwa we wspólnym dziele udoskonalania narzędzi informatycznych – oprogramowania. Same programy pojmowane są przez hakerów w kategoriach dziedzictwa naukowego i w takiej perspektywie uznawane za wspólne dobro całego społeczeństwa. Zdaniem Stallmana, wolność oprogramowania rozpatrywać należy na czterech zasadniczych poziomach. Są to: a) możliwość uruchamiania i wykorzystania programu w dowolnym celu i w dowolny sposób, b) wolność tworzenia rozumiana jako

6 Wielu crackerów to tzw. *script kiddies* korzystający z gotowych programów i nieposiadający dużych umiejętności informatycznych.

przyzwolenie na modyfikowanie, usprawnianie i personalizowanie programów, c) swobodna dystrybucja i wolny dostęp do oprogramowania, d) możliwość publikowania ulepszonych/zmodyfikowanych wersji programów [31]. Co ważne, Stallman nie ogranicza swoich postulatów jedynie do poziomu bytów informatycznych. Autor manifestu uznaje je za uniwersalne w warunkach społecznych jakie powstały w wyniku rewolucji komputerowej. Jego analizy wydają się wpisywać w castellsowską logikę społeczeństwa sieci i nowy porządek funkcjonujący w ramach gospodarki opartej na wiedzy [4]. W zaistniałej sytuacji ekonomicznej, którą niekiedy określa się mianem *kapitalizmu sieciowego*, odpowiednio zmodyfikowana etyka hakerska stać się może, jak twierdzi Pekka Himanen, nowym modelem moralności [2]. W społeczności hackerskiej o sukcesie jednostki nie decydują kwestie materialne czy czynniki o charakterze społecznym. Podstawowym wymogiem jest tu typowy dla środowisk naukowych prestiż merytoryczny. Wartość prymarna utożsamiana jest z wiedzą i umiejętnościami danego programisty. Pracę wykonuje się często, nie dla korzyści materialnych, ale dla wewnątrzśrodowiskowego prestiżu. Czynnik ten rozpatrywać możemy w kategoriach hegelowskiej potrzeby uznania, godności (gr. *thymos*), motywu który w swojej koncepcji filozoficznej wykorzystuje współczesny amerykański filozof i ekonomista Francis Fukuyama [13, s. 262 – 276].

Kwestia ochrony prawnej programów komputerowych związana jest ponadto z pytaniem o ontologiczną naturę samego oprogramowania. Już na wstępie wyróżnić możemy dwa zasadnicze sposoby rozumienia analizowanego pojęcia. Pierwsze - w myśl którego program to produkt podlegający typowym mechanizmom rynkowym - charakterystyczne jest głównie dla przedstawicieli przemysłu komputerowego. W tej perspektywie oprogramowanie jest po prostu wytworem (produktem) techniki. Przeciwnicy takiego podejścia uznają jednak programy komputerowe za obiekty o charakterze naukowym, kładąc nacisk na ich abstrakcyjny – w sensie ontologicznym - charakter [30]. Efekty aktywności zawodowej programistów postrzegają w kategoriach naukowych – poznawczych. Ich zdaniem nie mogą być one traktowane na równi z tradycyjnymi wynikami działalność produkcyjnej. Ta dychotomia pozwoliła na wyłonienie się trzech zasadniczych stanowisk w sporze o własność programów komputerowych: a) radykalnych zwolenników prawa do ochrony własności oprogramowania, b) tych, którzy uznają, że jedynie niektóre elementy oprogramowania podlegać mogą podobnym przepisom, i c) grupie rzeczników wolnego dostępu do wszystkich form programów komputerowych. Grupa pierwsza oskarżana jest niejednokrotnie o przywiązanie do anachronicznych form myślenia ekonomicznego, adekwatnych w warunkach kapitalizmu sprzed rewolucji informatycznej. Z kolei radykałowie w rodzaju Richarda Stallmana, Sama Williamsa [39] i Ebena Moglena [25], atakowani są za propagowanie idei cyberkomunistycznych. Interesujące wydaje się jednak stanowisko pośrednie, którego stronnicy zwracają uwagę na złożoność programów komputerowych, wskazując jednocześnie na to, że poszczególne ich elementy nie powinny być traktowane w systemie prawa w identyczny sposób. Deborah G. Johnson twierdzi, że głównym problem w określeniu etycznego i prawnego charakteru ochrony wytworów działalności informatycznej jest brak jednoznacznej definicji programu komputerowego. Johnson zwraca uwagę na istnienie co najmniej trzech form w jakich występują programy komputerowe [Szerzej: 18, s. 108]. Jej zdaniem obecna ochrona prawna oprogramowania może być postrzegana jako rozszerzenie tradycyjnych praw autorskich, przepisów dotyczących tajemnicy handlowej oraz prawa patentowego. Johnson (etyczka), podobnie jak Stallman (programista) i Moglen (prawnik), podkreśla matematyczny – a więc naukowy - charakter wybranych elementów programów komputerowych. Na przykład w odniesieniu do algorytmów

komputerowych stwierdza, że jako formuły matematyczne nie powinny być one niczyją własnością [Zob.: 18, s. 115-116].

Zaufanie

Zaufanie to jeden z głównych filarów życia społecznego. Najczęściej pojmowane jest ono jako przekonanie o tym, że przyszły stan rzeczy – na przykład rezultat określonych działań – odpowiadać będzie naszym oczekiwaniom. Zaufanie opierać się może na takich przesłankach jak wiedza, wiara czy nawyk. Jego adresatem są rozmaite podmioty - drugi człowiek, grupa społeczna, grupa zawodowa, instytucja, metoda, byt ponadnaturalny lub technologia. W kontekście zagadnień omawianych w niniejszym tekście chciałbym wyeksponować pierwszą i ostatnią w wymienionych kategorii: zaufanie do człowieka i zaufanie do technologii. W tym pierwszym przypadku odwołujemy się najczęściej do innego, trudnego do zdefiniowania pojęcia - uczciwości. Cecha ta ufundowana jest na przekonaniach moralnych danej jednostki. Zaufanie, to fundamentalny składnik każdej więzi społecznej [32], istotny także w kontekście ekonomicznym[7]. Jak słusznie zauważa Grzegorz Graff*: Gęsta sieć powiązań i interakcji łącząca członków dzisiejszego społeczeństwa wymusza swoisty rodzaj zaufania, bez którego aktywność jednostki w złożonym, zaawansowanym technologicznie środowisku nie byłaby możliwa* [16]. W warunkach postępującej technicyzacji świata coraz większego znaczenia nabiera także inny jego typ: zaufanie do technologii. Ma ono bardziej instrumentalny charakter i opiera się na przekonaniu, że dane rozwiązanie techniczne, urządzenie, procedura, program itp. działać będą zgodnie z naszymi oczekiwaniami. Najczęstszym jego wyrazem jest żądanie niezawodności i stabilności (np. stabilności programów). Możemy więc zapytać o to, jak w kontekście rewolucji informatycznej powinniśmy rozumieć pojęcie zaufania? W pierwszej z wymienionych perspektyw, gdy adresatem naszego zaufania jest drugi człowiek, odpowiedź na tak postawione pytanie wydaje się oczywista. W relacji fachowiec – odbiorca zaufanie wiąże się z wiarą w umiejętności, profesjonalizm i uczciwość specjalisty. Analizowany problem może przybrać jeszcze inną formę, która związana jest z zagadnieniem dostępu do informacji. Jak już wspominałem, każda dyscyplina zawodowa, zwłaszcza taka, która jest niezbędna dla realizacji podstawowych funkcji społeczeństwa, wymaga określonej deontologii. Wzorcem dla istniejących obecnie kodeksów zawodowych są najczęściej deontologie medyczne. Oczywiście każdy z zawodów posiada swoją specyfikę. Zróżnicowanie wkrada się także w ich wewnętrzną strukturę, czego wyrazem jest postępująca specjalizacja poszczególnych branż. Istnieją jednak zasady o charakterze uniwersalnym, wspólne dla przedstawicieli niemal wszystkich profesji. Jedną z takich dyrektyw deontologicznych, funkcjonujących m.in. w etyce zawodów medycznych, urzędniczych i prawnych jest klauzula dotycząca ochrony informacji oraz prawa do prywatności. Zasada ta, w coraz większym stopniu obejmować zaczyna działalność informatyczną. Przedstawiciele branż komputerowych uzyskują dostęp do danych i informacji dotyczących nas samych i rozmaitych aspektów naszej aktywności w świecie. Jest to jeden z dodatkowych kosztów związanych z procesem szerokorozumianej digitalizacji rzeczywistości. Zawody informatyczne stają się obecnie zawodami zaufania społecznego. Czynnik zaufania odgrywa więc ważną rolę w funkcjonowaniu technologii informatycznych, i jak można oczekiwać jego znaczenie będzie coraz bardziej istotne[8].

7 Zaufanie rozpatrywane w kontekście etycznym ma także ważne znaczenie dla życia gospodarczego. Szerzej na temat wpływu etyki na procesy zarządzania i wyniki ekonomiczne przedsiębiorstw: [24]

8 Tak pojmowane zaufanie staje się istotne również w zwykłych sytuacjach życiowych – np. wtedy, gdy zwracamy się do firmy komputerowej o odzyskanie danych, znajdujących się na dysku prywatnego komputera domowego.

Zaufanie w informatyce ma także drugi, mniej osobowy charakter. Jest ono związane z tym, co kolokwialnie nazwać możemy *wiarą w technologię*. Ten typ zaufania łączy się z dwoma ważnymi aspektami funkcjonowania nowoczesnych społeczeństw. Pierwszy z nich ma wymiar epistemologiczny i odnosi się do zagadnienia źródeł informacji. Jego przejawem jest tendencja do traktowania Internetu jako głównego - a często jedynego - źródła wiedzy [33]. Drugi przybiera charakter instrumentalny i związany jest z zaufaniem do skuteczności, adekwatności i niezawodności technologii komputerowych. Kwestia niezawodności narzędzi informatycznych (i „niezawodności" programistów) jest żywo dyskutowana przy okazji rozmaitych wydarzeń i wypadków, w których istotną rolę odgrywają systemy komputerowe. W procesie postępującej digitalizacji i automatyzacji świata coraz większe obszary naszego życia trafiają pod kontrolę narzędzi informatycznych. Systemy bankowe, telekomunikacja, kontrola ruchu, projektowanie w naukach inżynieryjnych, to przykłady nie budzące już dzisiaj większych kontrowersji. Narzędzia informatyczne wkraczają jednak i do innych sfer funkcjonowania nowoczesnych społeczeństw. Należą do nich m.in., tak ważne z etycznego punktu widzenia dziedziny życia, jak medycyna czy wojskowość. Szczególnie interesujący wydaje się drugi z wymienionych przykładów. W warunkach współczesnego pola walki wyraźnie wzrasta znaczenie urządzeń komputerowych (np. robotów wojskowych). Jak podkreślają specjaliści, w niektórych przypadkach już dziś, to właśnie one podejmują decyzje, których potencjalny skutek stanowić może śmierć ludzi [Szerzej: 23].

Zaufanie do niezawodności technologii informatycznych i wiara w możliwości maszyn cyfrowych przybierać mogą jeszcze inny, mniej ważki etycznie, wymiar. Ma ono raczej charakter epistemologiczny i nawiązuje do problemu, który w metodologii nauk określamy mianem kontekstu uzasadnienia. Współczesne komputery zdolne są do wykonywania zadań, które – np. z uwagi na poziom złożoności obliczeniowej – niejednokrotnie wykraczają poza zakres możliwości człowieka. Z taką sytuacją stykamy się w przypadku pewnych procedur dowodowych w logice i matematyce. Niektóre z nich są tak skomplikowane i czasochłonne, że uznaje się je za praktycznie niewykonalne. Rozwiązaniem może okazać się użycie odpowiednich narzędzi komputerowych. Jako przypadek tego rodzaju wymienić należy historię prac nad skonstruowaniem dowodu *twierdzenia o czterech barwach* (pierwsza hipoteza mówiąca o jego poprawności postawiona została w roku 1852). Pełny - sprawdzony przy pomocy tzw. asystenta komputerowego - dowód tego twierdzenia ogłoszono niespełna dekadę temu [1]. Do dnia dzisiejszego nie dysponujemy jednak możliwością bezpośredniego (niewymagającego użycia komputerów) sprawdzenia jego poprawności. Procedura dowodowa pozostaje więc dla nas w pewnym sensie ukryta. Sprawia to, że przekonanie o poprawności samego dowodu opiera się na zaufaniu do narzędzi informatycznych, czyli w wierze w niezawodność maszyny.

Wykluczenie cyfrowe

Wilhelm Ostwald, wybitny chemik i twórca prądu filozoficznego zwanego energetyzmem, nadawał etyce wymiar praktyczny. W jego systemie pełniła ona rolę czynnika integrującego społeczeństwo. Zdaniem Ostwalda, każda tego typu struktura opiera się na akceptacji wspólnych wartości moralnych. Warunkiem koniecznym prawidłowego funkcjonowania w społeczeństwie jest także współuczestnictwo. Co się jednak dzieje kiedy jednostka – a nawet całe grupy – spychane są poza obręb wspólnoty? Mamy wtedy do czynienia ze zjawiskiem marginalizacji, określanej często mianem wykluczenia. Sytuacje tego typu występują wtedy, gdy określony podmiot (jednostka, grupa, społeczność) nie może partycypować w działaniach danego

środowiska. Wykluczenie ogranicza jego dostęp do takich aspektów życia społecznego jak polityka, edukacja, kultura czy działalność gospodarcza. Co ważne, odrzucenie i alienacja nie wynikają w takich przypadkach, z woli podlegającego tym procesom podmiotu. Wykluczenie kojarzone jest najczęściej w czynnikami ekonomicznymi, (poziomem zamożności) co znajduje swoje odzwierciedlenie w metodologii badania poziomu wykluczenia społecznego zaproponowanej przez ONZ. Odwołuje się ona do trzech zasadniczych czynników – średniej długości życia, poziomu edukacji i poziomu zamożności [7]. Tak rozumiane wykluczenie prowadzi do marginalizacji, którą pojmować można zarówno w kategoriach lokalnych (gdy dotyczy ono określonych jednostek i grup funkcjonujących w obrębie społeczeństwa), jaki i globalnych (kiedy wykluczeniu podlegają całe narody lub grupy etniczne). Tradycyjnie wykluczenie przybierało kilka zasadniczych form. W przeszłości miało ono zazwyczaj charakter ekonomiczny, rasowy (jak np. w III Rzeszy), społeczny, etniczny czy religijny. Marginalizacja prowadziła do podziałów społecznych, których efektem było m.in. powstawanie gett. Jak wiadomo współczesne getta mają głównie – choć nie jedynie – charakter ekonomiczny. Ich tworzenie wzmacnia istniejące wcześniej rozwarstwienia i sprzyja utrwalaniu podziałów na gorszych i lepszych, naszych i obcych. Wykluczenie ogranicza więc możliwość partycypacji podmiotu w określonej sferze szerokorozumianej aktywności społecznej. W ostatnich dekadach, do znanych od wieków rodzajów wykluczenia, dołączył nowy jego typ – wykluczenie cyfrowe (*digital divide)*. Zjawisko to, w interesujących nas tutaj aspektach etycznych i społecznych, wynikać może z dwóch głównych przyczyn: ekonomicznych – brak dostępu do Internetu spowodowany jest zacofaniem ekonomicznym danego regionu (np. poziom internetyzacji niektórych państw afrykańskich) i politycznych – kiedy uczestnictwo w wymianie informacji drogą cyfrową ograniczane jest (w całości – Korea Północna lub w części – Chiny) [28] przez władze [12]. Sytuację tę rozpatrywać należy na dwóch zasadniczych płaszczyznach. Ograniczanie dostępu do Internetu można uznać za nieetyczne gdy jest ono powodowane arbitralnymi pobudkami politycznymi i ideologicznymi (Korea Północna). Stanowi to wyraźne ograniczenie wolności i swobód obywatelskich oraz dodatkowo utrudnia proces demokratyzacji społeczeństw. W takich przypadkach efekty działania cenzury nie sprowadzają się jedynie do relacji o charakterze wewnętrznym. Ich skutki, np. brak dostępu do informacji obywateli konkretnych państw, generują pewną formę wykluczenia informacyjnego, którego efekty mają zewnętrzny (międzynarodowy) charakter[9]. Z drugiej strony wykluczenie cyfrowe ma również istotne konsekwencje o charakterze ekonomicznym. W warunkach gospodarki opartej na wiedzy brak dostępu do informacji wyklucza całe społeczeństwa z wybranych aspektów życia gospodarczego. Ogranicza ono dodatkowo ich pełną, swobodną partycypację w życiu politycznym i kulturowym [Szerzej: 3].

Klimat społeczny getta wytwarza poczucie enklawowości, która może przybierać rozmaite formy. Jedną z nich jest specyficzny rodzaj nieświadomości społecznej. W dzisiejszych czasach, kiedy partycypacja społeczna, ekonomiczna i kulturowa coraz częściej opierają się na funkcjonowaniu w ramach ontologii świata internetowego, odcięcie od cyfrowych źródeł informacji równa się odcięciu od wiedzy na temat świata, znajdującego się poza

9 Nie należy jednak identyfikować ograniczenia dostępu do informacji z typowymi dla państw dyktatorskich celami politycznymi. Pewien poziom cenzury istnieje też w krajach demokratycznych i jest on związany m.in. z polityką bezpieczeństwa wewnętrznego.

granicami zamkniętej informacyjnie żony. Podręcznikowym przykładem *getta informacyjnego* jest oczywiście współczesna Korea Północna. Symbolem braku obiektywnej wiedzy na temat rzeczywistego poziomu życia politycznego i gospodarczego poza granicami tego kraju może być jedno z haseł propagandy koreańskiej, które brzmi *światu nie mamy czego zazdrościć* [9, s. 19].

Podsumowanie

Zdaniem amerykańskiego filozofa Terrella Bynuma, technologia komputerowa jest najpotężniejszą i najbardziej uniwersalną spośród dotychczas wynalezionych. Bynum zauważa ponadto, że jej najważniejsze konsekwencje rozpatrywać powinniśmy właśnie w omawianej tu perspektywie społecznej i etycznej [6, s. 26 – 35]. Trudno byłoby przecenić transformacyjny potencjał nauk i technologii informatycznych. Nie tylko zmieniły one obraz i kształt rzeczywistości, w której żyjemy, ale także przyczyniły się do powstania zupełnie nowego jej wymiaru ontologicznego – świata wirtualnego. W warunkach nowej ontologii rodzą się jednak nowe problemy filozoficzne i społeczne. Zmieniona, a częściowo wykreowana od podstaw, struktura rzeczywistości pozwala nam na umieszczenie wielu tradycyjnych zagadnień i dylematów etycznych w przekształconej jakościowo perspektywie (np. problem własności bytów wirtualnych). Informatyzacja świata jest procesem, bez którego nie sposób wyobrazić sobie globalizacji w jej obecnej postaci. Logika Internetu wymusza zmianę dotychczasowego spojrzenia na procesy społeczne, polityczne, gospodarcze i prawne, procesy, których podwaliny mają charakter etyczny. Proces informatyzacji rzeczywistości, w której żyjemy postępuje nadal i trudno przewidzieć kierunki w jakich podążą, zarówno same technologie komputerowe, jak i inne sprzężone z nimi zjawiska o charakterze społecznym. Pewne jest jednak, że rozważania etyczne, związane z naukami i technologiami komputerowymi, odgrywać będą tym większą rolę, im bardziej proces komputeryzacji oddziaływać będzie na strukturę zjawisk społecznych. Współczesna etyka wzbogaciła się o nowe, niezwykle ważne pole badawcze – obszar, którego eksploracja staje się jednym w kluczowych zadań nauk o moralności.

Bibliografia

1. *Angle D., Last doubts removed about the proof of the Four Color Theorem, (w:) http://www.maa.org/devlin/devlin_01_05.html, (01.08.2012),*
2. *Bendyk E., Jak nas zmieniają nowe technologie. Niezapowiedziane rewolucje, (w:) Polityka 18/12/2005,*
3. *Bendyk E., Wykluczeni cyfrowo stanowić będą grupę o coraz mniejszym znaczeniu politycznym, (w:) Gazeta wyborcza, http://info.wyborcza.pl/temat/wyborcza/%C5%BCycia+spo%C5%82ecznego, (01.08.2012),*
4. *Blikle A. J., Doktryna jakości, (w:) http://firmyrodzinne.pl/download/tqm/Doktryna-jakosci.pdf, s. 14 – 17, (01.08.2012),*
5. *Bober W. J., Powinność w świecie cyfrowym. Etyka komputerowa w świetle filozofii moralnej, WAiP, 2008,*
6. *Bynum T., Etyka a rewolucja informatyczna, (w:) A. Kocikowski, K. Górniak – Kocikowska, T. Bynum, (red.:), Wprowadzenie do etyki informatycznej, Poznań 2001,*
7. *Calculating the human development indices, (w:) http://hdr.undp.org/en/media/HDR_20072008_Tech_Note_1.pdf, (01.08.2012),*
8. *Copyright Law of the United Satates (Copyright Act.), & 101, s. 2, (01.08.2012),*
9. *Demick B., Światu nie mamy czego zazdrościć, Wołowiec 2011,*
10. *Dyżewski A., Kodeksy etyczne w informatyce – komentarz, (w:) DiS-biuro badawczo analityczne, 10/2000, http://dis2.waw.pl/dis/artykuy-i-polemiki/132-kodeksy-etyczne-w-informatyce-komentarz, 901.08.2012),*

11. *Ethical Principles of Psychologists and Code of Conduct, (w:) http://www.apa.org/ethics/code/index.aspx, (01.08.2012),*
12. *Feliksiak M., CBOS - Komunikat z badań: Korzystanie z komputera i internetu (06/2010), (w:) http://www.cbos.pl/SPISKOM.POL/2010/K_079_10.PDF, (01.08.2012),*
13. *Fukuyama F., Koniec historii, Poznań 1996,*
14. *Górniak-Kocikowska K., Droga do etyki komputerowej, (w:) Computerworld, nr 3/2002,*
15. *Grabowska A., Program komputerowy nie jest dziełem literackim, (w:) Rzeczpospolita, 18/10.2007,*
16. *Graff G., Czy istnieje cnota zaufania, (w:) Przegląd Powszechny 2001, nr 12,*
17. *Irlik J., Etyka zawodowa (uwagi w kwestii etycznego kodeksu informatyków), (w:) Biuletyn PTI, nr 3-4/1985,*
18. *Johnson D. G., Czy programy komputerowe powinny stanowić czyjąkolwiek własność, (w:) A. Kocikowski, K. Górniak – Kocikowska, T. Bynum, (red.:), Wprowadzenie do etyki informatycznej, Poznań 2001,*
19. *Kodeks etyczny ACM: ACM Code of Ethics and Professional Conduct (Adopted by ACM Council 10/16/92), (w:) http://www.acm.org/about/code-of-ethics/#preamble (01.08.2012),*
20. *Kodeks Etyki Lekarskiej (art. 25 – 29), (w:) http://www.nil.org.pl/__data/assets/pdf_file/0003/4764/Kodeks-Etyki-Lekarskiej.pdf, s. 5 – 6, (01.08.2012),*
21. *Kodeks Zawodowy Informatyków, (w:) http://www.pti.org.pl/index.php/corporate/KZI-Kodeks-zawodowy-informatykow-PTI-29-maja-2011-r2 (01.08.2012),*
22. *Levi S., Hackers: Heroes of the Computer Revolution, USA, wyd. Doubleday 1984,*
23. *Marczuk J., Etyka zabijania, czyli wszystko o robotach bojowych (wywiad z prof. Ronaldem Craigiem Arkinem), (w:) Gazeta Wyborcza, 21/07/2012,*
24. *McGill R. Murphy, Etyka popłaca, (w:) http://www. m.obserwatorfinansowy.pl, (01.08.2012),*
25. *Moglen E., Anarchizm triumfujący: wolne oprogramowanie i śmierć praw autorskich, (w:) http://www.miasik.net/articles/moglen.html, (01.06.2012),*
26. *Moor J. H., Czym jest etyka komputerowa? [1], (w:) A. Kocikowski, K. Górniak – Kocikowska, T. Bynum, (red.:), Wprowadzenie do etyki informatycznej, Poznań 2001,*
27. *Ossowska M., Wzór obywatela w ustroju demokratycznym, Warszawa 1946,*
28. *Reporters Without Borders, Enemies of the Internet Report - 2012, (w:) http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf, (01.08.2012),*
29. *Stallman R., Free Software, Free Society: Selected Essays of Richard M. Stallman. Filadelfia 2002,*
30. *Stallman R. M., Nauka musi odsunąć na bok prawa autorskie, (w:) http://www.gnu.org/philosophy/push-copyright-aside.pl.xhtml, (01.08.2012),*
31. *Stallman R. M., Projekt GNU, (w:) http://www.gnu.org/gnu/thegnuproject.pl.html, (01.08.2012),*
32. *Sztompka P., Zaufanie. Fundament społeczeństwa, Kraków 2007,*
33. *Tadeusiewicz R., W dymie i we mgle, (w:) http://www.solidarnosc.org.pl/~ksn/Docs/rystad.pdf (01.08.2012),*
34. *Turski W. M., Po co nam kodeks etyczny? (w:) Teleinfo nr 20, 06/2003, http://www.wampnm.webd.pl/~dorozynskij/_kei/fpwmt.html, (01.08.2012),*
35. *Unsere Etischen Leitlinien, (w:) http://www.gi.de/fileadmin/redaktion/Download/ethische-leitlinien.pdf, (01.08.2012),*
36. *Waglowski P., Program komputerowy, utwór literacki i zapobieganie podwójnemu opodatkowaniu, (w:) http://prawo.vagla.pl/node/7536,*
37. *Wiener N., Cybernetyka a społeczeństwo, Warszawa 1961,*
38. *Wiener N., God and Golem, Inc. A Comment on Certain Points where Cybernetics Impinges on Religion, Cambridge – Massachusetts, 1964,*
39. *Williams S., W obronie wolności: Krucjata hakera na rzecz wolnego oprogramowania, Gliwice 2003,*

Abstract:

Computer Technologies from the Viewpoint of Ethics. Morality in Virtual Reality. Part II

This paper focuses on the concepts of ethics and morality and such domains of normative ethics as axiology or deontology. The main objective of the considerations presented in the paper is to identify and analyse the topics crucial for contemporary computer ethics.

Keywords: computer science, ethics, morality, internet.

Mariusz Szynkiewicz - doktor filozofii (specjalność: filozofia nauki, filozofia fizyki), adiunkt w IF UAM w Poznaniu.

Zapraszamy do udziału

FORUM

I FORUM INFORMATYCZNEGO ZARZĄDZANIA UCZELNIĄ

Łochów k/ Wyszkowa, 16-17.10.2012 r.

Zapraszamy Państwa do udziału w programie Forum Informatycznego Zarządzania Uczelnią, 16 - 17 października 2012 r. - Pałac w Łochowie (Mazowieckie). Forum jest śmiałą kontynuacją cyklu Informatycznego Wspomagania Zarządzania Uczelnią, które liczy sobie już 15 edycji. Pierwszy raz program przygotowany jest w konwencji dwudniowego forum. Podczas realizacji agendy poruszone zostaną ciekawe zagadnienia z zakresu informatyzacji i zastosowania nowych technologii w zarządzaniu i obsłudze uczelni wyższej. Swoje wystąpienia w programie będą mieli m.in.: dr Olaf Gajl (OPI), Prof. Włodzimierz Gogołek (UW), Kazimierz Schmidt (Naczelne Archiwa Państwowe). W trakcie przerw i podczas uroczystej kolacji, będą Państwo mieli okazję do wymiany doświadczeń i nawiązania kontaktów z przedstawicielami firm teleinformatycznych. Część prezentacji firmowych, dla podniesienia atrakcyjności, przygotowana będzie przy współudziale uczelni zamawiających.

W programie m.in.:

- Systemy informacyjne a potrzeby uczelni wyższych
- Rozwój systemu Uczelnia.XP w świetle najnowszych zmian ustawowych oraz potrzeb Uczelni Wyższych
- Sposoby komunikacji pomiędzy uczelnią a studentami w perspektywie nowych technologii
- Jak zbudować infrastrukturę PKI w Uczelni z wykorzystaniem legitymacji elektronicznych
- Integracja systemu informatycznego uczelni wyższej z sieciami społecznościowymi i urządzeniami mobilnymi
- Prawo własności intelektualnej a działalność naukowa pracowników uczelni wyższych
- Obsługa kancelaryjna i archiwizacja dokumentacji elektronicznej
- Nowoczesne systemy bezpieczeństwa w sieciach Akademickich
- Od systemu informatycznego do systemu informacyjnego - wyzwania współczesnej uczelni Wyższej
- Doświadczenia z zastosowania zintegrowanego systemu do zarządzania wraz elektronicznym obiegiem dokumentów na przykładzie Uniwersytetu Przyrodniczego we Wrocławiu
- Doskonalenie procesowej orientacji uczelni, jako element analizy przedwdrożeniowej systemów informatycznych

Więcej informacji: www.cpi.com.pl

Elektroniczne dowody osobiste w Polsce – co dalej z projektem PL.ID

Pewne jest tylko jedno: nasze dowody nie są bezpieczne. Tymczasem władze nie mogą się zdecydować, jakie mają być nowe dokumenty. W kwietniu tego roku unieważniono przetarg. Dostawcy rozwiązań głowią się, co to znaczy. Ich zdaniem wyjaśnienia zamawiającego nie są zrozumiałe, bo nie ma podstaw prawnych do takich działań.

Mieczysław T. Starkowski

Czesi wprowadzają nowe dowody osobiste od 1 stycznia tego roku. Obywatele mają przy tym wybór. Każdy sam decyduje, czy chce mieć elektroniczny, czy nie. Natomiast Niemcy podejmują decyzję, czy chcą mieć dowody z zapisanym elektronicznie wzorem odcisku palca.

Wybory to iście hamletowskie. Ale polskie władze lubią przeciągać decyzje w nieskończoność. Tak właśnie jest w tym przypadku. O dowodach dyskutujemy od lat. Rozstrzygnięcia nie widać.

W połowie kwietnia br. Ministerstwo Spraw Wewnętrznych opublikowało komunikat w sprawie nowego dowodu osobistego. Poinformowało w nim, że podjęło decyzję o *unieważnieniu* przetargu na dostawę nowych blankietów dowodów osobistych. Wcześniej stanowisko w sprawie wprowadzenia nowego dowodu osobistego przedstawił Komitet Rady Ministrów do Spraw Cyfryzacji.

Jak się okazuje, już w marcu br. Komitet rekomendował między innymi *przesunięcie terminu wdrożenia elektronicznych dowodów osobistych do czasu:*

- *przeprowadzenia testów, które będą mogły potwierdzić pełną integrację rejestrów państwowych;*
- *opracowania jednolitej polityki w zakresie uwierzytelniania obywateli w systemach teleinformatycznych administracji publicznej, na podstawie której będzie możliwe precyzyjne określenie niezbędnych funkcjonalności elektronicznego dowodu osobistego, w tym także rozstrzygnięcie celowości wprowadzania kolejnej metody uwierzytelniania – podpisu osobistego;*
- *nowelizacji ustawy o dowodach osobistych, która będzie uwzględniała wymagania wynikające z opracowanej polityki w zakresie uwierzytelniania, a także będzie zgodna ze znowelizowaną dyrektywą 1999/93/WE ws. wspólnotowych ram prawnych dla podpisów elektronicznych*.

Mając na uwadze stanowisko Komitetu Rady Ministrów ds. Cyfryzacji, MSW zdecydowało o podjęciu prac nad zmianą ustawy z 6 sierpnia 2010 r. o dowodach osobistych. Zmiana ta ma dotyczyć rezygnacji z *warstwy elektronicznej* dowodu osobistego.

Decyzja o podjęciu prac nad zmianą ustawy o dowodach osobistych powoduje, że dalsze prowadzenie przetargu wiązałoby się z nieuzasadnionym wydatkowaniem środków publicznych. Należy podkreślić, że przedmiotem postępowania przetargowego

było między innymi *wytworzenie i dostawa blankietów dowodu osobistego wyposażonego w mikroprocesor wraz z oprogramowaniem middleware zapewniającym komunikację z mikroprocesorem*.

Ze względu na nowe okoliczności, Ministerstwo podjęło decyzję o unieważnieniu przetargu, zgodnie z art. 93 ust. 1 pkt 6 ustawy z 29 stycznia 2004 r. Prawo zamówień publicznych.

Dlatego 16 kwietnia br. Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych zawiadomiło Centrum Projektów Informatycznych o unieważnieniu postępowania o udzielenie zamówienia publicznego na *„Dostawę niespersonalizowanych blankietów dowodów osobistych wyposażonych w mikroprocesor wraz z oprogramowaniem middleware zapewniającym komunikację z mikroprocesorem i wykonanie projektu technicznego dowodu osobistego”*.

- To była niedobra wiadomość – uważa Sławomir Cieśliński, właściciel firmy doradczej Medien Service. – W naszej nowej rzeczywistości prawie nie posunęliśmy się do przodu oprócz tego, że ponad 10 lat temu zmieniliśmy tradycyjne dowody osobiste książeczkowe na karty. Wtedy nie zdecydowano się na dowody z mikroprocesorem, argumentując że przyjdzie na to czas po kolejnej dekadzie. Dziś nic nie wskazuje na taki scenariusz wydarzeń, aktualne jest za to pytanie jak długo mamy jeszcze czekać na takie rozwiązanie?!

Od wielu lat toczą się dyskusje na ten temat. Cały czas mówi się o tym, że będziemy wydawać nowe dowody. Elektroniczne. Dlatego tak trudno zrozumieć kwietniowy komunikat. Przedstawiciele branży *kartowej* są zdezorientowani.

- Przygotowanie oferty w takim przetargu oznacza ogromny wysiłek dla firmy – potwierdza Konrad Piotrowski, Sales Manager w dziale Government Programs firmy Gemalto. – Trzeba opracować analizę techniczną, biznesową, prawną, operacyjną. Bardzo kosztowne są gwarancje bankowe. W ten sposób nie można prowadzić biznesu.

Do współzawodnictwa stanęło 5 firm (konsorcjów). Oferty złożyły 3. Według naszego informatora dla każdej z nich złożony proces przygotowania się do przetargu oznacza nakłady rzędu setek tysięcy złotych.

W całej branży nikt nie rozumie, o co chodzi. Poprzedni ministrowie spraw wewnętrznych uważali, że dokument taki jak dowód osobisty nie powinien być zamawiany w jednoosobowej spółce skarbu państwa. Najlepszym rozwiązaniem jest przetarg, na podstawie prawa zamówień publicznych, przypomina przedstawiciel firmy zaangażowanej w postępowanie, proszący o zachowanie anonimowości.

Polska Wytwórnia Papierów Wartościowych jest monopolistą w dziedzinie produkcji dokumentów, denerwuje się inna osoba z branży. Dostarcza po absurdalnie zawyżonych cenach. Twierdzi przy tym, że chodzi o bezpieczeństwo państwa. To bzdura. Przecież tajna jest tylko personalizacja. A tę wykonuje Centrum Personalizacji Dokumentów MSW.

Władze mają pewnie swoje argumenty. Ale do nas one nie docierają. To, co słyszymy, nie przekonuje nas. Być może chodzi o wynegocjowanie lepszej ceny od potencjalnego dostawcy, przypuszcza przedstawiciel innej firmy, proszący o zachowanie anonimowości.

W rzeczywistości sytuacja jest zupełnie niezrozumiała. Za dostawę obecnie obowiązujących dowodów osobistych – nie

zawierających mikroprocesora – państwo płaci PWPW 23,60 zł brutto za blankiet poliwęglanowy, czyli około 5,80 euro. Tymczasem na świecie średnia cena blankietu z warstwą elektroniczną (zawierającego chip, ale bez personalizacji) uzyskiwana w publicznych przetargach oscyluje wokół 5 euro. Oznacza to, że cena e-dowodu z mikroprocesorem od dostawcy wybranego w przetargu jest porównywalna z ceną jaką państwo płaci dzisiaj za dowód bez chipa. Dlaczego państwo tak bardzo przepłaca?, pytają przedstawiciele branży. Nie mówiąc o tym, że potencjalną konsekwencją obecnej sytuacji jest ryzyko utraty dotacji unijnych.

Projekt był pomyślany w ten sposób, że koszty wymiany dokumentu bierze na siebie budżet państwa. Obywatel płaci tylko wtedy, gdy zgubi. Choć były też inne pomysły, na przykład odpłatne sprawdzanie dokumentu w pewnych instytucjach, między innymi w bankach. Fiskus zastanawia się, w jaki sposób odzyskać trochę pieniędzy. Koszty mają być też niższe dzięki temu, że dowód nie będzie łączony z kartą zdrowia.

Podobno Ministerstwo Spraw Wewnętrznych pracuje nad nowym dokumentem bez elementu elektronicznego. Ale cały czas utrzymuje, że ma to być *nowa jakość*. W jaki sposób tego dokonać, skoro w grę ma wchodzić tylko warstwa graficzna? Fachowcy nie potrafią tego wytłumaczyć.

Nasze dokumenty są niebezpieczne, bo łatwe do sfałszowania. Istnieją między innymi dowody na to, jakie są straty operatorów telekomunikacyjnych z powodu fałszowania obecnego dowodu poliwęglanowego. Nic jednak dziwnego, skoro w ciągu 15 lat nie był on w zasadzie modernizowany. A fachowcy nie mają wątpliwości, że bez dołożenia części elektronicznej nie będzie lepszy.

Dowód osobisty służy do identyfikacji – zarówno w świecie rzeczywistym, jak i elektronicznym. Istnieje określony zestaw atrybutów charakteryzujących daną osobę. Są to między innymi imię i nazwisko, data urodzenia, wzrost, kolor oczu, adres zamieszkania. Te atrybuty nazywane są tożsamością osoby, zaś parametry tej tożsamości są zapisane w dowodzie osobistym. Na tej podstawie identyfikuje się osobę.

Część elektroniczna dokumentu to po prostu elektroniczny zapis tożsamości. W największym uproszczeniu można powiedzieć, że już dzisiaj banki, przydzielając nam karty, wydają nam elektroniczną tożsamość. A od dawna wiadomo, że podstawowym elementem fałszerstw jest identyfikacja na podstawie zmienionej tożsamości.

Nasza branża jest poważnie zaniepokojona trybem i tempem postępowania – podkreśla Wiesław Paluszyński, prezes firmy doradczej Trusted Information Consulting, członek Rady Polskiej Izby Informatyki i Telekomunikacji. – Niemcy zaczynali mniej więcej w tym samym czasie. W ciągu 7 lat zmodernizowali już swoje dokumenty, podobnie jak Francuzi i kilka innych społeczeństw w Europie.

Gdy w Niemczech rozpoczęto wydawanie elektronicznych dowodów osobistych, najważniejszym partnerem dla rządu byli przedsiębiorcy. Wiadomo bowiem, że im więcej aplikacji korzystających z elektronicznej tożsamości zbudują, tym lepiej. Na tegorocznych targach CeBIT niemiecki rząd miał własne stoisko, na którym zachęcał do współpracy wszystkich przedsiębiorców, którzy zechcą skorzystać z elektronicznej tożsamości w dokumentach identyfikacyjnych.

Dowody osobiste miały być również kołem zamachowym w procesie unowocześniania polskiej gospodarki. Chodzi o podpis

elektroniczny i możliwość załatwiania wielu spraw przez Internet w kontaktach z administracją publiczną. Na razie zatrzymaliśmy się w pół drogi.

- Ministerstwo ma rację, mówiąc o konieczności zakończenia modernizacji rejestów publicznych – przyznaje Wiesław Paluszyński. – Tylko, że nowy dowód nie ma nic wspólnego z modernizacją rejestrów, ponieważ nie będzie zawierał nic innego niż dzisiejszy dokument. Dlaczego władze nie robią nic konstruktywnego? Dlaczego wzorem władz niemieckich nie prowadzą najmniejszego publicznego dialogu z biznesem?

Nie ma sporu co do tego, że polskie rejestry nie są uporządkowane. Jednak według Komisji Europejskiej nie mamy już odwrotu. Można tylko przedłużyć postępowanie do 2015 r. Termin pozornie odległy, ale niedługo może się okazać za krótki. I będziemy płacić kary.

Załóżmy, że jeszcze w tym roku Ministerstwo nagle zaprasza biznes do współpracy i następują konkretne uzgodnienia. Biorąc pod uwagę realia trzeba na to co najmniej trzech lat. Nikt nie ma bowiem produktu, który w całości spełnia wymogi zamawiającego. Zwłaszcza że Ministerstwo Spraw Wewnętrznych zamówiło zaawansowane rozwiązanie. Sporządzenie projektu technicznego i uzyskanie certyfikacji musi zająć około 2 lat. Do tego należy dołożyć jeszcze rok na wybór dostawcy. Czyli w najlepszym razie możemy liczyć na koniec 2015 r. Naturalnie pod warunkiem, że nie będzie odwołań.

Na razie brak dowodów elektronicznych szkodzi całej gospodarce. Istnieje kilka dużych systemów informatycznych, które nie mogą być obsługiwane z zastosowaniem powszechnie dostępnej elektronicznej tożsamości. Należą do nich ZUS, ewidencja działalności gospodarczej, księgi wieczyste, KRS. Z powodu braku e-dowodu każdy z nich stosuje inne metody uwierzytelniania i dodatkowo wymaga kolejnych wizyt obywateli w urzędach, aby taką elektroniczna tożsamość uzyskać.

- Tymczasem według Komitetu Cyfryzacji nie ma systemów informatycznych, które by mogły z elektronicznego dowodu korzystać – przypomina Wiesław Paluszyński. – Miała być nowelizacja ustawy o dowodach. Do tej pory nic się nie dzieje. Widać, że władze nie mają strategii w tym zakresie. Podejmowane działania to kwadratura koła.

Minęły 4 miesiące. Komisja Europejska opublikowała w tym czasie propozycję decyzji Parlamentu Europejskiego w sprawie jednolitej identyfikacji i podpisu elektronicznego. W naszym kraju bez dowodu elektronicznego w zasadzie nie będzie można jej wprowadzić. Natomiast w opinii, którą minister spraw wewnętrznych przedłożył Komitetowi Cyfryzacji, będącą podstawą rekomendacji wydanych przez ten Komitet, było napisane, że Unia Europejska nie planuje żadnych działań w zakresie identyfikacji w elektronicznych dokumentach tożsamości.

- Rekomendacja dotyczyła tylko tego, żeby opóźnić wprowadzenie nowych dowodów dopóki nie nastąpi integracja rejestrów publicznych – zwraca uwagę Sławomir Cieśliński. – Rozpoczęła się wówczas dyskusja, co kto rozumie pod pojęciem integracji. Jak się okazało, problem nie w integracji rejestrów, tylko w tym, żeby one się ze sobą porozumiewały. Czyli nie chodzi o integrację, a interoperacyjność. Tylko co to ma wspólnego z wydawaniem dowodu osobistego?

Zdaniem naszych rozmówców jest jeden wygrany tej *zabawy*: dotychczasowy producent blankietów dowodów. Jak już była

mowa, nowy dokument osobisty z mikroprocesorem mógłby kosztować mniej niż wydawany dzisiaj plastikowy bez chipu. Czyli wszystkie argumenty dotyczące finansowej strony przedsięwzięcia tracą wiarygodność. A doniesienia te muszą być prawdziwe, bowiem nikt z administracji rządowej ich nie podważa.

Sprawa jest poważna. Były już skargi do Urzędu Zamówień Publicznych i Krajowej Izby Odwoławczej. Bezskuteczne. Jeden z oferentów – firma Signity – zaskarżył więc decyzję MSW do sądu.

Udało nam się dotrzeć do tej skargi. Spółka powołuje się na wiele nieprawidłowości w postępowaniu. I wnosi między innymi o:

(…)

- stwierdzenie, iż zamawiającym w postę powaniu jest Centrum Projektów Informatycznych (poprzednio Centrum Projektów Informatycznych MSWiA);
- stwierdzenie, iż decyzja o unieważnieniu postępowania została podjęta przez podmiot nieuprawniony, a zatem nie wywołuje żadnych skutków prawnych;
- unieważnienie czynności polegającej na unieważnieniu postępowania na podstawie art. 93 ust. 1 pkt 6 Pzp wobec braku rzeczywistego wystąpienia przesłanek do unieważnienia postępowania w przypadku uznania, iż przeciwnikiem skargi i zamawiającym w postępowaniu jest Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji (obecnie CPD MSW);
- nakazanie przeciwnikowi skargi dalszego prowadzenia postępowania, a w związku z tym wyznaczenie nowego terminu składania ofert względnie przyjęcie oferty skarżącej złożonej 17 lutego 2012 r. i zwróconej jej 16 kwietnia 2012 r. (…)

Termin rozpatrzenia sprawy został wyznaczony na 28 września br.

- Wygląda na to, że musi zarobić jedna firma: Polska Wytwórnia Papierów Wartościowych – twierdzi Wiesław Paluszyński. – I my to nawet rozumiemy. Państwo może zbudować monopol, jeżeli zrobi to zgodnie z przepisami. Skoro państwo uważa, że regulacje unijne dopuszczają wyjęcie z rynkowych działań określonych obszarów i specjalnie do tego celu trzeba powołać podmiot gospodarczy, to należy taki podmiot powołać zgodnie z prawem i dać mu takie uprawnienia. Ten podmiot obowiązuje wtedy ustawa o zamówieniach publicznych i wszystkie ograniczenia o zatrudnieniu i wysokości wynagrodzeń władz i tak dalej. Na tej zasadzie działa Centrum Personalizacji Dokumentów MSW.

Jeśli państwo zakłada, że dowody osobiste czy paszporty powinny być produkowane przez podmiot, który nie uczestniczy w grze rynkowej, to państwu wolno to zrobić. Ale państwu nie wolno podejmować na rynku działań o charakterze: nieuczciwej konkurencji, niedozwolonej pomocy publicznej i wydawać pieniędzy podatników w sposób nietransparentny, czyli poza ustawą o zamówieniach publicznych.

- W tej sprawie protestujemy z całą stanowczością – mówi Wiesław Paluszyński. – PWPW może się przekształcić w agendę skarbu państwa. Przestanie być wtedy spółką funkcjonującą na rynku. Będzie działała poza regulacjami obowiązującymi spółki akcyjne na polskim rynku. Państwo będzie jej wtedy zlecać prace na innych warunkach, które musi określić w ustawie. Podejdziemy do tego z pokorą. I nie będziemy się angażowali wydatkując prywatne pieniądze firm na postępowania, które później są unieważniane w niejasnych okolicznościach. Ale na razie dziwi nas, że władze akceptują takie postępowanie.

- Brakuje strategicznej wizji unowocześniania państwa ponad podziałami politycznymi oraz jej kompleksowej, profesjonalnej realizacji prowadzonej w oparciu o wieloletni harmonogram i według reguł właściwych dla zarządzania wielkimi projektami – dodaje Sławomir Cieśliński. – Administracja centralna niestety nie pełni funkcji służebnych wobec obywateli i ich potrzeb. A przecież dzisiaj wiele procesów biznesowych przenosi się do elektronicznego świata. I one muszą być dobrze i w odpowiednim czasie uregulowane przez instytucje państwowe ale przede wszystkim w interesie społecznym i gospodarczym, a nie w sposób i w terminach wygodnych dla państwowych urzędów i stojących za nimi partii politycznych .

Nigdzie na świecie systemy tej skali nie są realizowane bez porozumienia politycznego. Trzeba dokonać pewnych uzgodnień strategicznych ponad podziałami, które powodują, że nie zmienia się celów strategicznych. Można dyskutować o modyfikacjach technicznych, o zmianie rozwiązań cząstkowych, ale zasadnicze cele muszą być zachowane. U nas był konsensus między PiS (które uruchamiało ten projekt) i PO. Tym trudniej zrozumieć zmianę stanowiska partii rządzącej w listopadzie ubiegłego roku.

Na razie wiemy wyłącznie o *odroczeniu* przetargu. Jego uczestnicy podkreślają, że nie rozumieją tego pojęcia. Niestety, wątpliwości nie udało nam się rozstrzygnąć u źródła. Rzecznicy Ministerstwa Spraw Wewnętrznych oraz Ministerstwa Administracji i Cyfryzacji odesłali nas jedynie do cytowanego już kwietniowego komunikatu.

Takie postępowanie władz stawia Polskę w niekorzystnym świetle. Psuje wizerunek kraju i państwa. Wyrzucamy przy tym pieniądze do kosza. Rząd wydał już 160 mln zł na projekty wspierające. Odszkodowania dla dostawców mogą sięgnąć kilkudziesięciu mln zł. To nie jest racjonalne działanie, podkreśla fachowiec z branży.

W połowie kwietnia br. Ministerstwo Spraw Wewnętrznych opublikowało komunikat w sprawie nowego dowodu osobistego. Poinformowało w nim, że podjęło decyzję o *unieważnieniu* przetargu na dostawę nowych blankietów dowodów osobistych. Wcześniej stanowisko w sprawie wprowadzenia nowego dowodu osobistego przedstawił Komitet Rady Ministrów do Spraw Cyfryzacji. Jak się okazuje, już w marcu br. Komitet rekomendował między innymi *przesunięcie terminu wdrożenia elektronicznych dowodów osobistych.*

Mając na uwadze stanowisko Komitetu Rady Ministrów ds. Cyfryzacji, MSW zdecydowało o podjęciu prac nad zmianą ustawy z 6 sierpnia 2010 r. o dowodach osobistych. Zmiana ta ma dotyczyć rezygnacji z *warstwy elektronicznej* dowodu osobistego. Decyzja o podjęciu prac nad zmianą ustawy o dowodach osobistych powoduje, że dalsze prowadzenie przetargu wiązałoby się z nieuzasadnionym wydatkowaniem środków publicznych. Ze względu na nowe okoliczności, Ministerstwo podjęło decyzję o unieważnieniu przetargu, zgodnie z art. 93 ust. 1 pkt 6 ustawy z 29 stycznia 2004 r. Prawo zamówień publicznych.

W naszej nowej rzeczywistości prawie nie posunęliśmy się do przodu oprócz tego, że zmieniliśmy tradycyjne dowody osobiste książeczkowe na karty. Od wielu lat toczą się dyskusje na ten temat. Cały czas mówi się o tym, że będziemy wydawać nowe dowody. Elektroniczne. Dlatego tak trudno zrozumieć kwietniowy komunikat MSW. Przedstawiciele branży *kartowej* są zdezorientowani.

Podobno Ministerstwo Spraw Wewnętrznych pracuje nad nowym dokumentem bez elementu elektronicznego. Ale cały czas utrzymuje, że ma to być *nowa jakość*. W jaki sposób tego dokonać, skoro w grę ma wchodzić tylko warstwa graficzna? Fachowcy nie potrafią tego wytłumaczyć. Nasze dokumenty są niebezpieczne, bo łatwe do sfałszowania. Istnieją między innymi dowody na to, jakie są straty operatorów telekomunikacyjnych z powodu fałszowania obecnego dowodu poliwęglanowego. Nic jednak dziwnego, skoro w ciągu 15 lat nie był on w zasadzie modernizowany. A fachowcy nie mają wątpliwości, że bez dołożenia części elektronicznej nie będzie lepszy.

Branża *kartowa* jest poważnie zaniepokojona trybem i tempem postępowania. Niemcy zaczynali mniej więcej w tym samym czasie. W ciągu 7 lat zmodernizowali już swoje dokumenty, podobnie jak Francuzi i kilka innych społeczeństw w Europie.

Dowody osobiste miały być kołem zamachowym w procesie unowocześniania polskiej gospodarki. Chodzi o podpis elektroniczny i możliwość załatwiania wielu spraw przez Internet w kontaktach z administracją publiczną. Na razie zatrzymaliśmy się w pół drogi.

Mieczysław T. Starkowski - jest dziennikarzem. Od wielu lat zajmuje się między innymi szeroko pojętą teleinformatyką.

Zapraszamy do udziału

KONFERENCJA

POLITYKA ZARZĄDZANIA OPROGRAMOWANIEM (PZO) - ASPEKTY PRAKTYCZNE, ORGANIZACYJNE I PRAWNE

8 listopada 2012 r., Warszawa

Spotkanie ma na celu przybliżyć aktualną problematykę procesowego zarządzania oprogramowaniem komputerowym, bezpieczeństwa informacji oraz zapoznać z możliwościami systemowego zarządzania zasobami IT.

Zaproszenia kierujemy do dyrektorów finansowych i dyrektorów departamentów odpowiedzialnych za infrastrukturę teleinformatyczną oraz kierowników działów IT.

Prowadzenie obrad: Jarosław Kwiatkiewicz

W programie m.in.:

- Polityka zarządzania oprogramowaniem w praktyce
- Odpowiedzialność prawna za używanie nielegalnego oprogramowania i za nadużycia licencyjne
- Narzędzie wspierające Zarządzanie Oprogramowaniem (SAM)
- Zarządzanie oprogramowaniem w administracji publicznej - wyniki badań jakości zarządzania zasobami IT
- Ujawnianie nielegalnego oprogramowania w firmach
- Procedury postępowań w przypadkach włamań do systemu informatycznego (zbieranie i zabezpieczanie materiałów, dowody cyfrowe, analiza powłamaniowa)
- Nowe strategie i narzędzia w przeciwdziałaniu stosowania nielegalnego oprogramowania

Więcej informacji: www.cpi-sk.pl

Trochę historii informatyzacji w kraju i na świecie – dlaczego wybuchła „wielka rewolucja" SOA

Piotr Kociński

Przed przedstawieniem propozycji skutecznego stworzenia e-administracji musimy określić punkt zerowy. Jest to niezwykle ważne z dwóch względów:

- budowę e-administracji należy prowadzić jako transformację do SOA, zatem znajomość punktu zerowego, choćby ze względu na konieczność określenia jakie usługi będą udostępniane i przez kogo, jest konieczna
- posiadając punkt odniesienia można obserwować postępy działań.

W celu określenia „informatycznej charakterystyki" punktu zerowego, posługując się wprowadzonymi wyżej terminami i koncepcjami, pokażemy jak informatyzacja sfery publicznej postępowała wpierw w PRL-u, później już w Polsce.

Typ BC dominował na całym świecie do początku lat 90-tych, w Polsce również. To co jednak wyróżniało Polskę na tle innych krajów to fakt, że wtedy byliśmy krajem komunistycznym, który miał utrudniony dostęp do nowoczesnych technologii informatycznych (te „pozyskane" nowoczesne egzemplarze komputerów były w dyspozycji różnorakich służb i PZPR-u), najczęściej używano więc polskich bądź sowieckich podróbek rozwiązań zachodnich. Rozwiązania informatyczne stosowano przede wszystkim w sektorze publicznym, a właściwie w sektorze inwigilacji obywateli – taką rolę pełnił między innymi system PESEL. Firmy (banki, fabryki) były państwowe i nowoczesne metody zarządzania informacją, które w latach 70-tych i 80-tych gwałtownie zmieniły ich funkcjonowanie w świecie zachodnim, w Polsce odgrywały niewielką rolę. Natomiast warto zwrócić uwagę, że forma dostarczania usług informatycznych dla firm (państwowych) była na wskroś nowoczesna! Mianowicie, najczęściej usługi były dostarczane przez firmy (też naturalnie państwowe) zewnętrzne tzw. ZETO (Zakład Elektronicznej Techniki Obliczeniowej), czyli mieliśmy do czynienia z tym, co współcześnie nazywamy *outsourcingiem*. W ogólności Polska była słabo nasycona techniką informatyczną w porównaniu z zachodnią Europą, a do tego nawet te słabe nasycenie było nierównomierne, lepiej prezentowała się sfera publiczno-administracyjna, gorzej baza produkcyjna i banki, czy firmy ubezpieczeniowe (ZUS, PZU, Warta).

Typ AD zaczął zdobywać rynek w latach 90-tych i „rządził" do połowy lat 2000-cznych. W tym okresie Polska w obszarze komercyjnym (banki, firmy) wręcz korzystnie zaczęła wyróżniać się w świecie, gdyż z racji wspomnianego już wyżej zapóźnienia przejawiającego się w niewielkiej liczbie wdrożeń typu BC, wdrażano rozwiązania od razu typu AD, a co za tym idzie, uniknięto trudów żmudnej transformacji wielu rozwiązań z typu BC na AD. Transformacji, która tak wiele kłopotów sprawiła w krajach cywilizacyjnie bardziej zaawansowanych. W Polsce firmy „wskoczyły" od razu w ówcześnie nowoczesne rozwiązania informatyczne typu AD. W rezultacie wiele procesów biznesowych przebiega w Polsce szybciej niż USA, czy innych krajach zachodnich! Przykładem najbardziej spektakularnym niech tu będzie przelew międzybankowy, który w Polsce realizowany jest niezwykle szybko w porównaniu z krajami zachodniej Europy, a to dzięki dobrym rozwiązaniom instytucjonalnym

(Krajowa Izba Rozliczeniowa) i dobrym wspierającym je rozwiązaniom informatycznym. W ogólności „Polska biznesowa" dość sprawnie nasyciła się dobrymi w swojej klasie rozwiązaniami, w tej dziedzinie zdecydowanie „dogoniliśmy" kraje niedotknięte wcześniej plagą komunizmu. Jeśli jednak chodzi o interesującą nas sferę publiczną, to tu działo się gorzej. Z jednej strony pod koniec lat 90-tych zeszłego stulecia i na początku 2000-cznego nastąpił gwałtowny rozwój informatyki samorządowej. Różne urzędy gminne czy miejskie starały się wchodzić w „erę" informatyczną. Niestety na ogół wdrażane rozwiązania nie były wysokiej, a nawet średniej klasy, lecz przede wszystkim były bardzo zróżnicowane, słabo interoperacyjne, co przy próbie stworzenia z nich w miarę jednego środowiska informatycznego administracji publicznej, skutkowało porażką. Mimo wszystko, nawet w sferze publicznej, paradoksalnie, trochę dzięki komunistycznym zaszłościom, Polska ciągle nie odstawała bardzo od krajów zachodnich.

Od połowy lat 2000-cznych, w Polsce wiele firm, na początku przede wszystkim banków, przeszło już transformację do SOA. Jeśli chodzi o wykorzystanie informatyki (w jej szerokim znaczeniu) w firmach, to w Polsce osiągnięty poziom jest wysoki. Niestety nie da się tego powiedzieć o zastosowaniu informatyki w administracji. Funkcjonuje w niej na poziomie centralnym trochę „dinozaurów", takich jak system PESEL (klasyka aplikacji typu BC, choć przerobiona trochę w stronę typu AD) oraz w samorządach i gminach trochę aplikacji typu AD. Próby wdrożenia nowoczesnych rozwiązań, czy to dla zapewnienia efektywnej obsługi obywatela w urzędach samorządowych, czy to polepszeniu funkcjonowania jakiejś specjalnej sfery życia publicznego, czy to dla umożliwienia obywatelom załatwiania spraw urzędowych przez Internet, kończyły się umiarkowanym sukcesem (rzecz ujmując najdelikatniej), bądź nawet realnie się nie zaczęły (patrz informatyzacja służby zdrowia), chyba, że okresową produkcję opracowań, standardów, dokumentów przetargowych, przepięknych niekiedy diagramów obrazujących procesy biznesowe (zawsze z napisem Internet umieszczonym w chmurce) uznamy za byt realny. Uznać możemy naturalnie wszystko, tyle, że na przykład w obszarze służby zdrowia, na poziomie centralnym, czy regionalnym, poza województwem śląskim, gdzie przed dziesięciu laty coś naprawdę zrobiono w tej dziedzinie, nie działa nic, czego boleśnie doświadczyliśmy w styczniu 2012 roku. Przyczyną tej sytuacji, poza mankamentami ustawowymi, jest naszym zdaniem fakt, że nie korzystano z dobrodziejstw architektury typu SOA. Choć oczywiście mówiono o SOA dużo, zamawiano gotowe pakiety typu *enterprise service bus*, to tak naprawdę usiłowano wdrażać za „jednym zamachem" aplikacje typu AD, wielkie funkcjonalne „mastodonty". Do tego poziom projektowania takich rozwiązań (określanie zbiorów funkcji, architektury, wspólnych semantyk, dobierania sprzętu pod aplikacje) był niski. To się nie mogło udać. I to wszystko właśnie stanowi punkt zerowy, w którym przychodzi podjąć działania.

Do czego dążymy, do czego dążyć winniśmy. Propozycja nowego podejścia do informatyzacji polskiej administracji

Mamy nadzieję, ze dla uważnego czytelnika staje się jasnym, że jesteśmy zwolennikiem następującego poglądu. O ile stan informatyzacji polskiej administracji w roku 2000 mieścił się w pewnej światowej normie wynikającej z naturalnego rozwoju technologii informatycznych, w trzech dekadach poprzedzających rok 2000 (komunistyczne zacofanie nie miało na stan z 2000 wielkiego wpływu), to ostatnie 10 lat uznać należy za czas zmarnowany. Wyjątki takie jak na przykład informatyzacja ksiąg wieczystych, informatyczne oprzyrządowanie Straży Granicznej, elementy ciekawych rozwiązań informatycznych w Instytucie Pamięci Narodowej, PIT 37 przez Internet, nieustająca, coraz skuteczniejsza walka z informatyką w ZUS, ostatnio

możliwość rejestracji firm przez Internet, pozostają ciągle wyjątkami. Samotnymi wyspami w morzu informatycznej nicości. Właśnie ta swoista autonomiczność funkcjonowania tych nielicznych rozwiązań stoi w żywej sprzeczności z możliwościami oferowanymi przez architekturę typu SOA. Nie ma wsparcia informatycznego dla mnóstwa obszarów sfery publicznej. Dla tych obszarów, z którymi obywatel spotyka się najczęściej, a których informatyzacja, zwłaszcza ta przeprowadzona w wyżej opisanym trybie iteracyjnym w celu stworzenia środowiska informatycznego w typie SOA, wprowadziłaby jakościową zmianę ich funkcjonowania! Jak to zrobić? Jak dobrze zdefiniowane wymagania funkcjonalne „przetłumaczyć" na realne rozwiązania informatyczne? Jak całym instrumentarium typowym dla wykonywania informatycznego rzemiosła, przedstawionym wyżej posłużyć się, żeby osiągnąć cel jakim jest e-administracja? Przedstawiając naszą propozycję będziemy posługiwali się terminami wprowadzonymi wyżej, jak również, będziemy odnosili się do konkretnego obszaru działania sfery publicznej, do obszaru służby zdrowia.

Zacząć należy od fundamentalnego stwierdzenia, że proponujemy wdrażanie rozwiązania w architekturze typu SOA, w sposób iteracyjny i organiczny (w sensie w jakim te pojęcia zostały wprowadzone powyżej) przy wykorzystaniu, w możliwie maksymalnym stopniu, funkcjonujących aplikacji typu BC, rzadziej typu AD. Będziemy prowadzili zatem budowę e-administracji jako transformację do SOA. Naturalnie, zgodnie z powyższymi sugestiami, mocno rekomendujemy podjęcie próby dywersyfikacji dostawców poprzez przydzielanie poszczególnym dostawcom grup usług do wdrożenia.

Właściwe, zważywszy na szczegółowe wyjaśnienie terminów i okoliczności (skąd zaczynamy bieg), na powyższej deklaracji można zakończyć prezentację propozycji nowego otwarcia budowy e-administracji. Jednak zdajemy sobie sprawę, że zastosowanie szeregu nowych pojęć i koncepcji w praktyce jest zawsze trudne. Trochę przypomina napisanie pierwszego listu w obcym języku, którego właśnie się nauczyliśmy. Przedstawimy więc na przykładzie obszaru służby zdrowia, jak w praktyce dokonywać transformacji, którą ma nam przynieść e-administracja.

Zacząć zawsze należy od zbudowania funkcji i zdefiniowania procesów biznesowych. W pewnym uproszczeniu, winno być tak:

- pacjent przychodząc do lekarza, już na samym początku wizyty ma *zweryfikowaną tożsamość (*czy to przez staranne badanie dowodu osobistego przez odpowiednio przeszkoloną w tym celu pielęgniarkę, czy to przez odczytanie odpowiedniej karty w czytniku),
- w oparciu o jego numer identyfikacyjny (może być PESEL) *lekarz w momencie rozpoczęcia badania widzi na ekranie komputera historię zdrowotną pacjenta*, jak i stan jego ubezpieczenia,
- lekarz *stawia diagnozę*,
- *zapisuje* ją w wersji elektronicznej,
- wystawia receptę
- aptekarz *weryfikuje tożsamość* pacjenta, podobnie jak lekarz,
- *widzi stan ubezpieczenia* pacjenta na monitorze komputera (bądź jedynie widzi, że tego pacjenta nie ma na liście nieubezpieczonych, co może być również traktowane jako pozytywna weryfikacja stanu ubezpieczenia!)
- lekarz stawia diagnozę, posługując się dodatkową pomocą
- wydaje lekarstwo i *zapisuje w formie elektronicznej* fakt wydania lekarstwa, potencjalnie w dwóch bazach, gromadzącej dane o pacjentach – to do niej dostęp mają lekarze - oraz w bazie sprzedanych leków.

W kolejnych iteracjach wdrożenia można określać, a następnie dodawać do rozwiązania nowe funkcje, takie jak na przykład:

- dostęp przez Internet do opisów prześwietleń i skanów CT, dla właściwych kategorii użytkowników,
- umawianie wizyt ze specjalistą z informowaniem pacjentów za pomocą SMS,
- poszukiwanie oszustw w obrocie lekami itd.

Mając zdefiniowany proces i funkcje, rozpoczynamy fazę ustalania szczegółowych oczekiwań, względem poszczególnych funkcji. To jest moment, w którym dyskutujemy takie sprawy jak na przykład:

- czy lekarz winien widzieć dane z ostatniego roku oraz dane o uczuleniach, alergiach czy też wszystko, bądź wszystko razem, ale pod pewnymi warunkami,
- skąd te dane winny być czytane, z jakiejś centralnej bazy danych przesłane przez Internet do komputera lekarza, albo z karty czipowej, którą pacjent przyniósł ze sobą,
- czy dodatkowa pomoc przy diagnozowaniu winna być w formie programu lokalnego, czy będącego częścią centralnego rozwiązania dostępnego za pomocą przeglądarki, czy też w formie zwykłej książki (to jest przykład oceny *podatności funkcji na informatyzację*, czynności którą warto wykonywać, gdyż nie wszystko musi być informatyzowane),
- czy wypisanie recepty winno być wykonane w formie elektronicznego zapisu w dostępnej aptekarzom bazie danych, czy w formie tradycyjnej (to jest znów przykład oceny podatności funkcji na informatyzację).

To są szczegóły, które w zależności od warunków prawnych uzgodnień pomiędzy właściwymi organami, dostępnymi w danym momencie środkami finansowymi, mogą być różnie realizowane w różnych iteracjach wdrożenia. Pracując w architekturze typu SOA możemy wpierw zdecydować się na jeden wariant rozwiązania, a potem zmieniając tylko sposób czytania danych w wyspecjalizowanej usłudze zrealizować inny wariant. Ważne jest, że ta dyskusja nie powinna wstrzymywać wdrażania rozwiązania! Pamiętajmy, że podejście SOA właśnie po to zostało wymyślone, żeby rozwiązania były elastyczne, to znaczy, żeby można łatwo je zmieniać, dopasowywać do nowych warunków itd. Widać też, że dostarczenie funkcji będzie wymagało odwołania się odpowiednio do kilku rozwiązań, zapewne pozostających w gestii różnych instytucji, gdyż nasz przykładowy proces ma charakter hybrydowy – patrz wyżej – co jest typowe dla procesów w obszarze publicznym.

Jak już podkreślaliśmy wyżej, nie trzeba, a nawet nie należy, zaczynać od dużego zakresu funkcjonalnego, bo niewiele dobrego powstanie, co zresztą widać w Polsce, gdzie rozwiązanie kompleksowe dla służby zdrowia wdrażane jest od 1999 roku, bez efektów. Na początek stwórzmy rozwiązanie informatyczne, które powyższy prosty scenariusz użycia efektywnie wesprze, a nawet można się zdecydowaćna wdrożenie rozwiązania, które na początku będzie umożliwiało informatyczne wsparcie tylko fragmentu powyższego scenariusza. Czas na zdefiniowanie usług, które trzeba stworzyć w formie takich czy innych programów, a które wykonywane w odpowiednim porządku zrealizują zdefiniowany proces, bądź jego wybrane fragmenty.

Odpowiednie dla naszego przykładu wydają się być następujące usługi:

- Zapisanie danych o pacjencie w przypadku pierwszego jego kontaktu ze służbą zdrowia w formie elektronicznego rekordu w jakimś głównym rejestrze (nazywajmy go dalej R1),

- Zapisanie danych o każdym leczeniu pacjenta w formie elektronicznego rekordu w rejestrze R1,
- Zapisanie każdej nowo wprowadzonej procedury medycznej w formie elektronicznego rekordu, w jakimś głównym właściwym dla tej sprawy rejestrze,
- Sprawdzanie tożsamości (autentykacja) pacjenta,
- Sprawdzenie autentyczności dowodu osobistego,
- Sprawdzanie czy pacjent jest ubezpieczony,
- Wyświetlenie informacji i podpowiedzi wspomagających diagnozowanie,
- Zapisanie danych o zakupie lekarstw przez pacjenta, w formie elektronicznych rekordów w jakimś właściwym dla tej sprawy rejestrze.

Zwróćmy uwagę, że usługa „wyświetlenie informacji i podpowiedzi wspomagających diagnozowanie", byłaby tworzona w którejś z kolejnych iteracji – pamiętamy wszak o iteracyjnym charakterze naszego postępowania – gdyż jest trudna i kosztowna do zrobienia. Takie właśnie decyzje, polegające na badaniu stopnia podatności na informatyzację różnych funkcji i w konsekwencji na hierarchizowaniu zdefiniowanych usług celem określenia, w której iteracji będą tworzone, winne być podejmowane w tym właśnie momencie.

Kolejny ważny krok to dokonanie przeglądu działających „starych" aplikacji (typu AD czy BC), żeby ocenić które z nich są kandydatami do udostępniania potrzebnych usług. W przypadku administracji publicznej nie warto, a nawet nie należy, ograniczać się tylko do aplikacji z własnej instytucji, ale należy spojrzeć szerzej, gdyż realizacja większości procesów z różnych obszarów publicznych będzie zawsze wymagała pewnych usług udostępnianych z systemów MSW. Tworzymy rozwiązanie typu SOA do realizacji procesów hybrydowych, więc integracja różnych rozwiązań, czy udostępnianie usług z innych rozwiązań niż to, które projektujemy, jest czymś naturalnym.

W tym momencie przechodzimy już do precyzyjnego projektowania poszczególnych usług. Weźmy na przykład „Sprawdzanie tożsamości (autentykacja)". Usługa będzie najprawdopodobniej stworzona poprzez udostępnienie właściwej funkcjonalności z systemu PESEL 2, a polegać będzie na sprawdzeniu czy numer identyfikacyjny pacjenta istnieje w tej bazie. Wszystkie powyższe usługi, mogą być w sensie informatycznym zrealizowane w różny sposób, choć pewne sposoby wydają się lepsze niż inne (na przykład usługa „Sprawdzanie czy pacjent jest ubezpieczony" może być stworzona poprzez jej udostępnienie z odpowiedniego systemu ZUS za pośrednictwem Internet-u - a więc jej jakże ważna skuteczność będzie determinowana bezbłędnym funkcjonowaniem polskich *providerów* Internetu - albo może być stworzona od nowa, jako autonomiczny program działający na komputerze w każdej aptece, odwołujący się do lokalnej niewielkiej bazy danych nieubezpieczonych, której aktualizowana wersja byłaby dystrybuowana wśród aptek raz w miesiącu).

Należy zawsze sprawdzać, czy usługi wdrażać trzeba „od zera", czy też *udostępnić* (jak wyżej). Zwróćmy też jeszcze raz uwagę, że implementując te usługi myślimy i działamy już w kategoriach środowiska informatycznego dla całej administracji, jako że wiele usług tworzyć będziemy w oparciu o mechanizm udostępnienia z aplikacji (typu BC) będącej w gestii MSW.

Prowadząc wdrożenie w jednym obszarze należy zbadać, czy istnieją już określone standardy semantyczne z których możemy skorzystać, bądź uzupełnić je o te, które powstaną w ramach tworzenia naszego rozwiązania.

W ten sposób uniknie się znaczących problemów z interoperacyjnością różnych środowisk informatycznych administracji publicznej.

No i naturalnie prowadząc budowę w ten sposób, należy pamiętać o sprawnym zarządzaniu projektem, zważywszy choćby jak wiele zależy od uzgodnień pomiędzy różnym instytucjami.

To co proponujemy wydaje się nam ważne zważywszy na fakt, że w przypadku ciągnącej się już latami informatyzacji służby zdrowia, funkcje i procesy są kiepsko zdefiniowane, a odwzorowanie funkcji na usługi nie istnieje. Nie może być inaczej skoro, choć mówi się o SOA, to w zamian - dość niekonsekwentnie zresztą - usiłuje się wdrażać w trybie „za jednym dużym zamachem", środowisko składające się z trzech aplikacji w architekturze typu AD. O realnym oparciu rozwiązania na usługach mowy nie ma, w każdym razie nie w ogłoszonych rok temu zapytaniach przedofertowych. Efekty są jak każdy widzi.

Reasumując, prowadząc budowę rozwiązania w architekturze typu SOA, służącego do realizacji procesów hybrydowych, należy:

a) Zdefiniować funkcje i procesy
b) Wprowadzić hierarchię funkcji, zacząć od funkcji najważniejszych
c) Zbadać, realizacja których z tych funkcji nie musi być wsparta narzędziami informatycznymi (powody mogą być różne: finansowe, technologiczne, kwestie pewnych przyzwyczajeń użytkowników itd.)
d) Starannie przeanalizować jakimi usługami musimy dysponować, żeby zrealizować te najważniejsze
e) Zbadać, które z tych usług mogą być *udostępnione* w oparciu o aplikacje typu BC czy AD, funkcjonujące już gdzieś w obrębie administracji publicznej
f) Zaprojektować usługi
g) Stworzyć usługi od zera, bądź przez udostępnienie testować, wdrażać zgodnie z regułami informatycznego rzemiosła

Potem można w kolejnej iteracji wrócić do punktu a. , definiując kolejne funkcje, a następnie przejść przez punkty od c. - g. Przypomnijmy, że usługi można podzielić na paczki i powierzać wykonanie czynności f. - g. dla pojedynczych paczek różnym firmom, w ten sposób dywersyfikując ryzyko porażki projektu.

Na koniec wspomnijmy tylko, że należałoby rozważyć stosowanie metody mierzenia *wartości* w sektorze publicznym (*ang.* public sector value), która służy do oceny korzyści płynących z wdrożenia jakiegoś rozwiązania informatycznego przez policzenie tzw. *wartości publicznej*. *Wartość* ta zależy od różnych *miar*, które - analizując dany przypadek – definiujemy wraz z odpowiednimi *wagami*, jako najlepiej opisujące funkcjonowanie instytucji. Co więcej, owa *wartość* może być odniesiona do poniesionych na wdrożenie oraz eksploatację kosztów. Ponieważ koszty te, jak i konkretne wartości miar, silnie zależą od zastosowanej architektury, technologii, to porównując *wartości względne* (*wartość/koszty*) można oceniać jakość rozwiązań proponowanych przez różnych dostawców. Ekstrapolując koszty i dobrze definiując choć część miar, odpowiednich wag oraz sposobów ekstrapolowania wartości poszczególnych miar, w zależności od różnych aspektów rozwiązania, zamawiający może zbudować zestaw kryteriów umożliwiający skuteczny wybór dostawców. Takie kryteria, uwzględniając kwestię ceny, silnie jednak uzależniają wybór od jakości rozwiązania. Powszechniejsze stosowanie tej metody mierzenia korzyści pozwoliłoby w obszarze administracji publicznej poprawić sposób wybierania dostawców, co nawet w przypadku wybierania wielu dostawców dla wdrożenia odpowiednich „paczek" usług i w połączeniu

z precyzyjnym określeniem punktu początkowego do dalszych działań informatyzacyjnych, przyniosłoby pozytywne skutki.

Nie odnieśliśmy się do kwestii dobierania serwerów czy oprogramowania narzędziowego. Po pierwsze tym zajmują się wszyscy, właściwie dotychczasowe działania informatyzacyjne w sferze publicznej do wybierania i kupowania sprzętu się sprowadzały. Jest już tego mnóstwo. To czym się zajmowaliśmy w tym artykule jest za to często w ogóle pomijane, bądź traktowane jako dodatek do wielkich zakupów *hardware*. Naszym zdaniem bez zdefiniowania *po co*, bez stworzenia dobrej, korporacyjnej architektury, nawet najlepsze serwery nie pomogą zbudować e-administracji.

Podsumowanie

Dysponujemy koncepcjami i technologiami, które nawet w reżimie Ustawy z dnia 29 stycznia 2004 pozwalają dokonać informatyzacji szybko i efektywnie. Warunkiem powodzenia jest postępowanie w sposób iteracyjny w celu budowy rozwiązań w architekturze SOA. Istnieją metody pomiaru jakości wdrożenia, dzięki którym możliwe jest również sprawne nadzorowanie procesów przetargowych i wdrożeniowych. A jednak, choć cały ten wachlarz możliwości jest skutecznie stosowany w wielu krajach, to w Polsce nie jest. A nawet jak niekiedy coś się jednak uda zrobić, to brak odpowiednich regulacji prawnych uniemożliwia właściwe w XXI wieku tego użycie, a jedynie czyni to udane „coś" kolejnym narzędziem udręki urzędników, którzy mają więcej do „wklepywania" czegoś na komputerze.

Informatyzacja administracji publicznej przypomina mitologiczne syzyfowe prace. Wydaje się, że tak niewiele potrzeba, żeby za parę lat obraz informatyzacyjnych wysiłków był bliższy nie mitologicznym syzyfowym pracom, ale tym, które Żeromski opisał w „Syzyfowych pracach", a mianowicie trudnym, z początku zwłaszcza, wydawałoby się beznadziejnym, choć niekiedy entuzjastycznie prowadzonym, konsekwentnie organicznym działaniom, skutkującym – o czym czytelnicy wiedzą, a autor nie mówi – wolną Polską, kończącym się zatem sukcesem. Niestety póki co, nikt z tego swojego kawałka „niewiele" nie robi.

Piotr Kociński - z wykształcenia dr fizyki, od 14 lat w branży I/T. Obecnie w Accenture.

Zapraszamy do udziału

SEMINARIUM
WŁASNE SERWEROWNIE CZY ZEWNĘTRZNE USŁUGI? PROFESJONALNA KOLOKACJA LUB HOSTING
24 października 2012 r., Warszawa

W programie m.in.:
- Omówienie raportu Audytel „Budować Data Center czy kupować usługi"
- Kryteria oceny kolokacji
- Problematyka modułowości w kontekście obiektów typu Data Center
- Zabezpieczenie zasilania w energię elektryczną - prezentacja Centrum Energetycznego NZ²®
- Budowa Miejskiego Centrum Przetwarzania Danych
- Miejskie Centrum Przetwarzania Danych
- Własna serwerownia czy zewnętrzne usługi - przegląd możliwości, analiza kosztów

Więcej informacji: www.cpi.com.pl

O czym mówiono na imprezach ŚDSI 2012

Tegoroczne obchody Światowego Dnia Społeczeństwa Informacyjnego (ŚDSI), których główna część odbyła się w maju 2012 r., przyniosły szereg interesujących ustaleń, będących wynikiem przedstawionych referatów i odbytych debat.

Organizatorzy ŚDSI 2012 nie poszli na łatwiznę podejmując tematy, którymi w owym czasie huczały wszystkie media, a których głównymi „inspiratorami" były służby śledcze. Za to wzięli na tapetę prawdziwe problemy, których rozwiązywanie warunkuje faktyczny rozwój społeczny w kierunku adaptacji wysokich technologii to życia społecznego.

Jedyny ślad medialnych przesileń w dorobku ŚDSI 2012 można było znaleźć w przemówieniu, jakie prezes PTI Marian Noga wygłosił na półformalnym spotkaniu poprzedzającym Wielką Galę Dnia Społeczeństwa Informacyjnego. Klimat panujący wówczas wokół branży teleinformatycznej prezes skomentował starą anegdotą (takie są najlepsze) na temat uniwersalnego cyklu wszelkich dużych projektów, na który ponoć składa się pięć faz: euforia, otrzeźwienie, panika, szukanie winnych, karanie niewinnych...

Panel dyskusyjny „Innowacyjność przemysłu ICT motorem innowacyjności w energetyce", odbyty w ramach IV Forum Gospodarczego TIME „Prosument – Energetyka obywatelska – Innowacyjna gospodarka" pozwolił uczestnikom zyskać porządny ogląd problematyki smart grids. Teza główna panelu, wokół której toczyła się dyskusja, zawierała stwierdzenie, że: „*...warunkiem koniecznym uruchomienia postaw proinnowacyjnych w energetyce jest budowa warunków prawnych i ekonomicznych, które będą sprzyjać przyspieszeniu wykorzystania inwestycji w szerokopasmowy powszechny dostęp do Internetu do modernizacji sieci energetycznych (...) Dziesięciolecia relacji monopolistycznych na rynku energetycznym spowodowały znaczne spowolnienie postępu technicznego w całej branży. Ponowne uruchomienie procesów i postaw proinnowacyjnych wymaga zmiany tych relacji oraz budowy infrastruktury umożliwiającej implementację nowoczesnych rozwiązań technicznych*."

Uczestnicy debaty „Telewizja cyfrowa – atuty i pułapki konwersji" szeroko omówili zagadnienia związane z procesem przechodzenia telewizji rozsiewczej na platformę cyfrową. Socjologiczne tło dyskusji narzuciła Monika Mizielińska-Chmielewska, przedstawiając częściowe wyniki swych własnych badań nad społecznym zasięgiem telewizji interaktywnej, które wykazały m.in., że co drugi telewizor znajdujący się w polskim mieszkaniu to model nowoczesny, przystosowany do odbioru telewizji cyfrowej; wieś i małe miasta są silniej nasycone nowoczesnymi modelami telewizorów niż duże metropolie (!); oczekiwania wobec możliwości doboru treści nie idą zbyt daleko, ograniczając się tylko do podstawowych opcji. Min. Igor Ostrowski zapewnił, że techniki rozsiewcze ciągle są niezbędne, dlatego MAiC wspiera proces konwersji telewizji z analogowej na cyfrową. Póki, co, telewizja internetowa, uważana za platformę docelową, napotyka ograniczenia popytowe. W dyskusji zwrócono uwagę m.in. na konieczność pilnego opracowania takich zasad nabywania konwerterów niezbędnych do odbioru telewizji cyfrowej po zaprzestaniu nadawania w systemie analogowym takich, aby najuboższa część społeczeństwa nie została przez to wykluczona cyfrowo.

Nadzwyczaj obfity plon przyniosła konferencja nt. znaczenia nowoczesnych technologii cyfrowych, zwłaszcza chmury obliczeniowej, dla edukacji. Podsekretarz Stanu w Ministerstwie Edukacji Narodowej p. Joanna Berdzik szeroko omówiła program „Cyfrowa Szkoła" informując m.in., że działa już projekt pilotażowy, do którego przystąpiło 400 szkół, zaś chętnych było o rząd wielkości więcej. Wiceprezes Microsoftu Orland Ayala zaprezentował wizjonerskie, globalne spojrzenie na edukację, umieszczając problem w kontekście globalnych problemów ekonomicznych, politycznych i kulturowych. Znakomity przykład efektywnego wdrożenia technologii Cloud do procesu szkolnego przedstawił Lesław Tomczak – autor projektu „Opolska e-szkoła", łączącego ponad 100 szkół jednolitą chmurą wspólnych zasobów. Natomiast Marek Jędryka z Nauczycielskiego Kolegium Języków Obcych w Bydgoszczy ostudził nieco entuzjazm podając wiele szeroko znanych przykładów rzekomo udanych projektów wdrożenia zinformatyzowanych systemów edukacyjnych, które po bliższej analizie bynajmniej nie prezentuje się różowo. Powszechnie popełniane błędy to m.in. nadmierna wiara pokładana w dystrybucji sprzętu, niedostateczne szkolenie nauczycieli, narzucanie jednolitych rozwiązań zwłaszcza e-podręczników, niedoszacowanie kosztów projektów, standaryzacja mylona z uniformizacją, brak jasnych kryteriów oceny dający pole do manipulacji danymi i ogłaszania porażek jako sukcesów.

Chlubiąca się wieloletnią tradycją Konferencja Okrągłego Stołu: „Polska w drodze do Społeczeństwa Informacyjnego", odbywająca się w Sali Kolumnowej Sejmu RP, tym razem została poświęcona ustalonemu przez ITU, wiodącemu tematowi ŚDSI 2012: „Kobiety i dziewczęta wobec technik informacyjno-komunikacyjnych". W inauguracyjnym wystąpieniu wicemarszałek Sejmu Cezary Grabarczyk zauważył, że w rewolucji informatycznej czynnie uczestniczą kobiety, podając przykłady m.in. prezes UKE Magdaleny Gaj, min. Małgorzaty Olszewskiej z Ministerstwa Administracji i Cyfryzacji oraz byłej prezes UKE Anny Streżyńskiej. Zastępca Rzecznika Praw Obywatelskich Ryszard Czerniawski zapewnił, że polski ustawodawca stara się dostosować prawo do nowej sytuacji, stworzonej przez wszechobecną sieć ale na tej drodze czai się wiele trudności, sprowadzających się do antynomii bezpieczeństwo-wolność; poczyniono wiele błędów mających źródło w braku dostatecznego rozeznania istoty zagadnienia. Natomiast prezes NOT Ewa Mańkiewicz-Cudny zadeklarowała dystans wobec prób wyodrębniania problemu „kobieta w świecie ICT", sugerującego rzekomo ograniczone możliwości kobiet w tym zakresie.

Fascynujący przebieg miała (szkoda, że przy niewielkiej frekwencji) konferencja „Kultura w cyfrowym świecie – ewolucja czy rewolucja?". Czy upowszechnienie inteligentnych, połączonych w globalną sieć narzędzi towarzyszących na co dzień ludziom na całym świecie stwarza nową jakość dla kultury i jej twórców? Uczestniczący w debacie twórcy uważają, że tak. Procesy twórcze w obszarach takich jak muzyka czy film przechodzą znaczące transformacje dzięki zastosowaniu cyfrowych technologii wytwarzania, postprodukcji i selekcji treści. Impuls do tej transformacji daje zarówno kultura masowa – w której motywacja do zmian ma charakter głównie ekonomiczny – jak i kultura wysoka, jak zawsze poszukująca nowych środków wyrazu i nowego języka. Pojawiają się też nowe, nieoczekiwane zjawiska.

Organizatorzy ŚDSI 2012 nie zapomnieli o najmłodszych, dla których zorganizowano atrakcyjne konkursy z nagrodami: „eDukacja z Panem T.I.K.-iem – przewodnik multimedialny", w którym młodzież miała okazje popisać się zdolnościami twórczymi, oraz „TIK?-TAK!", w którym uczniowi szkół podstawowych, gimnazjalnych i ponadgimnazjalnych wykazali się spora wiedzą w zakresie informatyki.

Studium wykonalności projektu informatycznego w administracji

dr inż. Dariusz Bogucki

część I refleksji redaktora

Niedawno (piszę te słowa w lutym 2012 roku) miałem okazję wziąć udział w warsztacie na temat informatyzacji administracji, a zasadniczo informatyzacji w rysującej się nowej perspektywie finansowej UE na lata 2014-2020. Głównym punktem dyskusji okazały się kontrowersje związane ze studium wykonalności. Rozstrzał poglądów był totalny: od całkowitej negacji *„(...) potrzeby studium wykonalności w administracji"* (opinia przedstawiciela pewnego NGO) do stwierdzenia, że projekty informatyczne idą źle, bo jednostki zlecają wykonanie studiów „na zewnątrz", a nie potrafią wykonać ich same. Wiele innych wypowiedzi wskazywało na studium wykonalności, jako coś niezrozumiałego i obcego administracji.

Zainspirowany tą dyskusją postanowiłem spisać przemyślenia, jakie zebrałem podczas mojej pracy redakcyjnej nad dwunastoma studiami wykonalności dla projektów IT w administracji. Były to przedsięwzięcia z różnych obszarów ICT i różnej wielkości projekty, miałem możność współredagować studium dla największego polskiego projektu ICT tj. Sieci Szerokopasmowej Polski Wschodniej.

Z całą mocą podkreślam, że są to uwagi subiektywne. Mam nadzieję, że mimo to staną się przyczynkiem do dyskusji nie tylko o projekcie IT w administracji.

Uwaga 1: Studium wykonalności to nie jest „unijny formalizm", a element procesu inwestycyjnego z wykorzystaniem środków UE

W pewnym projekcie, zamawiający uznał sporządzone przez nas studium, za jak to ujął „niestarannie przygotowane", albowiem w pierwotnych ramach (nałożonych arbitralnie przez zamawiającego) projekt okazał się nierealizowany. Dopiero po dłuższych dyskusjach przebiło się do świadomości zamawiającego, że studium jest jak najbardziej poprawne tylko, że jego pierwotne założenia nt. czasu projektu, jego zakresu i środków, jakie przeznaczono, jako tzw. wkład własny, uniemożliwiają osiągnięcie zakładanych rezultatów. To niestety dość częsty casus wynikający z niezrozumienia roli studium wykonalności w procesie inwestycyjnym.

W literaturze **cykl życia projektu inwestycyjnego**, dzieli się na 3 fazy:

- fazę przedinwestycyjną (przygotowawczą), w której projekt musi być przygotowany,
- fazę inwestycyjną, w której projekt jest realizowany,
- fazę operacyjną (eksploatację) / poinwestycyjną, w której zbieramy owoce projektu.

Studium Wykonalności (feasibility study) jest dokumentem fazy przedinwestycyjnej, którego celem jest dostarczenie inwestorowi wszelkich danych niezbędnych do podjęcia decyzji o rozpoczęciu, bądź zaniechaniu inwestycji. Dlatego przedmiotem Studium muszą być uwarunkowania techniczne, ekonomiczne, finansowe, prawne

i inne (np. związane ze środowiskiem naturalnym i strukturą organizacyjną inwestora), dotyczące planowanej inwestycji.

Możemy zatem powiedzieć, że **studium wykonalności** projektu to nic innego jak kompendium wiedzy na temat projektu oraz jego otoczenia społecznego i biznesowego, niezbędne do podjęcia właściwej decyzji biznesowej. Z edytorskiego punktu widzenia jest to zbiór opisów, analiz, prognoz, oszacowań możliwości realizacji projektu. Na podstawie oceny obecnej sytuacji strategicznej i operacyjnej projektodawcy oraz jego danych historycznych zaprojektowano cele projektu i sposoby ich osiągania, przy uwzględnieniu istniejących uwarunkowań natury:

- technologicznej,
- społecznej,
- rynkowej i marketingowej,
- organizacyjnej i kadrowej,
- finansowej i ekonomicznej.

Studium Wykonalności jest zatem narzędziem decyzyjnym, dzięki któremu inwestor może zaplanować i zarządzać inwestycją z uwzględnieniem jej specyfiki w sposób:

- pozwalający na racjonalne ograniczenie ryzyka wynikającego z nieprzewidzianych zdarzeń w trakcie realizacji,
- umożliwiający odpowiednie zagospodarowanie posiadanych zasobów inwestora na wszystkich etapach realizacji, a później także eksploatacji wyników projektu.

Studium Wykonalności jest podstawowym dokumentem, na podstawie którego inwestor podejmuje decyzję o rozpoczęciu/zaniechaniu realizacji inwestycji.

Dlaczego to inwestycyjne podejście jest tak ważne? Ano dlatego, że realizacja projektu współ finansowanego ze środków UE jest niczym innym jak procesem inwestycyjnym, w którym (współ) finansującym jest strona wspólnotowa. DG REGIO w oficjalnym podręczniku z 2002 roku *„Guide to cost-benefit analysis structural of investment projects”* definiuje studium wykonalności, jako: **badanie proponowanego projektu, które ma ustalić, czy proponowana inwestycja jest na tyle atrakcyjna, aby uzasadniać dalsze szczegółowe prace przygotowawcze**. Innymi słowy, dobrze sporządzone studium wykonalności projektu UE powinno dać odpowiedzi na następujące pytania:

1. Czy nie istnieją jakiekolwiek ograniczenia natury finansowej, technicznej, organizacyjnej, prawnej, rynkowej lub innej, uniemożliwiające realizację projektu?
2. Czy są przesłanki do uznania, że projekt będzie miał charakter trwały, tzn. czy dochody z prowadzonej działalności pozwolą na pokrycie kosztów eksploatacyjnych, a jeśli nie - to skąd będą pochodzić środki na zapewnienie funkcjonowania projektu w fazie poinwestycyjnej?
3. Czy projekt jest racjonalny finansowo i społecznie, jakie korzyści społeczne dla jednostki terytorialnej, w której realizowany jest projekt, powstaną na skutek podjęcia inwestycji i jaka będzie ich wartość?
4. Czy i jak wysokim ryzykiem jest obarczony projekt, tzn. jakim czynnikom ryzyka podlega przedsięwzięcie i w jakim stopniu mogą one w efekcie uniemożliwić jego przeprowadzenie?

Obszary wykonalności projektu często określa się w literaturze akronimem **TELOS,** od pierwszych liter pytań, jakie należy postawić sobie badając wykonalność projektu

- **T** - Technical – Czy projekt jest technicznie wykonalny?
- **E** - Economic – Czy projekt jest ekonomicznie uzasadniony?
- **L** - Legal - Czy projekt jest realizowalny w ramach prawnych?

- **O**- Organizational – Czy organizacja jest gotowa na zmianę?
- **S** - Scheduling – Czy projekt da się zrealizować w zakładanym czasie?

Negatywna odpowiedź na którekolwiek z pytań powoduje, że projekt należy uznać za niewykonalny w zakładanych ramach. Studium Wykonalności, które wykazuje bezzasadność realizacji inwestycji, nie jest źle wykonanym Studium, a posiada dużą wartość, jako że zapobiega złej alokacji zasobów.

Na marginesie, można się czasem spotkać w literaturze z rozróżnieniem pojęć Biznesplan i Studium Wykonalności. Z punktu widzenia realizacji projektów UE merytorycznie nie ma różnic pomiędzy obydwoma pojęciami:

- Biznesplan to zwyczajowa nazwa przyjęta dla bardziej zwięzłej formy dokumentu stosowanej dla inwestycji realizowanych przez przedsiębiorców
- Studium wykonalności to bardziej szczegółowa forma dotycząca projektów jednostek rządowych i samorządowych (budżetowych) oraz NGO's

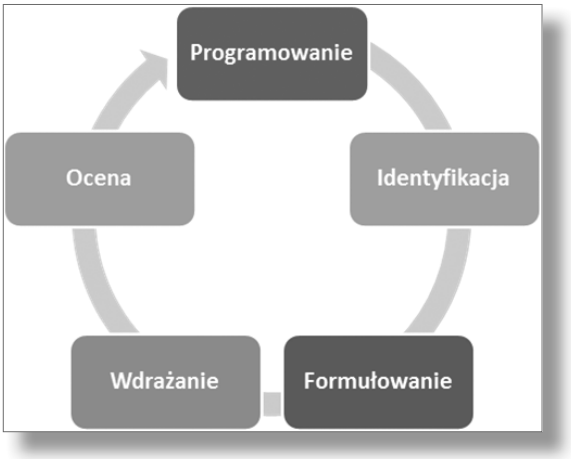
W opisanym na wstępie casusie największa satysfakcję mam do dziś z tego, że zamawiający zrozumiał, że studium wykonalności to nie jest formalna podkładka do uruchomienia projektu, a naprawdę ważny dla tego projektu i użyteczny dla niego dokument.

Refleksja 2: Studium wykonalności projektu UE jest elementem metodyki PCM, a nie odwrotnie

Zastanawiam się, czy owo „formalne" podejście do studium wykonalności nie wynika zpraktykowanej unas interpretacji wspomnianego podręcznika DG REGIO. Wykonawcy studiów „mechanicznie" podchodzą do jego zaleceń, ignorując kompletnie, że na samym jego wstępie jest wyraźnie napisane, że studium jest tylko narzędziem metodyki **Project Cycle Management**, która jest stosowana do wszystkich projektów współfinansowanych przez UE.

Metodyka PCM nie jest to rzecz nowa, bo sięga lat 60-tych, kiedy to w Korpus Pokoju USA opracował dla oceny projektów pomocowych metodykę oparta na dokładnym opisie celów projektu. Doświadczenia amerykańskie zostały przeszczepione w latach 80-tych na grunt europejski. Komisja Europejska poszukiwała rozwiązań, które w sposób logiczny i transparentny pozwoliłyby na dystrybucję środków pomocowych Unii Europejskiej oraz umożliwiały podniesienie jakości realizowanych projektów, a tym samym wpływ na efektywność pomocy dla społeczeństw. W związku z powyższym w 1992 roku Komisja Europejska rozpoczęła pracę nad własną, autorską metodologią zarządzania projektami. Nadano jej nazwę **Project Cycle Management** (PCM) - w polskim tłumaczeniu - Zarządzanie Cyklem Projektu (ZCP). Od tego czasu PCM stała się oficjalną i stale obowiązująca metodyką zarządzania projektami i programami realizowanymi z zaangażowaniem środków europejskich.

Głównym celem stworzenia PCM było dostarczenie narzędzia pomagającego wykonanie wszystkich zamierzeń w zaplanowanym czasie, w ramach zatwierdzonego budżetu i z osiągnięciem założonych rezultatów. Osią metodyki PCM jest założenie, że naturalny dla pomocy publicznej sposób planowania i realizacji projektów podlega pewnemu cyklowi, który rozpoczyna się od uzgodnienia globalnej strategii dla realizacji. W jej wyniku powstaje pomysł na pewne działanie, który jest następnie formułowany i rozwijany, wdrażany formie projektu, a na końcu ewaluowany (patrz poniższy rysunek):



Rysunek 1: *Fazy metodyki PCM*

Fazy cyklu możemy opisać w następujący sposób:

Faza planowania (programowania) – na tym etapie następuje zdefiniowane kluczowych problemów oraz możliwości realizacji projektu, a także szans na współpracę pomiędzy zarządzającymi możliwymi źródłami finansowania (w tym programami Unii Europejskiej), a aplikującym o dofinansowanie programem/projektem. Efektem tej fazy jest wstępny wybór projektów lub programów, których przeprowadzenie przyczyni się do poprawy sytuacji – czyli pewnej zmiany społecznej.

Identyfikacja – w tej fazie weryfikowane są wszystkie zgłoszone projekty pod względem ich przydatności i opłacalności. Następuje ich selekcja zgodnie z przyjętymi kryteriami. Po takiej selekcji, dla niektórych projektów przeprowadza się dodatkowe analizy, które służą wykazaniu ich celowości. Na tym etapie określa się zakres projektu, jego rozmiary oraz działania, które powinny wchodzić w jego obręb. Stosowane w tej fazie narzędzia to:

- **Analiza interesariuszy** - identyfikacja i charakterystyka głównych interesariuszy, grup docelowych i beneficjentów projektu, z uwzględnieniem problemów wymagających interwencji;
- **Analiza problemów** – identyfikacja kluczowych problemów, zagrożeń oraz ich skutków z uwzględnieniem wzajemnych relacji;
- **Analiza celów** – ustalenie celów wynikających z istniejących problemów, wskazanie środków prowadzących do pożądanych rezultatów, czyli usunięcia lub ograniczenia problemów;
- **Analiza strategii** – określenie różnych strategii prowadzących do osiągnięcia celów, a w rezultacie wybór najwłaściwszej strategii (analiza wariantów) oraz określenie celów nadrzędnych i celów projektu.

Formułowanie – na tym etapie prowadzona jest szczegółowa analiza pomysłu i zdefiniowanie projektu – pomysły są rozwijane w operacyjne plany projektów: przeprowadza się analizy finansowe, ekonomiczne, środowiskowe, techniczne dla wybranego wariantu realizacji projektu. Dla niego tez planuje się harmonogram działań i alokacje zasobów. Głównym narzędziem weryfikacji poprawności opisu jest w PCM tzw. **matryca logiczna** (logframe).

Rysunek 2: *Identyfikacja i formułowanie projektu zgodnei z PCM*

Generalnie po tym etapie posiadamy już wstępny montaż finansowy i ocenę projektu pod kątem wykonalności (czy ma szanse powodzenia) i trwałości (czy będzie w stanie dostarczyć trwałych korzyści beneficjentom).

Wdrażanie – realizacja projektu oraz jego stałe monitorowanie. Uruchomione zostają wszelkie procedury, które pozwalają na skuteczne i efektywne przeprowadzenie przedsięwzięcia. Dotyczy to zarówno części technicznej, merytorycznej, finansowania oraz dokumentacji prawnej etc.

Ocena – podsumowanie przedsięwzięcia. Określenie jego rezultatów, przydatności, trwałości i efektywności. W tej fazie porównujemy to, co chcieliśmy poprzez projekt osiągnąć z uzyskanymi wynikami. Podczas zakończenia projektów możemy zidentyfikować potrzebę przeprowadzenia kolejnych.

W praktyce z takim metodycznym podejściem było u nas różnie, albowiem beneficjenci opracowując wniosek skupiali się na spełnieniu oczekiwań / wymagań oceniających wniosek, a nie jego metodologicznej poprawności. Pamiętam wzmożony ruch szkoleniowy w 2011 roku, po informacji MRR, że wnioski o dofinansowanie będą zmieniane w kierunku pełnej zgodności z PCM. Na szkoleniach opowiadałem o analizie interesariuszy i macierzy logicznej beneficjentom, których nigdy nie podejrzewałbym o braki w tym obszarze.

Refleksja 3: Macierz logiczna to nie formalizm, a narzędzie weryfikacji poprawności sformułowania projektu

Można opisany w poprzednim punkcie mechanizm zilustrować poniższym schematem „dochodzenia do projektu" wg. PCM.

Jak widać kluczowe znaczenie w tym scenariuszu ma tzw. **Macierz Logiczna**, która z jednej strony jest kluczowym elementem całej metodyki PCM, a z drugiej jest fundamentem w konstrukcji Studium Wykonalności. Macierz Logiczna jest też sposobem wizualizacji celów projektu w systematyczny i logiczny sposób. Dzięki temu mamy z jednej strony możliwość zobaczenia relacji przyczynowo-skutkowej pomiędzy różnymi poziomami celów projektu. Z drugiej zaś pokazuje, jak sprawdzać czy cele te zostały osiągnięte. Konstrukcja macierzy Logicznej jest następująca (patrz poniższa tabela):

	A Opis (Logika Interwencji)	B Obiektywnie weryfikowalne wskaźniki	C Źródła weryfikacji	D Założenia
① Cel nadrzędny				
② Cele projektu (bezpośredni)				
③ Rezultaty				
④ Działania		Środki	Koszt	Czas
				⑤ Założenia podstawowe

Tabela 1.

1. **Pierwszy wiersz macierzy opisuje cel nadrzędny (ogólny) projektu, czyli to**, jaką zmianę wniesie projekt. Cel nadrzędny powinien wyjaśniać, dlaczego projekt jest ważny dla społeczeństwa, w kategoriach długoterminowych korzyści dla beneficjentów i szerszych korzyści dla innych grup interesariuszy. Z drugiej strony, cel nadrzędny powinien pokazywać, w jaki sposób projekt wpisuje się w polityki UE (w szczególności w zasady polityki regionalnej UE). Można, zatem powiedzieć, że cele ogólne nie zostaną osiągnięte wyłącznie dzięki danemu projektowi, ale będzie on wkładem w realizacje tych celów.
2. **Drugi wiersz zawiera informacje na temat bezpośredniego celu projektu**. Cel projektu powinien odnosić się do kluczowego problemu i być definiowany w kategoriach korzyści dla beneficjentów, będących rezultatem działań zaplanowanych w ramach projektu.
3. **Trzeci wiersz nosi nazwę Rezultaty**, które opisują produkty projektu, jakie będą dostarczane beneficjentom. Rezultaty powinny zaspokajać główne potrzeby grup docelowych.
4. **W czwartym wierszu opisane są Działania**, które określają poszczególne zadania / czynności do wykonania w projekcie i pokazują, w jaki sposób osiągane będą rezultaty projektu. Konstrukcja tego wiersza jest troszkę inna jak poprzednich. W kolejne komórki wpisywane są:
   - Środki, czyli ludzkie, rzeczowe i finansowe zasoby wymagane do podjęcia planowanych działań i zarzadzania projektem.
   - Koszt, czyli szacowany budżet projektu ze wskazaniem źródeł jego finansowania.
   - Czas oznacza szacowany czas realizacji projektu.

Pierwsza kolumna (A) macierzy logicznej, nazywana zwyczajowo **logiką interwencji**, zawiera opisy, które wyznaczają strategię leżącą u podstaw projektu wg następującego schematu:

- Działania ④, które zostaną wykonane w ramach projektu umożliwiają osiągnięcie Rezultatów projektu ③.
- Suma rezultatów projektu prowadzi do osiągnięcia celu projektu ②, który powinien przynosić korzyści bezpośrednim beneficjentom projektu.
- Cel projektu przyczynia się do osiągnięcia celów nadrzędnych (ogólnych) ①, czyli do zmiany sytuacji w szerszym aspekcie i zniwelowania problemu kluczowego.

Kolumna druga (B) to tzw. obiektywnie weryfikowane wskaźniki (OWW), które opisują cele projektu przy użyciu mierzalnych pojęć (ilość, jakość, grupy docelowe, czas, miejsce). Specyfikacja OWW działa, jako sprawdzenie wykonalności celów oraz formuje bazę dla systemu monitorowania projektu. Należy pamiętać, że w poszczególnych wierszach definiujemy wskaźniki odnoszące się do poszczególnych poziomów celów i tak:

- Osiągniecie celu nadrzędnego opisują **wskaźniki oddziaływania** – umożliwiają one ocenę osiągnięcia szerszych i bardziej długofalowych konsekwencji realizacji projektu (np. % populacji korzystającej z e-usług po 18 miesiącach od zakończenia projektu).
- Cel bezpośredni opisują **wskaźniki rezultatu** – oceniające osiągnięcie efektów wdrożonych działań w postaci zmian w sytuacji grupy docelowej projektu (np. liczba korzystających z e-usługi po zakończeniu projektu).
- **Wskaźniki produktu** opisują bezpośrednie, fizyczne wyniki realizacji działań (np. liczba uruchomionych e-usług).

Trzecia kolumna (C) wskazuje, gdzie i w jakiej formie można znaleźć informacje (opisane przez obiektywnie weryfikowalne wskaźniki) dotyczące celów ogólnych, celów projektu i rezultatów. Generalnie źródłami weryfikacji są dokumenty, raporty i inne źródła zapewniające informację, która pozwala na pomiar wskaźników.

Czwarta kolumna (D), czyli założenia zawiera opis czynników zewnętrznych, mających wpływ na wdrażanie projektu i trwałość projektu w dłuższym okresie, ale pozostających poza jego kontrolą. Pod pojęciem tym rozumiane jest zaistnienie czynników warunkujących realizację projektu np.:

- Naturalnych – np. prawdopodobieństwo powodzi, suszy, itp.;
- Instytucjonalnych – dobra (zła) koordynacja pracy różnych komórek jednostki realizującej projekt ministerstwa;
- Prawnych - zmiany prawne w obszarze projektu, pozytywna opinia Komisji Europejskiej (notyfikacja tzw. dużych projektów);
- Społecznych – wykluczenie/trudny dostęp/niechęć niektórych grup społecznych do udziału w projekcie, itd.;
- Innych projektów – konieczność zakończenia / uruchomienia innych projektów, aby „nasz" był wykonalny.

Założenia są zatem odpowiedzią na pytanie: „*Jakie zewnętrzne czynniki nie są objęte wpływem projektu, a mogą oddziaływać na jego wdrażanie i trwałość w długim okresie"?*

Założenia podstawowe do realizacji projektu wpisuje się w samotna komórkę na końcu piątego wiersza macierzy.

Praktyka, z która niestety się zetknąłem się w ocenie wniosków wskazuje, że w konstrukcji macierzy logicznej występuje wiele błędów.

Po pierwsze - wiele błędów formalnych i logicznych błędów występuje w formułowaniu celów projektów. Cele musza jasno być zidentyfikowane w LFA, w czym pomaga reguła **SMART**. Oznacza ona, że prawidłowo zdefiniowany cel powinien być:

- **S**pecific (konkretny – z konkretnym prze kazem)
- **M**aesurable (mierzalny – liczbowo wyrażać stan realizacji)
- **A**chievable (osiągalny – cel zbyt ambitny podkopuje wiarę w jego osiągnięcie)
- **R**elevant (istotny - cel powinien być ważnym krokiem naprzód dla organizacji)
- On **T**ime (na czas – cel musi mieć jasny horyzont czasowy)

Po drugie - definiując wskaźniki nie należy przeceniać możliwych skutków projektu. Innymi słowy: wyznaczenie poziomu wskaźników na realistycznym poziomie zabezpiecza przed koniecznością wyjaśniania, dlaczego nasz projekt nie zakończył się sukcesem.

Po trzecie - wnioskodawcy próbując wymyślić wskaźniki „korzystne dla siebie" zapominają, że w ich interesie leży, aby wskaźnik był:

- Precyzyjny – mierzył to, co powinien, tj. odpowiadać temu, czego dotyczy, a nie „około", „na przykład" itp.
- Konkretny (nie „dużo", „mało", ale opisywał kwantyfikowalne wartości).
- Dostępny za umiarkowaną cenę. Optymalnie powinny to być wskaźniki dostępne bez przeprowadzania specjalnych badań, np. dane GUS, ale wiadomo też, że nie zawsze to da się osiągnąć.
- Odpowiedni, to jest odnosił się do określonego celu, który opisuje.

Po czwarte - źródła weryfikacji wskaźników powinny być rzetelne, a nie wygodne dla beneficjenta. Sam widziałem projekt, w którym beneficjent wymyślił sobie, że zakończenie projektu sieci szerokopasmowej „zweryfikuje" … uchwałą zarządu gminy.

Błędy w podejściu metodologicznym to nie wszystko. Dlatego w następnej części artykułu skupimy się na problemach, jakie występują z konstrukcja samego Studium Wykonalności.

Dr inż. Dariusz Bogucki - dyrektor ds. Sektora Publicznego w EFICOM SA, wykładowca na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie.

Zapraszamy do udziału

SEMINARIUM

NOWE REGULACJE PRAWNE DOTYCZĄCE ENERGETYKI I TELEKOMUNIKACJI A PROBLEMY OCHRONY ŚRODOWISKA

23 października 2012 r., Warszawa

W programie m.in.:

- Energetyka i telekomunikacja a ochrona środowiska
- Ochrona środowiska w unijnym i polskim prawie telekomunikacyjnym
- Polityka energetyczna UE w zakresie przeciwdziałaniu zmianom klimatu
- Rozwój energetyki (w tym nuklearnej) - wyzwania klimatyczne
- Bezpieczeństwo energetyczne a odnawialne źródła energii. Projekt ustawy o odnawialnych źródłach energii
- Alternatywne źródła energii a ochrona środowiska
- Wybrane instytucje prawa ochrony środowiska w kontekście bezpieczeństwa energetycznego
- Środowisko a korytarze przesyłowe. Warunki inwestowania w stosunku do ochrony środowiska (tereny wyłączone, obszary chronione Natura 2000, etc)

Więcej informacji: www.cpi.com.pl

Koncepcje rozwoju i modyfikacji ePUAP

Piotr Walesiak

Elektroniczna Platforma Usług Administracji Publicznej – centralny system administracji rządowej wybudowany w ramach poprzedniej perspektywy finansowania unijnego (tzw. SPO-WKP), jeden z niezbyt licznych projektów tej perspektywy, który w sensie techniczno-organizacyjnym w całości powiódł się dostarczając zakładane produkty ePUAP jest i działa.

Niestety nikt nie wie co z nim dalej zrobić. Pogląd samych gestorów systemu oscyluje pomiędzy szeroko zakrojonymi wizjami opisanymi w Studium Wykonalności projektu ePUAP2, czy też w sławnej i niesławnej tzw. „Linii Współpracy", aż do hipotezy, że ePUAP to sztucznie podtrzymywany przy życiu trup, któremu raczej należy się miłosierna eutanazja. Jako jeden z autorów koncepcji ePUAP, tej obecnie zaimplementowanej, jak również rozmaitych przyszłych koncepcji dotyczących ePUAP, często zauważam popełniany błąd nadmiernego uogólnienia, polegający na wypowiadaniu poglądów dotyczących ePUAP jako całości. ePUAP nie jest systemem jednorodnym i co więcej, są jego części, które są znaczącymi sukcesami biznesowymi (jak np. zaufany profil) i części, o których istnieniu mało kto wie. Zatem dyskusja o rozwoju ePUAP powinna odnosić się do jego konkretnych części i funkcji. Dzisiejszy ePUAP to współdzielony system identyfikacji i uwierzytelnienia użytkowników, w szczególności wyposażony od niedawna w tzw. zaufany profil. To również współdzielona platforma budowy i udostępniania e-usług administracji publicznej oraz kilka innych funkcji. Funkcje te zasadniczo różnią się co do swojego przeznaczenia, jak również od obecnego poziomu „biznesowego sukcesu" ich wdrożenia. Dlatego też, inaczej powinny wyglądać pomysły dotyczące dalszych losów ePUAP w zakresie poszczególnych funkcji.

Zaufany Profil

W największym uproszczeniu, zaufany profil to koncepcja uwierzytelnienia dokumentu lub transakcji przekazywanej za pośrednictwem Internetu, zbliżona do tego co można spotkać w detalicznej bankowości elektronicznej. Zamiast podpisu składanego pod dokumentem przy pomocy bezpiecznego podpisu elektronicznego, ePUAP do dokumentu dołącza informacje o tożsamości użytkownika uzyskaną z konta ePUAP i potwierdzoną przy pomocy dokumentu tożsamości i oświadczeń danej osoby złożonych podczas zakładania takiego konta z zaufanym profilem. Dodatkowo wykonanie całej operacji potwierdzane jest jednorazowym hasłem wysyłanym użytkownikowi pocztą elektroniczną.

O zaufanym profilu jest ostatnio bardzo głośno, jako o dostępnej alternatywie dla bezpiecznego podpisu elektronicznego. Niestety równie głośne są wątpliwości dotyczące bezpieczeństwa tego rozwiązania. Niezależnie od swoich wad, Zaufany Profil jest wielkim sukcesem i najgorszym z możliwych pomysłów byłoby porzucanie go dla tego, że wskazano jakieś podatności w jego zabezpieczeniach. Oczywiście nie ulega wątpliwości, że zaufany profil nie jest produktem idealnym i wymaga rozwoju, w szczególności zaś oceny i likwidacji wskazywanych podatności oraz ustanowienia ciągłych procesów zarządzania bezpieczeństwem, oceny ryzyka, identyfikacji i likwidacji podatności (być może nawet certyfikowanego systemu

zarządzania bezpieczeństwem informacji). Nie mniej potencjał Zaufanego Profilu jest oczywisty i należy dążyć do zwiększania „sieci" usług i usługodawców skupionych wokół niego.

Innym kierunkiem, który sygnalizowany był jako interesujący nawet już przy narodzinach koncepcji zaufanego profilu ePUAP, jest rozbudowa tego produktu w kierunku stworzenia Zaufanego Profilu dla osób prawnych i jednostek organizacyjnych. Jest to szczególnie obiecujący obszar, ponieważ nawet planowane wdrożenie PL.ID nie rozwiązuje problemu uwierzytelnienia i potwierdzenia reprezentacji osób prawnych i jednostek organizacyjnych podczas kontaktu w kanale elektronicznym.

Platforma e-usług

Kluczowym elementem ePUAP, jest platforma budowy i udostępniania e-usług administracji publicznej. W obecnym kształcie e-PUAP platforma ta pomyślana jest jako zestaw podstawowych bloków, które odpowiednio skonfigurowane, razem tworzą mechanizm dostępu do określonej usługi publicznej. Sama realizacja usługi publicznej (np. odpowiedni flow dokumentu) nie jest już rzeczą e-PUAP, tylko systemu do którego e-PUAP będzie przesyłał dokumenty stworzone przy pomocy mechanizmów platformy. Platformę zbudowano tak, aby po uzyskaniu odpowiednich uprawnień instytucje publiczne mogły samodzielnie tworzyć i udostępniać e-usługi definiując i odpowiednio konfigurując własne zasoby na platformie e-PUAP.

W opisanym modelu gestor systemu e-PUAP nie ma bezpośredniego wpływu na to, czy i jakie usługi na platformie powstaną. Może on co najwyżej promować wykorzystanie platformy, oferować wsparcie, wzorce, przykłady, narzędzia i inne udogodnienia dla instytucji, które zamierzają udostępnić swoje usługi przy pomocy e-PUAP. Tak działającą platformę e-usług można porównać do serwisu aukcyjnego jak Allegro lub e-BAY, działających w podobnym modelu biznesowym. W obu przypadkach operator platformy ma wpływ na treść pośrednio, poprzez formułowanie określonych zasad i regulaminów korzystania z platformy, a jego bezpośredni wpływ ogranicza się do możliwości usunięcia treści naruszającej ustanowione polityki. e-PUAP funkcjonujący w tym modelu jest dość powszechnie krytykowany ze względu na ubóstwo udostępnionej przy jego pomocy treści. W szczególności często można usłyszeć, że nie ma tam żadnych istotnych usług publicznych (np. tych wskazanych w tzw. e-gov benchmark), ważnych i potrzebnych dużym grupom klientów, natomiast te, które można tam znaleźć, to przede wszystkim usługi o charakterze niszowym, przydatne dla wąskich grup użytkowników, dodatkowo często dostępne wyłącznie dla osób zamieszkałych na jakimś istotnie ograniczonym terenie, jak gmina, powiat czy miasto. Powoduje to, że liczba osób korzystających z usług na e-PUAP jest bardzo mocno ograniczona.

Gdzie są nasze publiczne e-usługi?

Kiedy ePUAP był wymyślany, uważano, że zasadniczą barierą dla udostępniania e-usług jest techniczna zdolność podmiotów do udostępnienia usług z uwzględnieniem wszystkich normatywnych wymagań związanych przede wszystkim z bezpieczeństwem i wiarygodnością komunikacji w kanale elektronicznym. Stąd wziął się przyjęty i opisany wcześniej model biznesowy platformy, jako pewnej współdzielonej infrastruktury stanowiącej zestaw samoobsługowych, dostępnych nieodpłatnie narzędzi służących udostępnieniu usług publicznych z uwzględnieniem wszystkich właściwych normatywnych wymagań.

Sytuacja, która zaistniała po wdrożeniu platformy w tym kształcie wskazuje, że brak technicznej zdolności nie jest jedynym problemem. Narzędzia już są, a istotnych e-usług, dostępnych na e-PUAP lub poza e-PUAP, nadal niezbyt wiele. Z jakiegoś powodu administracja publiczna nie udostępnia swoich istotnych

usług w kanałach elektronicznych. Może to robić, prawo na to pozwala, ale tego nie robi, ponieważ …

… „Organy władzy publicznej działają na podstawie i w granicach prawa". Cytowany artykuł z konstytucji stanowi jedno z pryncypiów funkcjonowania każdej instytucji publicznej. W szczególności wynika z niego, że nie wystarczy aby prawo nie zabraniało podjęcia określonych działań w określony sposób. Organ władzy publicznej dla swoich działań musi mieć podstawę (nakaz) w przepisie prawa. Menedżer w administracji publicznej nie może podjąć lub zaniechać jakiegoś działania, w oparciu o swoją ocenę sytuacji i doświadczenie zawodowe związane z jakimś typem działalności. Coś co jest normą działania i zarządzania w przedsiębiorstwie, nie zachodzi w administracji. Istotnych e-usług publicznych nie ma, ponieważ jako obywatele (poprzez naszą reprezentację w parlamencie) nie nakazaliśmy organom władzy publicznej aby je stworzyły, a im nie wolno tego zrobić bez naszego nakazu.

Gdzie powinny być publiczne e-usługi?

Biorąc pod uwagę powyższe, oczywiste jest, że aby pojawiły się istotne e-usługi z istotnym terytorialnie zasięgiem (najlepiej ogólnokrajowym), przepis prawa musi nakazać ich stworzenie lub udostępnienie. Najważniejsze pytanie brzmi, komu, który organ władzy publicznej powinien być do tego zobowiązany. Przestrzeń odpowiedzi na to pytanie rozpięta jest pomiędzy dwoma biegunami. Jedna skrajność - każdy organ władzy w zakresie swoich usług. Druga skrajność - jeden wskazany, centralny organ władzy w odniesieniu do wszystkich usług. Każda z tych skrajności w czystej formie stosowana w pełnym zakresie zapewne nie jest właściwym podejściem.

Zastosowanie pierwszej spowoduje, że powstaną dziesiątki lub setki tysięcy e-usług wśród których nie koniecznie znajdą się te najważniejsze. Te same usługi o różnym zasięgu terytorialnym będą udostępnione w całkowicie różny sposób, łącznie z tym, że pomimo tej samej nazwy nawet ich zakres może być różny. Nie będzie możliwe kreowanie jakiejkolwiek polityki czy strategii, związanej z kolejnością, czy ważnością określonych usług. To które z usług i w jakiej kolejności będą udostępniane, zależeć będzie od sprawności ich implementacji przez tysiące instytucji, z których znaczna część nie podlega żadnej koordynacji na poziomie krajowym. W znacznym stopniu sytuacja będzie podobna do dzisiejszej sytuacji usług na e-PUAP, w której nikt nie będzie miał bezpośredniego wpływu na treść i formę powstających e- usług. Ponadto w modelu tym, dostarczenie części istotnych usług w pełnym zakresie w ogóle nie będzie możliwe ze względu na strukturę kompetencyjną organów władzy. Przykładowo, nie jest możliwe w tym modelu udostępnienie usługi zmiany adresu, gdyż taka usługa, to w szczególności zmiana adresu zameldowania w ewidencji ludności, zmiana adresu zamieszkania w Urzędzie Skarbowym, potencjalnie również zmiana danych w ZUS, prawie jazdy, dowodzie rejestracyjnym pojazdu i być może jeszcze kilku innych miejscach, w zależności od tego jak zdefiniowany został zakres takiej usługi. Nie istnieje instytucja, która miałaby w swoich kompetencjach realizację usługi o takim zakresie.

Zastosowanie w pełnym zakresie drugiej ze skrajnych strategii również niesie szereg zagrożeń. Lokalne uwarunkowania terytorialne lub związane z jakąś domeną działania administracji, mogą powodować, że pewne e-usługi mają szczególnie duże lokalne znaczenie. Uzależnienie ich implementacji od jednej centralnej instytucji mogłoby powodować, że ważne lokalne lub dziedzinowe potrzeby pozostawałyby na takim centralnym poziomie

zaniedbywane. Ponadto niektóre istotne usługi mają bardzo dużo lokalnej specyfiki, gdyż podstawą dla ich realizacji jest prawo lokalne, a nie prawo powszechne. Takich e-usług w zasadzie nie daje się udostępniać centralnie, gdyż oznaczałoby to potencjalnie konieczność budowy wielu, zupełnie odrębnych e-usług. Przykładem tego typu e-usług, są wszystkie usługi związane z lokalnymi podatkami. Dlatego próba udostępnienia ich w kanale elektronicznym przez centralną instytucję byłaby absurdalna. Natomiast strategia ta jest szczególnie korzystna w przypadku usług, które realizowane są przez setki, czy nawet tysiące organów na terenie całego kraju oraz regulowane są przez przepisy prawa powszechnego, tj. realizowane w zasadniczo ten sam sposób na terenie całego kraju.

Warto zwrócić uwagę, że znaczna część owych istotnych usług publicznych (odnosząc się do przytoczonego wcześniej e-gov benchmark), to właśnie usługi spełniające obie powyższe własności. Zastosowanie dla tych usług strategii ich e-udostępnienia, polegającej na powierzeniu tego zadania centralnej instytucji, przy zachowaniu obecnych kompetencji dotyczących samej realizacji usług, spowoduje, że usługi te będą mogły być udostępnione szybko, w jednolity sposób oraz w zasięgu ogólnokrajowym. Co więcej może się to odbyć, bez istotnych dodatkowych nakładów po stronie instytucji lokalnych, gdyż już dziś każda z nich zobowiązana jest posiadać tzw. elektroniczną skrzynkę podawczą, która jako uniwersalny środek komunikacji może być wykorzystana do realizacji każdej usługi, w której postępowanie regulowane jest przepisami Kodeksu Postępowania Administracyjnego.

Oczywistym kandydatem na instytucję, której można by powierzyć zadania związane z udostępnianiem e-usług w opisanym wyżej modelu jest powołane niedawno Ministerstwo Administracji i Cyfryzacji, a narzędziem którym mogłaby się ona posłużyć jest będący w jej dyspozycji ePUAP, który zapewne wymagałby daleko idących rozszerzeń i modyfikacji, aby móc z jego pomocą realizować takie funkcje sprawnie i na dużą skalę.

Ciekawym jest fakt, że koncepcja ta była już przez gestora ePUAP rozważana i co więcej była przedmiotem dyskusji ze środowiskiem samorządowym w ramach prac nad tzw. „Linią współpracy". Wiele z opracowanych wtedy scenariuszy współdziałania ePUAP z innymi systemami w zakresie realizacji e-usług pozycjonowały go jako agregatora/integratora usług, których realizacja miała pozostać bez zmian na poziomie samorządów i ew. odpowiednich resortów, czyli systemów regionalnych i dziedzinowych. Koncepcje te zostały uzgodnione z przedstawicielami środowisk samorządowych, a później bez jasnych powodów porzucone przez MSWiA.

Front-Office, Back-Office i komercyjne pośrednictwo

Implementacja idei, o której mowa wyżej, wymaga pewnego przeramowania w sposobie myślenia administracji o swojej działalności. Polega ono na koncepcyjnym oddzieleniu procesów i mechanizmów kontaktu z klientem (front-office), od procesów i mechanizmów samej realizacji określonych usług (back-office). W tradycyjnie działających urzędach te dwie funkcje są nierozerwalnie połączone. Świadomość ich rozdzielenia to kluczowa innowacja, otwierająca drogę do wielu nowych możliwości. Jedną z tych możliwości jest opisana wyżej koncepcja pozwalająca na relatywnie łatwą ogólnokrajową jednokrotną implementację zagregowanych i zintegrowanych e-usług publicznych, w zakresie usług najistotniejszych dla obywateli i przedsiębiorców. Wiele innych fascynujących możliwości osiągalnych może być dzięki połączeniu trzech koncepcji, jakimi są: oddzielenie front-office i back-office w działalności administracji, „opakowanie" usług back-office administracji w łatwo i standardowo

dostępne usługi sieciowe oraz akceptacja faktu, że front-office nie musi znajdować się wewnątrz administracji.

Pomyślmy o tym: wypis z ewidencji gruntów i budynków, czy też księgi wieczystej, albo odpis aktu urodzenia, czy małżeństwa albo zaświadczenie o niezaleganiu z podatkami czy składami ZUS, które możemy dostać na poczcie. Albo wypis czy zaświadczenie które może być dla nas uzyskane przez profesjonalny podmiot, który uczestniczy w transakcji do której ten dokument jest potrzebny. Przykładowo: przy zakupie nieruchomości notariusz „od ręki" uzyskuje dla nas wypis z księgi wieczystej; z salonu sprzedaży samochodów czy też autokomisu wychodzimy z zarejestrowanym samochodem. I zapewne wiele innych możliwości, gdzie ograniczeniem jest pomysłowość przedsiębiorców (która jak wiadomo jest nieograniczona) i dostępność publicznego „back-office" w postaci e-usług.

Podejście takie polega na wprowadzeniu do kontaktu pomiędzy administracja i jej klientem pośrednika, przedsiębiorcy, który działając na komercyjnych zasadach, aby uczynić swoje produkty bardziej wartościowymi dla końcowego klienta, wzbogaca je o elementy usług publicznych. Model taki jest korzystny dla wszystkich trzech uczestników i powoduje, że klient zwolniony jest z obowiązku biegania po urzędach, co więcej, nawet nie musi znać i rozumieć elektronicznych form kontaktu z urzędami. Pośrednik uzyskuje możliwość dostarczania lepszych, bardziej wartościowych usług, potencjalnie uzyskując większą marżę z ich sprzedaży. Administracja pracuje z profesjonalnym podmiotem, który kontaktując się z nią regularnie w zakresie określonych spraw, zna i rozumie zasady realizacji konkretnych usług publicznych, zasady dostępu do nich i ich wykorzystania. W ten sposób realizacja usług przebiega sprawnie i efektywnie bez konieczności wielokrotnego uzupełniania braków formalnych w składanych wnioskach oraz tłumaczenia indywidualnemu klientowi zawiłości konkretnych procedur administracyjnych.

Podsumowanie

W naszym kraju jesteśmy jeszcze bardzo odlegli od realizacji tego typu wizji i jest wiele przeszkód, które dziś uniemożliwiłyby jej realizację. Nie mniej zdaniem wielu światowych ekspertów jest to kierunek transformacji czekający administracje całego świata w ciągu najbliższych 10-15 lat, pozwalający na uzyskanie prawdziwej efektywności i zwrotu z budowy e-usług w administracji publicznej. Dla transformacji w tym kierunku niezbędne jest stworzenie środowiska, w którym e-usługi publiczne dostępne są do wykorzystania w jednolity, wystandaryzowany, opisany sposób, łatwe do znalezienia i włączenia w procesy biznesowe komercyjnych organizacji (niezależnie od tego gdzie i przez kogo same usługi są realizowane). W szczególności w implementacji takiej koncepcji szczególnego nowego znaczenia nabiera katalog usług publicznych, którego model i zakres działania powinien być również odpowiednio do niej dostosowany. Dostarczanie elementów takiego środowiska to zdecydowanie miejsce dla takich elementów wspólnej infrastruktury e-usług jak e-PUAP.

Piotr Walesiak - ekspert obszaru biznesowego w sektorze administracji publicznej w Infovide-Matrix SA

XVIII Forum Teleinformatyki 27-28 września br., Warszawa-Międzylesie

Tematem przewodnim tegorocznego Forum będą koncepcje i uwarunkowania wykorzystania technologii cyfrowej chmury do modernizacji funkcjonowania państwa. Obrady rozpocznie sesja metodologiczna **„CYFROWA CHMURA A DYLEMATY NOWOCZESNEGO PAŃSTWA".** Zaproszeni Autorzy w swoich prezentacjach swobodnie odniosą się do relacji między koncepcjami technicznymi i prawnymi cyfrowej chmury, a oczekiwaniami nowoczesnego państwa obywatelskiego.

Głównym instrumentem osiągania celów stawianych w Agendzie Cyfrowej Europy są kluczowe projekty rządowe i samorządowe. W tym roku będzie kontynuowany przegląd stanu najbardziej zaawansowanych projektów. Omawiane będą zarówno sukcesy, jak i główne problemy, a także technologiczne i organizacyjne możliwości wykorzystania „technologii chmurowych". Konfrontacja zamierzeń z osiągniętymi efektami będzie głównym celem sesji „KLUCZOWE, RZĄDOWE I SAMORZĄDOWE PROJEKTY INFORMATYCZNE - STAN, WYZWANIA, PERSPEKTYWY".

Wytwarzaniu i udostępnianiu nowych usług towarzyszy intensywny rozwój inicjatyw o charakterze społecznościowym, wspierających partycypacyjny model rządzenia krajem. Coraz mocniej są formułowane żądania dostosowania prawa oraz architektury do tych nowych potrzeb, w tym do przetwarzania w cyfrowej chmurze. Tej tematyce poświęcimy sesje zatytułowane: „ARCHITEKTURY, METODY, INTEROPERACYJNOŚĆ CYFROWEJ CHMURY" oraz „BEZPIECZEŃSTWO CYFROWEJ CHMURY".

W ubiegłym roku została zapoczątkowana współpraca Forum ze środowiskiem energetyki. Infrastruktura informacyjna musi być traktowana kompleksowo, zwłaszcza w dziedzinie zarządzania elementami infrastruktury krytycznej. Dlatego Forum staje się stałym miejscem wymiany poglądów tworzących warunki dla synergii działań wszystkich środowisk (administracja, nauka, biznes) zaangażowanych w modernizację państwa. Tak reprezentatywna sesja pt. „ARCHITEKTURY I TECHNOLOGIE INFORMATYCZNEGO WSPARCIA ZADAŃ OPERATORA INFORMACJI POMIAROWYCH W ENERGETYCE" wpłynie na pewno na lepsze zrozumienie problemów i skali informatycznych potrzeb sektora energetycznego.

Pierwszy dzień Forum zakończy „NOC ARCHITEKTÓW" z zagadkowym podtytułem „ZAWSZE PRZED PÓŁNOCĄ".

W ubiegłym roku wielu uczestników, mimo nocnej pory, wzięło udział w merytorycznym, nieskrępowanym ograniczeniami czasowymi „zgłębianiu" istoty szyny. W tym roku będzie omawiane równie kontrowersyjne pojęcie cyfrowej chmury. Kanwą dyskusji będą wypowiedzi kilku bardzo doświadczonych i twórczych architektów systemów informatycznych.

Drugi dzień Forum wypełnią sesje równoległe i kocioł dyskusyjny.

Znane już uczestnikom „FORUM MŁODYCH MISTRZÓW" - EKONOMICZNE ASPEKTY INFORMATYZACJI PAŃSTWA" nie jest przeznaczone wyłącznie dla młodych, choć merytorycznie właśnie przez nich przygotowane.

Sesja „FORUM STRATEGII SPOŁECZEŃSTWA INFORMACYJNEGO" w bieżącej edycji Forum będzie przebiegać w zupełnie nowej formule. Pragniemy skupić uwagę na zagadnieniu „INFORMATYZACJA ZINTEGROWANA A IDEA OTWARTEGO RZĄDU". Sądzimy, że dzięki uczestnikom, tematyce i wprowadzonym zmianom sesja ta będzie stałym miejscem najbardziej dociekliwych dyskusji nt. kluczowych, dla nowej strategii rządu, koncepcji i pojęć.

Sesja „FORUM POSZUKUJĄCEJ ADMINISTRACJI" - USŁUGI I DOBRE PRAKTYKI DO WZIĘCIA, to sposób na spopularyzowanie i upowszechnienie sprawdzonych już „na swoim podwórku" metod i usług.

„KOCIOŁ DYSKUSYJNY" jest tradycyjnie zwieńczeniem programu Forum. Istnieje bowiem bardzo wiele trudnych problemów związanych z technicznym, prawnym i mentalnym zrozumieniem nowych idei, w tym tych związanych z koncepcjami wykorzystania „cyfrowej chmury". Planowane prezentacje wprowadzające odniosą się do formułowanych publicznie ocen i wątpliwości.

Wszyscy uczestnicy, oprócz materiałów konferencyjnych, otrzymają certyfikat potwierdzający merytoryczną wiedzę, jaką zdobyli na Forum.

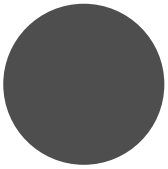
Honorowymi patronami Forum są: Michał Boni - Minister Administracji i Cyfryzacji, prof. dr hab. Katarzyna Chałasińska-Macukow - Rektor Uniwersytetu Warszawskiego, dr inż. Wacław Iszkowski - Prezes Polskiej Izby Informatyki i Telekomunikacji i Marek Woszczyk - Prezes Urzędu Regulacji Energetyki.

Patronem Forum jest Polska Agencja Rozwoju Przedsiebiorczości, a **Partnerami**: Hewlett-Packard Polska, Infovide-Matrix SA i Polska Wytwórnia Papierów Wartościowych.

Organizatorem Forum jest BizTech Konsulting SA - www.biztech.pl

Szczegółowa agenda i formularz rejestracyjny - www.forumti.pl

Wirtualne zakupy - czyli jak kupować w sklepach i na aukcjach internetowych?



Katarzyna Czajkowska-Matosiuk

Zasady kupowania w Internecie

W dzisiejszych czasach w Internecie można kupić wszystko – od paczki papierosów, poprzez lekarstwa (nawet te na receptę) i rozmaite usługi, aż po samochody i nieruchomości. Taką formę zakupów preferuję coraz więcej osób. Można spokojnie zastanowić się, porównać oferty, wyszukać szczególne okazje nie tracąc przy tym czasu na wycieczki po sklepach. Z zakupami internetowymi wiążą się jednak dodatkowe koszty oraz spore ryzyko nieudanej transakcji. Warto zatem wiedzieć, jakie prawa przysługują kupującym w przypadku, gdy zakup okaże się nieudany, a przede wszystkim, jak postępować, by takiej sytuacji uniknąć…

…Świadomie wybrać produkt

Zazwyczaj na rynku dostępnych jest wiele rodzajów interesującego nas towaru lub usługi. Można wybrać różne modele, marki, czy producentów. Aby nie kupować w ciemno, warto zapoznać się z **opiniami innych kupujących**. Można to zrobić zadając na odpowiednim **forum internetowym** pytanie dotyczące danego towaru lub prześledzić istniejące już wpisy. Użytkownicy chętnie dzielą się wrażeniami na temat dokonanych zakupów.

Trzeba jednak pamiętać o tym, że na forach internetowych powszechnie uprawiana jest tzw. **reklama szeptana**, która może zaburzyć obiektywny obraz danej oferty. Polega ona na tym, że sprzedający „podszywa" się pod kupującego użytkownika forum i zachwala swój produkt lub usługę. Tego typu marketing jest niestety całkowicie legalny i trudny do wychwycenia. Osoby uprawiające marketing szeptany zazwyczaj nie są stałymi bywalcami forów. Korzystają z nich jedynie doraźnie, **jako tzw. goście**, a w ich wypowiedziach przebija się nakłanianie innych użytkowników do konkretnego zakupu. Doświadczeni internetowi „zakupowicze" potrafią wprawdzie rozszyfrować utajoną reklamę, jednak nigdy nie ma co do tego 100%-towej pewności, a utajeni reklamodawcy zyskują w takich działaniach coraz większą wprawę, przez co stają się bardziej przekonujący. Warto więc przejrzeć **kilka różnych forów**, by uzyskać możliwie obiektywną, pełną opinię i wyrobić sobie własny pogląd w sprawie danego produktu.

Porównać oferty i ceny

Kiedy już podejmiemy decyzję o wyborze konkretnego produktu, zakup można poprzedzić **porównaniem ofert i cen konkretnego produktu**. W tym celu najlepiej skorzystać z **porównywarek cenowych**. Serwisy takie są bezpłatne, a obok zestawienia ofert i cen można znaleźć również zdjęcia i adresy sklepów, w których dostępny jest dany produkt. Zazwyczaj podane są także linki przekierowujące kupującego na stronę e-sklepu, na której można dokonać transakcji. W serwisach cenowych często też można zapoznać się z opiniami innych osób na temat produktu i zamieścić własny komentarz.

Porównywarek jest w sieci wiele, a najlepsze z nich umożliwiają porównywanie nawet kilkudziesięciu kategorii produktów i usług. Korzystanie z usług takich serwisów **nie musi być poprzedzone rejestrowaniem się na stronie, czy uiszczaniem jakichkolwiek**

opłat. Oferty wyświetlają się w kolejności od najtańszej do najdroższej już po wpisaniu w specjalnym okienku nazwy produktu.

Niestety serwisy cenowe nie dają gwarancji, że zamieszczone ceny są zawsze zgodne z rzeczywistością. Najczęściej wiąże się to z opóźnieniem w aktualizowaniu ofert, czy faktem, że sklepy podają w pierwszej kolejności **cenę bez VAT** lub „wyrównują" zaniżoną cenę wygórowanymi **kosztami wysyłki**.

Uwaga!

Porównywarki cen nie współpracują ze wszystkimi e-sklepami a jedynie tymi, które zostały z nimi zintegrowane. Oznacza to, że w sieci mogą funkcjonować sklepy, które posiadają jeszcze korzystniejsze oferty niż te, które wskazuje porównywarka.

Sprawdzić sprzedawcę

Następnym krokiem, po wyborze konkretnego produktu i sklepu, w którym chcemy dokonać zakupu, jest **sprawdzenie sprzedawcy**. Sprzedający ma obowiązek podać na stronie internetowej **dane umożliwiające jego identyfikację**, **a także informację o prawie konsumenta do odstąpienia od umowy.** Zgodnie z art. 9 ust. 1 ustawy z 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny, konsument powinien być poinformowany, przy użyciu środka porozumiewania się na odległość, **najpóźniej w chwili złożenia mu propozycji zawarcia umowy** m.in. o imieniu i nazwisku (nazwie), adresie zamieszkania (siedziby) przedsiębiorcy oraz organie, który zarejestrował działalność gospodarczą przedsiębiorcy, a także numerze, pod którym przedsiębiorca został zarejestrowany, istotnych właściwościach świadczenia i jego przedmiotu, kosztach oraz terminie i sposobie dostawy, prawie odstąpienia od umowy w terminie dziesięciu dni, ze wskazaniem wyjątków wymienionych w ustawie, miejscu i sposobie składania reklamacji.

Brak którejkolwiek z tych informacji może świadczyć o nierzetelności sprzedawcy, dlatego też powinien skłaniać kupujących do zachowania szczególnej ostrożności. W każdym sklepie internetowym powinien też być dostępny **przejrzysty regulamin**. Muszą się w nim znajdować informacje dotyczące rodzajów i zakresu oferowanych usług, warunków ich świadczenia oraz zawierania umów pomiędzy sklepem a internautami, a także opis procedury reklamacyjnej. Informacje te powinny być sformułowane **jednoznacznie, w sposób zrozumiały i łatwy do odczytania.**

Zanim zostanie dokonany zakup:

- ***należy sprawdzić adres i numer telefonu do przedsiębiorcy; nie można zakładać, że przedsiębiorca ma siedzibę w Polsce tylko dlatego, że adres internetowy ma skrót .pl***
- ***zaleca się korzystanie z takich witryn internetowych, które zapewniają bezpieczne sposoby płatności (w szczególności bezpieczne połączenia) - sygnalizowane poprzez symbol („ikonkę") kłódki na spodzie ekranu monitora.***
- ***warto sprawdzić, czy przedsiębiorca deklaruje reguły zachowania prywatności (tzw. politykę prywatności) i wskazuje, w jakim trybie będą przetwarzane dane osobowe.***
- ***koniecznie trzeba sprawdzić, czy nabywany towar np. urządzenie elektryczne odpowiada technicznym wymogom w danym kraju.***
- ***konsument powinien upewnić się, czy gwarancja jest honorowana w kraju jego stałego pobytu, a jeżeli zajdzie konieczność zwrotu towar sprzedawcy w jego kraju, to warto wyjaśnić jak przebiega procedura zwrotu produktu.***

- ***rekomenduje się kalkulację wysokości dodatkowych kosztów zakupu, takich jak podatki, cło, koszty dostawy, przesyłki pocztowej lub paczki.***
- ***można upewnić się, czy przedsiębiorca należy do systemu gwarantującego stosowanie określonych dobrych praktyk; jeśli tak, to będzie łatwiej dochodzić swoich praw; o przynależności do systemu świadczyć będą oznaczenia graficzne (logo); do systemów takich należy między innymi Euro-label.***

Źródło: www.konsument.gov.pl

Jak zawrzeć umowę przez Internet?

Warto wiedzieć, że każda transakcja, która odbywa się za pośrednictwem Internetu jest tzw. **umową zawieraną za pomocą środka porozumiewania się na odległość**. Jest to o tyle istotne, że przepisy prawa przyznają **szczególne uprawnienia i obowiązki** stronom takich umów. Przede wszystkim kupującemu przysługuje prawo odstąpienia od umowy zawartej przez Internet. Ponadto sprzedawca ma obowiązek precyzyjnie uregulować warunki sprzedaży.

Zakupu w sieci można dokonać na różne sposoby. Tym samym istnieje kilka trybów zawierania umów przez Internet. Kupujący może przesłać odpowiedź na ofertę zamieszczoną na stronie sklepu. Jest to **tzw. tryb ofertowy**. Druga możliwość to wypełnienie aktywnego formularza lub przeniesienie do koszyka i potwierdzenie poprzez kliknięcie. Ten sposób nazywa się **trybem interaktywnym**. Jeszcze inna możliwość to **licytacja internetowa**. Sprzedający podaje tu cenę wywoławczą towaru, a zainteresowana osoba proponuje kwotę wyższą niż konkurent. Na wielu takich aukcjach możliwa jest także opcja natychmiastowego zakupu (tzw. „Kup teraz") bez angażowania się w licytację. Cena towaru ustalona jest tu na sztywno i zazwyczaj jest znacznie wyższa niż cena wywoławcza w przypadku licytacji.

Jak ustalić moment zawarcia umowy przez Internet?

Istotne znaczenie ma również chwila zawarcia umowy internetowej. Jeżeli przedsiębiorca oferuje towary w swoim e-sklepie, zamówienie złożone przez kupującego wiąże sprzedającego. Oznacza to, że w chwili **dojścia do sprzedającego zamówienia** dochodzi do zawarcia umowy.

Sprzedający może też podać na swojej stronie internetowej szczegółowe informacje o towarach i tym samym **zapraszać zainteresowane osoby do rokowań lub do zawarcia umowy**. Zgodnie z art. 71 Kodeksu cywilnego, **ogłoszenia, reklamy, cenniki i inne informacje, skierowane do ogółu lub do poszczególnych osób, poczytuje się w razie wątpliwości nie za ofertę, lecz za zaproszenie do zawarcia umowy**. W takiej sytuacji składającym ofertę jest nabywca, a przyjmującym ofertę - sprzedawca. Chwilą zawarcia umowy będzie wówczas **potwierdzenie przyjęcia oferty** przez przedsiębiorcę internetowego, albo - jeśli takie potwierdzenie nie jest wymagane - **przystąpienie do wykonania umowy** (nadanie przesyłki z towarem).

Kto odpowiada za paczkę z towarem kupionym w Internecie?

Dostarczenie towaru zakupionego przez Internet zazwyczaj odbywa się **drogą wysyłkową**, choć sklepy, które istnieją również „w realu", czyli mają swoją fizyczną siedzibę, umożliwiają także **osobisty odbiór** zakupów. W przypadku osób nieprowadzących działalności gospodarczej, które handlują na portalach aukcyjnych, towary są przeważnie wysyłane. Można oczywiście próbować umówić się ze sprzedającym, na osobisty odbiór przesyłki (np. jeśli mieszka w tej samej

miejscowości), jednak sprzedawca nie ma obowiązku godzić się na takie rozwiązanie. Zatem najczęściej kupujący muszą ponieść **dodatkowe koszty przesyłki**, nie są również w stanie na miejscu sprawdzić towaru i jego zgodności z zawartą umową. Warto więc **wiedzieć**, co zrobić, jeżeli nadesłana paczka będzie uszkodzona lub otrzymamy towar inny niż ten, za który zapłaciliśmy.

Jaki jest czas realizacji zamówień?

Może się zdarzyć, że towar zakupiony przez Internet **nie dociera do kupującego na czas albo nawet nie dociera w ogóle.** Tego typu przypadki mają miejsce najczęściej w okresie przedświątecznym, kiedy poczta i firmy kurierskie są „przeciążone". Wówczas wina leży po stronie przewoźnika i jeśli sprzedający okaże dowód nadania przesyłki w odpowiednim terminie, trudno mieć do niego pretensje za zwłokę w dostarczeniu towaru.

Niedostarczenie towaru na czas może jednak wynikać z **zaniedbania lub nierzetelności sprzedawcy**. Przed dokonaniem zakupu warto więc zwrócić uwagę na podany czas realizacji zamówienia i czas dostawy zamówionej paczki.

Uwaga!

Realizacja transakcji nie powinna być liczona od złożenia zamówienia do momentu dostarczenia towaru przez przewoźnika, lecz od przyjęcia zamówienia do nadania paczki przez sprzedawcę internetowego wybraną przez klienta formą dostawy.

Zazwyczaj sklepy internetowe dają **gwarancję dostarczenia zakupów** w okresie od 24 do 72 godzin (chodzi tu jednak wyłącznie o dni robocze). Z kolei sprzedawcy oferujący swoje towary na portalach aukcyjnych zabezpieczają się podając dłuższe terminy dostawy. Najczęściej już w opisie oferowanego produktu można przeczytać, w jakim czasie towar zostanie do nas dostarczony. Zanim zdecydujemy się na zakup, dobrze jest sprawdzić tę kwestię. Dotyczy to szczególnie przypadków, gdy zależy nam na czasie, bo kupujemy coś co będzie nam potrzebne w określonym terminie (np. prezent z jakiejś okazji). Zdarza się też (zwłaszcza na portalach aukcyjnych), że sprzedawcy zastrzegają w opisie aukcji, że przesyłki będą realizowane dopiero po określonej dacie (np. dopiero od września 2012 r.) lub, że nie będą realizowane w ogóle w danym terminie (np. od 12 kwietnia do 1 maja, ze względu na wyjazd sprzedawcy).

Czas dostawy zamówionych towarów jest również ściśle **uzależniony od formy przesyłki** wybranej przez kupującego. Można bowiem zdecydować się na zwykłą przesyłkę pocztową, priorytet lub dostarczenie towaru przez kuriera. Niektórzy sprzedawcy zapewniają również własny transport (zazwyczaj płatny). W przypadku Poczty Polskiej czas dostawy na terenie kraju wynosi zazwyczaj od **2 do 5 dni roboczych**. Firmy kurierskie dostarczają najczęściej towary w ciągu **jednego dnia roboczego**. Istotne jest również to, że zamówienie na towary o różnym czasie realizacji wysyłane jest najczęściej w chwili skompletowania całego zamówienia, a termin wysyłki określany jest na podstawie towaru o najdłuższym czasie realizacji.

Uwaga!

Termin otrzymania paczki = czas realizacji + czas dostawy.

Przykład

1 marca 2012 (w sobotę) Pan Kowalski kupił w sklepie internetowym płytę DVD. Sklep zastrzega na swojej stronie internetowej,

że dostawy dokonuje w ciągu 24 godzin. W takim przypadku upływ 24-godzinnego terminu należy liczyć dopiero od poniedziałku, ponieważ sobota jest dniem wolnym od pracy.

Kto odpowiada za zagubione paczki?

Zdarza się, że z powodu błędu lub zaniedbania przewoźnika, kupujący nie otrzyma zakupionego towaru. Oczywiście w takim przypadku, za utratę, ubytek lub uszkodzenie przesyłki **odpowiada przewoźnik**.

Uwaga!

Odpowiedzialność spoczywa na przewoźniku od momentu przyjęcia przesyłki do przewozu, aż do jej wydania.

Niestety w takiej sytuacji **to kupujący musi dochodzić rekompensaty od przewoźnika**. Jeśli więc przesyłka nie dociera na czas, należy zgłosić ten fakt sprzedającemu. Ten powinien skontaktować się z firmą kurierską i wyjaśnić sprawę. Dalsze postępowanie uzależnione jest od tego, czy ustalono, co stało się z przesyłką. Jeśli okaże się, że zaginęła, można ubiegać się o **odszkodowanie od przewoźnika.**

Co robić, gdy przesyłka jest uszkodzona?

Kupujący powinni wiedzieć, że w przypadku, gdy przewoźnik dostarczy **towar w uszkodzonym opakowaniu,** maja prawo odmówić przyjęcia paczki lub spisać protokół zniszczeń.

Zdarza się też, że mimo nienaruszonego opakowania towar znajdujący się w środku jest uszkodzony. Dlatego prawo gwarantuje kupującym **możliwość otworzenia przesyłki w obecności dostawcy i sprawdzenia jej zawartości**. Takie postępowanie możliwe jest jednak **dopiero po opłaceniu towaru i pokwitowaniu jej odbioru**. Dostawca może bowiem odmówić sprawdzenia paczki przed zapłatą.

W przypadku gdy w wyniku sprawdzenia zawartości przesyłki okaże się, że towar jest wadliwy, kupujący powinien domagać się od dostawcy spisania tzw. **protokołu niezgodności (inaczej: protokołu reklamacyjnego).**

Uwaga!

Dostawca nie ma prawa odmówić spisania protokołu niezgodności.

Protokół spisuje się zawsze na specjalnym formularzu (egzemplarzami takiego formularza powinien dysponować dostawca) pozwalającym na szczegółowy opis szkód lub niezgodności towaru.

Uwaga!

Formularza protokołu niezgodności nie można zastępować adnotacją na liście prze- wozowym.

Taki dokument jest **podstawą do późniejszej reklamacji**. Jeżeli kupujący tego nie zrobi, sklep może nie uznać skargi i powstałe szkody będą usuwane na jego koszt.

Zgodne z przepisami Prawa przewozowego, jeżeli przed wydaniem przesyłki okaże się, że doznała ona ubytku lub uszkodzenia, przewoźnika ma obowiązek **ustalić niezwłocznie protokolarnie stan**

przesyłki oraz okoliczności powstania szkody. Musi on wykonać te czynności także na żądanie odbierającego paczkę adresata, jeżeli twierdzi on, że przesyłka jest naruszona. Protokół powinien zostać spisany w obecności uprawnionego.

Uwaga!

Przyjęcie przesyłki bez zastrzeżeń powoduje wygaśnięcie roszczeń z tytułu ubytku lub uszkodzenia, co oznacza, że kupujący nie będzie mógł egzekwować od sprzedawcy rekompensaty z tego tytułu.

Kupujący będzie miał jednak prawo dochodzić swoich roszczeń od sprzedawcy, w przypadku gdy:

- szkodę stwierdzono protokolarnie przed przyjęciem przesyłki przez adresata,
- zaniechano takiego stwierdzenia z winy przewoźnika,
- ubytek lub uszkodzenie wynikły z winy umyślnej lub rażącego niedbalstwa przewoźnika,
- szkodę niedającą się z zewnątrz zauważyć uprawniony stwierdził po przyjęciu przesyłki i w terminie 7 dni zażądał ustalenia jej stanu oraz udowodnił, że szkoda powstała w czasie między przyjęciem przesyłki do przewozu, a jej wydaniem.

Przykład

Pani Kasia kupiła lampę w sklepie internetowym. Sprzedawca zadbał o odpowiednie zapakowanie i oznakowanie przesyłki jako wymagającej szczególnej ostrożności. Tak przygotowaną paczkę sprzedawca wysłał pocztą. Po jej rozpakowaniu kupujący zorientował się, że paczka została uszkodzona przez przewoźnika. Co powinien zrobić kupujący?

Przede wszystkim skontaktować się ze sprzedawcą i opisać mu problem. Do obowiązku sprzedawcy będzie należało wyjaśnienie sprawy na poczcie. Jednak w przypadku, gdy okaże się, że winę ponosi poczta, to Pani Kasia, a nie sprzedawca, będzie musiała dochodzić swoich praw od przewoźnika (poczty).

Szczegółową procedurę ustalania stanu paczek określa rozporządzenie ministra transportu i budownictwa z 24 lutego 2006 r. w sprawie ustalania stanu przesyłek oraz postępowania reklamacyjnego. Zgodnie z przepisami rozporządzenia, za naruszenie stanu przesyłki uważa się **każde obniżenie wartości przesyłki spowodowane nieprawidłowościami lub zaniedbaniami w okresie od przyjęcia jej do przewozu, aż do jej wydania uprawnionemu**.

Protokół ustalenia stanu przesyłki powinien zawierać w szczególności informacje dotyczące:

1) pierwotnego stanu przesyłki i wartości przesyłki wynikającej z zapisów w dokumencie przewozowym,
2) rodzaju naruszeń stanu przesyłki, pojemnika transportowego lub środka transportowego,
3) rozmiarów naruszenia, w tym ubytków ilości, masy lub objętości przesyłki,
4) przypuszczalnego czasu i miejsca, w którym nastąpiło naruszenie stanu przesyłki,
5) przypuszczalnych przyczyn naruszenia stanu przesyłki,
6) okoliczności ujawnienia naruszenia stanu przesyłki.

Reklamacja u sprzedawcy

Jeżeli dostarczony towar ma wady, (usterki fabryczne, uszkodzenia mechaniczne, niezgodności towaru z zawartym w zamówieniu), kupującemu przysługuje prawo do złożenia reklamacji u sprzedawcy. W takim

przypadku kupujący powinien odesłać towar wraz z fakturą i pismem reklamacyjnym. Kopię faktury warto też zachować dla siebie.

Sprzedający ma obowiązek rozpatrzeć reklamację w ciągu 14 dni od daty otrzymania przesyłki z reklamowanym towarem. Jeżeli nie uczyni tego we wskazanym terminie, będzie to równoznaczne z uznaniem reklamacji zgodnie z twierdzeniami kupującego. W przypadku uznania reklamacji, towar uszkodzony powinien zostać naprawiony lub wymieniony na inny, pełnowartościowy, a jeśli będzie to już niemożliwe, sprzedawca powinien zwrócić kupującemu cenę towaru lub zaoferować mu inny towar. Pozytywne rozpatrzenie reklamacji oznacza też, że sprzedawca ma obowiązek zwrócić kupującemu koszty przesyłki.

Ważne!

Kupującemu przysługuje prawo reklamacji towaru niezgodnego z umową w terminie dwóch lat od jego zakupu.

Kupujący może żądać naprawienia rzeczy, wymiany jej na nową, obniżenia ceny lub zwrotu pieniędzy. Sprzedawca ma obowiązek rozpatrzenia reklamacji w ciągu 14 dni. Jeżeli tego nie zrobi, uznaje się, że skarga została uwzględniona według żądania klienta.

Jak reklamować towar na poczcie?

Z uwagi na wysokie koszty usług kurierskich wielu kupujących wybiera formę wysyłki za pośrednictwem Poczty Polskiej. W przypadku zagubienia lub uszkodzenia paczki przez pocztę, reklamację może zgłosić **zarówno adresat, jak i nadawca przesyłki**. Obowiązują tutaj szczególne zasady. Jeżeli zaś doszło do niewykonania lub nienależytego wykonania powszechnej usługi pocztowej w zakresie **przesyłki rejestrowanej** (listu poleconego, paczki pocztowej) i przekazu pocztowego, to prawo wniesienia reklamacji z roszczeniem o odszkodowanie lub bez takiego roszczenia **przysługuje nadawcy** (czyli sprzedawcy).

Uwaga!

Powszechną usługę pocztową w zakresie przesyłki rejestrowanej uważa się za niewykonaną, jeżeli doręczenie przesyłki rejestrowanej lub zawiadomienia o próbie jej doręczenia nie nastąpiło w terminie 14 dni od dnia nadania. Do terminu tego nie wlicza się dni ustawowo wolnych od pracy.

Kupujący będzie miał prawo samodzielnie złożyć reklamację na poczcie jedynie w przypadku, gdy nadawca **zrzeknie się na jego rzecz prawa dochodzenia roszczeń albo gdy przesyłka zostanie doręczona adresatowi**.

Procedury dotyczące reklamacji przesyłek rejestrowanych zawarte zostały w rozporządzeniu ministra infrastruktury z 13 października 2003 r. w sprawie reklamacji powszechnej usługi pocztowej w zakresie przesyłki rejestrowanej i przekazu pocztowego. Rozporządzenie określa również szczegółowe warunki, jakim powinna odpowiadać reklamacja.

Reklamację zgłasza się w formie:
1) pisemnej;
2) ustnej do protokołu;
3) innej niż wymienione w pkt. 1 i 2, która ujawnia wolę reklamującego w sposób dostateczny (w tym również w formie elektronicznej).

Reklamacja powinna zawierać:
1) imię i nazwisko albo nazwę lub firmę oraz adres zamieszkania albo siedziby nadawcy lub adresata (tj. reklamującego);

2) rodzaj reklamowanej przesyłki;
3) uzasadnienie reklamacji;
4) kwotę odszkodowania w przypadku, gdy reklamujący żąda odszkodowania;
5) podpis reklamującego.

Do reklamacji należy dołączyć:
1) oryginał potwierdzenia nadania przesyłki rejestrowanej lub przekazu pocztowego;
2) oświadczenie o zrzeczeniu się prawa do dochodzenia roszczeń - w przypadku przeniesienia uprawnień przez nadawcę na adresata;
3) protokół sporządzony bezpośrednio przy przyjęciu uszkodzonej przesyłki rejestrowanej - w przypadku jej przyjęcia przez adresata, oraz opakowanie uszkodzonej przesyłki;
4) oświadczenie o stwierdzeniu:
   a) widocznych ubytków lub uszkodzeń przesyłki rejestrowanej złożone bezpośrednio przy przyjęciu przesyłki albo
   b) niewidocznych ubytków lub uszkodzeń przesyłki rejestrowanej, z zachowaniem terminu 7 dni od przyjęcia przesyłki.

Reklamacja zgłoszona w innej formie niż pisemna lub ustna do protokołu, czyli np. w formie elektronicznej) powinna zawierać dodatkowo informacje **o dacie i miejscu nadania przesyłki rejestrowanej lub przekazu pocztowego,** a w przypadku przesyłki rejestrowanej - **o numerze nadanym jej przez operatora.**

Jeżeli reklamacja zgłoszona w formie pisemnej lub ustnej nie spełnia omawianych wymogów Poczta powinna **wezwać reklamującego do usunięcia braków formalno-prawnych w terminie 7 dni od dnia doręczenia wezwania.** Okresu tego nie wlicza się do terminu rozpatrzenia reklamacji.

W przypadku reklamacji zgłoszonej w innej formie niż pisemna lub ustna Poczta wezwie reklamującego do uzupełnienia reklamacji o wymagane dokumenty oraz do złożenia pisemnego oświadczenia potwierdzającego zgłoszenie reklamacji opatrzone podpisem reklamującego, w terminie **7 dni od dnia doręczenia wezwania**. Okresu tego również nie wlicza się do terminu rozpatrzenia reklamacji.

Jeżeli braki nie zostaną uzupełnione w powyższych terminach, reklamacja **zostanie pozostawiona bez rozpoznania,** o czym Poczta powiadomi reklamującego.

Uwaga!

Reklamację z tytułu niewykonania usługi można zgłosić po upływie 14 dni od dnia nadania przesyłki rejestrowanej lub przekazu pocztowego, nie później jednak niż w terminie 12 miesięcy od dnia ich nadania.

Reklamację z tytułu nienależytego wykonania usługi kupujący powinien zgłosić:
1) bezpośrednio przy przyjęciu przez adresata uszkodzonej przesyłki rejestrowanej, w której adresat stwierdzi ubytek zawartości;
2) po przyjęciu przesyłki rejestrowanej przez adresata, jeżeli bezpośrednio przy przyjęciu tej przesyłki złożył on pisemne oświadczenie o stwierdzeniu ubytków lub uszkodzeń, nie później jednak niż w terminie 12 miesięcy od dnia jej nadania;
3) w terminie 7 dni od przyjęcia przesyłki - w przypadku stwierdzenia ubytków lub uszkodzeń przesyłki rejestrowanej, niewidocznych bezpośrednio przy przyjęciu przesyłki.

Reklamacja zgłoszona po upływie tych terminów **zostanie pozostawiona bez rozpoznania,** o czym Poczta powiadomi reklamującego.

Po otrzymaniu reklamacji Poczta ma **14 dni na udzielenie pisemnej odpowiedzi**. W szczególnych przypadkach Poczta może poinformować reklamującego o niemożności udzielenia odpowiedzi na reklamację w terminie 14 dni od dnia jej otrzymania. Musi jednak podać przyczynę zwłoki oraz termin udzielenia odpowiedzi na reklamację, przy czym termin ten **nie może przekroczyć 30 dni od dnia otrzymania reklamacji**.

Czasem termin ten może być dłuższy. Dotyczy to w szczególności przypadków, gdy:
1) zebrane w dotychczasowym postępowaniu dowody i wyjaśnienia wymagają uzupełnienia dla rzetelnego rozpatrzenia reklamacji;
2) uzyskanie dowodów i wyjaśnień w terminie 14 dni od dnia otrzymania reklamacji nie było możliwe pomimo zachowania należytej staranności operatora w ustalaniu stanu faktycznego.

W przypadku odmowy przez Pocztę uwzględnienia reklamacji w całości lub w części, reklamujący może wnieść **odwołanie do jednostki odwoławczej wskazanej w odpowiedzi na reklamację. Termin na wniesienie odwołania wynosi 14 dni od dnia jej doręczenia**.

Jak poczta zadośćuczyni szkodę?

Zasady odpowiedzialności operatorów pocztowych reguluje rozdział 5 ustawy z 12 czerwca 2003 r. - Prawo pocztowe. Zgodnie z tymi przepisami operator publiczny, czyli Poczta, odpowiada za **niewykonanie lub nienależyte wykonanie powszechnej usługi pocztowej**, chyba że niewykonanie lub nienależyte wykonanie nastąpiło:
1) wskutek siły wyższej (np. z powodu pożaru w placówce pocztowej spłonęły przesyłki);
2) wyłącznie z powodu naruszenia przez nadawcę lub adresata przepisów prawnych albo regulaminu świadczenia powszechnych usług pocztowych;
3) wyłącznie z powodu szczególnej podatności przesyłanej rzeczy na uszkodzenia wynikającej z jej wad lub naturalnych właściwości (np. wysłano w paczce produkty żywnościowe, które w trakcie transportu uległy zepsuciu).

Uwaga!

Roszczenie z tytułu nienależytego wykonania usługi pocztowej wygasa wskutek przyjęcia przesyłki bez zastrzeżeń. Nie dotyczy to jednak roszczeń z tytułu niewidocznych ubytków lub uszkodzeń przesyłki zgłoszonych przez adresata operatorowi nie później niż po upływie 7 dni od przyjęcia przesyłki.

Z tytułu niewykonania lub nienależytego wykonania usługi pocztowej poszkodowanemu przysługuje **odszkodowanie**. Jest ono przekazywane **przekazem pocztowym tego samego dnia lub dnia następnego po pozytywnym rozpatrzeniu reklamacji** na korzyść klienta. Przepisy określają jednak górną granicę odszkodowania, jakie można w takich przypadkach uzyskać od operatora pocztowego:
1) za utratę przesyłki poleconej - w wysokości żądanej przez nadawcę, nie wyższej jednak niż pięćdziesięciokrotność opłaty pobranej przez operatora publicznego za traktowanie przesyłki jako przesyłki poleconej;
2) za utratę paczki pocztowej - w wysokości żądanej przez nadawcę, nie wyższej jednak niż dziesięciokrotność opłaty pobranej za jej nadanie;
3) za utratę przesyłki z zadeklarowaną wartością - w wysokości żądanej przez nadawcę, nie wyższej jednak niż zadeklarowana wartość przesyłki;
4) za ubytek zawartości lub uszkodzenie paczki pocztowej lub przesyłki poleconej - w wysokości żądanej przez nadawcę lub

w wysokości zwykłej wartości utraconych lub uszkodzonych rzeczy, nie wyższej jednak niż maksymalna wysokość odszkodowania, o którym mowa w pkt 1 lub 2;

5) za ubytek zawartości przesyłki z zadeklarowaną wartością - w wysokości zwykłej wartości utraconych rzeczy;
6) za uszkodzenie zawartości przesyłki z zadeklarowaną wartością - w wysokości zwykłej wartości rzeczy, których uszkodzenie stwierdzono.

Odszkodowanie, o którym mowa w pkt 5 i 6, **nie może być wyższe niż zadeklarowana wartość przesyłki.**

W przypadku niewykonania usługi, Poczta niezależnie od należnego odszkodowania, **zwraca w całości opłatę pobraną za wykonanie usługi.**

Uwaga!

Nadawca albo adresat mogą zgłosić reklamację w każdej placówce operatora świadczącego powszechne usługi pocztowe.

Po wyczerpaniu drogi postępowania reklamacyjnego, czyli w sytuacji odmowy uznania reklamacji przez Pocztę albo niezapłacenia dochodzonej należności w terminie 90 dni od dnia wniesienia reklamacji, **nadawca albo adresat mogą dochodzić swoich roszczeń w postępowaniu sądowym.**

Trzeba jednak pamiętać, że roszczenia te **przedawniają się z upływem 12 miesięcy od dnia nadania przesyłki lub przekazu pocztowego.** Oznacza to, że po tym terminie nie można już dochodzić swoich praw.

Uwaga!

Do odpowiedzialności operatorów za niewykonanie lub nienależyte wykonanie usługi pocztowej stosuje się przepisy kodeksu cywilnego, jeżeli przepisy ustawy nie stanowią inaczej.

Czy można zrezygnować z zakupu dokonanego przez Internet?

Osoby, które dokonują zakupów przez Internet są chronione w sposób szczególny. Kwestię tę reguluje ustawa z 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny.

Zgodnie z przywołaną ustawa, konsument, który zawarł umowę na odległość, **może od niej odstąpić bez podania przyczyn, składając stosowne oświadczenie na piśmie w terminie dziesięciu dni**. Termin dziesięciodniowy, w którym konsument może odstąpić od umowy, liczy się **od dnia wydania rzeczy,** a gdy umowa dotyczy świadczenia usługi - **od dnia jej zawarcia**. Do zachowania tego terminu wystarczy **wysłanie oświadczenia przed jego upływem**.

Uwaga!

Nie jest dopuszczalne zastrzeżenie, że konsumentowi wolno odstąpić od umowy za zapłatą oznaczonej sumy (odstępne).

W razie odstąpienia umowa jest **uważana za niezawartą**, a konsument jest **zwolniony z wszelkich zobowiązań**. To, co strony świadczyły, ulega zwrotowi. Zwrot powinien nastąpić **niezwłocznie**, **nie później niż w terminie czternastu dni.** Jeżeli konsument

dokonał jakichkolwiek przedpłat, należą się od nich **odsetki ustawowe od daty dokonania przedpłaty.**

Sprzedawca ma **obowiązek poinformowania kupującego** najpóźniej w chwili złożenia mu propozycji zawarcia umowy (np. na swojej stronie lub w przesyłce) o:

1) imieniu i nazwisku (nazwie), adresie zamieszkania (siedziby) przedsiębiorcy oraz organie, który zarejestrował działalność gospodarczą przedsiębiorcy, a także numerze, pod którym przedsiębiorca został zarejestrowany,
2) istotnych właściwościach świadczenia i jego przedmiotu,
3) cenie lub wynagrodzeniu obejmujących wszystkie ich składniki, a w szczególności cła i podatki,
4) zasadach zapłaty ceny lub wynagrodzenia,
5) kosztach oraz terminie i sposobie dostawy,
6) prawie odstąpienia od umowy w terminie dziesięciu dni,
7) kosztach wynikających z korzystania ze środków porozumiewania się na odległość, jeżeli są one skalkulowane inaczej niż wedle normalnej taryfy,
8) terminie, w jakim oferta lub informacja o cenie albo wynagrodzeniu mają charakter wiążący,
9) minimalnym okresie, na jaki ma być zawarta umowa o świadczenia ciągłe lub okresowe,
10) miejscu i sposobie składania reklamacji,
11) prawie wypowiedzenia umowy.

Informacje te powinny być sformułowane **jednoznacznie**, w sposób zrozumiały i łatwy do odczytania.

Jeżeli sprzedawca nie udostępni kupującemu tych informacji, kupujący ma prawo odesłać towar nawet w czasie **do trzech miesięcy od otrzymania towaru, jednak nie później niż w ciągu dziesięciu dni od uzyskania informacji o prawie rezygnacji z umowy**.

Sprzedawca może oczywiście **wydłużyć czas,** w którym można odstąpić od umowy zawartej na odległość. Wiele sklepów internetowych daje nawet 30 dni na dokonanie takich czynności. 10-dniowego terminu w żadnym przypadku nie można skracać.

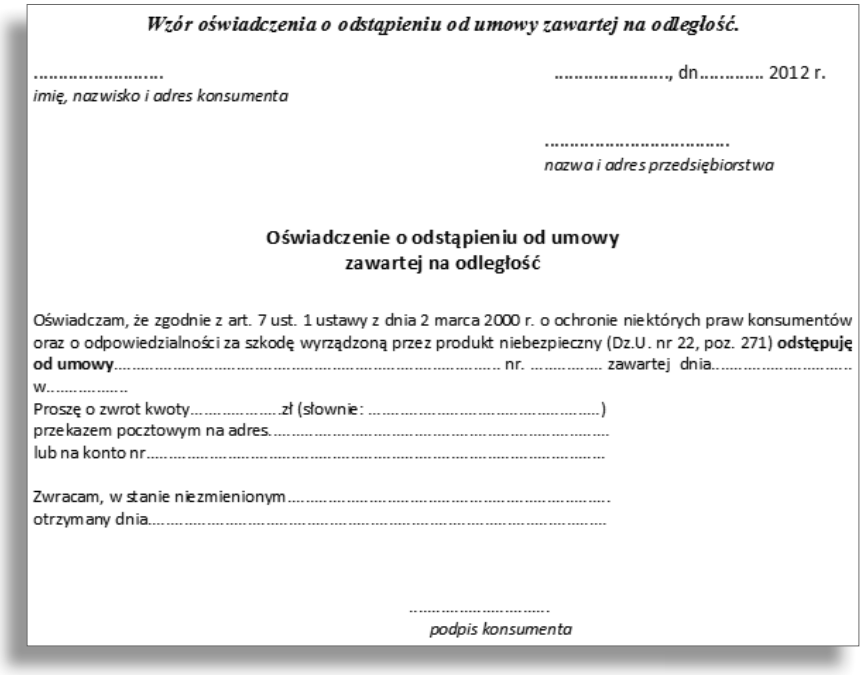
Aby skutecznie odstąpić od umowy, należy wysłać do sprzedawcy **oświadczenie o odstąpieniu od umowy.** Oświadczenie należy przygotować **na piśmie i przesłać listem poleconym** pod adresem firmy **najpóźniej dziesiątego dnia od daty zawarcia umowy o wykonanie usługi lub daty otrzymania zamówionego towaru.**

Uwaga!

Sprzedawca ma obowiązek poinformować kupującego o prawie zwrotu zakupionego towaru w ciągu 10 dni od jego doręczenia. Jeśli tego nie zrobi, kupujący może odesłać towar nawet do trzech miesięcy od dnia wykonania umowy.

Kopię oświadczenia oraz potwierdzenie nadania listu kupujący powinien **zachować na dowód**, że zachował przewidziane prawem terminy.

Sprzedawca **nie ma prawa pobierania jakichkolwiek opłat z tytułu rezygnacji kupującego** z zakupionego towaru. Nie może żądać kosztów związanych z zawarciem i rezygnacją z umowy, jak też kosztów marketingowych oraz innych opłat ustalonych przez firmę na potrzeby danej umowy. Takie żądanie jest bezprawne. Nawet jeśli zostało zapisane w umowie lub regulaminie sklepu, jest uważane za **nieważne**.



Wzór oświadczenia o odstąpieniu od umowy zawartej na odległość.

…… ……., dn…… 2012 r.
imię, nazwisko i adres konsumenta

……
nazwa i adres przedsiębiorstwa

Oświadczenie o odstąpieniu od umowy zawartej na odległość

Oświadczam, że zgodnie z art. 7 ust. 1 ustawy z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. nr 22, poz. 271) **odstępuję od umowy**…… nr. …… zawartej dnia…… w……
Proszę o zwrot kwoty……zł (słownie: ……)
przekazem pocztowym na adres……
lub na konto nr……

Zwracam, w stanie niezmienionym……
otrzymany dnia……

……
podpis konsumenta

Koszty odesłania towaru ponosi **kupujący**. Inaczej jest w przypadku reklamacji (gdy kupiony towar zawiera wady i chcemy, żeby zostały one usunięte, lub żeby przesłano nam produkt bez usterek). W przypadku uwzględnienia reklamacji sprzedawca ma obowiązek zwrócić kupującemu koszty przesyłki.

Przykład

Sprzedawca – sklep internetowy „Ciuch" prowadzi wysyłkową sprzedaż odzieży. Na swojej stronie internetowej podaje wszystkie wymagane przez prawo informacje o prawie odstąpienia konsumenta od umowy w terminie dziesięciu dni. Zapoznawszy się z tymi informacjami, Pani Marta zdecydowała się na zakup spodni. Po otrzymaniu towaru okazało się, że spodnie źle na niej leżą. Chciałaby zwrócić zakup. Czy ma do tego prawo?

W takim przypadku Pani Marta może odstąpić od umowy bez podania przyczyn. W tym celu powinna w ciągu dziesięciu dni wysłać listem poleconym lub mailem oświadczenie o odstąpieniu od umowy zawartej na odległość i odesłać towar na adres sklepu.

Jakie są ograniczenia w zwrocie zakupionych towarów?

Jeżeli strony nie umówiły się inaczej, **prawo odstąpienia od umowy zawartej na odległość nie przysługuje** konsumentowi w wypadkach:

1) świadczenia usług rozpoczętego za zgodą konsumenta, przed upływem dziesięciu dni przewidzianych na odstąpienie od umowy;
2) dotyczących nagrań audialnych i wizualnych oraz zapisanych na informatycznych nośnikach danych (np. muzyka, gry i programy zapisane na płytach CD i DVD) po usunięciu przez konsumenta ich oryginalnego opakowania,

3) umów dotyczących świadczeń, za które cena lub wynagrodzenie zależy wyłącznie od ruchu cen na rynku finansowym (np. umowy obejmujące obrót instrumentami finansowymi takich jak internetowy zakup akcji czy jednostek uczestnictwa w funduszach inwestycyjnych),
4) świadczeń o właściwościach określonych przez konsumenta w złożonym przez niego zamówieniu lub ściśle związanych z jego osobą (np. umowy o dostawę dzieła stworzonego według indywidualnego zamówienia konsumenta takich jak umowy o stworzenie strony WWW),
5) świadczeń, które z uwagi na ich charakter nie mogą zostać zwrócone (np. przeprowadzenie szkolenia lub kursu językowego albo zamieszczenie ogłoszenia w prasie) lub których przedmiot ulega szybkiemu zepsuciu (np. artykuły żywnościowe),
6) dostarczania prasy (np. internetowe wydania czasopism),
7) usług w zakresie gier hazardowych (np. loterie pieniężne lub loterie promocyjne, w których uczestniczy się przez nabycie towaru, usługi lub innego dowodu udziału w grze, albo o zakłady wzajemne takie jak totalizatory i buk macherstwo).

Co z towarami kupionymi od nie-przedsiębiorców?

Podkreślenia wymaga, że omówione prawo do odstąpienia od umowy zawartej na odległość dotyczy **wyłącznie zakupów dokonanych u przedsiębiorców**. Tymczasem w praktyce sprzedającymi **na aukcjach internetowych** bywają zarówno przedsiębiorcy, czyli osoby prowadzące własne firmy, jak i **osoby prywatne**, które chcą się pozbyć niepotrzebnych rzeczy.

W przypadku dokonania na aukcji internetowej zakupu u przedsiębiorcy, kupujący możne odstąpić od takiej umowy **tak jak przy zwykłej sprzedaży internetowej**, stosując się do opisanych powyżej warunków.

Uwaga!

Nie dotyczy to sytuacji, gdy cena towaru była licytowana.

Natomiast w sytuacji gdy sprzedający na aukcji będzie **osobą prywatną nieprowadzącą działalności gospodarczej,** kupujący będzie mógł dochodzić od niego jedynie **odpowiedzialności za wady towaru z tytułu rękojmi**. Dotyczy to towarów, których wady zmniejszają wartość rzeczy. Sprzedawca ponosi odpowiedzialność z tytułu rękojmi, gdy w chwili zawarcia umowy konsument nie wiedział o wadzie kupowanej rzeczy.

Przykład

Pan Jan kupił na aukcji internetowej (poprzez opcję „kup teraz") nowego laptopa od sprzedającego o loginie Maiusz333, który nie prowadzi działalności gospodarczej. Pan Jan wybrał formę płatności „za pobraniem". Po dwóch dniach kurier dostarczył Panu Janowi towar, a Pan Jan zapłacił należną cenę. Następnie znalazł na innej aukcji identycznego laptopa w znacznie niższej cenie. Słyszał, że kupując przez Internet można w ciągu 10 dni odstąpić od umowy. Zamierza więc skorzystać z tego uprawnienia. Czy ma do tego prawo?

Niestety w tym przypadku Panu Janowi nie przysługuje omawiane prawo odstąpienia od umowy. Sprzedawca nie jest bowiem przedsiębiorcą, a osobą prywatną nieprowadzącą działalności gospodarczej. Pan Jan mógłby natomiast dochodzić od sprzedawcy odpowiedzialności za wady towaru z tytułu rękojmi, gdyby okazało się, że laptop ma wady zmniejszające jego użyteczność, np. odbiega od norm technicznych ustalonych dla tego rodzaju sprzętu, gdy rzecz nie ma

Różnice między odstąpieniem a reklamacją	
Odstąpienie:	Reklamacja:
• towar nie ma wad	• towar ma wady
• przyczyna zwrotu jest dowolna	• przyczyna zwrotu- towar nie jest zgodny z umową
• koszt przesyłki do sprzedawcy ponosi konsument	• koszt przesyłki do sprzedawcy ponosi sprzedawca
• konsument żąda zwrotu pieniędzy	• konsument żąda naprawy albo wymiany towaru, ewentualnie obniżenia ceny albo odstąpienia od umowy

Tabela 1.

właściwości, o których istnieniu zapewniał sprzedawca, lub gdy wydano go w stanie niekompletnym.

Jak reklamować towary zakupione za granicą?

Jeżeli dokonujemy zakupów w zagranicznym sklepie internetowym, to należy pamiętać, że:

- rożne państwa Unii Europejskiej, mają odmienne terminy na zwrot towaru, można to zrobić w ciągu 7,10 lub 14 dni. Termin odstąpienia od umowy liczony jest od dnia wydania towaru, ale także liczy się go od dnia zawarcia transakcji,
- w krajach Unii Europejskiej reklamacji można dokonać w ciągu dwóch lat od dokonania zakupu. Reklamacja rzeczy używanej może być ograniczona do 1 roku, ale musi na to wyrazić zgodę osoba kupująca,
- w przypadku zakupów w Stanach Zjednoczonych, trzeba pamiętać, że zwroty nawet artykułów nieuszkodzonych i pełnowartościowych są z reguły niedopuszczalne. W razie problemów z reklamacją, należy zgłosić się do Europejskiego Centrum Konsumenckiego.

Uwaga!

Informacje na temat sposobu rozwiązywania konsumenckich sporów transgranicznych można znaleźć na stronie internetowej www.konsument.gov.pl lub pod warszawskim numerem infolinii - 22 55 60 474. Poszkodowani konsumenci mogą również osobiście składać skargi - ECK mieści się w budynku Urzędu Ochrony Konkurencji i Konsumentów w Warszawie, pl. Powstańców Warszawy 1.

Jak reklamować towary niezgodne z umową?

Każdy internauta może reklamować towar niezgodny z umową w terminie **dwóch lat od jego zakupu.** W piśmie reklamacyjnym można żądać:

- naprawienia rzeczy,
- wymiany jej na nową,
- obniżenia ceny lub
- zwrotu pieniędzy.

Uwaga!

Reklamacja, w przeciwieństwie do gwarancji, jest uprawnieniem przysługującym kupującemu z mocy prawa. Oznacza to, że kupujący może reklamować niezgodny z umową towar niezależnie od tego, czy sprzedawca mu przyznaje taką możliwość czy też nie.

W przypadku złożenia przez kupującego zastrzeżeń do zakupionego towaru sprzedawca ma **obowiązek rozpatrzenia reklamacji w ciągu**

14 dni. Jeżeli tego nie zrobi, uznaje się, że reklamacja została uwzględniona według żądania klienta. Konsument, składając reklamację, powinien **powołać się na taką niezgodność** zakupionego towaru z umową, która może spowodować, że rzecz nie nadaje się do celu, do jakiego jest zwykle używana, lub nie ma właściwości, jakie powinny ją cechować.

Przy roszczeniach wynikających z niezgodności towaru z umową sprzedawca odpowiada za wadę towaru **jedynie w razie stwierdzenia jej przed upływem dwóch lat od wydania rzeczy kupującemu**. Gdyby klient kupił rzecz używaną, to konsument i sprzedawca mogą ustalić krótszy termin, jednak musi być **co najmniej roczny**.

Zawsze jednak konsument ma obowiązek złożenia reklamacji **w ciągu dwóch miesięcy od dnia wykrycia wady.** Mimo upływu ustawowych terminów, w jakich należało zgłosić reklamację, klient może dochodzić swoich praw związanych z nabyciem wadliwego towaru, jeżeli sprzedawca **wiedział o wadzie w chwili zawarcia umowy i nie zwrócił na to uwagi kupującego.**

Należy jednak pamiętać, że sprzedawca internetowy nie odpowiada za niezgodność towaru konsumpcyjnego z umową, gdy kupujący w chwili zawarcia umowy o tej niezgodności **wiedział lub, oceniając rozsądnie, powinien był wiedzieć**. To samo odnosi się do niezgodności, która wynikła z przyczyny tkwiącej w materiale dostarczonym przez kupującego.

Sprzedawca, u którego kupujący złożył reklamację, ma obowiązek wykonania takich **działań, jakich żądał klient**, nawet jeżeli w rzeczywistości nie były one uzasadnione. Jeżeli zatem klient żądał od razu zwrotu pieniędzy, a towar można było naprawić, ale sprzedawca nie uczynił tego w terminie 14 dni, to powinien on zwrócić klientowi pieniądze za wadliwy towar. Jeżeli zgłoszenie reklamacyjne zostanie rozpatrzone odmownie, konsument ma prawo **wystąpienia ze sprawą do polubownego sądu konsumenckiego**. Może on również złożyć **pozew do sądu powszechnego**.

Przykład

Pan Marcin kupił w sklepie internetowym nowy zegarek reklamowany przez sprzedawcę jako wodoodporny. Jednak od razu po zanurzeniu w wodzie zegarek się zepsuł. Pan Marcin nie wie co ma w takiej sytuacji zrobić.

Otóż, w ciągu dwóch miesięcy od momentu, w którym Pan Marcin zorientował się, że zegarek nie jest wodoodporny, powinien on złożyć reklamację do sprzedawcy powołując się na niezgodność zakupionego towaru z umową. Może przy tym wedle własnego uznania żądać naprawienia rzeczy, wymiany jej na nową, obniżenia ceny lub zwrotu pieniędzy. Jeśli sprzedawca rozpatrzy reklamację odmownie, Pan Marek może wystąpić ze sprawą do polubownego sądu konsumenckiego lub złożyć pozew do sądu powszechnego.

Kiedy można dochodzić uprawnień z gwarancji?

Gwarancja jest ustanawiana w drodze **dobrowolnej umowy** bądź oświadczenia dotyczącego umowy sprzedaży. Stanowi ona zatem wyłącznie dodatkowe uprawnienie uzyskiwane przez nabywcę od sprzedającego bądź producenta, który jednak **nie ma obowiązku jej wystawiania.**

Gwarancja ma służyć zapewnieniu **właściwej jakości towaru sprzedanego**. Z reguły gwarancja uprawnia nabywców do **żądania usunięcia wady rzeczy, bądź dostarczenia**

towaru bez wad. Zakres uprawnień z tytułu gwarancji zależy jednak każdorazowo od postanowień sprzedawcy czy producenta.

W praktyce najczęściej gwarancją objęte są przedmioty trwałego użytku, np. meble, samochody, sprzęt AGD i RTV czy komputery. Gwarancja jest oświadczeniem gwaranta, w którym określa on swoje obowiązki oraz uprawnienia kupującego, gdy właściwość sprzedanego towaru **nie odpowiada właściwości wskazanej w tym oświadczeniu**. Jeśli na nabyty przez klienta towar została udzielona gwarancja, to sprzedawca powinien wydać klientowi, wraz z towarem, dokument gwarancyjny. Najczęściej kupującemu przysługuje również prawo do nieodpłatnej naprawy w punktach serwisowych. Nieodpłatność naprawy oznacza, że sprzedawca powinien kupującemu zwrócić koszty demontażu, dostarczenia, robocizny, materiałów, a także ponownego zamontowania i uruchomienia rzeczy.

Uwaga na oszustwa i triki w cyberprzestrzeni

Przestrzeń internetowa stała się dla przestępców nowym miejscem, w którym istnieje możliwość łatwego oszukania konsumentów. Jak podaje serwis www.konsument.gov.pl do najbardziej popularnych trików zalicza się:

- **Ukryte adresy** - pseudo-przedsiębiorcy próbują sprzedawać towary lub usługi stosując anonimowe adresy poczty elektronicznej albo numery skrzynki pocztowej i utrudniają tym samym ustalenie ich aktualnej lokalizacji.
- **Atak za pośrednictwem haseł** – to ogłoszenia w rodzaju „TAJEMNICA GWARANTOWANEGO SUKCESU" albo „JAK ZAROBIĆ MILION", lecz te hasła w obcym języku nie zapewniają obiecywanego rezultatu.
- **Niejasne listy referencyjne, listy pochwalne** - „Tysiące usatysfakcjonowanych klientów!" - brzmi dumnie i robi wrażenie, ale rzadko jest to informacja, która pozwoli sprawdzić wiarygodność twierdzenia.
- **„To nie jest trik"/"This is not scam"** - nie należy dać się zwieść takim hasłom. Uczciwy biznes nie potrzebuje tego typu zapewnień.
- **Obietnice natychmiastowego bogactwa** - zwykle brzmią zbyt dobrze by być prawdziwymi.
- **Zapłać za ujawnienie sekretu** - czasem można spotkać w Internecie ofertę uzyskania sekretnej metody wzbogacenia się dla wybrańców. Tymczasem zwykle ofiarami tego wybiegu są tysiące użytkowników. Oszuści sugerują, że tajemnica ta jest dostępna za stosowną opłatą.
- **Ukryte wydatki** – należy uważać na ogłoszenia i reklamy obiecujące brak jakichkolwiek kosztów wstępnych, a następnie zwracających się o tylko jednorazową opłatę.
- **Testy usług** – zalecane jest sprawdzanie czy oferowana usługa testowa na kilka dni nieodpłatnie nie stanowi umowy, która przedłuży się automatycznie w drogą i niepotrzebną umowę.

Reasumując…

Polska jest wciąż daleko w tyle za pozostałymi krajami Unii Europejskiej pod względem ilości konsumentów kupujących za pośrednictwem Internetu. Jednak handel elektroniczny rozwija się w zawrotnie szybkim tempie i coraz mniej osób czuje strach przed „wirtualnymi" zakupami. Demitologizacja handlu internetowego musi jednak iść w parze ze świadomością realnych zagrożeń związanych z tego typu transakcjami. Konsumenci powinni wiedzieć, na co zwracać uwagę dokonując zakupów przez Internet i jakie kroki podjąć w przypadku nieuczciwości lub nierzetelności sprzedawcy.

Podstawy prawne

- Ustawa z 23 kwietnia 1964 r. - Kodeks cywilny (Dz.U. nr 16, poz. 93 z późn. zm.).
- Ustawa z 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. nr 22, poz. 271 z późn. zm.).
- Ustawa z 27 lipca 2002 r. o szczególnych warunkach sprzedaży konsumenckiej oraz o zmianie Kodeksu cywilnego (Dz.U. nr 141, poz. 1176 z późn. zm.).
- Ustawa z 12 czerwca 2003 r. - Prawo pocztowe (t.j. Dz.U. z 2008 r. nr 189, poz. 1159 z późn. zm.).
- Ustawa z 15 listopada 1984 r. - Prawo przewozowe (t.j. Dz.U. 2000 r. nr 50 poz. 601 z późn. zm.).
- Rozporządzenie ministra transportu i budownictwa z 24 lutego 2006 r. w sprawie ustalania stanu przesyłek oraz postępowania reklamacyjnego (Dz.U. nr 38, poz. 266).
- Rozporządzenie ministra infrastruktury z 13 października 2003 r. w sprawie reklamacji powszechnej usługi pocztowej w zakresie przesyłki rejestrowanej i przekazu pocztowego (Dz.U. nr 183, poz. 1795).

Katarzyna Czajkowska-Matosiuk - doktorantka na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, autorka kilkudziesięciu artykułów i podręczników prawniczych.

Zapraszamy do udziału

WARSZTATY

WYKONYWANIE FUNKCJI ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI

- poziom II

18 października 2012 r., Warszawa

Warsztat prowadzą:

Dr Grzegorz Sibiga (Instytut Nauk Prawnych PAN w Warszawie)
Łukasz Wrona (administrator bezpieczeństwa informacji, Krajowy Rejestr Długów Biura Informacji Gospodarczej S.A.)

Do kogo skierowane są warsztaty:

Warsztaty skierowane są do administratorów bezpieczeństwa informacji oraz innych osób odpowiedzialnych za ochronę danych osobowych w jednostkach organizacyjnych. Będą one również przydatne dla prawników zajmujących się sprawami ochrony danych osobowych (w tym prawników wewnętrznych) oraz osób, w których zakresie obowiązków pozostaje wykonywanie wymogów ochrony danych osobowych.

W szczególności warsztaty są przeznaczone dla osób posiadających doświadczenie w wykonywaniu obowiązków prawnej ochrony danych osobowych, w tym uczestników warsztatów ABI pierwszego stopnia.

Korzyści z uczestnictwa w warsztatach:

- Rozwiązanie podstawowych problemów związanych z wykonaniem obowiązków bezpieczeństwa technicznego i organizacyjnego w zakresie ochrony danych osobowych.
- Praktyczne wskazówki dotyczące opracowywania dokumentacji przetwarzania danych osobowych, następnie monitorowania jej przestrzegania.
- Omówienie aktualnych prawnych problemów przestrzegania przepisów o ochronie danych osobowych.
- Praktyczne przygotowanie do kontroli GIODO.

Więcej informacji: www.cpi.com.pl

Dystrybucja oprogramowania – modele, szanse i zagrożenia

Marcin Maruta

Wstęp

Oprogramowanie ewoluuje w szybkim tempie, biznes IT jeszcze szybciej, prawo – konserwatywnie – dostosowuje się do wymagań e-gospodarki powoli, czasami bardzo, bardzo powoli. W dystrybucji oprogramowania z jednej strony panuje wygodne status quo, znane i powszechnie stosowanie modele się umocniły, nauka i praktyka prawa wreszcie je przetrawiła i zrozumiała, łaskawy ustawodawca zniósł największe przeszkody (vide koszmar dylematu vat/brak vat-u od licencji), orzecznictwo też zadziałało zaskakująco korzystnie dla branży IT (vide podatek u źródła od importu oprogramowania, swoją drogą błędny wyrok/wyroki w mojej opinii). Z drugiej strony atakują nas wynalazki w postaci cloud computing czy modeli SaaS, które zmuszają do gruntownej rewizji nasze przemyślenia. Poniżej krótki przegląd najpopularniejszych modeli dystrybucji oprogramowania z autorskim komentarzem, na co uważać, a gdzie korzystać z dobrodziejstw poszczególnych rozwiązań.

Program - utwór czy nie utwór

Zacznijmy od uwagi zasadniczej – nie każdy kawałek software jest chroniony prawem autorskim. Choć w praktyce zakres prawa autorskiego jest olbrzymi (trudno się nie zgodzić z wieloma głosami, że zaczyna to zakrawać na absurd), cały czas obowiązuje nas przesłanka „twórczości" i „indywidualności". Upraszczając – jeżeli dane rozwiązanie informatyczne jest w danym środowisku i założeniach technicznych czy biznesowych jedynym możliwym do zrealizowania, czy – nie daj Boże – rozwiązaniem optymalnym, nie jest indywidualne, twórcze. Jeżeli dowolna grupa informatyków dany problem (np. akcyza od paliw płynnych w systemie SAP) rozwiązałaby podobnie, czy wręcz identycznie, mamy do czynienia z olbrzymim nakładem pracy analitycznej i programistycznej, ale nie autorskiej w rozumieniu przepisów. W przemyśle IT (poza grami i nielicznymi innymi wyjątkami) nikt nie żąda ani twórczości, ani indywidualności. W cenie jest poprawność, wydajność etc etc. To zresztą grzech pierworodny objęcia programów prawem autorskim i jedna z przyczyn, dlaczego tak mocno przemysł popiera opatentowanie oprogramowania.

Tak czy inaczej, na samym początku musimy się zastanowić, czy dany kawałek kodu jest twórczy i indywidualny – program tworzony od podstaw z reguły twórczy będzie, określony kod w ABAP-ie niekoniecznie. Jeżeli odmówić mu przesłanki indywidualności, ochrona autorska zostanie wyłączona i o ile producent nie zadbał o inny zakres ochrony (np. patent), kod ten będzie mógł być swobodnie wykorzystywany bez martwienia się o licencje. Jedno zastrzeżenie – powyższe to uwagi przede wszystkim dla producentów, użytkownikom zdecydowanie lepiej przyjąć założenie, że wszystko jest utworem i jest chronione. Obecny system jest zbyt restrykcyjny, żeby ryzykować spór, chyba, że nie mamy wyjścia (i tak nas pozwali) lub chcemy się zapisać jako twórcy precedensu w orzecznictwie polskim. Albo jesteśmy na 100% przekonani, że mamy rację.

Co wolno z programem czynić?

Jeżeli program podlega prawu autorskiemu (a tak jednak będzie prawie zawsze), musimy się zastanowić, co wolno nam z programem zrobić bez konieczności uzyskania zgody

twórcy. I niestety, odpowiedź brzmi, że niewiele – dozwolony użytek jest w większości wyłączony, mamy na pocieszenie pewne uprawnienia „bezwzględne" czyli art. 75 ust.2 prawa autorskiego (prawo do kopii zapasowej, badania programu, dekompilacji). Uprawnienie te są jednak obwarowane, co więcej i tak wymagają legalnego wejścia w posiadanie kopii danego programu – jedyna dla użytkownika korzyść, że autor programu nie może wyłączyć opisanych tam uprawnień (przynajmniej teoretycznie, vide DRM). W praktyce, aby skorzystać z programu musimy mieć prawa majątkowe lub licencję (lub inną umowę w połączeniu z art. 75 ust. 1, ale ten wątek pomijam jako rzadko spotykany w biznesie). Chyba że zastanowimy się nad SaaS, ale to później.

Co kontroluje twórca (uprawniony)?

Prawa majątkowe (osobiste de facto nie istnieją, poza autorstwem i prawem oznaczenia utworu nazwiskiem lub pseudonimem) do programu obejmują trzy grupy czynności – zwielokrotnianie kodu (także w pamięci operacyjnej), jego modyfikację oraz rozpowszechnianie. Gdyby znaleźć sposób na korzystanie z programu, który nie wkraczałby w jedną z tych trzech grup, nie wymagałbym on zezwolenia. W praktyce póki co, jednak zezwolenie jest potrzebne. Możemy go uzyskać albo nabywając autorskie prawa majątkowe (rzadkość) albo licencje (częściej). Prawa te możemy nabyć zarówno od podmiotu mającego te prawa (autor, producent), albo do dystrybutora.

Relacje bezpośrednie producent – użytkownik

Są one dość rzadkie, choć w dużych przetargach spotykane, zwłaszcza w przypadku polskich firm informatycznych bezpośrednio składających oferty. Zaletą tego modelu jest bezpośrednia relacja i możliwość negocjowania warunków umowy, w tym rozwiązań mniej typowych, jako sprzedaż praw czy udziału w prawie. Tutaj jedna dość ważna uwaga – trochę wzorem rynku publicznego wzięło się przekonanie o bezwzględnej „wyższości" nabycia praw nad licencjami. Ta „wyższość" faktycznie występuje, ale z reguły nie tam, gdzie się sądzi – przede wszystkim ZAKRES korzystania z oprogramowania jest niezależny od typu umowy – licencja może pozwalać na więcej niż nabycie praw (choć zgoda, to rzadki przypadek, ale dobrze ilustrujący tezę – jeśli priorytetem jest określenie uprawnień, nie ma znaczenia który model zastosujemy). Licencja jest „gorsza" głównie dlatego, że można ją wypowiedzieć – można też się przed tym chronić. Bardzo dobrze napisana umowa licencyjna nigdy nam nie da aż takiej pewności, jak nabycie praw, ale da nam z reguły rozsądne bezpieczeństwo prawne. Nie zawsze jest potrzeba walki o te prawa i potrzeba ta powinna wypływać głównie z założeń biznesowych – np. niechęć do dalszego rozpowszechniania software u konkurencji, czy nakłady na stworzenie danej modyfikacji / rozszerzenia – bywa tak, że to klient daje cały know how i zwyczajnie nie chce by producent wersji podstawowej korzystał z opracowanego w wyniku współpracy rozwiązania, gdyż wycenia know how wyżej niż kod. Czasami wynika to z potrzeby ultra bezpieczeństwa – np. systemy bankowe czy energetyczne – nikt nie zamierza zastanawiać się nad możliwością wygaśnięcia/wypowiedzenia licencji – system jest zbyt ważny by ryzykować. Wtedy faktycznie prawa lepiej kupić.

Model ten – pomijając same rozwiązania kontraktowe – jest w swojej istocie prosty, możemy umówić się na co chcemy. Jeżeli to duża transakcja (np. jeden producent kupuje rozwiązania drugiego), warto zrobić audyt, czy aby na pewno ten co sprzedaje, ma prawa do kodu. Z chęci oszczędzenia na ZUS i tym podobnych, wielu producentów zawiera pełne błędów i braków „umowy o dzieło", na mocy których prawa na nich nie przechodzą. Ale to inny temat.

Podsumowując – model stosunkowo rzadko spotykany, ale umożliwiający szerokie negocjacje łącznie z nabyciem praw majątkowych do rozwiązania lub części rozwiązania (modyfikacje). Treść licencji jest ograniczona tylko przepisami i wyobraźnią negocjatorów.

Pośrednictwo

Bardzo często spotykany model, np. w przypadku licencji Microsoft. Użytkownik negocjuje i otrzymuje faktury od pośrednika (resellera, wskazanego agenta, dystrybutora, jak zwał, tak zwał), ale umowę licencyjną zawiera bezpośrednio z producentem. Tylko producent może mu te warunki zmienić, ale ewentualne roszczenia też tylko do producenta.

Model popularny, bo producent zachowuje olbrzymią kontrolę nad swoją siecią. Model ten stosowany jest przede wszystkim w przypadku rozwiązań standardowych, w których i tak nie negocjuje się warunków – można je przyjąć, albo nie. Czasami przy dużych umowach, takie negocjacje są możliwe i wtedy warto zwrócić uwagę, czy pośrednik – jeśli to on negocjuje, a zazwyczaj tak - ma prawa do zmiany warunków licencji. Nikt tyle nie obieca, co skuszony wizją lukratywnego kontraktu dystrybutor. Sęk w tym, że zmiany niepotwierdzone przez producenta są nieskuteczne i użytkownik zawsze naraża się na roszczenia za naruszenie licencji. Oczywiście z reguły będzie miał z kolei roszczenia do pośrednika, ale to bezsensowna walka prawna. Warto więc te uprawnienia sprawdzić.

Na marginesie – w dobie cyfryzacji, model ten zaczyna zyskiwać na znaczeniu do tego stopnia, że to pośrednik narzuca warunki gry i producentowi i użytkownikowi – vide appstore.

Sublicencje

Model częsty przy dużym oprogramowaniu aplikacyjnym, jak systemy ERP – tak działa m.in. SAP. Producent, dajmy na to amerykański, upoważnia poszczególnych dystrybutorów w różnych krajach (często są to jego oddziały) do udzielania licencji na jego software. Klient podpisuje umowę licencyjną (a precyzyjnie sublicencyjną, choć to określenie doktrynalne, nie ma go w ustawie) z dystrybutorem i to dystrybutor jest licencjodawcą – może np. licencję wypowiedzieć. Często dystrybutor na dany kraj ma prawo udzielania dalszych licencji innym dystrybutorom i powstaje nam cały ciąg licencji i sublicencji. Model sublicencyjny powoduje powstanie ciągu licencji i sublicencji, każda z nich jest „pełnoprawną" licencją, która może być np. amortyzowana (niezłe rozwiązanie dla grup kapitałowych).

W modelu tym użytkownik negocjuje bezpośrednio z sublicenjodawcą, czyli stroną umowy – w modelu poprzednim negocjacje z pośrednikiem, to tylko negocjacje z „przekaźnikiem". Nie zmienia to faktu, że sublicencjodawca musi mieć prawo do zmiany warunków licencji dla użytkownika – tak więc z tego punktu widzenia oba modele są podobne, i tak musi być zgoda producenta. Tyle, że znacznie częściej dystrybutor już z góry ma pewną swobodę przyznaną mu na mocy kontraktu dystrybutorskiego.

W praktyce dla pojedynczego użytkownika końcowego nie ma de facto znaczenia, w którym modelu nabywa licencję – i tak warunki są narzucane przez producenta, a negocjowanie ich wymaga upoważnienia dla dystrybutora. Różnice mogą pojawić się w modelach biznesowych (np. jeśli klient nabywa prawo do dalszego sublicencjonowania dla spółek zależnych), pojawia się też ryzyko prawne, wygaśnięcia sublicencji z momentem wygaśnięcia licencji. To dłuższy wywód, do końca w chwili obecnej nierozstrzygnięty, ale takie ryzyko istnieje. Swoją drogą pojawia się ono też przy sprzedaży praw – pytanie czy licencje „przechodzą" na nabywcę czy wygasają.

Są głosy i za jednym i za drugim, co ciekawe w praktyce, mimo że takie sytuacje miały miejsce, sporów wielkich nie było.

Sprzedaż licencji

Model do tej pory rzadki i stosowany raczej okazjonalnie, a nie będący dystrybucją w znaczeniu ścisłym. Polega on na przenoszeniu istniejących prawa z licencji na nowy podmiot, przy jednoczesnej rezygnacji z używania tej licencji – najprostszy przykład to sprzedaż notebooka z systemem operacyjnym. Model ten bywa stosowany w grupach kapitałowych do zarządzania portfolio licencyjnym.

Dużo zamieszania może przynieść świeżutki wyrok Trybunału Sprawiedliwości w sprawie C-128/11 UsedSoft GmbH vs Oracle International Corp. Wyrok jest bardzo ciekawy i dla wielu prawników szokujący, choć pewnie zgodny z tzw. poczuciem sprawiedliwości - Trybunał stwierdził w nim, że można „handlować używanymi licencjami" do oprogramowania pobieranego z sieci – jednym słowem, zapisy standardowych licencji (w tym przypadku Oracle) zabraniające takich praktyk są nieskuteczne. To może otworzyć wtórny rynek handlu licencjami i bardzo zdynamizować ten model quasi-dystrybucji.

SaaS

Zdecydowanie najwięcej emocji i wątpliwości prawnych budzą rozwiązania SaaS. Jeżeli pomyślimy o nich jako modelu usługowym, polegającym na udostępnieniu software, ale bez zawierania umów licencyjnych, narzucają się nam co najmniej trzy koncepcje prawne co to jest: pierwsza bazuje na tezie, że w modelu SaaS w ogóle nie dochodzi do zwielokrotnienia kodu. Znam informatyków co się z tym zgadzają i takich, co uważają to za bzdurę. Nie mnie się wypowiadać, ale jeśli faktycznie nie ma tam zwielokrotnienia, to wychodzimy z monopolu autorskiego i nie stosuje w ogóle prawa autorskiego, przechodzimy na czystą umowę usługową. Druga koncepcja (im dłużej nad nią myślę, tym bardziej mi się podoba) zakłada, że zwielokrotnienie jest, ale zwielokratniającym jest świadczący usługę, a nie użytkownik. Jeśli tak, to znów w relacji usługodawca – usługobiorca nie ma potrzeby stosowania konstrukcji licencyjnych, pozostaje sama usługa. Koncepcja trzecia (ciut pokraczna, ale chroniąca użytkownika, gdyby padły dwie poprzednie) przyznaje, że użytkownik zwielokrotnia kod, ale nie jako licencjobiorca (bo nie ma zawartej umowy licencyjnej), ale na mocy art. 75 ust.1 prawa autorskiego, jako „osoba, która legalnie weszła w posiadanie programu". Oczywiście istnieje ryzyko, że tak naprawdę SaaS to dorozumiana umowa licencyjna - moim zdaniem wykładnia błędna, ale spotykana. Tak naprawdę różnica usługa/licencja będzie miała przede wszystkim praktyczne znaczenie dla zasad księgowych i podatkowych czyli dylematy OPEX/CAPEX. Ma ona też znaczenie dla spółek zainteresowanych skorzystaniem z art. 136 prawa zamówień publicznych, gdyż SaaS byłby usługą, a licencja dostawcą, wykluczającą możliwość zastosowania tego artykułu.

W przypadku SaaS, jako instytucji stosunkowo młodej i łączącej w sobie kilka mechanizmów prawnych, potrzebujemy czasu, by ustabilizowały się poglądy na jej temat. Według mojej opinii jest to usługa, próba bronienia tego modelu na siłę, jako dorozumianej licencji - jest sprzeczna i z cechami tej usługi i z wolą stron.

Umowy SaaS są z reguły o wiele bardziej skomplikowane niż licencje – tu chodzi głównie o parametry usługi, jak systemy KPI i SLA, gwarantowane dostępności, kary umowne etc. Wymaga to więcej pracy, ale użytkownik otrzymuje wiele więcej, niż w wypadku samej licencji. Nie ulega dla mnie wątpliwości, ze ten model dystrybucji oprogramowania będzie przybierał na znaczeniu.

Dystrybucja oprogramowania w grupach kapitałowych

Grupy kapitałowe mają swoje potrzeby, które znajdują odzwierciedlenie w warunkach licencyjnych. Wersja minimum to mniej lub bardziej elastyczny mechanizm dystrybucji oprogramowania w grupie. Jest on uzależniony od kilku czynników, jak ilość podmiotów nabywających oprogramowanie (jeden centralny czy każda spółka z osobna), prawne mechanizmy przekazywania licencji (transfer licencji a sprzedaż licencji, sublicencje, wyłącznie możliwość przystąpienia do umowy grupowej), ograniczenia związane z wstępowaniem/występowaniem z grupy. Jest to fascynująca działka, gdyż umożliwia już na samym wstępie różne oszczędności i to na samym procesie scentralizowanego zakupu, ale też np. na możliwości CAPEX-owania modelu sublicencyjnego. A przy pzp – wejścia w tryb art. 136 pzp. Temat na odrębny artykuł.

Dystrybucja oprogramowania w reżimie prawa zamówień publicznych

Też temat rzeka, też na osobny artykuł. Warte uwagi są rekomendacje Prezesa Urzędu Zamówień Publicznych na temat nabywania systemów IT, choć w wielu miejscach bardzo rozsądne, to – być może wskutek mało szczęśliwej redakcji - narzucające, czy preferujące model nabywania praw zamiast licencji. Pomijając humorystyczne zapytania ofertowe (ile kosztowałyby prawa do oprogramowania Office), znów dyskusja zbacza z istoty problemu (zakres uprawnień, vendor lock-in) na kwestie formalne (jaka umowa). A na szczęście wciąż prawo to tylko mechanizm pomocniczy do implementacji założeń biznesowych – i źle się dzieje, kiedy owe potrzeby i założenia utożsamia się z jednym modelem prawnym.

Marcin Maruta - radca prawny, wspólnik w kancelarii radców prawnych Maruta i Wspólnicy Sp. j.

Zapraszamy do udziału

FORUM

INFORMACJE I TECHNOLOGIE W INSTYTUCJACH KULTURY

11 października 2012 r., Warszawa

Dwie dekady przemian technologicznych przełomu XX i XXI wieku przyniosły poza rozwojem metod cyfrowej dokumentacji także wiele refleksji nad kierunkiem rozwoju instytucji kultury. Wypowiedziane w 1964 roku przez Marshalla McLuhana zdanie *„The Medium is the Message"* (pochodzące z publikacji: *Understanding Media: The Extensions of Man*) odnoszone do teorii mediów, jest ważnym ostrzeżeniem dla instytucji zajmujących się dziedzictwem kultury i natury. Forma, metoda, technologia używanych mediów stopniowo zmieniają naszą percepcję, oczekiwania i rozumienie formy i znaczeń niesionych przez obiekty historyczne. Jak powinniśmy działać planując digitalizację dziedzictwa, jaki rodzaj informacji powinien towarzyszyć temu procesowi? Jakie możliwości i jakie zagrożenia dają nowe, szybko rozwijające się technologie?

Prowadzenie obrad: prof. dr hab. Dorota Folga-Januszewska (Uniwersytet Kardynała Stefana Wyszyńskiego, Instytut Muzeologii), dr Henryk Hollender (Uczelnia Łazarskiego).

W programie m.in.:

- Udostępnianie cyfrowych zasobów Kultury
- Bazy danych w kulturze
- Dematerializacja instytucji kultury. Oryginał obiektu czy wtórnik - przyszłość kolekcji muzealnych, bibliotecznych, archiwalnych
- Arena - portal biblioteczny 2.0
- Odtwarzanie dawnych obiektów kultury na podstawie zachowanych danych i źródeł archiwalnych
- Przyszłość tradycyjnego tekstu w nauce i kulturze
- Priorytety digitalizacji obiektów kultury i dziedzictwa narodowego

Więcej informacji: www.cpi-sk.pl

Podpis elektroniczny - nowa regulacja

Michał Tabor

Od blisko roku Komisja Europejska informowała o postępujących pracach nad zmianami w dyrektywie 1999/93/EC[1] Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie Wspólnotowej struktury dla elektronicznych podpisów. W pierwszych dniach czerwca br. przedstawiono propozycję nowych przepisów[2], którą w kilku zwięzłych punktach omówię poniżej.

1. Dyrektywę zastąpi rozporządzenie (ang. regulation) – czyli akt prawny obowiązujący w całej unii i nie wymagający implementacji w prawie krajowym. To znaczy, że nie będzie potrzeby tworzenia własnej ustawy o podpisie elektronicznym – a rozporządzenie będzie stosowane bezpośrednio i na jego podstawie będzie działała polska administracja i polskie sądy. Takie działanie ma swoje głębokie uzasadnienie, ponieważ dotychczasowa dyrektywa doczekała się wielu różnych interpretacji, a co za tym idzie wielu różnych implementacji w przepisach wszystkich członków unii. Brak jednolitego rozumienia przepisów traktujących o podpisie elektronicznym wskazywano jako jeden z podstawowych powodów braku interoperacyjności w obszarze wymiany dokumentów elektronicznych w UE.
2. Treścią rozporządzenia nie jest sam podpis elektroniczny – już sam tytuł wskazuje, że rozporządzenie ma znacznie szerszy zakres: identyfikacja elektroniczna i usługi zaufania. Rozporządzenie to wskazuje kilka nowych mechanizmów związanych z zaufaniem do transakcji elektronicznych, wśród nich jest pieczęć elektroniczna, elektroniczny znacznik czasu, usługa przekazu elektronicznego oraz kwalifikowany certyfikat witryn internetowych.
3. Rozporządzenie nie zamyka katalogu usług zaufania, umożliwiając tworzenie nowych usług zaufania, jednak nie wskazuje mechanizmów jakimi będzie można budować takie usługi.
4. Bardzo ważnym wskazaniem w rozporządzeniu jest przypisanie podpisu elektronicznego jedynie osobie fizycznej. O ile w polskiej ustawie tak właśnie był zdefiniowany podpis elektroniczny, o tyle w innych krajach podpisem mogły posługiwać się osoby prawne oraz inne jednostki niebędące osobami fizycznymi i osobami prawnymi. Dla osób prawnych (i ew. takich, które nie mają osobowości prawnej – ang. legal person) rozporządzenie wprowadza elektroniczną pieczęć/znak (ang. electronic seal).
5. Zostały zdefiniowane 3 rodzaje podpisu elektronicznego – podpis elektroniczny, zaawansowany podpis elektroniczny

1 Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ, uwzględniając Traktat ustanawiający Wspólnotę Europejską - http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

2 Projekt rozporządzenia parlamentu europejskiego I rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (COM/2012/0238) http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=EN&type_doc=COMfinal&an_doc=2012&nu_doc=238

i kwalifikowany podpis elektroniczny. Same definicje ujednolicają w tym zakresie rynek podpisów – co spowoduje, że będą one tak samo interpretowane w całej unii. O tym jak różne były dotychczas interpretacje dyrektywy świadczy fakt, że w Polsce nie został dotychczas zaimplementowany zaawansowany podpis elektroniczny, który w tej dyrektywie występował. Znaczenie podpisu kwalifikowanego pozostaje takie jak dotychczas, natomiast duże wątpliwości budzi definicja samego podpisu elektronicznego (podpisu zwykłego), która może ograniczać stosowanie podpisu tylko do oświadczeń woli. Dotychczas podpis elektroniczny mógł służyć do potwierdzenia integralności lub autentyczności komunikatu lub dokumentu (np. maila) – to rozporządzenie wyklucza taką możliwość.

6. Znak elektroniczny (ang. elektronic seal) – w polskim tłumaczeniu występuje jako pieczęć elektroniczna – jest to nowe narzędzie, przeznaczone dla podmiotów nie będących osobami fizycznymi i służącym do potwierdzania źródła pochodzenia i integralności. Narzędzie to dotychczas w polskim porządku prawnym było stosowane do Urzędowego Potwierdzenia Odbioru przez skrzynki podawcze, podpisywania wzorów na ePUAP oraz zabezpieczania podpisu potwierdzonego profilem zaufanym. Jego głównym zastosowaniem będzie automatyczne potwierdzanie danych z rejestrów, danych z systemów księgowych lub odpisów z systemów zarządzania dokumentami. Znak elektroniczny nie niesie za sobą oświadczenia woli (zobowiązania) podmiotu, który się nim posługuje, służy raczej do potwierdzenia stanu, zabezpieczenia procesu, wskazania źródła, zapewnienia integralności.
7. Całkowicie nową jest usługa przekazu elektronicznego, która ma zapewnić potwierdzenie nadania lub otrzymania dokumentów elektronicznych. Określenie wymagań dla tej usługi stanowi podstawę do możliwości świadczenia jej przez podmioty zewnętrzne, realizacji wymiany w oparciu o opracowywane standardy elektronicznej poczty rejestrowanej (registred mail), oraz zastosowanie tego mechanizmu poza obszarem administracji publicznej.
8. Przepisy polskie przypisywały znacznikowi czasu znaczenie daty pewnej, co samo w sobie stanowiło spory problem prawno-techniczny. Nowe rozporządzenie definiuje czym jest znacznik czasu i jaką niesie wartość dowodową.
9. Wszystkie 4 wymienione powyżej usługi, tj. podpis elektroniczny, pieczęć elektroniczna, przekaz elektroniczny oraz znacznik czasu, mogą występować jako usługa kwalifikowana, czyli taka, która podlega szczególnej kontroli, musi być uznawana przez administracje krajów UE.
10. Rozporządzenie wprowadza pojęcie Identyfikacji Elektronicznej – czyli mechanizmu, który ma umożliwiać osobom prawnym i fizycznym dostęp do systemów administracji publicznej w oparciu o wydawane im identyfikatory. Najważniejszy jest fakt, że każdy kraj członkowski musi udostępnić przynajmniej jeden system identyfikacji elektronicznej oraz musi akceptować wszystkie notyfikowane systemy identyfikacji elektronicznej z Unii Europejskiej. Na uwagę zasługuje fakt, że systemy identyfikacji będą musiały być udostępnione do wykorzystania przez podmioty komercyjne, a odpowiedzialność za prawidłowość udostępnianych identyfikatorów bierze na siebie kraj, który ten identyfikator wydał.
11. Ostatnim mechanizmem opisanym w rozporządzaniu jest kwalifikowany certyfikat uwierzytelniania witryn internetowych, który ma umożliwiać zbudowanie europejskiej sieci zaufania do witryn internetowych. Mechanizm ciekawy, ale idzie wspak dotychczas stosowanym metodom, opartym o dostawców przeglądarek internetowych.
12. Niezależnie od usług elektronicznych Komisja Europejska postanowiła w niniejszym rozporządzeniu zrównać dokument elektroniczny

z dokumentem papierowym uznając jego za równoważny i dopuszczalny w postępowaniu sądowym. Jest to o tyle ważny fakt, że cały czas spotykamy się z sytuacjami, gdzie dokument elektroniczny jest uznawany za gorszy i niewystarczający w różnego rodzaju postępowaniach administracyjnych lub sądowych.

Rozpoczyna się aktualnie faza negocjacji proponowanego aktu. Ministerstwo Gospodarki przygotowało polskie stanowisko negocjacyjne. W stanowisku tym strona polska popiera inicjatywę, wskazuje, że będzie to ważne uregulowanie rynku. Zwraca uwagę na konieczność poprawienia definicji podpisu elektronicznego oraz problemy w tłumaczeniu i różnym rozumieniu niektórych pojęć. Ważnym elementem implementacji rozporządzenia w polskim porządku prawnym jest występowanie podmiotów nieposiadających osobowości prawnej, które będą korzystały z mechanizmu pieczęci elektronicznej.

Projekt rozporządzenia jest bardzo ciekawy i wskazuje nowy kierunek, gdzie usługi będą udzielane w oparciu o identyfikatory związane z dokumentami tożsamości, a świat komercyjny będzie mógł korzystać ze struktury zaufania zbudowanej na potrzeby administracji publicznej. Projekt wymaga jeszcze prac i doszlifowania kilku kwestii, ale dla rynku bardzo ważne jest, aby jak najszybciej stał się obowiązującym prawem.

Michał Tabor - ekspert w dziedzinie podpisu elektronicznego i zarządzania bezpieczeństwem informacji, autor rozwiązania składania deklaracji PIT bez podpisu, autor koncepcji profilu zaufanego ePUAP. Dyrektor ds. operacyjnych Trusted Information Consulting sp. z o.o.

Zapraszamy do udziału

SEMINARIUM

BEZPIECZNA TELEFONIA W BIZNESIE - UWARUNKOWANIA PRAWNE I TECHNOLOGICZNE

3 października 2012 r., Warszawa

Rozwój globalnej sieci Internet pozwolił na dynamiczne rozszerzenie zakresu i terytorium działalności wielu firm. Korzystanie z urządzeń mobilnych powoduje stały kontakt z kontrahentami i pracownikami w dowolnym miejscu na świecie a co za tym idzie przyspieszenie podejmowania decyzji. Dzięki wykorzystaniu protokołu IP i sieci radiowych oraz budowie coraz mniejszych (a jednocześnie pojemniejszych) urządzeń przenośnych, współczesny biznes zyskał nowy, lepszy wymiar, a praca stała się wygodniejsza i efektywniejsza. - Równocześnie z nowymi funkcjonalnościami, pojawiły się jednak także zagrożenia... Pierwszy „trojan" zaatakował telefony komórkowe w 2006r. Świadomość niebezpieczeństw potencjalnie zagrażających komunikacji i zdalnemu przesyłaniu danych, nie powinna zniechęcać do ich stosowania, a jedynie zmotywować do wdrożenia narzędzi i procedur, które skutecznie je zabezpieczą.

Zapraszamy do udziału w seminarium poświęconemu bezpiecznym kontaktom mobilnym w biznesie. Podczas seminarium dowiedzą się Państwo o najczęściej stosowanych metodach wywiadu gospodarczego i atakach socjotechnicznych. W jaki sposób należy „dbać„ o telefon komórkowy - główny nośnik tajemnic biznesowych. Jakie są zagrożenia podsłuchem oraz w jaki sposób szyfrować rozmowy telefoniczne na urządzeniach mobilnych. Poruszone zostaną aspekty techniczne i bezpieczeństwo dostępnych komunikatorów oraz audyt bezpieczeństwa informacji urządzeń mobilnych. Dowiedzą się Państwo jaka jest praktyka sądowa spraw związanych z bezpieczeństwem biznesowym.

Więcej informacji: www.cpi.com.pl

Nowa unijna regulacja w zakresie danych osobowych – uwagi na temat projektu rozporządzenia z dnia 25 stycznia 2012 r. (część II)

Damian Karwala

Opublikowany 25 stycznia 2012 r. projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych; dalej również jako „Projekt Rozporządzenia" lub „Projekt[1]"), stanowi podstawowy element mający tworzyć nowe ramy prawne w zakresie ochrony danych osobowych w Unii Europejskiej. Projekt ten, po jego przyjęciu, zastąpić ma Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2], a jego znaczenie wyraża się nie tylko w samej treści proponowanych zmian, czy też ich skali, lecz – przede wszystkim – w zupełnie nowym podejściu do regulacji tej problematyki w ramach UE. Stąd też nieprzypadkowo w dokumentach Komisji Europejskiej mowa o „gruntownej reformie" unijnego prawa dotyczącego ochrony danych osobowych[3], a w doktrynie europejskiej nawet o swoistej „rewolucji kopernikańskiej" w tym zakresie[4].

Niniejsza publikacja omawia najważniejsze zmiany, jakie przewiduje Projekt Rozporządzenia, odrębnie dla kolejnych jego rozdziałów. Z uwagi na obszerność regulacji, skoncentrowano się na kluczowych zmianach i propozycjach.

Przepisy ogólne (Rozdział I)

Wyznaczając zakres przedmiotowy nowej regulacji wskazano, że będzie ona miała zastosowanie do przetwarzania danych osobowych, w sposób w całości lub w części zautomatyzowany, jak również do innych operacji przetwarzania danych osobowych, w sytuacji, gdy stanowią one lub mają stanowić część zbioru danych (art. 2 ust. 1 Projektu). Rozszerzeniu – w porównaniu z przepisami Dyrektywy – uległ katalog wyłączeń (art. 2 ust. 2), spośród których na uwagę zasługuje wyłączenie dotyczące „**działań o charakterze czysto osobistym lub domowym**". Podjęto w tym zakresie próbę doprecyzowania oraz pewnego ograniczenia tej przesłanki, która na gruncie Dyrektywy budziła wątpliwości, w szczególności w kontekście przetwarzania danych w ramach serwisów społecznościowych[5]. Wątpliwe jest jednak, czy próba ta okaże się skuteczna. W szczególności zwrócić należy uwagę, iż

1 COM(2012) 11 final; projekt dostępny pod adresem http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

2 Dz. U. UE L nr 281, s. 31 z 23.11.1995 r., zwana dalej również jako „Dyrektywa" lub „Dyrektywa 95/46/WE".

3 *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku (COM(2012)* 9 final, s. 3.

4 Ch. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Bloomberg BNA. Privacy & Security Law Review, 11 PVLR 06, 2012, s. 14.

5 Dokument Grupy Roboczej Art. 29 Dyrektywy, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (WP168 z 1.12.2009 r.), pkt. 71, s. 18.

wersja wstępna Projektu (z listopada 2011 r.) przewidywała dodatkowe ograniczenie, zastrzegając, iż wyłączenie to nie powinno znajdować zastosowania w sytuacji, gdy „dane dotyczące innej osoby fizycznej są udostępniane nieograniczonej liczbie jednostek" (w wersji Projektu z 25.01.2012 r. doprecyzowania tego nie wprowadzono nawet do preambuły, gdzie – jak się wydaje – powinno być jej miejsce).

Projekt Rozporządzenia przewiduje daleko idące zmiany w zakresie zasad **stosowania unijnych przepisów w stosunku do podmiotów spoza Unii Europejskiej** (art. 3 ust. 2). Dotychczasowa przesłanka wykorzystania środków znajdujących się na terytorium UE (art. 4 ust. 1 lit. c Dyrektywy) zastąpiona ma zostać przesłanką „oferowania towarów lub usług" podmiotom danych z UE lub „monitorowania ich zachowania". Jak prognozuje się, efektem tych zmian będzie objęcie unijnymi przepisami większej liczby podmiotów oferujących usługi w Internecie, mających siedzibę poza UE[6]. Wątpliwości na gruncie tej propozycji budzi jednak w szczególności, co należy rozumieć po pojęciem „monitorowanie zachowania". Pewnych wskazówek udziela tu pkt 21 preambuły, zgodnie z którym „aby stwierdzić, czy przetwarzanie można uznać za „monitorowanie zachowania" podmiotów danych, należy upewnić się, czy osoby fizyczne można wyszukać w internecie, korzystając z technik przetwarzania danych, które polegają na przypisaniu „profilu" danej osobie fizycznej, w szczególności w celu podejmowania decyzji dotyczących tej osoby, analizowania jej preferencji osobistych, zachowań i postaw lub ich przewidywania". Ponadto, zakres zastosowania art. 3 ust. 2 Projektu ograniczono wyłącznie do podmiotów danych mających miejsce zamieszkania w Unii, co wydaje się stać w sprzeczności z deklaracjami projektodawcy unijnego, zgodnie z którymi „ochrona zapewniona na mocy niniejszego rozporządzenia dotyczy osób fizycznych, niezależnie od ich obywatelstwa lub miejsca zamieszkania" (tak pkt 12 oraz pkt 2 preambuły). Podstawowa trudność w tym zakresie związana jest jednak z praktycznym stosowaniem przepisu art. 3 ust. 2 w stosunku do podmiotów, które nie podlagają jurysdykcji państw unijnych[7].

Zmiany dotyczą również definicji (art. 4 Projektu), w tym tak istotnych, jak **definicja danych osobowych**, którą to definicję objęto ramami definicji „podmiotu danych"; samo zaś pojęcie „danych osobowych" ograniczono do wskazania, iż obejmuje ono „wszelkie informacje dotyczące podmiotu danych" (art. 4 pkt 1 w zw. z pkt 2 Projektu). W zmodyfikowanej definicji uwzględniono przesłankę „środków, które z rozsądnym prawdopodobieństwem mogą być użyte" dla celów identyfikacji (ang. *means reasonably likey to be used*), co jak się wydaje pozwalało będzie na pewne „uelastycznienie" tej kluczowej dla całej regulacji instytucji (element „prawdopodobieństwa", w dodatku „rozsądnego"). Wątpliwości budzić może nadal przetwarzanie takich rodzajów danych, jak np. numery IP, czy tzw. „ciasteczka" (ang. *cookies*): z jednej bowiem strony w pkt. 24 preambuły wskazano, że tego rodzaju dane niekoniecznie muszą być traktowane jako dane osobowe, z drugiej jednak strony – w art. 4 pkt 1 Projektu – wyraźnie odniesiono się do

6 Ch. Kuner, *The European Commission's Proposed Data Protection Regulation*..., s. 3.

7 Zwraca na to uwagę brytyjski organ ochrony danych, w dokumencie *Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework* (27.02.2012, dostępny na stronie internetowej organu www.ico.gov.uk), podkreślając, że „Rozporządzenie powinno być w tym zakresie realistyczne i nie powinno sprawiać u konsumentów wrażenia, że prawo oferuje im ochronę, gdy w rzeczywistości nie jest im jej w stanie zapewnić" (s. 5).

identyfikatorów internetowych, jako czynników umożliwiających identyfikację osoby. Skutkować to może różnicami w traktowaniu tego rodzaju danych w poszczególnych Państwach Członkowskich, a tym samym w stosowaniu (lub nie) projektowanej regulacji do określonych stanów faktycznych.

Istotne zmiany w stosunku do Dyrektywy 95/46/WE przewidziano w zakresie **definicji zgody** (art. 4 pkt 8 Projektu), jako podstawy przetwarzania danych osobowych, zastrzegając iż musi być ona wyrażona w sposób wyraźny (ang. *explicit indication of his or her wishes*)[8]. Projektowane ograniczenie konstrukcji zgody do modelu *opt-in* przeprowadzono jednakże w sposób nie pozbawiony wątpliwości. W dalszym fragmencie definicji, jak również w pkt 25 preambuły zastrzeżono bowiem, że zgoda może zostać wyrażona „w drodze wyraźnego działania potwierdzającego podmiotu danych" (ang. *clear affirmative action by the data subject*), co może sugerować, iż pewne elementy modelu *opt-out* nadal będą możliwe do zastosowania.

Projekt wprowadza również liczne **nowe definicje**, m.in. pojęcia „naruszenia ochrony danych osobowych", „danych genetycznych", „danych biometrycznych", „danych dotyczących zdrowia", „wiążących reguł korporacyjnych", czy „głównej siedziby" – która to definicja będzie miała kluczowe znaczenie w kontekście stosowania przepisów nowej regulacji (por. dalsze uwagi w tym zakresie).

Zasady (Rozdział II)

Projekt zmierza do **wzmocnienia zasad ochrony danych osobowych** (art. 5), w szczególności podkreślono w nim: znaczenie zasady transparentności („przejrzystości", ang. *transparency*, art. 5 lit. a); konieczność ograniczenia przetwarzania danych „do minimum", zarówno co do zakresu, jak i ilości przetwarzanych danych (ang. *data minimization*, art. 5 lit. c); potrzebę wykonywania okresowej kontroli w zakresie konieczności dalszego przechowywania danych (art. 5 lit. e); zasadę odpowiedzialności administratora danych, który „zapewnia i wykazuje zgodność każdej operacji przetwarzania z przepisami" (ang. *accountability principle*, art. 5 lit. f); wskazano również wyraźnie na brak obowiązku pozyskiwania dodatkowych informacji w celu identyfikacji podmiotu danych, w sytuacji, gdy miałoby to odbywać się wyłącznie dla celów wypełnienia obowiązku wynikającego z rozporządzenia (art. 10 Projektu).

Zmiany widoczne są również w zakresie **podstaw przetwarzania danych** (art. 6 Projektu). W szczególności podkreślono, że usprawiedliwione cele („słuszne interesy" – jak zaproponowano w oficjalnym tłumaczeniu Projektu; ang. *legitimate interests*) nie mogą stanowić podstawy przetwarzania danych przez organy publiczne w zakresie wykonywanych przez nie zadań (art. 6 ust. 1 lit. f *in fine*). W sposób wyraźny zastrzeżono również, że „obowiązek prawny" lub „interes publiczny" – o których mowa w art. 6 ust. 1 lit. c oraz e – mogą wynikać wyłącznie z prawa UE lub prawa państw członkowskich (art. 6 ust. 3), tym samym dążąc do usunięcia wcześniejszych wątpliwości, co do możliwości powoływania się w tym zakresie na przepisy prawa państw trzecich. Wskazano również, że zmiana celu przetwarzania danych wymaga oparcia się na co najmniej jednej z podstaw przetwarzania

8 Zaznaczyć jednak należy, iż uwaga o znaczeniu tej zmiany nie będzie odnosić się do stanu prawnego obowiązującego na gruncie krajowej regulacji, gdzie definiując pojęcie zgody (art. 7 pkt 5 ustawy o ochronie danych osobowych), zastrzeżono, że nie może być ona domniemana lub dorozumiana z oświadczenia woli o innej treści.

danych, z wyłączeniem jednakże możliwości skorzystania w takiej sytuacji z przesłanki usprawiedliwionych celów (art. 6 ust. 4)[9]. Dalszych ograniczeń dokonano w zakresie przesłanki zgody, zastrzegając, że nie może stanowić ona podstawy prawnej przetwarzania danych osobowych „w sytuacji poważnej nierówności między podmiotem danych a administratorem" (art. 7 ust. 4); jak wyjaśniono w pkt 34 preambuły, „dotyczy to w szczególności przypadku, gdy między podmiotem danych a administratorem istnieje stosunek zależności, między innymi wtedy, gdy dane osobowe pracowników są przetwarzane przez pracodawcę w kontekście zatrudnienia". Wstępny Projekt Rozporządzenia przewidywał również rozwiązanie, zgodnie z którym przetwarzanie danych osobowych dla celów marketingu bezpośredniego (ang. *direct marketing for commercial purposes*) dopuszczalne było wyłącznie na podstawie zgody podmiotu danych (art. 5 ust. 2 w wersji z listopada 2011 r.); z wymogu tego zrezygnowano jednak na etapie dalszych prac w ramach Komisji.

Planowana jest również szczególna regulacja w zakresie **ochrony danych osobowych dzieci** (art. 8 Projektu). Sama granica wieku decydująca o kwalifikacji podmiotu danych, jako dziecka wyznaczona została – co do zasady (zob. art. 4 pkt 18) – na stosunkowo wysokim poziomie (18 lat); obniżono ją jednak, w kontekście „oferowania usług społeczeństwa informacyjnego", do 13 lat (art. 8 ust. 1). Zgodnie z tym ostatnim przepisem, przetwarzanie danych osobowych dziecka, w związku z oferowaniem usług społeczeństwa informacyjnego „bezpośrednio dziecku", wymaga uzyskania zgody rodzica lub opiekuna prawnego dziecka. W tym zakresie administratorów danych obciążać ma, dość tajemniczo brzmiący, obowiązek podjęcia „racjonalnych starań w celu uzyskania możliwej do zweryfikowania zgody" (ang. *reasonable efforts to obtain verificable consent*), uwzględniając dostępną technologię (art. 8 ust. 1 zdanie drugie).

Prawa podmiotu danych (Rozdział III)

Projekt, dążąc do wzmocnienia przez podmioty danych kontroli nad ich własnymi danymi, wprowadza rozbudowaną regulację w zakresie realizacji zasady **transparentności** (art. 11-15). Administratorów danych obciążać mają w tym zakresie w szczególności obowiązki: „dysponowania przejrzystymi i łatwo dostępnymi politykami w zakresie przetwarzania danych osobowych i wykonywania praw przez podmioty danych" (art. 11 ust. 1)[10]; przekazywania wymaganych informacji „w czytelnej formie, w jasnym i prostym języku", w sposób dostosowany do potrzeb podmiotu danych (art. 11 ust. 2); ustanowienia określonych procedur wewnętrznych dotyczących wykonywania praw przez osoby, których dane dotyczą (art. 12 ust. 1); podania określonych informacji podmiotom danych, których zakres uległ w porównaniu z wymogami Dyrektywy rozszerzeniu (art. 14). Ponadto, w sposób wyraźny (co obecnie budzi pewne wątpliwości), nakłada się na administratora obowiązek informowania

9 Co ciekawe, planuje się wydawanie przez Komisję aktów delegowanych do rozporządzenia, w celu doprecyzowania przesłanki usprawiedliwionych celów, „dla różnych sektorów i sytuacji, w których przetwarza się dane" (art. 6 ust. 5). Z uwagi na przewidywane ograniczenie przetwarzania danych na podstawie zgody, znaczenie tej przesłanki – a w konsekwencji i aktów wykonawczych Komisji – może być szczególnie istotne. Jednocześnie jednak, biorąc pod uwagę poziom komplikacji stanów faktycznych, a także konieczność „ważenia" przeciwstawnych interesów (administratora oraz podmiotu danych), zadanie stojące przed Komisją ocenić należy jako wyjątkowo trudne i odpowiedzialne jednocześnie.

10 Wydaje się, iż chodzić będzie tu m.in. o polityki prywatności, stosowane w ramach stron internetowych.

wszystkich odbiorców danych, któremu ujawnił on dane, o każdym przypadku uaktualnienia lub usunięcia tych danych na żądanie podmiotu danych, ograniczając ten obowiązek jednakże w sytuacji, gdy „okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku" (art. 13).

„Prawa do bycia zapomnianym" (ang. *right to be forgotten*), określone w art. 17 Projektu, nawiązuje do występującego na gruncie Dyrektywy (art. 12) prawa do usunięcia danych. Zakres obowiązków, jakie obciążać mają administratorów w związku z realizacją tego prawa znacznie jednak rozszerzono: administrator danych zobowiązany jest bowiem nie tylko do usunięcia danych, za które ponosi odpowiedzialność, lecz również – w sytuacji „podania danych do wiadomości publicznej" – do poinformowania osób trzecich, które przetwarzają takie dane o zgłoszonym przez podmiot danych żądaniu usunięcia „linków do danych, kopii lub replikacji tych danych osobowych" (art. 17 ust. 2)[11]. Znaczenie tej regulacji przejawiać będzie się w szczególności w związku z przetwarzaniem danych osobowych w środowisku internetowym. Wątpić należy jednak w pełną jej wykonalność w praktyce, co wynikać może zarówno z przyczyn faktycznych (gł. technicznych, związanych ze specyfiką otwartych sieci, takich jak Internet), jak i prawnych (konieczność „ważenia" przez administratora danych prawa do ochrony danych z takimi prawami, jak wolność wypowiedzi czy realizacja interesu publicznego – co wynika z art. 17 ust. 3). Dlatego też nie bez podstaw w doktrynie europejskiej wskazuje się, że art. 17 Projektu „wydaje się być jednym z najbardziej kontrowersyjnych jego postanowień (…), trudnym do zastosowania w praktyce, może też wywołać on niekorzystne [dosł. chłodzące, ang. *chilling*] skutki w zakresie wykorzystania Internetu w UE"[12].

Kolejne z praw – **„prawo przenoszenia danych"** (ang. *right to data portability*, art. 18 Projektu) – również wydaje się już obecnie gwarantowane poprzez mechanizmy zapewnienia podmiotom danych efektywnej kontroli nad ich danymi osobowymi. W szczególności podmiot danych może zadecydować o opuszczeniu np. określonego serwisu internetowego i usunięcia z niego swoich danych, a następnie zalogowania się do nowego serwisu i zamieszczania tam swych danych. Propozycja Komisji ma na celu usprawnienie realizacji tego prawa (jednak wyłącznie w sytuacji, gdy dane są przetwarzane „w sposób elektroniczny oraz w zorganizowanym i powszechnie używanym formacie"), przenosząc jednocześnie koszty z tym związane na podmioty przetwarzające dane: nakłada ona bowiem na administratorów danych obowiązek przekazania podmiotowi danych „kopii danych", w formacie „który jest powszechnie używany i umożliwia dalsze wykorzystywanie przez podmiot danych". Komisja – w oparciu o art. 18 ust. 3 – może na drodze aktu wykonawczego określić ów format elektroniczny, jak również techniczne standardy, sposoby i procedury przekazywania (przenoszenia) danych osobowych.

Projekt Rozporządzenia wyodrębnia **profilowanie** jako odrębną operację na danych, poddając ją szczegółowej, restrykcyjnej regulacji (art. 20)[13]. Regulacja w tym zakresie bazuje na przepisie art. 15 Dyrektywy, jak również

11 Wersja Projektu z listopada 2011 r. obowiązek ten kształtowała jeszcze szerzej, wymagając od administratorów danych „zapewnienia usunięcia linków do danych, kopii lub replikacji tych danych osobowych", z czego jednak – z uwagi m.in. na praktyczną niewykonalność tego obowiązku – zrezygnowano.

12 Ch. Kuner, *The European Commission's Proposed Data Protection Regulation*..., s. 6.

13 Operacje „profilowania" są powszechnie stosowane w ramach różnych branż gospodarki i stosunków prawnych, np.: w działalności finansowej (np. ocena zdolności kredytowej), w ramach stosunku pracy, w działalności marketingowej, naukowej, itd.

rekomendacjach przyjętych w ramach prac Rady Europy[14], porządkuje – w porównaniu z rozwiązaniami znanymi z Dyrektywy – katalog sytuacji, w których dopuszczalne jest profilowanie (m.in. wskazano wyraźnie możliwość oparcia tego rodzaju działań na podstawie zgody podmiotu danych). Nadal jednak przesłanki dopuszczające tego rodzaju działania wydają się być określone zbyt wąsko, zawierają też one niejasności, mogące budzić poważne rozbieżności interpretacyjne i skutkować odmiennym podejściem do problemu w poszczególnych państwach EU (np. pojęcia „właściwych środków" oraz „właściwych gwarancji"). Co więcej, w porównaniu w regulacją przyjętą w Dyrektywie znacznie rozszerzono zakres jej zastosowania, do wszelkich „środków", które wywołują skutki prawne dotyczące osoby fizycznej lub które mają na nią istotny wpływ, nie ograniczając ich wyłącznie do „decyzji". Dodatkowo, rozszerzono zakres zastosowania przepisu poprzez odniesienie określonego w nim zakazu nie tylko do operacji przetwarzania mających służyć "ocenie" (ang. *evaluate*) określonych aspektów osobistych, lecz również do tych działań, które służą jedynie „analizie bądź przewidzeniu" (ang. *analyse or predict*) tychże aspektów. Całej tej regulacji wydaje się przyświecać przekonanie o generalnie negatywnej ocenie zjawiska „profilowania", w sytuacji, gdy wiele działań opartych „wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów osobistych" nie wykazuje takich elementów zagrożenia, a wprost przeciwnie – pozwala na zapewnienie korzystanych dla podmiotów danych skutków (np. analiza efektywności w ramach stosunku pracy).

Administrator i podmiot przetwarzający (Rozdział IV)

Projekt Rozporządzenia przewiduje **zniesienie generalnego obowiązku notyfikacji** organom ochrony danych operacji przetwarzania danych[15], powszechnie krytykowanego, stanowiącego obciążenie administracyjne dla administratorów danych, nie zapewniającego przy tym oczekiwanych korzyści. Niejako jednak „w zamian", proponuje się wprowadzenie szeregu innych obowiązków, w tym również takich, które w praktyce mogą skutkować znacznymi nawet obciążeniami. Obowiązki te mają na celu zwiększenie odpowiedzialności podmiotów przetwarzających dane osobowe, stanowiąc realizację tzw. zasady *accountability* (ang. *accountability principle*, co można tłumaczyć jako „zasadę odpowiedzialności" administratora danych osobowych)[16]. Zasada ta – w dużym skrócie – obejmuje obowiązki administratora danych: po pierwsze, przestrzegania przepisów prawa oraz po drugie, wykazywania przez niego takiej zgodności[17]. Dlatego też projektowany art. 22 ust. 1 nakłada na administratorów danych obowiązek „przyjęcia polityk" oraz zastosowania „odpowiednich środków"

14 Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23.11.2010 r.

15 W Polsce – obowiązek rejestracji zbiorów danych osobowych (art. 40 i nn. ustawy o ochronie danych osobowych).

16 Co prawda termin accountability lub też accountability principle nie występuje w tekście samego Projektu Rozporządzenia, jednak odniesienie do niego zawarto m.in. w pkt. 3.4. (Szczegółowe wyjaśnienia), gdzie wskazano, że propozycja art. 22 „uwzględnia wnioski z dyskusji na temat >>zasady odpowiedzialności<< i szczegółowo opisuje obowiązek przestrzegania przez administratora przepisów niniejszego rozporządzenia oraz wykazywania takiej zgodności, w tym poprzez przyjmowanie służących temu wewnętrznych polityk i mechanizmów".

17Zob. w szczególności opinię Grupy Roboczej Art. 29 Dyrektywy z 13 lipca 2010 r. (WP173), której polskie tłumaczenie posługuje się terminem „zasada rozliczalności" oraz dokumenty opracowane przez Center for Information Policy Leadership, dostępne pod adresem: http://www.informationpolicycentre.com/accountability-based_privacy_governance.

w celu zapewnienia, że dane przetwarzane są zgodnie z przepisami rozporządzenia oraz w celu wykazania tej zgodności (ang. *to ensure and be able to demonstrate (...) compliance with this Regulation*). Odpowiednie środki, zgodnie z art. 22 ust. 2 Projektu obejmują w szczególności:

a) prowadzenie **szczegółowej dokumentacji wewnętrznej**, dotyczącej wszelkich operacji na danych, za które podmiot podnosi odpowiedzialność (art. 28 Projektu); z wyłączeniem jednak spod tego obowiązku m.in. przedsiębiorstw zatrudniających mniej niż 250 osób, które „przetwarzają dane osobowe jedynie w ramach działalności pobocznej w stosunku do działalności głównej" (art. 28 ust. 4 lit. b);
b) **zabezpieczenie danych** (art. 30 Projektu), z uwzględnieniem m.in. najnowszych osiągnięć technicznych oraz kosztów wdrożenia „odpowiednich" środków technicznych i organizacyjnych; wymogi te doprecyzowane mają być przez Komisję Europejską, w formie aktów delegowanych oraz wykonawczych (art. 30 ust. 3 i 4);
c) obowiązek przeprowadzenia – w sytuacji, gdy operacje przetwarzania stwarzają „szczególne ryzyko" dla praw i wolności, osób których dane dotyczą[18] – **oceny skutków** w zakresie ochrony danych (art. 33 Projektu; ang. *data protection impact assessment*), bądź też uzyskania **uprzedniego zezwolenia** organu nadzoru (co dotyczy przekazywania danych osobowych do państw trzecich – art. 34 ust. 1) lub dokonania **uprzedniej konsultacji** z tym organem, zgodnie z art. 34 ust. 2 Projektu (co nawiązuje do istytucji tzw. *prior-checking*, znanej na gruncie art. 20 dyrektywy 95/46/WE); co interesujące, konsultacje takie może przeprowadzić również podmiot przetwarzający dane (*processor* danych), działając w imieniu administratora; organy krajowe wyposażone mają zostać w uprawnienia zakazowe wobec planowanych operacji przetwarzania danych, w sytuacji, gdy m.in. „ryzyka nie zostały dostatecznie zidentyfikowane lub złagodzone" (art. 34 ust. 3);
d) obowiązek wyznaczenia tzw. **„inspektora ochrony danych"** (ang. *data protection officer*)[19] m.in. przez podmioty z sektora publicznego oraz przedsiębiorców zatrudniających co najmniej 250 pracowników; przepisy art. 35-37 szczegółowo regulują zasady wyznaczania, pozycję oraz zadania „inspektora ochrony danych", dążąc w szczególności do zapewnienia niezbędnego poziomu jego niezależności w ramach organizacji administratora lub *processora* danych;
e) wdrożenie mechanizmów służących zapewnieniu **weryfikacji** skuteczności podjętych środków, np. z udziałem niezależnych audytorów wewnętrznych lub zewnętrznych (art. 22 ust. 3)[20].

Ponadto, Projekt (w art. 23) przewiduje wprowadzenie dwóch bardzo istotnych wymogów: stosowania zasad ochrony danych

18 Zgodnie z art. 33 ust. 2 Projektu ryzyko takie zachodzić będzie w szczególności w związku z „systematyczną i kompleksową oceną aspektów osobowych osoby fizycznej", monitorowaniem miejsc publicznych, bądź przetwarzaniem danych osobowych w „wielkoskalowych zbiorach danych dotyczących dzieci, danych genetycznych lub biometrycznych".

19 Polskie tłumaczenie Projektu jest w tym zakresie niezbyt szczęśliwe, jako że pojęcie „inspektora" odnosi się do organu ochrony danych (Generalny Inspektor Ochrony Danych Osobowych), jak również upoważnionych pracowników Biura GIODO, biorących udział w kontrolach (tj. „inspektorów" – art. 14 ustawy). Lepszą propozycją wydaje się pojęcie „oficera ds. ochrony danych".

20 Wcześniejsza wersja projektu z listopada 2011 r. przewidywała ponadto obowiązek uwzględnienia w raportach okresowych (np. raportach okresowych spółek giełdowych) „polityk administratora dotyczących ochrony danych, ryzyka związanego z przetwarzaniem przez administratora danych oraz środków podjętych w celu ograniczenia tego ryzyka" (art. 19 ust. 4).

„by design" (który wymaga uwzględnienia ochrony prywatności już na etapie projektowania określonych rozwiązań, produktów lub usług, bądź też planowania określonych operacji przetwarzania danych) oraz **„by default"** (wymagającego z kolei przyjmowania określonych ustawień chroniących prywatność, jako domyślnych, stosowanych jako zasada). Wymogi te – jak się przyjmuje – odnosić będą się nie tylko do administratorów danych, lecz również podmiotów przetwarzających dane na zlecenie[21] oraz podmiotów w ogóle nie przetwarzających danych lecz uczestniczących w projektowaniu określonych rozwiązań, produktów lub usług (np. firm informatycznych), jako że wprowadzane w rozporządzeniu obowiązki tworzyć mogą „zachęty dla właściwych rynków dóbr i usług"[22].

Zamiarem unijnego prawodawcy jest również doprecyzowanie sytuacji prawnej **podmiotów przetwarzających dane na zlecenie** (*processorów* danych), w szczególności rozszerzenie na tę grupę części obowiązków obciążających administratorów danych, w szczególności dotyczących zabezpieczenia danych. Sam wybór przez administratora podmiotu przetwarzającego dane na jego zlecenie, wymaga podjęcia odpowiednich kroków, m.in. podmiot przetwarzający powinien dawać „wystarczające gwarancje wdrożenia odpowiednich środków i procedur technicznych i organizacyjnych" (art. 26 ust. 1 Projektu). Rozbudowaniu uległ zakres umowy powierzenia danych do przetwarzania, która powinna obejmować m.in. wyraźną zgodę administratora na dalsze powierzenie danych (ang. *sub-processing*). Doprecyzowano również relacje **współadministratorów danych** (ang. *joint controllers*), którzy zobligowani zostali do wyraźnego określenia zakresu odpowiedzialności każdego z nich za zapewnienie zgodności z przepisami prawa, „w drodze wspólnych ustaleń", np. w ramach wiążącej ich umowy (art. 24).

Wśród obowiązków administratorów oraz *processorów* danych szczególnie istotne znaczenie ma proponowany **powszechny**[23] **obowiązek powiadamiania o naruszeniach ochrony danych osobowych** (ang. *personal data breach*, art. 31 i 32 Projektu). Przy czym Projekt szeroko definiuje pojęcie „naruszenia ochrony danych osobowych", jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób" (art. 4 pkt 9). Obowiązek ten obejmować ma:

- powiadomienie organu nadzorczego, co nastąpić ma „bez nieuzasadnionej zwłoki", a jeśli to możliwe, w terminie do 24 godzin od momentu dowiedzenia się o naruszeniu;
- powiadomienie osób, których dane dotyczą w sytuacji, gdy istnieje prawdopodobieństwo, że naruszenie takie może niekorzystnie wpłynąć na ochronę danych osobowych lub prywatność tych osób; co jednak istotne, powiadomienie osób, ktrórych dane dotyczą nie jest wymagane w sytuacji, gdy administrator wykaże, że „wdrożył odpowiednie technologiczne środki ochrony oraz że środki

21 Tak Europejski Inspektor Ochrony Danych, w opinii poświęconej ocenie Projektu, z dnia 7 marca 2012 r., s. 29, pkt. 179.

22 Tamże, s. 30, pkt. 182.

23 Obecnie obowiązek ten, wynikający z art. 4 dyrektywy 2002/58/WE o prywatności i łączności elektronicznej (zmienionej dyrektywą 2009/136/WE), znajduje zastosowanie wyłącznie w stosunku do dostawców publicznie dostępnych usług łączności elektronicznej.

te zostały zastosowane do danych, których dotyczyło naruszenie" (np. szyfrowanie danych; art. 32 ust. 3).

Propozycja powyższa wydaje się być sformułowana w sposób zbyt rygorystyczny (m.in. z uwagi na bardzo krótki, 24-godzinny termin na powiadomienie organu), a przy tym nieprecyzyjny (brak w szczególności jasnych kryteriów decydujących o kwalifikacji określonego zdarzenia jako „naruszenia")[24], co w praktyce skutkować może znacznym obciążeniem podmiotów odpowiedzialnych, a w konsekwencji – jak zauważa się w doktrynie – osiągnięciem skutków przeciwnych od zamierzonych, prowadzących nawet do osłabienia wymaganego poziomu ochrony danych, czego dowodzą przykłady państw, w których obowiązek ten funkcjonuje od dłuższego już czasu (np. Stany Zjednoczone)[25].

Damian Karwala - radca prawny przy Okręgowej Izbie Radców Prawnych w Krakowie, współpracujący z Kancelarią Prawną Traple Konarski Podrecki i Wspólnicy sp.j.

24 Por. opinię Europejskiego Inspektora Ochrony Danych z dnia 7 marca 2012 r., s. 32, pkt. 198.

25 Ch. Kuner, *The European Commission's Proposed Data Protection Regulation*..., s. 8, który podkreśla, że „nadmierne powiadomienia o naruszeniach bezpieczeństwa danych stały się poważnym problemem" w tym państwach. W szczególności zbyt krótki termin na powiadomienie organu prowadzi do swoistej „nad-notyfikacji" (tj. zbyt częstego i szybkiego powiadamiania), kosztem zaangażowania właściwych środków w celu dokładniejszego zbadania sytuacji naruszenia bezpieczeństwa danych.

Zapraszamy do udziału

WARSZTATY

AKADEMIA UMÓW IT - POZIOM I „WARSZTATY DLA PRAKTYKÓW"

3-4 października 2012 r., Warszawa

W ramach warsztatów, uczestnik w oparciu o praktyczne przykłady oraz samodzielną pracę pozna między innymi następujące zagadnienia:

- jakie są aktualne standardy panujące w zakresie tworzenia i negocjacji umów IT
- jak poprawnie sporządzić postanowienia dotyczące przeniesienia praw autorskich oraz umów licencji
- jak interpretować postanowienia umów autorsko prawnych
- jak zabezpieczyć się przed wypowiedzeniem licencji
- jakie są alternatywne możliwości zapewnienia uprawnień do korzystania z oprogramowania
- modele udostępnienia, ryzyka prawne oraz konsekwencje podatkowe wykorzystania oprogramowania w grupach kapitałowych
- modele, ryzyka prawne oraz konsekwencje podatkowe poszczególnych modeli dystrybucji oprogramowania
- standardowe konstrukcje w zakresie umów wdrożeniowych
- na jakie elementy zwracać szczególną uwagę w toku sporządzania, weryfikacji oraz negocjacji umów wdrożeniowych
- standardowe konstrukcje w zakresie umów outsourcingowych
- na jakie elementy zwracać szczególną uwagę w toku sporządzania, weryfikacji oraz negocjacji umów outsourcingowych, w tym umów serwisowych
- standardy w zakresie odpowiedzialności stron w umowach IT
- analiza klauzul umownych, typowe błędy
- komu przysługują majątkowe prawa autorskie do utworów wykonanych przez pracownika oraz jakie są optymalne rozwiązania w zakresie praw autorskich do utworów pracowniczych i konsekwencje podatkowe poszczególnych rozwiązań,
- jak zabezpieczyć umowę na wypadek upadłości lub zaprzestania działalności przez kontrahenta. Zasady sporządzania umów o depozyt kodu źródłowego oprogramowania.

Więcej informacji: www.cpi.com.pl

Wdrożenia systemów informatycznych w orzecznictwie Sądu Najwyższego

Bohdan Widła

1. Wstęp

Truizmem jest stwierdzenie, że polskie prawo cywilne nie jest dostosowane do realiów rynku IT, a prawnika przygotowującego umowę na wdrożenie systemu informatycznego lub zajmującego się sporem między wykonawcą a zamawiającym czekają wyzwania związane z zastosowaniem norm prawnych do tej specyficznej materii. Komplikacje te sprawiają, że spory realizacyjne związane z wdrożeniami systemów rzadko kończą się postępowaniem sądowym. Jeszcze mniej spraw trafia do Sądu Najwyższego, którego wypowiedzi mają istotne znaczenie dla praktyki sądów niższych instancji.

Celem artykułu jest omówienie wybranych zagadnień, które zostały poruszone przez Sąd Najwyższy w dwóch orzeczeniach, które dotyczyły wykonania lub wdrożenia systemu informatycznego. Rozważania nie będą skupiały się na okolicznościach konkretnej sprawy, ale na tych wypowiedziach Sądu Najwyższego, które można uogólnić, albo które obrazują sposób postrzegania umów IT przez organy orzekające.

2. Wyrok z 24 sierpnia 2007 r., V CSK 150/07

Pierwsze komentowane orzeczenie zapadło w stanie faktycznym, w którym strony zawarły „umowę sprzedaży, instalacji i wdrożenia systemu". Z przedstawionego w uzasadnieniu opisu stanu faktycznego wynika, że po przeprowadzeniu prac związanych z projektem wdrożenia, zamawiający uznał, że system nie spełnia jego oczekiwań i odstąpił od umowy.

Podstawowy problem rozstrzygany przez Sąd Najwyższy dotyczył charakteru umowy. Sąd przyjął, że celem umowy, której przedmiotem była sprzedaż nośników z oprogramowaniem, świadczenie usług wdrożeniowych oraz udzielenie licencji, było wdrożenie systemu informatycznego. W konsekwencji, Sąd uznał, że strony zawarły umowę o dzieło, w której rezultatem (dziełem) był właśnie system.

W praktyce, umowę wdrożeniową można skonstruować zarówno w modelu umowy o dzieło, jak w modelu umowy o świadczenie usług. Różnica między tymi modelami sprowadza się w uproszczeniu do tego, że o ile w pierwszym z nich gotowy system jest rezultatem, za którego osiągnięcie odpowiada wykonawca, to w drugim modelu wykonawca ma z należytą starannością wspierać proces wdrażania systemu przez zamawiającego, nie odpowiadając za sam rezultat. Obecnie większość umów wdrożeniowych zawierana jest w modelu umowy o dzieło. Wątpliwości co do poprawności takiej kwalifikacji mogą wynikać z tego, że według tradycyjnego poglądu, rezultat umowy o dzieło powinien być ściśle określony[1]. Tymczasem praktycznie każde wdrożenie systemu informatycznego obejmuje daleko idącą konkretyzację przedmiotu umowy dopiero podczas jej realizacji (w wyniku analizy przedwdrożeniowej,

1 Zamiast wielu zob. A. Brzozowski w: J. Rajski, *System Prawa Prywatnego. Tom 7. Prawo zobowiązań – część szczegółowa*, wyd. 3, Warszawa 2011, s. 384.

opracowania projektu technicznego itp.). W komentowanym wyroku, Sąd Najwyższy trafnie stwierdził, że „*umowa o dzieło dopuszcza takie wypadki, gdy ostateczny kształt dzieła wyłania się w trakcie tworzenia*", dając tym samym silny argument zwolennikom poglądu o dopuszczalności umowy o dzieło, której rezultat nie jest całkowicie zdeterminowany w chwili zawarcia.

Komentarza wymaga także stwierdzenie zawarte w uzasadnieniu wyroku: „...*gdy dziełem jest system informatyczny umowa o dzieło z chwilą wydania przenosi na zamawiającego egzemplarze utworów autorskich i baz danych nie będących utworami oraz daje mu prawo do korzystania z nich zgodnie z przeznaczeniem, mimo ze autorskie prawo majątkowe nie zostaje na zamawiającego przeniesione*". Z cytowanego fragmentu wynika, że zdaniem Sądu Najwyższego sama umowa o dzieło może stanowić podstawę do korzystania z utworów w rozumieniu ustawy z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[2] i baz danych chronionych prawem *sui generis* w rozumieniu ustawy z 27 lipca 2001 r. o ochronie baz danych[3].

Powyższa teza została sformułowana zbyt szeroko. Podstawą do korzystania z utworu, do którego autorskie prawa majątkowe przysługują podmiotowi trzeciemu, może być co do zasady uprawnienie wynikające z licencji, albo przepisy o dozwolonym użytku (art. 23 i nast. pr. aut.), przy czym w obrocie profesjonalnym w praktyce w grę wchodzi przede wszystkim ta pierwsza możliwość. Problematyka udzielania licencji uregulowana jest w art. 41 i nast. pr. aut. Przepisy o przejściu praw autorskich i udzieleniu licencji stanowią regulację autonomiczną w stosunku do przepisów kodeksu cywilnego dotyczących umów o dzieło i umów o świadczenie usług. Art. 52 ust. 1 pr. aut. wyraźnie przesądza, że przeniesienie własności utworu nie powoduje przejścia autorskich praw majątkowych i nie ma powodu by uznać, że *a contrario* samo przeniesienie własności egzemplarza powoduje udzielenie licencji. Dodatkowym argumentem za tym stanowiskiem jest regulacja art. 41 ust. 2 pr. aut., który uznaje licencję za odrębny typ umowy. Także ustawa o ochronie baz danych nie zawiera regulacji, która dawałaby podstawę do przyznania uprawnień do korzystania z bazy na podstawie samej umowy o dzieło.

Jeżeli zatem strony zawierają umowę, w której dominują elementy typowe umowy o dzieło, obok których funkcjonują postanowienia, na mocy której udzielana jest licencja, to podstawą korzystania z utworu nie jest sama umowa o dzieło, ale licencja. Dominujący charakter postanowień charakterystycznych do umowy o dzieło przemawia za stosowaniem do całej umowy przepisów kodeksu cywilnego dotyczących m.in. wynagrodzenia za dzieło, odstąpienia od umowy czy rękojmi. Nie zwalnia jednak od przestrzegania zasad ustawy o prawie autorskim i prawach pokrewnych, dotyczących udzielania licencji. Jedyny istotny wyjątek dotyczy oprogramowania komputerowego. Zgodnie z art. 75 ust. 1 pr. aut., ten kto legalnie wszedł w posiadanie programu może korzystać z niego w zakresie zwielokrotnienia i modyfikacji (art. 74 ust. 4 pkt 1-2 pr. aut.), jeśli czynności te są niezbędne do korzystania z programu komputerowego zgodnie z jego przeznaczeniem, w tym do poprawiania błędów. Status „legalnego posiadacza" może wynikać także z umowy o dzieło. Podsumowując, pogląd wyrażony przez Sąd Najwyższy ma uzasadnienie tylko w szczególnych wypadkach.

Na komentarz zasługuje także wypowiedź Sądu Najwyższego dotycząca baz danych. W umowie będącej podstawą sporu pojawia się pojęcie „bazy danych O.". Mimo anonimizacji orzeczenia dla

2 Dalej jako pr. aut.
3 Dalej jako u.o.b.d.

potrzeb publikacji, nawet osoba średnio zorientowana w realiach rynku IT, bez trudu zidentyfikuje tu oprogramowanie bazodanowe jednego z największych producentów na świecie. Tymczasem rozważania Sądu Najwyższego dotyczące „bazy danych O.", skupiają się na dwóch reżimach ochrony baz danych, rozumianych jako zbiór danych. Innymi słowy, pisząc o oprogramowaniu komputerowym wspomagającym zarządzanie zbiorem danych, Sąd Najwyższy opisuje podstawy ochrony właściwe dla danych jako takich. Przykład ten pokazuje, że zetknięcie sądów z nieznaną terminologią może spowodować oderwanie rozstrzygnięcia od stanu faktycznego. O ile wydaje się, że ten błąd nie wpłynął istotnie na treść komentowanego orzeczenia, w innym stanie faktycznym skutki mogłyby być znacznie dalej idące.

Ostatnia wypowiedź Sądu Najwyższego w komentowanym wyroku, która wymaga omówienia, dotyczy stosowania do umów na wdrożenie systemu informatycznego zasad odpowiedzialności za usterki utworu, uregulowanych w art. 55 ust. 1 pr. aut. Według Sądu, przepis ten nie powinien być zastosowany, ponieważ działania wykonawcy obejmowały dokonanie czynności nietwórczych, „*...nasyconych w tak dużym stopniu powtarzalnością, iż można założyć bardzo zbliżony wynik w razie wykonywania instalacji i wdrożenie przez inny wyspecjalizowany podmiot*". Innymi słowy, brak zastosowania art. 55 ust. 1 pr. aut. wiąże się z tym, że wdrożenie systemu jako takie nie jest utworem. Pogląd ten jest sam w sobie trafny, ale pomija problem usterek utworów wchodzących w skład wdrożonego systemu informatycznego, takich jak programy komputerowe. W ich przypadku można wyobrazić sobie zastosowanie art. 55 ust. 1 pr. aut., przy czym należy zwrócić uwagę, że przepis ten dotyczy odpowiedzialności „twórcy" i zawiera łagodniejsze reguły, aniżeli przepisy o rękojmi za wady dzieła, zawarte w kodeksie cywilnym. Z uwagi na ten wyjątkowy charakter, należy interpretować go zawężająco[4] i stosować go tylko dla umów, które są zawierane bezpośrednio z osobą fizyczną będącą twórcą, a ich przedmiotem jest wykonanie utworu. W praktyce, na rynku IT takie umowy wdrożeniowe będą należały do absolutnych wyjątków.

3. Wyrok z 25 lutego 2010 r., V CSK 297/09

Drugie z komentowanych orzeczeń dotyczyło umowy, której przedmiotem nie było typowe wdrożenie systemu informatycznego. Zgodnie z opisem stanu faktycznego, pozwany (wykonawca) miał opracować i dostarczyć system wraz z urządzeniami oraz udzielić licencji na korzystanie z oprogramowania, jednak powód – będący zamawiającym – miał je następnie wprowadzać do obrotu. System nie został wykonany w terminie, co skłoniło zamawiającego do zażądania zapłaty kar umownych. Rozważania prawne zawarte w uzasadnieniu komentowanego wyroku mają znaczenie także dla „klasycznych" umów wdrożeniowych.

Według art. 354 §2 kodeksu cywilnego, wykonanie umowy wymaga pewnego współdziałania ze strony wierzyciela. Powyższa zasada prawa zobowiązań ma niebagatelne znaczenie dla umów wdrożeniowych. O ile bowiem w przypadku mniej skomplikowanych kontraktów, współdziałanie wierzyciela często ogranicza się do „nie przeszkadzania", powodzenie projektu wdrożeniowego właściwie zawsze wymaga kooperacji między wykonawcą a zamawiającym. W praktyce umowy zawierają zwykle postanowienia, których celem jest doprecyzowanie, a niekiedy także wprowadzenie zamkniętego katalogu czynności, które zamawiający ma obowiązek wykonywać podczas wdrożenia.

Umowa, której dotyczył spór zakończony komentowanym orzeczeniem, zawierała postanowienie o obowiązku przekazania wykonawcy

4 Por. J. Barta, R. Markiewicz w: J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, R. Markiewicz, E. Traple, *Prawo autorskie i prawa pokrewne. Komentarz*, wyd. 5, Warszawa 2011, s. 377-378 oraz E. Traple, *Umowy o eksploatację utworów w prawie polskim*, Warszawa 2010, s. 120-124.

przez zamawiającego „*...wymogów dostosowania oprogramowania klienckiego do protokołu wymiany informacji*...". Wykonawca bronił się, zarzucając brak wykonania tych obowiązków przez zamawiającego. Zdaniem Sądu Najwyższego, z punktu widzenia odpowiedzialności wykonawcy kluczowe znaczenie ma kwalifikacja prawna powyższych obowiązków. Wskazane zostały dwie możliwości – mogą to być wzajemne zobowiązania zamawiającego, albo forma jego współdziałania w realizacji umowy.

W tym kontekście warto zwrócić uwagę na tę część uzasadnienia, w której Sąd Najwyższy stwierdza: „*Nie można zarzucać wierzycielowi braku współdziałania z dłużnikiem przy wykonywaniu przez niego zobowiązania wówczas, gdy wierzyciela obciąża przewidziany w umowie obowiązek określonego działania bądź zaniechania*". Sugeruje to, że w ocenie Sądu, gdy umowa wyraźnie definiuje obowiązki wierzyciela, to mają one charakter zobowiązań wzajemnych. Moim zdaniem byłby to pogląd zbyt daleko idący. Nie ma powodu, aby wykluczyć – zwłaszcza w obrocie profesjonalnym – doprecyzowanie zakresu obowiązku współdziałania w treści umowy[5]. Nie oznacza to, że w razie „pominięcia" przez strony niektórych działań, będą one zawsze obciążać dłużnika. Tam, gdzie wykonanie zobowiązań jest niemożliwe bez udziału wierzyciela, obowiązek współdziałania będzie wynikał z art. 354 §2 k.c. W zakresie doprecyzowanym w umowie, trudniej będzie jednak o spór co do skali potrzeb dłużnika.

Skutki kwalifikacji obowiązków zamawiającego różnią się od strony dogmatyczno-prawnej. Jeśli obowiązki zamawiającego traktować jako zobowiązanie wzajemne, to ich niewykonanie byłoby równoznaczne ze zwłoką dłużnika w wykonaniu zobowiązań wynikających z umowy wzajemnej, co pociąga za sobą roszczenie odszkodowawcze wykonawcy oraz możliwość wyznaczania przez wykonawcę terminu na ich wykonanie, z zagrożeniem, że po jego bezskutecznym upłynięciu będzie on mógł odstąpić od umowy (art. 491 §1 k.c.). W razie odstąpienia od umowy na tej podstawie, skutkiem byłby wzajemny zwrot świadczeń przez strony oraz dalsze roszczenia odszkodowawcze wykonawcy (art. 494 k.c.), przy czym nie można wykluczyć dochodzenia w ramach odszkodowania kwoty wynagrodzenia, które wykonawca otrzymałby, gdyby nie doszło do zwłoki zamawiającego. Z kolei jeśli obowiązki zamawiającego potraktować jako formę współdziałania, to jego brak stanowi przejaw zwłoki wierzyciela, jeśli następuje bez uzasadnionego powodu (art. 486 §1 k.c.)[6]. Skutkiem zwłoki wierzyciela jest powstanie po stronie wykonawcy roszczenia o naprawienie szkody wynikłej z tej zwłoki, a jeśli umowa łącząca strony ma charakter umowy o dzieło, także powstanie uprawnienia do odstąpienia od umowy po bezskutecznym upływie dodatkowego terminu (art. 640 k.c.). W tym ostatnim wypadku, wykonawca jest uprawniony do wynagrodzenia, po odliczeniu tego, co zaoszczędził w wyniku niewykonania dzieła (art. 639 k.c.).

Mimo powyższych różnic dogmatycznych wydaje się, że w praktyce skutki zastosowania obydwu koncepcji będą często zbliżone. W obydwu wypadkach wykonawca ma szanse na odstąpienie od umowy i uzyskanie przynajmniej części wynagrodzenia. Główna różnica polega na tym, że w przypadku powołania się na art. 494 k.c. miałoby ono charakter odszkodowania, podczas gdy wynagrodzenie należne zgodnie z art. 639 k.c. nie ma charakteru odszkodowawczego. Wydaje się też, że powołanie się na art. 639 k.c. byłoby dla wykonawcy znacznie korzystniejsze z dowodowego punktu

5 Przepis art. 354 §2 k.c. nie wspomina też o odpłatności czynności mieszczących się w ramach współdziałania, natomiast wprowadzenie takiej odpłatności dopuszcza się w doktrynie. Zob. P. Machnikowski w: E. Gniewek (red.), *Kodeks cywilny. Komentarz*, wyd. 3, Warszawa 2008, s. 538-539.

6 Por. F. Zoll w: A. Olejniczak, *System Prawa Prywatnego. Tom 6. Prawo zobowiązań – część ogólna. Suplement*, Warszawa 2010, s. 215-216.

widzenia. Przyjęcie, że obowiązki zamawiającego stanowią przejaw współdziałania, a nie autonomicznego zobowiązania, oznacza także brak możliwości przymusowego wyegzekwowania ich realizacji[7]. Odnośnie wpływu na odpowiedzialność wykonawcy, w komentowanym orzeczeniu Sąd Najwyższy wyraził pogląd, że brak aktywności zamawiającego, czy to w postaci niewykonania zobowiązania, czy to w postaci braku współdziałania, będzie całkowicie zwalniał wykonawcę z odpowiedzialności za zwłokę (w tym wypadku: z zapłaty kary umownej) tylko jeśli uniemożliwia to wykonanie jego zobowiązań. Natomiast jeśli brak aktywności powoduje jedynie utrudnienie terminowej realizacji zobowiązań, nie jest to podstawa do uznania kary za bezzasadną, a jedynie do jej miarkowania zgodnie z art. 484 §2 k.c.

Obok rozważań dotyczących współdziałania wierzyciela w wykonywaniu umowy, na uwagę zasługuje także wypowiedź na temat zasad interpretacji umów. Analizując sam tekst umowy, której dotyczy spór, Sąd Apelacyjny przyjął brak powiązań pomiędzy niektórymi obowiązkami wykonawcy i obowiązkami zamawiającego. Sąd Najwyższy skrytykował skupienie się na „*analizie logiczno-językowej*" umowy i stwierdził, że interpretując umowę nie można „*pomijać technicznych aspektów obowiązków stron i ich wzajemnych relacji*", a niezależnie od przyjętej w umowę terminologii, „*istotne jest, czy ze względu na uwarunkowania techniczne pozwany mógł wykonać swój obowiązek bez wcześniejszego wykonania obowiązków powoda*". Takie podejście zasługuje na pełną aprobatę i otwiera drogę do zdroworozsądkowej wykładni umów zawieranych w branży IT, z uwzględnieniem technicznego charakteru świadczeń stron, nawet jeśli nie został on przełożony na język prawniczy. Sąd Najwyższy trafnie zwrócił jednak uwagę, że rozstrzygnięcie o zagadnieniach ściśle technicznych nie jest możliwe bez posiadania wiadomości specjalnych w rozumieniu art. 278 §1 kodeksu postępowania cywilnego. W konsekwencji, aby uwzględnić ten aspekt sporu w postępowaniu sądowym, strona powinna wnioskować o przeprowadzenie dowodu z opinii biegłego.

4. Podsumowanie

Komentowane orzeczenia unaoczniają problemy, z jakimi borykają się organy orzekające niemające głębokiej wiedzy o przebiegu projektów wdrożeniowych i o rynku informatycznym, a zmuszone do rozstrzygania związanych z tym spraw. Zadaniem prawnika przygotowującego umowę na wdrożenie systemu jest współpraca z zespołem merytorycznym tak, aby treść umowy w jak najpełniejszym stopniu odpowiadała rzeczywistości „projektowej". Rolą pełnomocnika strony w procesie powinno być natomiast objaśnienie sądowi istotnych niuansów i - kiedy jest to konieczne - wnioskowanie o przeprowadzenie dowodu z opinii biegłego.

Bohdan Widła - absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, prawnik w kancelarii Maruta i Wspólnicy sp. j., aplikant radcowski.

W artykule Bohdana Widły „Jawność umów o zamówienie publiczne", opublikowanym w „Czasie Informacji" nr 1/2012, znalazły się rozważania na temat art. 5 ust. 1a ustawy o dostępie do informacji publicznej. Już po oddaniu artykułu do druku, przepis ten został pozbawiony mocy obowiązującej przez Trybunał Konstytucyjny, w wyroku z 18 kwietnia 2012 r., sygn. K 33/11. Wzorzec kontroli dotyczył jedynie trybu uchwalenia ustawy, a nie treści samego przepisu. W związku z tym, uwagi krytyczne zawarte w artykule pozostają aktualne.

7 Tak P. Machnikowski w: E. Gniewek (red.), *Kodeks*..., s. 538-539.

Wymiana plików w sieciach P2P od strony prawnej

Katarzyna Czajkowska-Matosiuk

Podstawowym założeniem sieci Peer-to-Peer (P2P) jest udostępnienie użytkownikom sieci mechanizmu wymiany plików i danych niezależnego od serwerów WWW i FTP. W praktyce oznacza to, że każdy, kto dysponuje łączem do Internetu, może włączyć się do sieci P2P, udostępnić swoje zbiory i znaleźć u innych potrzebne mu materiały. Sieć P2P to jednocześnie doskonałe miejsce do wymiany nielegalnego oprogramowania. Dlatego też, poza znajomością narzędzi do wymiany plików w sieci P2P warto wiedzieć, co można, a czego nie można udostępniać.

Krótka historia Peer-to-Peer

Peer-to-Peer (ang. równy z równym) to taki system komunikacji internetowej, który gwarantuje obydwu stronom **równorzędne prawa**. Wszystkie komputery znajdujące sie w takiej sieci są zarówno korzystającymi, jak i udostępniającymi (**klientami i serwerami**). Dzięki temu możliwa jest wzajemna wymiana plików pomiędzy użytkownikami.

Pierwszą siecią P2P był słynny **Napster**, założony w 1998 r. przez **Shawna Fanninga**. Fanning umożliwiał każdemu, kto pobrał i zainstalował aplikację, na udostępnienie wybranych zasobów swojego komputera innym użytkownikom w Internecie. Ważną cechą Napstera, która przyczyniła się do gwałtownej popularyzacji, była łatwość obsługi. Żeby stać się węzłem sieci, nie trzeba było wykazać się żadną wiedzą techniczną.

Zaraz po tym wydarzeniu, stworzone przez Fanninga rozwiązanie, zaczęli powielać informatycy z całego świata. Początkowo darmowe pobieranie i udostępnianie skopiowanych utworów nie budziło większych emocji, jednak na początku XXI wieku, kiedy z sieci P2P zaczęły korzystać miliony internautów, artyści i organizacje zbiorowego zarządzania prawami autorskimi ruszyły do walki. Wskutek działań potężnych koncernów muzycznych i filmowych, stopniowo zaczęły zmieniać się krajowe regulacje prawne i zaczęto ścigać zarówno twórców nowych sieci P2P, jak i osoby, które z nich korzystają.

W Polsce wymiana plików za pomocą P2P kwitnie, jednak to dopiero ostatnia afera związana z Acta uświadomiła wszystkim, jak doniosłe i kontrowersyjne jest to zagadnienie.

Peer-to-Peer a prawa autorskie

Przepisy ustawy o prawie autorskim i prawach pokrewnych przewidują bowiem, że każdy utwór podlega **ochronie prawnej**. Dotyczy to również utworów zamieszczanych na stronie internetowej lub pobieranych za pomocą łączy internetowych, przy wykorzystaniu programów P2P. Oznacza to, że pobieranie utworów i ich udostępnianie - od strony prawnej – jest możliwe tylko na zasadach określonych przez posiadacza majątkowych praw autorskich. Oznacza to, że sposób eksploatacji utworu zależy od twórcy lub osoby, która nabyła określone prawa majątkowe (np. wydawcy lub producenta) lub na rzecz, której ustanowiona została licencja.

Posiadacz majątkowych praw autorskich może bowiem decydować o losach swojego utworu, niezależnie od tego, czy jest to film, zdjęcie, piosenka, czy wypowiedz pisemna. Może zatem zdecydować o dystrybuowaniu swojego utworu, poprzez określone serwisy, za określoną cenę lub objąć utwór tzw. Licencją Creative Commons, która pozwala mi.in. na korzystanie z utworu za darmo, na określonym polu eksploatacji.

Aktualnie na stronach internetowych, najczęściej umieszczane są informacje dotyczące zakresu korzystania z zamieszczonych tam treści. Zazwyczaj przy poszczególnych utworach, umieszczany jest podpis copyright. Wskazuje on na posiadacza majątkowych praw autorskich, a jednocześnie stanowić ma ostrzeżenie, że pliku nie można pobierać, a tym bardziej rozpowszechniać bez zgody autora.

Takich informacji nie znajdzie się jednak przy wymianie plików za pośrednictwem sieci P2P. Użytkownik takiej sieci, otwiera innym dostęp do danych zgromadzonych na swoich dyskach, lecz nie załącza tu zazwyczaj informacji, na temat tego, czy ma prawo go legalnie rozpowszechniać. Oznacza to, że utwór w świetle prawa, jest rozpowszechniany nielegalnie.

WYMIANA PLIKÓW NA SWIECIE

10 pierwszych krajów według liczby udostępnionych plików*

1. *Stany Zjednoczone - 19 proc.,*
2. *Wielka Brytania - 7 proc.,*
3. *Kanada - 6 proc.,*
4. *Brazylia - 5 proc.,*
5. *Hiszpania - 5 proc.,*
6. *Polska - 5 proc.,*
7. *Francja - 4 proc.,*
8. *Szwecja - 3 proc.,*
9. *Holandia - 3 proc.,*
10. *Australia-2 proc.*

Liczba udostepnien wedtug kategorii*:

- *gry na PC - 49 proc.,*
- *aplikacje użytkowe - 16 proc.,*
- *aplikacje multimedialne - 11 proc.,*
- *gry na konsole - 9 proc.,*
- *inne aplikacje - 5 proc.,*
- *aplikacje biurowe - 5 proc.,*
- *systemy operacyjne - 4 proc.,*
- *aplikacje muzyczne - 1 proc.*

Źródło www.symantec.pl

Jaka odpowiedzialność grozi internautom?

Warto zaznaczyć, że innej odpowiedzialności prawnej podlegają osoby, które wyłącznie pobierają nielegalnie pliki, a innej osoby, które również rozpowszechniają, czyli udostępniają je z zasobów swojego komputera. Inna jest też odpowiedzialność za pobieranie utworów audiowizualnych, a inna za ściąganie programów komputerowych.

Za rozpowszechnianie utworu należy uznać sytuację, w której jest on **dostępny dla potencjalnie nieograniczonej liczby odbiorców.** Nie ma przy tym znaczenia, jakie środki techniczne wykorzystał sprawca w celu rozpowszechniania dzieła.

UWAGA!

Już samo umieszczenie utworu w sieci, uznaje się za formę jego rozpowszechniania. Potencjalnie do zasobów takich ma bowiem dostęp nieograniczona liczba osób.

Oznacza to, że z prawnego punktu widzenia, rozpowszechnianiem jest zarówno udostępnienie utworu w Internecie w wyniku

umieszczenia go na przestrzeni dyskowej, jak również przy wykorzystaniu aplikacji typu P2P.

Internauta będzie ponosił odpowiedzialność bez względu na fakt, iż pliki zostały udostępnione w ramach serwisu, który automatycznie **kasuje dane po upływie określonego czasu,** bądź w przypadku braku zainteresowania użytkowników Internetu w pobieraniu zasobów. Okres rozpowszechniania utworu bez uprawnienia, ma znaczenie jedynie **dla sądowego wymiaru kary.**

Nie ma także znaczenia, **ile razy doszło do skopiowania pliku** udostępnionego w Internecie, ani to, że skopiowany utwór **podzielono na kilka lub kilkanaście części**, aby usprawnić jego pobieranie. W praktyce często zdarza się, że internauci rozpowszechniający nielegalnie utwór **zmieniają jego nazwę** (często na zupełnie niezwiązaną z oryginalnym tytułem), aby plik dłużej utrzymał się w sieci i nie został wykryty. Tego typu działania również nie zwalniają sprawcy z odpowiedzialności.

Kiedy odpowiedzialność cywilna?

Internautom, którzy wyłącznie pobierają pliki audiowizualne z sieci grozi **odpowiedzialność cywilna** względem twórcy. Twórca ma bowiem prawo żądać od osoby, która naruszyła jego autorskie prawa majątkowe, do **zaprzestania ściągania** plików i **usunięcia ich** ze swojego komputera, wydania korzyści uzyskanych dzięki posiadaniu nielegalnie ściągniętego utworu albo **zapłacenia podwójnej**, a jeśli naruszenie jest zawinione, **potrójnej wysokości stosownego wynagrodzenia,** czyli najczęściej opłaty licencyjnej na rzecz autora.

Wysokość takiej kwoty zależy od **wysokości tantiem** (procentowy udział autora w dochodach uzyskanych z rozpowszechniania dzieła) pobieranych przy legalnym pobieraniu utworu. Jeżeli działanie internauty było zawinione, twórca może też żądać naprawienia wyrządzonej szkody.

Ponadto sąd może zasądzić **przepadek komputera** i innych przedmiotów, przy których użyciu dokonano naruszenia. Na wniosek , sąd może orzec przyznanie tych rzeczy na poczet należnego **odszkodowania**.

Wprawdzie odpowiedzialność taką przewidują przepisy prawa, jednak w rzeczywistości internaucie, który ściąga pliki na własny użytek nie wiele grozi. Tego typu naruszenia praw autorskich **nie są ścigane z urzędu** (przez policję), a jedynie **na wniosek poszkodowanego**. Trudno sobie zaś wyobrazić, żeby twórca zdołał wyśledzić i pozwać miliony internautów.

Taka sytuacja jest zatem bardzo **korzystna dla internautów**, natomiast kompletnie nieopłacalna dla artystów, którzy w zasadzie tracą zarobek wraz z każdym kolejnym ściągniętym plikiem. W związku z tym, twórcy i działające na ich rzecz organizacje prowadzą zażartą walkę z tzw. piractwem w Internecie. Postulują oni m.in. wprowadzenie dodatkowych opłat, które mieliby ponosić internauci na rzecz twórców i organizacji reprezentujących ich prawa.

Kiedy odpowiedzialność karna?

Surowiej kształtuje się odpowiedzialność internautów, którzy poza ściąganiem z sieci plików zawierających chronione utwory, również je udostępniają. Podlegają oni dodatkowo odpowiedzialności karnej. Udostępnianie utworów z zasobów własnego komputera (przede wszystkim poprzez P2P) to innymi słowy rozpowszechnianie, zwielokrotnianie plików w sieci.

W zakresie naruszeń praw osobistych ustawa uznaje za przestępstwa:

1) przywłaszczenie sobie autorstwa całości lub części cudzego utworu (plagiat),
2) przypisanie sobie artystycznego wykonania lub jego części,
3) wprowadzenie w błąd co do autorstwa lub artystycznego wykonawstwa,
4) rozpowszechnianie utworu, opracowania, artystycznego wykonania bez podania nazwiska twórcy (lub pseudonimu),
5) publiczne zniekształcanie utworu, artystycznego wykonania, a także fonogramu, wideogramu lub nadania.

Z perspektywy prawa autorskiego, działania takie jako **przestępstwa,** mogą być ścigane z urzędu, czyli w praktyce - przez policję i prokuraturę. Podstawą odpowiedzialności karnej za nielegalne udostępnianie plików jest **art. 116 prawa autorskiego**. Zgodnie z tym przepisem:

1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.
3. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5.
4. Jeżeli sprawca czynu określonego w ust. 1 działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Z powyższego wynika, że z pozoru błahe ściąganie plików przez internautę, może skutkować dla niego bardzo poważnymi konsekwencjami. Grozi mu bowiem **kara grzywny, ograniczenia wolności, a nawet kara pozbawienia wolności do lat dwóch**. Jeśli internauta udostępniał pliki, nie zdając sobie sprawy, że łamie prawo i zdoła to udowodnić grozi mu kara **do roku pozbawienia więzienia**. O rodzaju kary i jej wysokości decyduje sad. Kwota grzywny zależy miedzy innymi od warunków osobistych sprawcy, tego czy do tej pory był karany, jego możliwości zarobkowych i posiadanego majątku. W zależności od okoliczności sprawy, może ona wynieść od 100 zł do 1,08 mln zł.

Kara ograniczenia wolności, w wymiarze od miesiąca do 12 miesięcy polega na **wykonywaniu nieodpłatnej, kontrolowanej przez sąd lub kuratora pracy na cele społeczne.** Wymiar takiej pracy może kształtować się od 20 do 40 godzin miesięcznie. Jeśli oskarżony o rozpowszechnianie plików internauta pracuje, sąd może orzec **potrącenie część jego pensji** (od 15 do 25 proc.) na rzecz Skarbu Państwa lub na cel społeczny.

W zależności od tego, jak zakwalifikowany zostanie czyn internauty przez organy ścigania, tak będzie kształtowała się jego odpowiedzialność. Jeśli działanie sprawcy podyktowane było chęcią **osiągnięcia korzyści majątkowych** w związku z rozpowszechnianiem utworu, grozi mu **kara do trzech lat więzienia**. Dotyczy to wszelkich komercyjnych form rozpowszechniania utworów, w tym pobierania opłat za uzyskiwane dzieła, np. w postaci udostępniania haseł do zaszyfrowanych danych, w przypadku umieszczania ich w Internecie.

Najsurowsze sankcje grożą tym, którzy ze sprzedaży kopii nielegalnie ściągniętych plików lub ich wymiany uczyniły sobie **stałe** źródło **dochodu.** Działania sprawcy muszą więc charakteryzować się wielokrotnością

i systematycznością i być nacelowane na uzyskanie dochodu. Wtedy sprawcy grozi nawet **5 lat wiezienia.**

W wyjątkowych sytuacjach sprawcy będą mogli **uniknąć odpowiedzialności** karnej. Postępowanie karne można bowiem umorzyć, np. ze względu na niską szkodliwość społeczną czynu.

UWAGA!

Odpowiedzialności karnej podlegają również osoby, które bez zgody autora udostępniają legalnie nabyte utwory.

Oznacza to, że uiszczenie opłaty licencyjnej, czy zakup płyty z filmem, czy muzyka i następnie zrippowanie na komputer, nie jest równoznaczne z nabyciem praw autorskich do utworów. Można z nich zatem korzystać, ale nie można ich udostępniać, przekraczając granice dozwolonego użytku.

Czy policja przeszuka użytkownika P2P?

W Polsce zdarzały się przypadku, gdy **policja interweniowała** w konkretnych przypadkach wobec osób zajmujących się wymianą plików poprzez sieci P2P. Wprawdzie zdaniem samej policji, zjawisko rozpowszechniania nielegalnie ściągniętych plików jest nie do opanowania, jednak ci, którzy ściągają utwory na skalę masową i udostępniają zasoby liczone w terabajtach, mają się czego obawiać. W takich sytuacjach, Policja może pojawić się nawet w domu podejrzanego z nakazem przeszukania.

Podstawą przeszukania jest **postanowienie sądu lub prokuratora**. Musi ono wskazywać konkretny cel przeszukania oraz zawierać uzasadnienie. Bez uzasadnionego przypuszczenia, że w mieszkaniu znajdują sie dowody konkretnego przestępstwa, takie postanowienie nie powinno zostać wydane, a policja nie może dokonać przeszukania.

Jeśli istnieje **uzasadnione przypuszczenie**, że w mieszkaniu znajdują sie dowody bezpośrednie lub poszlaki popełnienia konkretnego przestępstwa, np. nielegalnego rozpowszechniania utworów audiowizualnych, sąd może wydać postanowienie o przeszukaniu. Informacja taka musi być uzyskana **w trakcie postępowania przygotowawczego** i jednocześnie musi być udokumentowana w taki sposób, aby z zebranych dowodów wynikało, że poszukiwany dowód przestępstwa, może znajdować sie w przeszukiwanym miejscu.

Może się jednak zdarzyć, że policja będzie miała prawo dokonać przeszukania domu internauty. Stanie się tak w tzw. **przypadkach niecierpiących zwłoki**, gdy postanowienie o przeszukaniu (z uwagi na konieczność szybkiej reakcji) nie mogło być wydane. Chodzi tu o sytuacje, gdy szybkie dokonanie takich czynności jest konieczne, z uwagi na możliwość ewentualnego zatarcia lub utraty śladów popełnionego przestępstwa. Wtedy policja może dokonać przeszukania na podstawie **pisemnego nakazu** kierownika swej jednostki lub okazując **legitymacje** służbową.

Policja ma przy tym obowiązek poinformować osobę, u której dokonuje sie przeszukania o prawie żądania doręczenia takiego zatwierdzenia w ciągu siedmiu dni od daty czynności. W przeciwnym razie, dowody znalezione w czasie przeszukania, nie mogą zostać wykorzystane w procesie. Na wszelkie czynności związane z przeszukaniem, osobom zainteresowanym przysługuje **prawo zażalenia**.

Policja może też zarekwirować znaleziony w mieszkaniu komputer. W takim przypadku jego właściciel powinien otrzymać pokwitowanie stwierdzające, jakie przedmioty i przez kogo zostały zatrzymane. Policja ma przy tym obowiązek zachowania tzw. umiaru i poszanowania godności.

PRAWA INTERNAUTY, U KTÓREGO JEST PRZESZUKANIE

- Prawo wglądu w nakaz przeszukania.
- Prawo żądania doręczenia, zatwierdzenia przeszukania, dokonanego bez nakazu w ciągu 7 dni.
- Prawo odmowy wpuszczenia chcącej dokonać przeszukania policji w godzinach 22.00–6.00 (chyba, że jest to przypadek niecierpiący zwłoki).
- Prawo otrzymania pisemnego potwierdzenia zatrzymanych rzeczy i ich zwrotu, gdy nie będą już przydatne w sprawie.
- Prawo zakazania wglądu w rzeczy mające charakter osobisty (wtedy zostaną przekazane bezpośrednio prokuratorowi lub sędziemu).
- Prawo zgłoszenia oświadczeń i wniosków do protokołu przeszukania oraz ich odczytania przed zakończeniem czynności.
- Prawo zgłoszenia zarzutów do treści protokołu przeszukania.
- Prawo złożenia zażalenia na postanowienie o przeszukaniu, zatrzymaniu rzeczy i inne czynności przeszukania, do sądu lub prokuratora nadrzędnego nad wydającym dane postanowienie.

Internetowe przestępstwa ścigane na wniosek…

Podkreślenia wymaga fakt, iż ściganie karne odbywa się albo **na wniosek pokrzywdzonego** (złożony na policji lub w prokuraturze), albo **wszczynane jest z urzędu** („piractwo", organizowanie, kierowanie). Pokrzywdzonym może być zarówno sam twórca lub artysta, wykonawca, jak również jego **spadkobierca lub inny podmiot będący właścicielem autorskich lub pokrewnych praw majątkowych,** a także **organizacja zbiorowego zarządzania prawami autorskimi lub pokrewnymi** np. ZAiKS, SAWP, ZASP, STOART.

Z chwilą złożenia wniosku, postępowanie **będzie toczyć się z urzędu**. W razie złożenia wniosku o ściganie niektórych tylko sprawców, obowiązek ścigania obejmuje również inne osoby, których czyny pozostają w ścisłym związku z czynem osoby wskazanej we wniosku. Wniosek może być **cofnięty w trakcie dochodzenia** lub śledztwa za zgodą prokuratora, a w postępowaniu sądowym za zgodą sądu - do rozpoczęcia przewodu sądowego na pierwszej rozprawie głównej, czyli do odczytania aktu oskarżenia.

Przepisy prawa **nie określają formy**, w jakiej pokrzywdzony ma wyrazić wolę ścigania, czyli złożyć wniosek o wszczęcie dochodzenia lub śledztwa. Wola ta może być zatem wyrażona np. do protokołu przesłuchania w charakterze świadka. Istotne jest to, by z dokumentu procesowego w sposób wyraźny wynikało żądanie przez pokrzywdzonego ścigania sprawcy.

Z powyższego wynika, że nawet, jeżeli policja trafi na ślad nielegalnego rozpowszechniania utworów, to **musi wystąpić do pokrzywdzonego o złożenie wniosku**. Jeżeli mimo takiej informacji nie zdecyduje sie on na ściganie sprawcy, to śledczy będą musieli odmówić wszczęcia postępowania karnego albo je umorzyć.

Z orzecznictwa…

„przestępstwo wnioskowe ***oznacza, że brak wniosku o ściganie pochodzącego od osoby uprawnionej stanowi ściśle procesową***

***przesłankę skutkującą niedopuszczalnością postępowania karnego. Brak wniosku jest bezwzględną przyczyną odwoławczą z art. 439 § 1 pkt 9 kpk skutkującą uchylenie orzeczenia i to, niezależnie od granic zaskarżenia i podniesionych zarzutów. Nie jest dopuszczalne przyjęcie kumulatywnej kwalifikacji prawnej czynu sprawcy, z przepisu przewidującego ściganie z urzędu oraz przepisu przewidującego ściganie na wniosek, a nawet nie jest dopuszczalne ujęcie w opisie czynu przypisanego sprawcy elementów faktycznych należących do istoty przestępstwa ściganego na wniosek*".**

(Wyrok Sądu Najwyższego - Izba Karna z dnia 15 października 2003 r., IV KK 299/2003.

Z urzędu ścigana jest jedynie kwalifikowana forma tego rodzaju czynu przestępczego, polegająca na uczynieniu sobie z takiego procederu stałego źródła dochodu albo kierowanie taką działalnością lub jej organizowanie. Chodzi tu o dużą szkodliwość społeczną czynu.

Z orzecznictwa…

Jednorazowe udostępnienie utworu tylko w najbliższym kręgu (bliscy krewni, znajomi lub współpracownicy) nie jest rozpowszechnianiem utworu w rozumieniu art. 116 ust. 1 ustawy o prawie autorskim i prawach pokrewnych.

(wyrok Sadu Okręgowego w Tarnowie z 8 listopada 2007 r. sygn. akt II Ka 464/2007).

Surowsza odpowiedzialność za ściąganie programów i gier

Znacznie surowiej przepisy prawa traktują nielegalne pobieranie programów i gier komputerowych. Uwagi na większą szkodliwość społeczną, czyn taki traktowany jest jako **przestępstwo, za które sankcje przewiduje sam kodeks karny** (art. 278 § 2).

Zgodnie z tym przepisem, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy (w tym także grę komputerową) w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności **od trzech miesięcy do pięciu lat**. Za korzyść majątkową może być uznany sam fakt, że internauta nie pójdzie do sklepu i nie wyda kilkudziesięciu złotych na legalny produkt.

Uwaga!

Przestępstwo kradzieży programu komputerowego z art. 278 § 2 k.k. oznacza wszelką formę przejęcia takiego programu bez zgody jego dysponenta w taki sposób, który umożliwia wykorzystywanie tego programu przez osobę nieuprawnioną. Jest to przestępstwo materialne, do którego znamion należy skutek w postaci uzyskania programu komputerowego, a wiec objecie przez sprawcę we władanie zapisu magnetycznego za pomocą którego zakodowany został odpowiedni utwór nazywany programem komputerowym. Skutek stanowiący znamię przestępstwa występuje w momencie objęcia przez sprawcę w posiadanie nośnika informacji z programem komputerowym.

(wyrok Sadu Apelacyjnego w Krakowie, z 8 lipca 2009 r. sygn. akt II AKa 98/2009).

Oczywiście można ściągać z Internetu **darmowe lub próbne wersje** takich programów i jest to działanie całkowicie legalne. Natomiast do korzystania z całych wersji bardziej wyrafinowanych gier potrzebna jest pełna licencja, którą najczęściej można uzyskać dopiero przy zakupie.

Co z użytkownikami Peer to Mail (P2M)?

W ostatnich latach, dużą popularnością wśród internautów cieszy sie nowa technologia wymiany plików Peer2Mail. Jest to technologia wymiany plików, opierająca się o **wykorzystanie kont pocztowych jako miejsca ich przechowywania**. Twórcą pierwszego na świecie programu, opierającego się na tej technologii, jak i również samego systemu wymiany Peer2Mail jest **Izraelczyk Ran Geva**.

P2M różni się od tradycyjnych Peer-to-Peer (P2P) miejscem lokalizacji ściąganego utworu. Wymiana plików za pomocą P2M odbywa się za pośrednictwem specjalnego oprogramowania, które w sposób automatyczny i przy ograniczonej ingerencji użytkownika, umożliwia masowe zakładanie kont pocztowych w darmowych i ogólnodostępnych serwisach, przygotowanie (np. podział na części o maksymalnej wielkości zgodnej z możliwością danego konta e-mail) oraz umieszczenie plików na tych kontach. Są to **darmowe skrzynki pocztowe** o dużej pojemności udostępniane przez wiele portali internetowych (np. Yahoo!, Google czy Tlen). W nich przechowywane są pliki z filmami, grami i muzyka.

W procesie wysyłania plików na konta generowany jest tzw. ***hashcode***, czyli zaszyfrowana informacja (często w postaci ciągu znaków ASCII), zawierająca **dane skrzynek** pocztowych, na których znalazły się pliki, **hasła do tych skrzynek** oraz dodatkowe informacje na temat danych, takie jak suma kontrolna. Osoba, dysponująca hashcode oraz ustalonym do niego hasłem, może je wykorzystać do pobrania plików za pomocą klienta obsługującego dany format hashcode. Mechanizm szyfrowania klientów P2M opiera się o hasła, jednak nie udostępnia użytkownikom wprost odszyfrowanych danych, nawet po podaniu prawidłowego hasła, a jedynie wykorzystuje je do zalogowania się i pobrania plików z kont pocztowych. W ten sposób wymieniane pliki chronione są przed umyślnym lub przypadkowym usunięciem.

Do pobrania zawartości skrzynki, wystarczy zatem znać zarejestrowany wcześniej na forum internetowym **login oraz hasło**. Wtedy można ściągać pliki tak samo, jak zwykłe listy z załącznikami.

Podstawową wadą P2M jest **brak wyszukiwarek**. Każdy użytkownik jest zdany po części na zasoby swoich znajomych, chociaż należy wspomnieć, iż już powstają strony indeksowe. Z kolei dużą zaletą P2M są **wysokie transfery** oraz brak problemów z lokalnymi adresami IP. Pobieranie poczty jest najpopularniejszym z protokołów i zazwyczaj ma wysoki priorytet w konfiguracji serwerów.

Korzystanie z P2M a przepisy prawa

Technologia P2M wkrótce po jej udostępnieniu internautom zdołała się tak rozwinąć, że wyprzedziła regulacje prawne dotyczące tej materii zawarte w ustawodawstwach poszczególnych państw. Obecnie w większości państw, służby policyjne **nie mogą** ścigać osób**, które pobierają pliki poprzez Peer-to-Mail i kopiują je tylko na własny użytek**.

Również w Polsce dopuszczalne jest pobieranie już rozpowszechnionych utworów audiowizualnych. Prawo zabrania jedynie ich nielegalnego rozpowszechniania. Legalne jest natomiast **udostępnianie plików znajomym** (np. pożyczenie płyty bratu) pod warunkiem, że nie są czerpane korzyści materialne z rozpowszechniania plików.

Wielu internautów za zaletę P2M uważa to, że ściąganie plików przy jego użyciu nie stanowi przestępstwa. Niestety nie jest to

prawdą. Obowiązuje tu bowiem taka sama zasada, jak przy korzystaniu z P2P. Jednak o ile w P2P ściągając pliki internauta ma również obowiązek udostępniać swoje pliki innym, o tyle w przypadku P2M nie ma takiego obowiązku.

Z drugiej strony, nawet w P2M zawsze musi znaleźć sie co najmniej kilku internautów, którzy będą musieli udostępniać swoje, przenosząc je na skrzynki pocztowe. Trzeba przy tym pamiętać, że policja ma możliwości techniczne dotarcia do takiej poczty i wykrycia sprawców nielegalnie rozpowszechniających pliki. Jest to jednak o wiele trudniejsze. Policja ma prawo jedynie wnioskować o kontrole takiej korespondencji, ale zgodę na kontrole i tak wydaje sąd.

Czy odpowiadają również hosterzy?

Aby doszło do rozpowszechnienia utworu w Internecie, pliki muszą zostać umieszczone na konkretnej przestrzeni dyskowej. Pojawia się zatem pytanie, czy odpowiedzialność ponoszą też podmioty świadczące **usługi hostingowe**, tj. polegające na udostępnianiu miejsca na pliki Internautów? Problem staje się bardzo istotny, gdyż popularność serwisów społecznościowych, w ramach których indywidualni użytkownicy mogą swobodnie umieszczać dane, rośnie bowiem w zawrotnym tempie.

Z prawnego punktu widzenia, działalność operatorów świadczących usługi hostingowe, wykorzystywane do nielegalnego rozpowszechnienia utworów w sieci, może być uznana za **pomocnictwo do popełnienia przestępstwa** z art. 116 kk.

Zgodnie z Kodeksem karnym, **odpowiada za pomocnictwo ten**, kto w zamiarze, aby inna osoba dokonała czynu zabronionego, swoim zachowaniem ułatwia jego popełnienie, a w szczególności dostarcza narzędzi, środka przewozu, udzielając rady lub informacji. Odpowiada za pomocnictwo także ten, kto wbrew prawnemu, szczególnemu obowiązkowi niedopuszczenia do popełnienia czynu zabronionego, swoim zaniechaniem ułatwia innej osobie jego popełnienie. W przypadku serwisów internetowych, w grę będzie wchodzić **popełnienie pomocnictwa poprzez działanie.**

Nie ma tu znaczenia, czy usługa hostingu jest **odpłatna**, czy też za umieszczanie materiałów przez internautów nie są pobierane jakiekolwiek opłaty. W obu przypadkach, aby uwolnić się od odpowiedzialności, hosternie będzie musiał wykazać, że **nie wiedział o bezprawnym charakterze danych użytkownika lub działalności z nimi związanej**. Jeśli zaś hoster otrzyma urzędowe zawiadomienie lub uzyska inną wiarygodną wiadomość o bezprawnym charakterze danych lub związanej z nimi działalności, powinien niezwłocznie uniemożliwić dostęp do tych danych.

Hoster, który otrzymał takie urzędowe zawiadomienie i uniemożliwił internaucie dostęp do tych danych, **nie odpowiada względem tego internauty za szkodę**, którą ten poniesie w wyniku zablokowania dostępu. Podobnie będzie w przypadku otrzymania przez hostera wiarygodnej wiadomości o bezprawnym charakterze danych dostarczonych przez internautę. Jeśli wówczas hoster uniemożliwił internaucie dostęp do danych, nie będzie odpowiadał względem tego internauty, za szkodę powstałą w wyniku zablokowania dostępu, jeżeli **niezwłocznie zawiadomił** go o zamiarze uniemożliwienia do nich dostępu .

UWAGA!

Zasadniczo Hoster nie ma obowiązku weryfikowania, czy materiały udostępniane przez internautów naruszają autorskie prawa majątkowe.

Jednakże w przypadku, gdy operator usługi hostingowej samodzielne wprowadzał utwory bez stosownego uprawnienia lub decydował, które z materiałów mogą pozostawać na stałe w serwisie, może zostać pociągnięty do **odpowiedzialności za pomocnictwo** lub nawet za **organizowanie bądź kierowanie rozpowszechnianiem dzieł bez uprawnienia**. Będzie to miało miejsce w szczególności w sytuacji, gdy przed ostatecznym udostępnieniem użytkownikom utworu, jest on umieszczany w „elektronicznej przechowalni", a finalną decyzję w przedmiocie rozpowszechniania danych podejmuje administrator (hoster).

Z orzecznictwa…

Warto tu przytoczyć orzeczenie Trybunału Sprawiedliwości Wspólnot Europejskich z 23.3.2010 r. w połączonych sprawach Google France SARL, Google Inc. p. Louis Vuitton Malletier SA (C-236/08), Google France SARL p. Viaticum SA, Luteciel SARL (C-237/08), Google France SARL p. Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Brunon Raboin, Tiger SARL (C-238/08). Rozstrzygnięcie dotyczyło kwestii stosowania reklamy kontekstowej w internecie, lecz poruszyło jednocześnie omawianą problematykę. Orzeczenie Trybunału wskazuje jednoznacznie, iż: „Artykuł 14 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), należy interpretować w ten sposób, że ustanowiona w nim zasada ma zastosowanie do podmiotu świadczącego usługę odsyłania w internecie, jeżeli przy świadczeniu swych usług usługodawca ten nie odgrywa czynnej roli, która mogłaby sprawić, że będzie on posiadał wiedzę o przechowywanych informacjach lub miał nad nimi kontrolę. Jeżeli wspomniany usługodawca nie odgrywa takiej roli, nie może być on pociągnięty do odpowiedzialności za treść przechowywanych przez siebie na żądanie reklamodawcy informacji, chyba że powziąwszy wiadomość o bezprawnym charakterze tych informacji lub działalności reklamodawcy, nie podjął niezwłocznie odpowiednich działań w celu usunięcia wspomnianych informacji lub uniemożliwienia dostępu do nich".

Od lat ustawodawstwa najbardziej rozwiniętych krajów starają się walczyć z nielegalną wymianą plików w Internecie. Tymczasem sieć, jakby żyła swoim życiem. Zawsze jest o krok przed prawem. Mimo zaostrzania kar, a nawet odcinania od sieci niepokornych internautów, liczba udostępnianych utworów ciągle wzrasta. Polscy ustawodawcy próbują w tej kwestii z jednej strony sprostać oczekiwaniom Unii, z drugiej zaś nadążyć za „cyberrozwojem". Jedno jest pewne - po ostatniej aferze związanej z Acta, politycy wreszcie zrozumieli, że Internet jest jak żywioł i że to prawo trzeba będzie dostosowywać do niego, a nie odwrotnie.

Podstawa prawna

- Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. nr 90, poz. 631 z pózn. zm.).
- Ustawa z 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. nr 89, poz. 555 z pózn. zm.).
- Ustawa z 6 czerwca 1997 r. – Kodeks karny (Dz.U. nr 88, poz. 55 3 z pózn. zm.).

Bohdan Widła - absolwent prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, prawnik w kancelarii Maruta i Wspólnicy sp. j., aplikant radcowski.

REWOLUCJA TECHNOLOGICZNA A DANE OSOBOWE

Tomasz Soczynski

Tempo zmian w technologii gromadzenia i przetwarzania w formie dźwięku i obrazu danych osób fizycznych, rodzi konieczność aktualizacji obowiązujących dotychczasowe regulacji prawnych w tej dziedzinie. *Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych* okazuje się niewystarczająca w obliczu zachodzących przemian. Nie dotyczy przetwarzania danych dla potrzeb bezpieczeństwa publicznego, działań organów państwowych w dziedzinie obronności, prawa karnego lub innych działań nie wchodzących w zakres prawa UE. Zmiany proponowane w projekcie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych COM (2012) uwzględniać mają zwiększenie ochrony prywatności[1]. Potrzeby organów bezpieczeństwa i porządku publicznego oraz prawo do zachowania prywatności obywateli stały się w Europie (także w Polsce) przedmiotem ożywionej dyskusji społecznej i politycznej[2].

Rozwój zintegrowanych systemów wideomonitoringu i wielomodalnych systemów pozyskiwania danych rodzi istotne z punktu widzenia ochrony danych osobowych pytania o skutki łączenia danych uzyskanych z systemów zarządzanych przez różne podmioty z systemami danych biometrycznych, stosujących niektóre unikalne właściwości jednostki ludzkiej do identyfikacji i/lub uwierzytelniania[3] (np. osobnicze cechy specyficzne i dystynktywne ruchu, kod DNA, tekstura tęczówki oka, dane medyczne itp.). Systemy biometryczne zbierają dane biometryczne z różnych czujników lub wielu jednostek tego samego źródła. Mogą użyć dwóch lub więcej cech biometrycznych/modalności tej samej osoby w procesie dopasowywania. Multimodalność w biometrii to połączenie różnych technologii biometrycznych w celu zwiększenia wydajności systemu (biometria wielopoziomowa). Źródło, z którego dane biometryczne zostały wyodrębnione (niekiedy bez zgody i wiedzy danej osoby) nie podlega zmianie i nie da się skasować w przypadku kompromitacji danych (np. odcisk palca - człowiek nie jest w stanie zmienić linii papilarnych). Ułatwia to kontrolę i inwigilację obywateli.

1 Wojciech Rafał Wiewiórowski: Privacy by Design jako paradygmat ochrony prywatności [w:] Internet. Prawno-informatyczne problemy sieci, portali i e-usług. Warszawa 2012, s.13-28;

2 https://www.law.kuleuven.be/icri/ and the Social Sciences Research Network electronic library at http://ssrn.com/link/ICRI-RES.html.

3 Opinion 3/2012 on developments in biometric technologies, http://ec.europa.eu/justice/data-protection/index_en.htm00720/12/ENWP193;

Technologia rozpoznawania twarzy, do niedawna temat fantastyki naukowej, jest obecnie dostępna dla organizacji publicznych i prywatnych. Stosuje się ją w dziedzinie usług *online* i telefonii komórkowej w celu identyfikacji i kategoryzacji osób oraz uwierzytelnienia ich tożsamości. Automatyczny odczyt danych i rozpoznawanie twarzy na podstawie obrazu cyfrowego omówiono w *Opinii WP 192 Grupy Roboczej Art. 29 w sprawie systemów rozpoznawania twarzy w usługach online i usługach komórkowych*[4] i w *Opinii WP 193 w sprawie rozwoju technologii biometrycznych*[5]. Uznano rozpoznawanie twarzy za technologię z zakresu biometrii (operowanie szczegółami wystarczającymi do precyzyjnej identyfikacji danej osoby).

Coraz częściej spotykamy się z rozwiązaniami technicznymi znanymi do tej pory tylko z filmów/książek science fiction drugiej połowy XX w. (G. Orwell, „Star Trek"). Zdążyliśmy przywyknąć do automatycznego rozpoznawania twarzy, skanowania pasażerów i ich bagażu na lotniskach, diagnostyki i terapii medycznej (np. urządzeń do błyskawicznej analizy ilości czerwonych krwinek, termometrów bezdotykowych itp). Doświadczenia dowodzą, że nowe technologie są użyteczne społecznie. Medycyna oferuje np. kapsułkę do nieinwazyjnego badania przewodu pokarmowego z miniaturową kamerą, nagrywającą sekwencyjnie obrazy, analizowane następnie przez lekarza.

Przykład innowacyjnego narzędzia pomiarowego i informatycznego (dane w formatach przemysłowych, m.in.: C3D, FBX, Acclaim, Biovision, Maya, 3DS Max) stosowanego w terapii narządów ruchu to *Human Motion Laboratory*[6]. Pozyskuje dane z zakresu ruchu przez jednoczesny synchroniczny pomiar i rejestrację obrazu postaci, umożliwia prowadzenie zdalnej reżyserii i nadzoru sesji pomiarowej oraz szybki dostęp do wyników. Pozwala przechwytywać ruch jednej lub wielu postaci niezależnie oraz w interakcji. Rejestruje cechy specyficzne mimiki, ruchów dłoni, palców i stóp, czyli akwizycję kinematyki ruchu znanej w przemyśle filmowym pod nazwą *Motion Capture*. Wspiera diagnozę schorzeń i leczenie pacjentów. Wykorzystywana jest w medycynie sportowej, diagnostyce chorób układu mięśniowo-szkieletowego. Korzysta się z niej w procesie produkcji reklam i gier komputerowych, ponieważ wyniki analizy i syntezy ruchu pozwalają uzyskać efekt realistycznego poruszania się postaci i elastycznego tworzenia animacji.

Osiągnięcia z zastosowaniem zintegrowanych systemów komputerowych w analizie kinematycznej ruchu zostały przedstawione podczas *VII Sympozjum „Analiza ruchu – teoria i praktyka w zastosowaniach klinicznych"* (Warszawa, 2 marca 2012 r.)[7]. W prezentowanym dorobku naukowym zwracają uwagę zakres zastosowań, metody oraz narzędzia pozyskiwania danych (np. *Biomechaniczna analiza parametrów dynamicznych chodu trójpunktowego o kulach na przykładzie pacjentów po jednostronnej endoprotezoplastyce stawu biodrowego* z użyciem trzech zintegrowanych systemów pomiarowych: Motion Capture BT Smart D, 2 platformy tensometryczne AMTI oraz 16 - kanałowy telemetryczny EMG NORAXON - typu telemyo 2400T G2, str. 16-17; *Ocena*

4 Opinia 02/2012 w sprawie systemów rozpoznawania twarzy w usługach *online* i usługach komórkowych, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_pl.pdf;

5 Patrz przyp. 3);

6 www.pjwstk.edu.pl;

7 (http://www.neuromed- sc.com.pl/attachments/File/Publikacje/VII_symp_analiza_ruchu.pdf);

funkcjonalna pacjentów z mózgowym porażeniem dziecięcym operowanych w obrębie tkanek miękkich leczonych uprzednio toksyną botulinową z wykorzystaniem systemu VICON, str. 27; *Implementacja modelu o sześciu stopniach swobody w analizie kinematyki kończyny dolnej człowieka* w oparciu o optyczny system analizy ruchu Optotrak Certus firmy NDI, str. 28-29; *Analiza porównawcza parametrów chodu u osób po prawo i lewostronnym udarze mózgu* w oparciu o system przetwarzania danych APAS i autorskie oprogramowanie opracowane w środowisku MATLAB, str. 18-19).

Zwraca też uwagę dokumentacja danych pozyskiwanych z użyciem proponowanego *Edytora Danych Ruchu* (str. 30-31), obejmująca dane personalne z fotografią, katalog jednostek chorobowych, bogate dane antropometryczne, wyniki badań - zanonimizowane dla celu badań naukowych, ale personalizowane w praktyce medycznej. Wykorzystanie systemów analizy ruchu w medycynie wiąże się z koniecznością pozyskania, gromadzenia, przechowywania danych biometrycznych konkretnego pacjenta, mogących służyć jego identyfikacji.

Obciążone wysokim ryzykiem przetwarzanie danych medycznych wymaga zapewnienia najwyższego poziomu bezpieczeństwa. Przywołane powyżej systemy dostarczają ogromnej ilości danych, w tym danych wrażliwych (np. stan zdrowia, kod genetyczny, nałogi, życie seksualne). Ośrodki medyczne i osoby w nich zatrudnione dysponują megabazami danych cyfrowych, a łatwość skopiowania rodzi obawy o ich bezpieczeństwo. Dokument WP 131 Grupy Roboczej Art. 29 dostarcza wskazówek co do wykładni ram prawnych ochrony danych w systemie elektronicznej dokumentacji zdrowotnej (EHR), ustala zasady ogólne i wstępne warunki tworzenia/zabezpieczania ogólnokrajowych systemów EHR[8].

Dokument WP 189 Grupy Roboczej Art. 29, z dnia 25 stycznia 2012[9], zawiera wytyczne w sprawie ochrony danych w związku z projektem epSOS, który zgodnie z wymogami *Dyrektywy 2011/25/WE w sprawie stosowania praw pacjenta w transgranicznej opiece zdrowotnej*, ma na celu zapewnienie usług ułatwiających dostęp do bezpiecznej transgranicznej opieki zdrowotnej[10]. Wskazuje konieczność zapewnienia poufności (wyłącznie autoryzowani użytkownicy, ochrona przed nieupoważnionym dostępem lub niezamierzonym ujawnieniem), integralności danych (ochrona przed nieautoryzowanymi zmianami), rozliczalności (odnotowanie/śledzenie kto z danych korzystał, kiedy i gdzie trafiają). Przy przesyłaniu danych zdrowotnych z użyciem sieci publicznej wymaga wiarygodnych certyfikatów cyfrowych dla systemów serwerowych usługowych i urządzeń końcowych. Szczególną uwagę zwraca na przyjęcie wiarygodnych i skutecznych elektronicznych systemów identyfikacji członków personelu i pacjentów.

Dostęp osób nieuprawnionych musi być zablokowany, przy nieograniczonej dostępności systemu dla uprawnionego personelu medycznego, środki ochrony sfery prywatnej należy stosować w najszerszym możliwym zakresie.

8 Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_pl.pdf;

9 Working Document 01/2012 on epSOS http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp189_en.pdf;

10 Więcej na temat projektu epSOS jest dostępne pod adresem http://www.epsos.eu/;

Niedostateczna ochrona danych zdrowotnych może generować poważne skutki, począwszy od dyskryminacji na rynku pracy lub instytucji finansowych (np. sektor usług bankowych, ubezpieczeniowych itp.) kończąc na inżynierii genetycznej lub handlu ludźmi i ich narządami. Stąd szczególnie ważna jest ochrona danych, które mogą posłużyć do identyfikacji osobniczej, czyli danych biometrycznych.

Nowoczesne technologie oparte na danych biometrycznych spotyka się coraz częściej: systemy dostępu (do pojazdu, pomieszczeń), rozpoznawanie twarzy z prywatnych zdjęć (Picasa), autoryzację na podstawie naczyń krwionośnych w bankomatach, dane biometryczne są w dokumentach (Paszport RFID). Dane te mogą być wykorzystywane także w procesie autoryzacji, w kryminalistyce, kontroli granicznej, kontroli dostępu i rejestracji czasu pracy.

Identyfikacji biometrycznej służy też analiza obrazu tęczówki oka[11]. Wielkie zróżnicowanie i niepowtarzalność jej tekstury czyni ją jedną z najpewniejszych metod weryfikacji osób. Celem identyfikacji konieczna jest rejestracja użytkownika w systemie, co wymaga wykonania serii zdjęć (najczęściej trzech), poddanych procesowi kompensacji obrotu gałki ocznej metodami korelacyjnymi. Dla automatycznie wyznaczonych obszarów tęczówki wyznaczany jest następnie wektor cech, zapamiętywany w systemie i umieszczony w bazie danych systemu weryfikacji jako wzorzec biometryczny, do którego odnoszone są pozyskane próbki. Weryfikacja, z racji jednolitej struktury otrzymanego binarnego wektora cech, polega na wyznaczeniu liczby zgodnych bitów w wektorze wzorcowym oraz wektorze weryfikowanym.

Ważnym krokiem w dążeniu do właściwej ochrony danych biometrycznych jest implementacja algorytmów wykorzystujących wzorzec tęczówki (także cech geometrii dłoni) na karcie mikroprocesorowej w technologii *match-on-token*[12]. Technologia ta rezygnuje z centralnych baz danych biometrycznych, ponieważ nie wymaga pobrania danych z karty do zewnętrznej jednostki obliczeniowej. Umożliwia bezpieczne porównywanie przechowywanych wzorców biometrycznych bez potrzeby przenoszenia ich z karty mikroprocesorowej, podobnie jak ma to miejsce w przypadku podpisu cyfrowego przez kartę mikroprocesorową, gdzie również zastosowano blokadę możliwości odczytania klucza prywatnego.

Źródłem pozwalającym na identyfikację osobniczą jest analiza cech chodu, bazująca na danych z kamer wideo, co pozwala na identyfikację bezpośrednio z nagrań systemów monitorujących (obrazy 2D), neutralną i nie wymagającą świadomości badanego. Zbadanie osobniczych cech chodu jest możliwe przy zastosowaniu systemu *Motion Capture*, umożliwiającego na dokładny pomiar parametrów chodu w czasie. Uciążliwość przygotowania procesu akwizycji (naklejenie w odpowiednich miejscach specjalnych znaczników śledzonych przez kamery wizyjne oraz ich kalibracja do określonego modelu szkieletowego) rekompensują zalety systemu, to jest uniezależnienie badania od jakości nagrań wideo i niedoskonałości metod wykrywania sylwetek postaci na obrazach 2D. System pozwala na ocenę całościową, szacującą z jaką skutecznością na podstawie danych chodu można przeprowadzić identyfikację lub dokonanie eksploracji cech chodu pod kątem różnicowania osobniczego. Badania[13] prowadzone na grupie

11 *Andrzej Pacut, Adam Czajka*: Biometria w Europie – Projekt BioSec – Biometrics and Security (IST-2002-001766-BIOSEC, http://www.biosec.org);

12 tamże, s. 7;

13 Adam Świtoński, Andrzej Polański, Konrad Wojciechowski: Osobnicze cechy chodu, Polsko-Japońska Wyższa Szkoła Technik Komputerowych;

mężczyzn w wieku 20-35 lat potwierdziły, że: *„chód posiada cechy osobnicze na podstawie których możliwa jest identyfikacja. Uzyskane wyniki dla ścieżek chodu dają praktyczne wskazówki przy budowie systemów biometrycznych bazujących na monitoringu mono- lub stereowizyjnym. Możliwa jest ocena doskonałości metod wyznaczania sylwetek postaci z obrazów 2D. W optymalnym przypadku skuteczności identyfikacji dla danych pochodzących z systemu Motion Capture i obrazów 2D powinny być zbliżone*"[14].

SZANSE i ZAGROŻENIA

Powszechnie uważa się, że wykorzystanie danych identyfikujących prowadzi do wzrostu bezpieczeństwa publicznego. Paradoksalnie to, co ma służyć ochronie, może stać się zagrożeniem utraty prywatności. Zawansowane technologie trafiły do domów i miejsc pracy. Dziś nie tylko odpowiednie służby państwa mogą bez trudu zidentyfikować tożsamość. Dane o stanie zdrowia, kontaktach, zachowaniach, nawykach i preferencjach stały się produktem komercyjnym. Bank-bibliotekę próbek DNA uruchomiono we Wrocławiu w czerwcu br., a ze względów bezpieczeństwa materiał genetyczny przechowywany w jest dwóch niezależnych miejscach, a dokumentacja wiążąca próbkę z konkretną osobą w trzecim. Kolejnym podmiotem przechowującym dane szczególnie chronione są banki komórek macierzystych. A przecież mimo stosowanych zabezpieczeń wycieki danych nie należą do rzadkości. Z ILITA[15] wyciekło 9 milionów danych dotyczących mieszkańców Izraela, a 77 milionów danych i haseł wyciekło z Sony Online Entertainment, oferującej gry typu MMOG.

Stosowanie technologii pozyskujących dane identyfikacyjne dla celów medycznych zdaje się nie budzić wątpliwości. Wiele jesteśmy w stanie poświecić dla zapewnienia zdrowia i życia sobie i naszym bliskim. To jeden z przejawów potrzeby bezpieczeństwa, jednej z najbardziej elementarnych potrzeb człowieka. Czy jednak poczucie bezpieczeństwa nie jest iluzoryczne? Jaką część wolności osobistej i społecznej jesteśmy gotowi poświęcić, by czuć się bezpiecznie?

Chętnie wskazuje się na kluczową rolę informacji w ochronie społeczeństwa, a kreowanie społeczeństwa informacyjnego uznaje za podstawowy warunek rozwoju. Przyspieszenie cywilizacyjne, cyfryzacja w gospodarce, nauce, kulturze, edukacji, komunikacji i transporcie, powszechne stosowanie technologii IC/ICT, komunikatory, urządzenia i czujniki generują możliwości pozyskiwania danych, co rodzi ich nadprodukcję i stymuluje popyt - zyskują one coraz wyższą wartość w sensie społecznym i ekonomicznym.

Największe kontrowersje, nie tylko w społeczeństwach dotkniętych w przeszłości totalitaryzmami i traktującymi wolność jako niezbywalną wartość uniwersalną, wzbudza dostęp służb bezpieczeństwa publicznego do nieograniczonej ilości informacji potencjalnie przydatnych, w tym danych identyfikujących, postrzegany jako zagrożenie dla prywatności i wolności indywidualnej obywateli. Dostosowanie działań policyjnych i wywiadowczych do zgodnego z prawem i interesem społecznym korzystania z informacji to szansa i wyzwanie dla służb publicznych. Korzystne dla bezpieczeństwa życia publicznego jest stosowanie przez organy ścigania narzędzi pozwalających na efektywne

14 Tamże;
15 Izraelski Urząd ds. Prawa, Informacji i Technologii;

przeciwdziałanie zagrożeniom. Systemy monitoringu internetowego, miejskiego i prywatnego zapewniają cenne informacje służące zapobieganiu i ściganiu przestępstw, a także ochronie ludności, np. dla zarządzania kryzysowego.

Realizowany w latach 2006-2008 projekt badawczy DYVINE (Dynamic Visual Networks) zakładał stworzenie dynamicznie konfigurowalnego systemu/sieci nadzoru wideo, dostarczającego precyzyjnych informacji o nadchodzących katastrofach (np. powodzie) i łączącego na stałe, wszystkie sieci wideonadzoru będące w posiadaniu władz lokalnych, także związanych z policją, z możliwością rozszerzenia go na żądanie o prywatne systemy monitoringu. Dzięki wykorzystaniu technologii IP jest to przedsięwzięcie realne i tanie (redukuje koszty instalacji i pozwala na przekazanie wszelkiego rodzaju danych: obrazów, dźwięku, instrukcji, oprogramowania, itp.). Wideosystemy, de facto wszechobecne, elastyczne i inteligentne są w stanie identyfikować, śledzić i analizować zachowania ludzi oraz zdarzenia. Umożliwiają także adaptowanie konfiguracji i charakterystyki sieci monitoringu do zmieniających się okoliczności (np. rozszerzenie monitorowanego obszaru).

Projekt INDECT realizowany pod hasłem „Zwiększania bezpieczeństwa obywateli" przez Akademię Górniczo-Hutniczą w Krakowie zakładał stworzenie inteligentnego systemu przetwarzania informacji multimedialnych do automatycznego wykrywania zagrożeń i rozpoznawania działań przestępczych lub przemocy (dziecięca pornografia w Internecie, promowanie zakazanych symboli, handel ludzkimi organami, rozprzestrzenianie niebezpiecznego oprogramowania, jak również akty terroryzmu itp.), a następnie wykrywanie źródła zidentyfikowanych przestępstw (np. konkretnych kryminalistów kryjących się za przestępstwami).

Generalny Inspektor Ochrony Danych Osobowych wskazał[16], iż w opinii GIODO projekt INDECT rodzi zagrożenia związane ze sposobem i granicami wykorzystania danych będących w posiadaniu organów bezpieczeństwa oraz z możliwą komercjalizacją projektu (stworzone narzędzia mogły być używane przez inne podmioty, w tym komercyjne).

W opinii publicznej system ten przypominał orwellowski ujednolicony system kontroli audiowizualnej i inwigilacji politycznej, wzbogacony o możliwość kontrolowania forów dyskusyjnych, połączeń telefonicznych, ulic, chatów, mms, e-maili, sms, a także rozmów w świecie rzeczywistym poprzez szereg kamer i podsłuchów rozmieszczonych praktycznie wszędzie tam, gdzie odbywa się ruch publiczny (puby, markety, firmy, przystanki, komunikacja miejska, ulice, domy prywatne - za pomocą kamer w urządzeniach elektronicznych). Miał analizować słowa, ich brzmienie, gesty, ruch gałek ocznych, ust, mimiki, również w prywatnym domu za pomocą laptopa lub telefonu wyposażonego w kamerę video, pozwalał uruchomić każde urządzenie za pomocą zdalnych kodów pozyskiwanych od producentów urządzeń. Wskazywano też, że promowane przez media połączenia wideo, kamery wbudowane w telewizory, laptopy tworzą już idealną siatkę kontroli publicznej.

W kwietniu 2012 r. Minister Spraw Wewnętrznych w porozumieniu z komendantem głównym policji podjął decyzję o wstrzymaniu współpracy Policji nad projektem INDECT i wykorzystania jego efektów. Nie planuje dalszego udziału w pracach nad projektem.

16 http://www.giodo.gov.pl/1520001/id_art/4644/j/pl/;

Od lat 70-tych XX wieku jednak funkcjonuje leciwy komputer w strukturach EWG (B.E.A.S.T – Bestia), pozwalający na katalogowanie ludzi oraz ich preferencji. Codziennie doświadczamy skutków działania logicznych systemów analizujących preferencje informacyjne, marketingowe, osobiste, seksualne w sieci. Systemy komunikacyjne są zdolne łączyć dane w historię życia zapisaną na twardych dyskach, której można użyć celem skandalu, szantażu, wymuszenia.

Przy ocenie skutków wdrażania nowych technologii z punktu widzenia ochrony danych osobowych, należy brać pod uwagę kryteria sformułowane w Dyrektywie 95/46 WE oraz w ustawie o ochronie danych osobowych tj. zasadę adekwatności, celowości i proporcjonalności zbieranych danych oraz zagwarantować skuteczne zabezpieczenia. I oczekiwać zapowiedzianej aktualizacji europejskich ram prawnych ochrony danych osobowych.

Tomasz Soczynski - Absolwent Uniwersytetu Śląskiego zatrudniony w Biurze Generalnego Inspektora Ochrony Danych Osobowych na stanowisku zastępcy dyrektora Departamentu Informatyki.

Zapraszamy do udziału

KONFERENCJA
INTEGRACJA SYSTEMÓW INFORMATYCZNYCH
4 października 2012 r., Warszawa

Kolejna, już dziewiąta, edycja konferencji ukierunkowana została na problemy integracji systemów informatycznych w instytucjach sektora finansowego. W tym sektorze integracja zawsze była zagadnieniem wyjątkowo złożonym i obarczonym dużym ryzykiem. Zaproszeni prelegenci podzielą się swoimi doświadczeniami z projektów integracyjnych realizowanych w szczególności w bankowości, sektorze ubezpieczeń, instytucjach związanych z rynkiem papierów wartościowych oraz w firmach, których podstawą działalności jest obsługa rozrachunków. Wystąpią zarówno przedstawiciele wiodących ośrodków naukowych, mający poza wiedzą teoretyczną praktyczne doświadczenie w omawianym temacie, jak i przedstawiciele firm informatycznych i instytucji finansowych, posiadający bogate doświadczenie projektowe. Większość prezentacji będzie połączeniem wykładu z elementami case study.
Celem konferencji jest prezentacja aktualnego spojrzenia na integrację systemów informatycznych w kilku różnorodnych aspektach, a także przedstawienie wykorzystywanych współcześnie technik i narzędzi. Zostaną zaprezentowane w szczególności takie zagadnienia jak:

- Architektura korporacyjna, będąca podstawą kluczowych decyzji dotyczących integracji systemów
- Integracja danych z wykorzystaniem koncepcji hurtowni danych, data martów, rozwiązań OLAP, narzędzi ETL
- Integracja aplikacji w oparciu o współczesne podejście do architektury SOA, usług sieciowych, modelu ESB
- Zagadnienia stosowania standardowych systemów zintegrowanych i oprogramowania dedykowanego
- Znaczenie modelowania procesów biznesowych dla integracji systemów informatycznych
- Wzorce projektowe w architekturze zorientowanej na usługi.

Poszczególne zagadnienia zostaną zobrazowane branżowymi przykładami.
Na konferencję zapraszamy zarówno przedstawicieli sektora finansowego, jak i innych branż gospodarki, ponieważ doświadczenia z projektów integracyjnych w instytucjach finansowych pozwalają na wyciągnięcie interesujących wniosków także dla innych przedsiębiorstw. Konferencja jak zawsze jest okazją nie tylko do poszerzenia wiedzy i merytorycznych dyskusji, ale także do nawiązania ciekawych kontaktów.

Więcej informacji: www.cpi.com.pl

Korzyści płynące ze stosowania strategii zarządzania komunikacją w projekcie

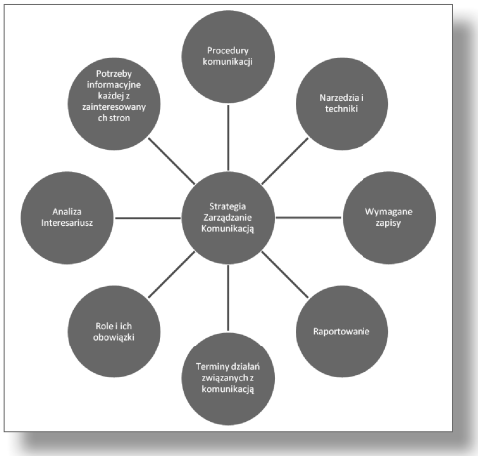
Ewa Szczepańska

Jednym z najważniejszych czynników, który wpływa na projekt, jest poprawna komunikacja pomiędzy wszystkimi osobami biorącymi udział w przedsięwzięciu, zarówno w całej strukturze zarządzania projektem, jak również pomiędzy interesariuszami zewnętrznymi. Chcąc mówić o korzyściach płynących ze stosowania strategii zarządzania komunikacją, w pierwszej kolejności należy prawidłowo zidentyfikować interesariuszy, którzy biorą udział w projekcie oraz osoby, które wpływają na projekt. Następnie, konieczna jest analiza, która pozwoli określić, jakie informacje podczas trwania projektu trzeba przekazać poszczególnym interesariuszom, ponieważ może mieć to wpływ na realizację zagadnień projektowych. Dlatego wskazane jest, aby w każdym projekcie opracować oraz stosować strategię zarządzania komunikacją, która określa sposób oraz częstotliwość komunikacji pomiędzy wszystkimi interesariuszami projektu.

W trakcie procesu przygotowania projektu, należy poświęć wystarczającą ilość czasu na przygotowanie ww. dokumentu oraz ustalić z jakich elementów będzie on składał się. Do głównego zakresu strategii zarządzania komunikacją, należy zaliczyć między innymi: opis środków komunikacji, częstotliwość przekazywania informacji pomiędzy stronami wewnętrznymi i zewnętrznymi projektu. W związku z powyższym szczególny nacisk powinno położyć się na identyfikację interesariuszy, którzy są zaangażowani i powiązani z projektem. Prawidłowa identyfikacja wszystkich interesariuszy ułatwi dalszą pracę w projekcie oraz pozwoli na pełen, jasny i przejrzysty przepływ informacji w realizowanym przedsięwzięciu. Zasadnicze pytania, na jakie należy odpowiedzieć w procesie przygotowania projektu to:

- kto będzie miał wpływ na sukces projektu,
- kto będzie wspierał procesy w projekcie,
- kto będzie przeprowadzał zmiany i
- na kogo będzie miał wpływ projekt?

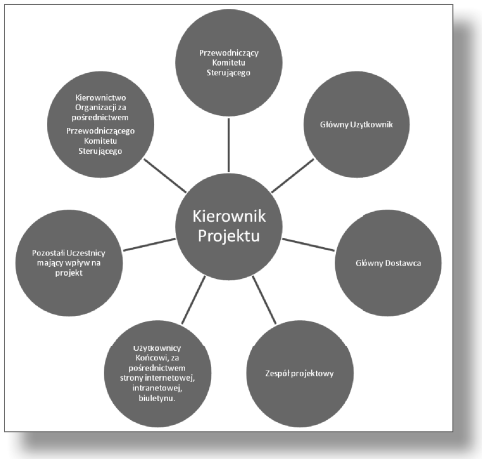
Przygotowując odpowiedzi na powyższe pytania, łatwiej będzie można zidentyfikować interesariuszy, którzy będą zarówno wspierać projekt oraz pojawią się takie grupy uczestników, które mogą sabotować prowadzone działania. Dlatego też prawidłowa identyfikacja interesariuszy, pomoże odpowiedzieć na pytanie „jak wykorzystać działania interesariuszy wspierających projekt"? oraz „jakie działania trzeba podjąć, aby przekonać osoby, które nie chcą angażować się w projekt i podejmować żadnych działań"? Należy pamiętać, że komunikacja w projekcie powinna być również kontrolowana. Czy wszystkie ustalone rodzaje informacji skierowane do poszczególnych interesariuszy są przekazywane w wyznaczonym czasie i w odpowiednim formacie. W strategii zarządzania komunikacją, powinny zostać określone następujące rzeczy:



Rysunek 1 Główne elementy Strategii Zarządzania Komunikacją.
Źródło: Opracowanie własne na podstawie „Skuteczne zarządzanie projektami PRINCE2", 2009.

jakie informacje mają być wysyłane do kogo, jak często i w jakim formacie. Nie należy zapominać o dwukierunkowości komunikacji, czyli informowaniu zainteresowanych stron o postępach prac, jak również udostępnienie kanału przekazywania informacji zwrotnej od interesariuszy, którzy mogą np. zgłaszać zagadnienia projektowe lub zagrożenia i okazje, które wpływają lub wpłyną na projekt. Wśród najważniejszych elementów w strategii zarządzania komunikacją, powinien znaleźć się: cel i zakres, jak również osoba odpowiedzialna za komunikację w projekcie. Konieczne jest określenie procedur komunikacyjnych, czyli uwzględnienie wszelkich przewidzianych metod komunikacji i technik. Ważne jest, aby podać, w jaki sposób ma być przekazywana informacja, jakiego typu raporty będą wytwarzane i udostępniane wyznaczonym grupom. Określenie stałych terminów dostarczania informacji, zdecydowanie umożliwi bieżący dostęp do aktualnych informacji o projekcie poszczególnym interesariuszom. Przechodząc do analizy interesariuszy, można wyróżnić interesariuszy wewnętrznych i zewnętrznych. Identyfikacja i analiza wszystkich zainteresowanych stron, jest kluczowym zadaniem w projekcie. Dzięki prawidłowemu i pełnemu zidentyfikowaniu wszystkich uczestników, jest większe prawdopodobieństwo, że wszystkie strategiczne i ważne informacje zostaną przekazane we właściwym czasie. Każda zainteresowana osoba, będzie wiedziała, w którym momencie znajduje sie projekt, jakie są postępy oraz najbliższe plany i działania. Wśród głównych grup interesariuszy powinni być zidentyfikowani ci, którzy muszą zaakceptować cele projektu. Kolejna grupa, to osoby, z którymi należy wykonać prace i przełożyć cele na działania, które następnie będą realizowane. Wyróżnia się też osoby, które powinny być informowane jedynie o postępach oraz działaniach podjętych w celu realizacji zadania. Do ostatniej grupy zaliczyć należy osoby, które informowane będą o zrealizowanych kamieniach milowych projektu.

Bardzo dobrym rozwiązaniem jest sytuacja, gdy punktem odniesienie dla strategii zarządzania komunikacją jest wdrożona polityka zarządzania organizacją. Jednak gdy organizacja nie posiada takiego dokumentu, to wytyczne dla strategii zarządzania komunikacją w projekcie powinny znaleźć się w dokumencie inicjującym projekt. Organizacja może też wprowadzić w życie odrębny produkt, którym będzie strategia zarządzania komunikacją i stosowana ona będzie we wszystkich prowadzonych projektach w jednostce organizacyjnej.



Rysunek 2 Kierownik projektu a interesariusze
Źródło: Opracowanie własne na podstawie „Skuteczne zarządzanie projektami PRINCE2", 2009.

Ogromna odpowiedzialność spoczywa na kierowniku projektu, który przygotowuje wszelkie raporty oraz informacje, które są dostarczane interesariuszom. Kierownik projektu musi pilnować terminów dostarczania poszczególnych danych oraz powinien zapewnić, że dane zawarte w dokumencie są zawsze aktualne i rzetelne. Poniższy rysunek przedstawia wybranych interesariuszy, z którymi kontaktuje się kierownik projektu i przekazuje im informacje o projekcie. Należy jednak pamiętać, że jest to komunikacja dwustronna i każda ze stron może przekazać kierownikowi projektu istotne informacje na temat prowadzonego przedsięwzięcia, które kierownik projektu powinien odnotować, uwzględnić je lub przekazać zainteresowanym stronom.

W strategii zarządzania komunikacją w projekcie, można zastosować kilka metod komunikacji, takich jak forma pisemna, gdzie dokumenty adresowane mogą być do przewodniczącego komitetu sterującego lub to kierownictwa organizacji za pośrednictwem przewodniczącego komitetu sterującego, wykorzystanie poczty elektronicznej, faksu, telefonu, komunikacji bezpośredniej, jak również spotkań projektowych. Repozytorium dokumentów, czy wykorzystanie systemów informatycznych, również można zaliczyć do metod komunikacji w projekcie. Wśród spotkań, które prowadzone są podczas trwania projektu wyróżnić można następujące rodzaje: spotkania rady projektu, posiedzenia komitetu sterującego, spotkania robocze kierownika projektu z dostawcą i użytkownikami oraz z zespołem projektowym. Oprócz rodzajów spotkań, określa się również ich częstotliwość oraz rodzaje dokumentów, które będą przygotowane na dane spotkanie i jakie będą wytworzone w trakcie i po spotkaniu. Rady projektu mogą odbywać się np. nie częściej niż raz w miesiącu lub w razie wystąpienia takiej potrzeby. Na poziomie ww. spotkań podejmowane są decyzje strategiczne, które mają wpływ na organizację lub też programy prowadzone przez instytucję. Posiedzenia komitetu sterującego mogą odbywać się np. nie częściej niż raz w miesiącu. Na każde posiedzenie komitetu sterującego konieczne jest przygotowanie dokumentacji, np. takiej jak:

- raport okresowy
- rejestr ryzyka
- rejestr zagadnień projektowych
- wiosek wprowadzenia zmiany
- plan nadzwyczajny

Przygotowana dokumentacja przez kierownika projektu, musi być dostarczona przed spotkaniem, tak aby zainteresowane strony, czyli przewodniczący komitetu sterującego, główny użytkownik oraz główny dostawca, mogli zapoznać się z zagadnieniem. W trakcie spotkania powinna powstać notatka, w której zawarte zostaną wszystkie ustalenia podjęte na posiedzeniu.

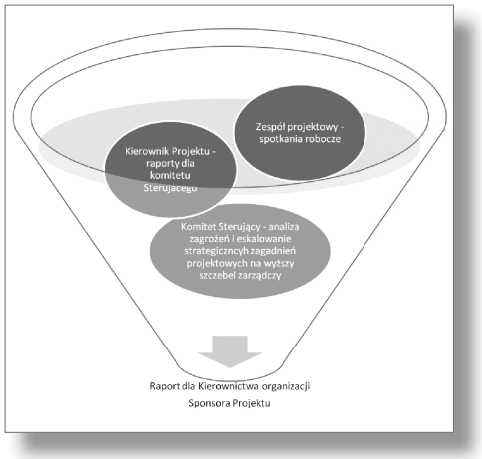
Ważne jest, aby kierownik projektu systematycznie spotykał się z zespołem projektowym, któremu powinien przekazywać najważniejsze ustalenia i wytyczne, jakie miały miejsce np. na spotkaniach rady projektu, czy posiedzeniach komitetu sterującego, a mają wpływ na zagadnienia projektowe. Spotkania projektowe powinny odbywać się nie rzadziej niż raz na dwa tygodnie.

W każdej strategii zarządzania komunikacja w projekcie, powinny znaleźć się również informacje ze spisem danych adresowych i kontaktów do poszczególnych interesariuszy. Przykładowo, można zamieścić tam: imię i nazwisko, rola w projekcie, adres e-mail, telefon oraz organizacja, którą dany interesariusz reprezentuje. Przygotowanie takiego zestawienia osób zdecydowanie ułatwi pracę w projekcie i zaoszczędzi sporo czasu, gdy konieczne będzie skontaktowanie się z konkretną osobą lub grupą osób.

Poprzez wdrożenie w organizacji, a co za tym idzie w każdym projekcie strategii zarządzania komunikacja, możliwe staje się uzyskanie systematycznych i terminowych informacji o przedsięwzięciu w określonej, jednakowej formie. Informacje o projekcie powinny być gromadzone w wyznaczonym miejscu tak, aby każda z zainteresowanych stron, miała dostęp do wyznaczonego zakresu informacji, który jest adekwatny do pełnionej przez nią roli w projekcie. Wszystkie osoby biorące udział w projekcie rozmawiają tym samym językiem projektowym, a przez stosowanie ustalonej formy przekazu informacji określonej w strategii zarządzania komunikacją otrzymują jednolite, spójne i kluczowe informacje do dalszego prowadzenia projektu, które w konsekwencji przyczyniają się do osiągnięcia wyznaczonego celu. Ideą strategii zarządzania komunikacją, jest zrozumienie przez każdego uczestnika procesu tego, jak ważne jest przekazywanie informacji i dostosowanie się do ustalonych reguł oraz zrozumienie powiązań pomiędzy poszczególnymi grupami interesariuszy.

Ważnym elementem w komunikacji jest model nadawca - odbiorca jak również dwukierunkowość przekazywania informacji. Należy pamiętać o barierach komunikacyjnych, jakie mogą wystąpić w trakcie trwania projektu. Oprócz zidentyfikowania intereasiuszy, należy zadać sobie pytanie, które informacje będzie potrzebował wybranym interesariuszom w poszczególnych etapach projektu? Jakie grupy informacji i interesariuszy można połączyć, aby osiągnąć pozytywny efekt dla przedsięwzięcia.

Koncentrując się na strukturze organizacji, a co za tym idzie, na strukturze zarządczej w projekcie, można odnieść to do ilości informacji jakie są wytwarzane i przekazywane na poszczególnych szczeblach zarządczych projektu. Istotnym zagadnieniem jest to, aby dane informacje, które są przekazywane na wyższy szczebel zarządczy, były filtrowane i przekazywane tylko kluczowe wydarzenia oraz istotne problemy czy sukcesy, które miały miejsce w projekcie. Ważne jest, aby

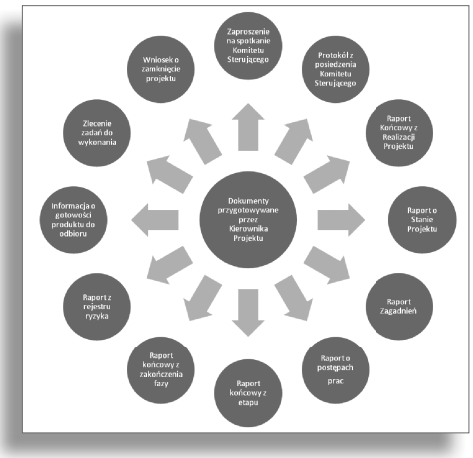


Rysunek 3 Filtracja informacji i raportów na poszczególnych poziomach zarządczych projektu.
Źródło: Opracowanie własne na podstawie „Skuteczne zarządzanie projektami PRINCE2", 2009.

informacje które dochodzą do kierownictwa organizacji, przeszły już drogę selekcji, co przedstawia poniższy rysunek.

Jak wiadomo, ważną rolę w projekcie pełni kierownik projektu, również w kontekście zarządzania komunikacją, gdzie rola kierownika projektu jest nieoceniona. Wiąże się to z przygotowywaniem przez niego wszelkich informacji na temat projektu, zarówno w formie raportów, jak też informacji na strony internetowe, czy informacji dla mediów. Poniższy rysunek przedstawia przykładowe rodzaje raportów, które wytwarza kierownik projektu dla interesariuszy.

Jakie korzyści można wyróżnić z zastosowania strategii zarządzania komunikacją w projekcie? Przede wszystkim, jest to



Rysunek 4 Kierownik projektu a produkty zarządcze
Źródło: Opracowanie własne na podstawie „Skuteczne zarządzanie projektami PRINCE2", 2009.

zaspokojenie funkcji informacyjnej wszystkich uczestników projektu. Poprzez stały dostęp do aktualnych informacji na temat projektu, możliwe staje się zarządzania, monitorowanie i kontrolowanie poszczególnymi działaniami, które są przypisane do poszczególnych interesariuszy. Przy prawidłowej identyfikacji interesariuszy, można mówić o identyfikacji potrzeb i oczekiwań zainteresowanych osób w projekcie. Komunikacja w projekcie powinna być audytowana. Jak wynika z audytów przeprowadzonych w projektach, możliwe staje się obniżenie kosztów przez organizację wynikających z ograniczonego czasu na poszukiwanie informacji, jak też uniknięciu wielu błędów i konfliktów międzyludzkich. Możliwy jest wzrost satysfakcji pracowników, poprzez otwarcie na dialog i wdrożenie najefektywniejszych dróg przekazywania informacji. Otrzymując informacje, raporty w wyznaczonym czasie, możliwe staje się uniknięcie lub też zapobieganie potencjalnym ryzykom opóźniającym wykonanie danego zadania czy grupy zadań. Właściwa komunikacja buduje zaufanie osób biorących udział w projekcie.

Głównymi korzyściami płynącymi ze stosowania strategii zarządzania komunikacją w projekcie, jest otrzymywanie informacji na czas, a dane i raporty są bardzo wysokiej jakości i zakres przekazywanych informacji jest dostosowany do odpowiednich grup interesariuszy, komunikaty są jasne i przejrzyste. Każda z zainteresowanych osób wie, gdzie przechowywane są informacje. Natomiast, przekazywane informacje ilustrują postępy prac w projekcie.

Jeżeli zadamy pytanie „co daje stosowanie strategii zarządzania komunikacją?", otrzymamy jednoznaczną odpowiedź, że dzięki ww. strategii zostaje ustalony jasny i przejrzysty sposób przekazywania informacji dla poszczególnych użytkowników, interesariuszy. Następuje ujednolicenie zasad zastosowania zarządzania komunikacją w projekcie, poprzez spójne określenie form komunikacji, podnosi się jakość przygotowanych dokumentów, w tym również raportów, stosowana jest systematyczność w dostarczaniu aktualnych danych oraz możliwy jest stały dostęp do informacji o postępach prac w projekcie.

Tworząc strategię komunikacji w projekcie, zawsze należy pamiętać o komunikacji dwukierunkowej, zarówno tej wewnętrznej, jak i zewnętrznej. Mówiąc o strukturze zarządzania projektem, nie należy zapominać o rolach w projekcie, czyli kierownictwu organizacji, przewodniczącym komitetu sterującego, głównym użytkowniku, głównym dostawcy, nadzorze projektu, jak również zespole projektowym. Nie można zapomnieć również o użytkownikach, dla których robione są projekty, czyli dla obywateli, urzędów, gmin, jednostek specjalistycznych. W tym przypadku konieczne jest określenie i ustalenie formy komunikacji, przekazywania informacji o postępach prac dla ww. wymienionych grup. Warto jest stworzyć np. strony dedykowane danemu zagadnieniu, gdzie każda zainteresowana osoba, organizacja, będzie mogła zajrzeć i dowiedzieć się, co dzieje się w projekcie w danym etapie. Jednakże samo wykonanie ww. strony nie jest jedynym elementem w procesie komunikacji. Należy jeszcze skutecznie poinformować wszystkie zainteresowane strony o udostępnieniu danego źródła informacji i konieczne jest stałe aktualizowanie tychże informacji, aby zachęcić interesariuszy do stałego śledzenia postępów prac. Wskazane jest również udostępnienie zwrotnego kanału informacji dla użytkowników, aby mogli oni zgłaszać zagadnienia projektowe lub zagrożenia, które mogą mieć miejsce w projekcie. Poprzez taką możliwość, następuje identyfikacja z projektem i większe zaangażowanie w działania projektowe.

Należy pamiętać, że korzyści ze stosowania strategii zarządzania komunikacją, możliwe są do osiągnięcia poprzez egzekwowanie

i monitorowanie np. przez przewodniczącego komitetu sterującego przekazywanych Informacji, przez kierownika projektu poszczególnym interesariuszom.

Przy tworzeniu strategii zarządzania komunikacją w projekcie, należy pamiętać o różnorodności przygotowywanych i przetwarzanych informacji dla wybranych grup interesariuszy. tzn. inne raporty będą dla komitetu sterującego, które przygotowuje kierownik projektu, inny zakres będą miały informacje dla kierownictwa organizacji, które powinny być zwięzłe, jasne i krótkie. Zupełnie inne informacje będą dla zespołu projektowego, gdzie można wykorzystać intranet do umieszczenia dokumentacji zarządczej projektu. Wykorzystać można również cykliczne spotkania zespołu projektowego, którego celem będzie wyrównanie wiedzy wszystkich osób w zespole, albo też, aby kierownik projektu mógł przekazać aktualne ustalenia z komitetu sterującego.

W wielu prowadzonych projektach występują informacje, które muszą podlegać zabezpieczeniu i nie powinny być dostępne dla wszystkich interesariuszy. Dlatego też, jest to kluczowe zadanie jakie stawia się w strategii zarządzania komunikacją, aby ustalić jasne reguły i wytyczne, kto może mieć dostęp do jakich informacji. W ten sposób unika się niepożądanych sytuacji dotyczących niewłaściwego przekazywania danych w projekcie. Bezpieczeństwo danych jest bardzo ważne i należy zadbać o bezpieczeństwo projektu. Dostęp do ww. danych, mogą mieć tylko i wyłącznie uprawnione osoby.

Stosując wytyczne strategii zarządzania komunikacją w projekcie, osobą wyznaczoną do przekazywania informacji jest najczęściej kierownik projektu, daje to pewność, że dane są zweryfikowane i aktualne. W przypadku przekazania informacji np. od wsparcia projektu, konieczna będzie powtórna weryfikacja danych, aby sprawdzić, czy są one aktualne. Dlatego też ważne jest ustalenie jednego źródła informacji. Korzyścią płynąca z zastosowania strategii zarządzania komunikacja, jest dostarczanie aktualnych informacji wszystkim interesariuszom biorącym udział w projekcie, jak również wykorzystywanie informacji zawartych w raportach, do określenia wykorzystania zasobów projektowych i ich zaangażowania w poszczególnych czynnościach.

Standaryzacja, dobre praktyki oraz pełna wiedza o projekcie, są kluczowymi elementami dla sprawnie prowadzonych przedsięwzięć, które poprzez właściwe zarządzanie, również w zakresie komunikacji, pozwalają osiągnąć zamierzony cel.

Ewa Szczepańska - od ponad 11 lat uczestniczy w budowie i wdrażaniu systemów IT dla potrzeb administracji państwowej

Zapraszamy do udziału

SEMINARIUM
SYSTEMY I USŁUGI TELEINFORMATYCZNE - WSPIERAJĄCE PRZEDSIĘBIORSTWA SIECIOWE (UTILITIES)
2 października 2012 r., Warszawa

Kolejna edycja seminarium w cyklu TELEINFORMATYKA W PRZEDSIĘBIORSTWACH SIECIOWYCH została poświęcona przedstawieniu systemów i usług teleinformatycznych. Zaproszeni specjaliści omówią zagadnienia dotyczące specyfiki zarządzania majątkiem sieciowym między innymi zwrócą uwagę na problematykę ochrony danych w inteligentnych systemach sieciowych, a także omówią polskie i wspólnotowe regulacje prawne kształtujące sytuację prawną klientów w sektorze utilities.

Więcej informacji: www.cpi.com.pl

Glosa do wyroku KIO z dnia 23 marca 2012 r., sygn. akt: KIO 467/12 oraz KIO 483/12

Wojciech Kaliński

W marcu bieżącego roku zapadło niezwykle ciekawe orzeczenie Krajowej Izby Odwoławczej dotyczące wadium wniesionego w postaci gwarancji bankowej. W orzeczeniu Krajowa Izba stara się określić granicę dopuszczalności zamieszczenia w treści gwarancji różnego rodzaju „warunków", stanowiących przesłankę wypłaty kwoty wadium na rzecz zamawiającego, formułując następującą tezę:

„(...) gwarancja ma charakter bezwarunkowy, jeżeli wypłata świadczenia uzależniona jest jedynie od złożenia żądania zapłaty w formie określonej w gwarancji oraz oświadczenia, że podmiot, za który bank udzielił gwarancji, nie wywiązał się ze zobowiązań wobec beneficjenta. Jednocześnie ***wskazuje się, że sam wymóg potwierdzenia przez beneficjenta zajścia okoliczności stanowiących podstawę wezwania do zapłaty, nie oznacza warunkowości gwarancji, lecz stanowi pewną formalność służącą weryfikacji skierowanego żądania przez gwaranta. Wprowadzenie takiego warunku formalnego nie należy mylić z badaniem przez gwaranta ziszczenia się materialnych przesłanek jego odpowiedzialności.*** *Niedopuszczalne jest zatem żądanie przez gwaranta przedstawienia jakichkolwiek dodatkowych dowodów, w szczególności pochodzących od innych niż beneficjent podmiotów, poświadczających zrealizowanie się zabezpieczonego rezultatu, w tym przypadku – ziszczenia się którejkolwiek z przesłanek opisanych w art. 45 ust. 4a i 5 pzp. W ocenie Izby wymóg załączenia do żądania zapłaty oryginału dokumentu gwarancji również stanowi wymóg formalny do zaakceptowania, zważając że prawidłowe wniesienie wadium w tej formie oznacza wejście przez beneficjenta w posiadanie tego dokumentu".*

Na wstępie należy przyjrzeć się pojęciu gwarancji warunkowej i bezwarunkowej. Jak zauważa J.Pisuliński[1], *podział na gwarancje bezwarunkowe i warunkowe może być mylący. Nie chodzi w nich bowiem o warunek w znaczeniu art. 89 k.c., lecz o przesłanki aktualizujące obowiązek zapłaty przez bank*. To pierwszy, niezwykle istotny, z punktu widzenia prawa zamówień publicznych, wniosek. Dalej

1 Bączyk Mirosław, Góral Lesław, Fojcik-Mastalska Eugenia (redakcja), Pisuliński Jerzy, Pyzioł Wojciech: Prawo bankowe. Komentarz, Warszawa 2007 Wydawnictwo Prawnicze LexisNexis

J.Pisuliński[2] zauważa, że *w przypadku gwarancji bezwarunkowych, znanych także jako gwarancje na pierwsze żądanie, bank ma obowiązek zapłaty po otrzymaniu wezwania od beneficjenta gwarancji, bez potrzeby dokumentowania, czy zabezpieczone gwarancją zdarzenie nastąpiło (dlatego art. 81 stanowi, że spełnienie warunków zapłaty może być stwierdzone określonymi dokumentami). Zapłata sumy gwarancyjnej nie jest więc uzależniona od sprawdzenia zasadności żądania beneficjenta. W związku z tym wskazuje się niekiedy na różnicę między materialnym i formalnym uprawnieniem beneficjenta gwarancji do żądania zapłaty sumy gwarancyjnej, podkreślając, iż o obowiązku świadczenia gwaranta decydują wyłącznie przesłanki formalne* ...W świetle tych wywodów można poddać w wątpliwość część tez zawartych w orzeczeniu KIO. W pierwszej kolejności należy zauważyć, że art. 45 ust. 6 pkt 2) pzp nie wymaga, by jedyną dopuszczalną formą bankowej gwarancji wadialnej była gwarancja bezwarunkowa. Wymaganie to nie wynika w żaden sposób z treści przedmiotowego przepisu. Zatem wykazywanie, że określone wymagania zawarte w gwarancji plasują ją jako gwarancję warunkową lub bezwarunkową, jurydycznie nie ma znaczenia. Po drugie, skoro analizowana przez KIO gwarancja zawierała konieczność złożenia zarówno żądania zapłaty w formie określonej w gwarancji jak i oświadczenia, że podmiot, za który bank udzielił gwarancji, nie wywiązał się ze zobowiązań wobec beneficjenta, to taką gwarancję trudno uznać za bezwarunkową w rozumieniu definicji wskazanej przez J.Pisulińskiego. O ile bowiem wymóg przedstawienia przez Zamawiającego żądania zapłaty nie stanowi warunku, a jedynie wezwanie do zapłaty, o tyle oświadczenie że podmiot, za który bank udzielił gwarancji, nie wywiązał się ze zobowiązań wobec beneficjenta nie jest konieczne dla postawienia zobowiązania banku w stan wymagalności. Tego typu oświadczenie stanowi właśnie warunek, czyli dodatkową przesłankę aktualizującą obowiązek zapłaty przez bank. Oświadczenie to nie jest bowiem w żaden sposób niezbędne dla zaistnienia przesłanki odpowiedzialności banku. Z samego faktu zwrócenia się o zapłatę wynika bowiem pośrednio, że zaistniała przesłanka tej zapłaty. Dodatkowe, odrębne oświadczenie wierzyciela (beneficjenta, zamawiającego) niczego w tym zakresie nie zmienia.

Stanowisko KIO da się jednak obronić w świetle niektórych poglądów doktryny prawa bankowego. Zdaniem L.Gromadzkiego[3] za warunkowe uważa się tylko te gwarancje, w których beneficjent ma obowiązek przedłożenia dokumentów pochodzących od osoby trzeciej, np. certyfikatu rzeczoznawcy, orzeczenia sądu polubownego. Wydaje się, że problem wykładni art. 45 ust. 6 pkt 2) pzp nie wiąże się z kwestią warunkowości lub bezwarunkowości gwarancji bankowej, lecz z pytaniem jakie ewentualnie warunki są możliwe do pogodzenia z istotą zabezpieczenia wadialnego na gruncie przepisów prawa zamówień publicznych. Jak bowiem wskazano, przepisy prawa zamówień publicznych nie wymagają, by udzielona gwarancja bankowa miała charakter bezwarunkowy, więc doszukiwanie się za wszelką cenę tej właściwości nie znajduje uzasadnienia. Jeżeli więc uważnie przyjrzymy się tezom analizowanego orzeczenia, to różnicowanie wymagań formalnych od materialnych służy w istocie znalezieniu granicy między dopuszczalnymi i niedopuszczalnymi

3 L. Gromadzki, Bankowe gwarancje..., s. 36
2 Tamże

warunkami gwarancji bankowej. Na tej zasadzie warunkami dopuszczalnymi, zdaniem KIO, jest: 1) konieczność złożenia oświadczenia, że podmiot, za który bank udzielił gwarancji, nie wywiązał się ze zobowiązań wobec beneficjenta; 2) wymóg załączenia do żądania zapłaty oryginału dokumentu gwarancji. Wymaganiem zaś niedopuszczalnym byłoby żądanie przez gwaranta przedstawienia jakichkolwiek dodatkowych dowodów, w szczególności pochodzących od innych niż beneficjent podmiotów, poświadczających zrealizowanie się zabezpieczonego rezultatu, w tym przypadku – ziszczenia się którejkolwiek z przesłanek opisanych w art. 45 ust. 4a i 5 pzp. I przy tak zinterpretowanych tezach Krajowej Izby stanowisko zawarte w komentowanym wyroku należy uznać za prawidłowe.

Dr Wojciech Kaliński - asystent w Katedrze Prawa Cywilnego Uniwersytetu Jagiellońskiego, wspólnik w kancelarii Maruta i Wspólnicy sp. j.

Zapraszamy do udziału

WARSZTATY
METODY POMIARU ROI/TCO W PRAKTYCE INWESTYCJI INFORMATYCZNYCH
17-18 października 2012 r., Warszawa

Cele warsztatu:
- poznanie finansowych zasad inwestowania w IT
- poznanie i sklasyfikowanie „mierzalnych" i „niemierzalnych" korzyści i kosztów informatyki
- poznanie metod kompleksowej wyceny rentowności dowolnej inwestycji informatycznej
- nabycie wiedzy o zasadach tworzenia dokumentacji projektu inwestycyjnego w IT przeznaczonej dla zarządu firmy

Zastosowanie wiedzy i korzyści z warsztatu:
- umiejętność precyzyjniej wyceny korzyści osiąganych na inwestycjach informatycznych
- rozumienie zasad rządzących ekonomicznym wymiarem inwestowania w IT
- umiejętność precyzyjnej klasyfikacji efektów ekonomicznych dla wdrożeń informatycznych w obszarze: systemów typu ERP, systemów typu CRM, systemów redukujących Total Cost of Ownership: modernizacje systemów, konsolidacje, cloud computing, utility computing, ASP, SaaS, systemów typu Business Intelligence, usług outsourcingu IT, portali korporacyjnych oraz narzędzi zarządzania wiedzą.

Podniesienie świadomości istnienia pewnych kosztów i korzyści, które pozostawały dotychczas w sferze „niemierzalnej" i uzyskanie dzięki temu wskazówek do zarządzania tymi obszarami, prowadząc w efekcie do zwiększenia efektywności firmy.

Materiały warsztatowe obejmują:
- oryginalny skrypt będący bazą merytoryczną szkoleń
- oryginalne komercyjne Case Studies zrealizowane w rzeczywistych przypadkach:
  - ERP w średniej firmie produkcyjnej
  - System zarządzania ruchem w dużej firmie produkcyjnej
  - Modernizacja sieci WAN w dużej firmie usługowej
  - System sprzedaży mobilnej w firmie telekomunikacyjnej
- software demonstracyjny stosowany w analizach ROI/TCO:
  - aplikacja Palisade @Risk Industrial
  - aplikacja iGrafx 2009 Six Sigma
- rozwiązane zadania szkoleniowe w plikach xls
- bibliotekę materiałów edukacyjnych w tym fragment książki „Praktyczne zarządzanie finansami firmy"

Więcej informacji: www.cpi.com.pl

Centrum Edukacji Medycznej CEMED

to nowoczesne centrum kształcenia kadry medycznej, organizator krajowych i międzynarodowych spotkań edukacyjnych

Dysponuje własnym **multimedialnym Centrum Konferencyjnym** z elastyczną możliwością konfiguracji pomieszczeń. Na blisko 500 m2 znajdują się 4 sale konferencyjne z naturalnym światłem, wyposażone w modułowe ściany przesuwne umożliwiające dostosowanie powierzchni do odpowiedniej liczby uczestników. Mogą one pomieścić od 35 do 170 osób. Wszystkie pomieszczenia są klimatyzowane i bardzo profesjonalnie wyposażone. Foyer konferencyjne o powierzchni 155 m2 pozwala na zorganizowanie wystawy i cateringu w bezpośrednim sąsiedztwie obrad. Do obsługi słuchaczy przygotowana jest profesjonalna recepcja z możliwością korzystania z niezbędnego sprzętu teleinformatycznego.

Profesjonalna reżyserka umożliwia kontrolę i zarządzanie **nowatorskimi systemami multimedialnymi** z jednego miejsca, z możliwością obserwacji całości imprezy. Centrum posiada:

- wyspecjalizowany system wideokonferencyjny umożliwiający połączenie z dowolnym miejscem na świecie w technologii HD,
- unikatowy system audio/video łączący sale konferencyjne z blokami operacyjnymi szpitala, umożliwiający uczestniczenie w operacji,
- system archiwizacji/nagrywania spotkań,
- obróbkę nagranego materiału audio/video,
- możliwość zorganizowania szkoleń z wykorzystaniem interaktywnego systemu Vote/PRS (Personal Response System).

Centrum Konferencyjne CEMED jest częścią kompleksu największego prywatnego szpitala ortopedycznego w Polsce (Carolina Medical Center), nasz nowatorski wyspecjalizowany system telekonferencyjny umożliwia przekaz na sale obrad obrazu z sal operacyjnych, gabinetów diagnostyki obrazowej, pomieszczeń fizjoterapii szpitala. Transmisji możemy dokonywać również z dowolnego punktu na świecie, dysponując urządzeniami o najlepszej jakości obrazu i dźwięku dostosowanymi do prezentacji medycznej treści edukacyjnej możemy transmitować np. obrazy RTG.

Dla organizatorów konferencji, szkoleń i imprez firmowych, menedżerów i prezesów firm szukających miejsc spotkań biznesowych Centrum Konferencyjne CEMED przedstawia ofertę wszechstronnych, fachowych usług według światowych standardów. Centrum położone jest w zacisznej części dolnego Mokotowa u zbiegu ulic Sikorskiego i Sobieskiego, tylko krok od centrum biznesowego i finansowego stolicy. Istotnym udogodnieniem Centrum jest duży parking poza strefą płatnego parkowania dostępny dla wszystkich gości.

Profesjonalna obsługa techniczna, jak i znakomita gastronomia gwarantują dobrą atmosferę towarzyszącą spotkaniom i konferencjom.
Wyjątkowe walory naszego centrum konferencyjnego sprawiają, że jesteśmy gotowi zorganizować najbardziej prestiżową konferencję, seminarium, szkolenie, jubileusz i galę.

Zapraszamy do skorzystania z naszych usług.

cemed
centrum edukacji medycznej

Centrum Konferencyjne
tel. 22 355 85 05
e-mail: **cemed@cemed.pl**

Centrum Edukacji Medycznej CEMED Sp. z o.o.
ul. Pory 78, 02-757 Warszawa
www.cemed.pl

Edwin Bendyk

Paradoksy realnego rynku

Podczas niedawnego Kongresu Innowacyjnej Gospodarki doświadczyłem inspirującej konfrontacji. Uczestniczyłem w panelu dyskutującym nowe modele biznesowe. Jako że przedsiębiorcą nie jestem, postanowiłem wystąpić w roli rzecznika konsumentów. Podzieliłem się więc obserwacją, która zastanawia mnie od wielu lat. Otóż, cyfrowa telefonia komórkowa istnieje w Polsce od 1996 r. Operatorzy chwalą się swym zasięgiem, dowodząc w reklamach, że już tylko promile dzielą ich od pełnego pokrycia obszaru Polski swymi usługami. Jak to jednak jest, że te brakujące promile zasięgu obejmują obszary pod względem wielkości nieistotne, lecz niezwykle ważne dla konsumentów.

Wystarczy wsiąść do jedynej linii polskiego metra, by przekonać się, że jest ono światowym ewenementem. W tej chwili jeden bodaj operator oferuje swoje usługi podróżującym pod ziemią. Potem można przesiąść się do pociągu relacji Warszawa-Kraków, Katowice lub Poznań – linie, którymi podróżuje mnóstwo osób potrzebujących zasięgu i dostępu do Internetu na całej trasie. Niedoczekanie! Operatorzy oferują w najlepszym przypadku *coitus interruptus*, co jak wiadomo prowadzi do nerwicy. A już na pewno do irytacji. Jak wytłumaczyć, że mimo ujawnionej konsumenckiej potrzeby nasi operatorzy nie wynaleźli modeli biznesowych umożliwiających obsłużenie tego popytu?

W odpowiedzi usłyszałem od jednej z uczestniczek Kongresu, że zachowuję się jak typowy Polak – narzekam, zamiast wziąć się do roboty i samemu wykorzystać nadarzającą się okazję na biznes. Żelazna logika odpowiedzi powaliła mnie, odjęło mi mowę i spokój. Kto miał rację? Ja wytykając lenistwo operatorom, czy słuchaczka wytykając lenistwo mnie?

Jako pilny czytelnik, choć znacznie mniej pilny uczeń Adama Smitha wiem, jakie korzyści przynosi podział pracy na wolnym rynku. Kiedy potrzebuję usługi telekomunikacyjnej, nie zaspokajam jej samodzielnie, lecz korzystam z rynku, który powinien ujawniony przez mnie popyt połączyć z podażą. I oczywiście, to nie dobra wola operatora, lecz jego egoistyczny interes powinien zmobilizować go do roboty. Gdy ujawniony popyt nie znajduje zaspokojenia, oznacza to, że rynek działa nieefektywnie.

Najwyraźniej tak właśnie dzieje się w Polsce w przypadku usług telefonii komórkowej. Dlaczego? Adam Smith znalazłby szybko odpowiedź – szwankuje konkurencja. Niestety, nie zanotowałem emaila do uczestniczki Kongresu i nie mogę się z nią podzielić uspokajającym odkryciem: to nie ja jestem do niczego, tylko po prostu nie działa rynek.

Potem jednak zauważyłem inną ciekawą sytuację, również obszaru telekomunikacji. Tym razem z pola usług dostępu do Internetu. Od kilku miesięcy systematycznie co jakiś czas na kilka godzin wysiada mi neostrada. Operator na tyle rozwinął serwis CRM, że gdy zgłaszam awarię na infolinię, automat sam odpowiada, że naprawa potrwa osiem godzin. Głos automatu działa kojąco, tym bardziej, że tym razem rynek działa doskonale – w czasie, gdy nie mam dostępu do neostrady, łączę się z Internetem za pośrednictwem modemu 3G (szczęśliwie nie mieszkam w tunelu metra ani przy Centralnej Magistrali Kolejowej).

Efekt jest taki, że nie chce mi się awanturować w sprawie neostrady z powodu zbyt moim zdaniem częstych awarii. Operator więc myśli, że jestem szczęśliwym klientem i nie ma bodźców, żeby poprawić jakość swoich usług. I tak oto paradoksalnie, tym razem sprawność rynku także prowadzi do pogorszenia poziom standardu obsługi klienta. Hm, i jak tu dogodzić Polakowi?

Wnioski z tych przygód nie będą jednak natury biznesowej, lecz, jak to w Polsce, politycznej. Otóż coraz częściej przekonuję się, że moja kondycja, jako obywatela naszego państwa nie różni się zbytnio od kondycji konsumenta na realnym rynku. Są usługi publiczne, z którymi państwo to sobie nie radzi, a rynek nie zapewnia alternatywy – pozostaje wówczas tylko ponarzekać. W wielu przypadkach można sobie poradzić z niedostatkiem oferty publicznej stosując protezy oferowane przez rynek, zwłaszcza wówczas, gdy rozwiązanie polega na dostępie do informacji. Gdy czekam w kolejce do izby przyjęć, nie marnuję czasu, bo mogę pracować dzięki laptopowi i 3G. Przykłady można mnożyć.

Efekt jest taki, że choć powody do narzekania nie maleją, to jednak maleje chęć do narzekania, bo rozładowują ją wspomniane protezy. Funkcjonariusze władzy publicznej pozbawieni są w rezultacie kluczowej informacji, a jej brak traktują jako wyraz, że wszystko jest w porządku. I choć może być coraz gorzej, to będą przekonani, że jest coraz lepiej i puchną z zadowolenia.

Czasem jednak rozbieżność między dobrym samopoczuciem a rzeczywistością staje się tak duża, że dochodzi do pęknięcia: wystarczy wspomnieć kryzys związany z ACTA i z receptami. Naprawdę, w drugiej dekadzie XXI wieku nie sposób wytłumaczyć, dlaczego lekarz ma kontrolować uprawnienia pacjenta, do których legitymacją jest papierowa książeczka zdrowia raz na miesiąc stemplowana przez pracodawcę. Tak być nie musi, tak jednak jest, a każda próba analizy problemu przy użyciu logiki prowadzi do wspomnianych paradoksów.

Edwin Bendyk

Zamówienie prenumeraty kwartalnika

„Czas informacji"

WYŚLIJ FAKSEM 22 871 85 56 lub 22 870 69 95

PRENUMERATA NA ROK 2012

Zamawiamy prenumeratę kwartalnika „**Czas Informacji**"

okres trwania prenumeraty (ilość egzemplarzy)	ilość zamawianych prenumerat	**cena**
prenumerata roczna 2012 od numeru 1/2012 - 3 kolejne numery		340 zł+5% VAT
prenumerata półroczna numer 1/2012 i 2/3/2012		200 zł+5% VAT

Prenumeratę prosimy przesłać do niżej wymienionego adresata

PRENUMERATOR		FIRMA	
imię		nazwa	
nazwisko		NIP	
stanowisko		ulica	
nr telefonu		kod, miasto	
nr faksu		nr telefonu	
e-mail		nr faksu; e-mail	

Wyrażam zgodę/ Nie wyrażam zgody na wykorzystywanie przez Centrum Promocji Informatyki sp. z o. o., Warszawa, ul. Międzyborska 50, moich danych (w tym adresu poczty elektronicznej), pod warunkiem przestrzegania przepisów ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t. jedn. Dz. U. z 2002 r. Nr 101, poz. 926), w zakresie prowadzonej przez CPI działalności gospodarczej (a w szczególności działalności marketingowej i na przekazywanie danych uczestnika firmom biorącym udział w opracowaniu programów szkoleń). Mam świadomość prawa do wglądu, poprawiania lub usunięcia swoich danych w bazie danych osobowych CPI oraz dobrowolności ich podania. W związku z obowiązkiem wynikającym z ustawy z dnia 18 lipca 2002 r. (Dz. U. nr 144, poz. 1204) o świadczeniu usług drogą elektroniczną wyrażam zgodę na

Oznaczoną należność z tytułu kosztów prenumeraty w wysokości _____zł wpłacę w terminie 14 dni od daty otrzymania faktury.

Należy wypełnić i odesłać faksem na numer
22 871 85 56 lub 22 870 69 95

.....
pieczęć i podpis osoby upoważnionej

redaktor naczelny: Wiesław Paluszyński, wieslaw.paluszynski@czasinformacji.pl

kolegium redakcyjne: Izabela Adamska, Dariusz Bogucki, Tomasz Kulisiewicz, Piotr Waglowski, Wojciech Wiewiórowski

sekretarz redakcji i reklama: Agata Soboń Modzelewska, redakcja@czasinformacji.pl

redakcja: Centrum Promocji Informatyki sp. z o. o., ul. Międzyborska 50, 04-041 Warszawa, tel. 22 870 69 78, 22 871 85 51, fax 22 870 69 95, 22 871 85 56, info@czasinformacji.pl, www.czasinformacji.pl

projekty graficzne: Mikołaj Ostaszewski, mikolaj.ostaszewski@zsrr.pl

skład i łamanie: Michał Nowosielski, michal@nowosielscy.com.pl

nakład: 400 egz.

prenumerata: prenumerata@czasinformacji.pl, www.czasinformacji.pl/prenumerata

Zamówienia prenumeraty również u kolporterów.

Redakcja nie zwraca materiałów niezamówionych oraz zastrzega sobie prawo do ich redagowania i skracania.

wydawca:

Centrum Promocji Informatyki sp. z o. o.
www.cpi.com.pl

rada naukowa:

prof. dr hab. Jacek Gołaczyński
prof. dr hab. Mirosław Kutyłowski
dr hab. Artur Nowak-Far
prof. dr hab. Ewa Nowińska
prof. dr hab. Witold M. Orłowski
dr hab. Grażyna Szpor

W części naukowej kwartalnika umieszczane są prace naukowe publikowane w języku polskim (ze streszczeniem), które podlegają recenzjom rady.

www.czasinformacji.pl/prenumerata.php

Czas Informacji

Zapraszamy do składania zamówień na prenumeratę na 2012 rok.