Dariusz Skalski
Państwowa Wyższa Szkoła Zawodowa w Wałczu

Antynomia społeczeństwa informacyjnego − szanse i zagrożenia

Streszczenie

W niniejszym artykule poruszono problematykę społeczeństwa informacyjnego, którego rozwój postrzegany jest obecnie jako gwarant rozwoju gospodarki opartej na wiedzy. Scharakteryzowane zostały najważniejsze komponenty innowacyjnych technologii informacyjnych i komunikacyjnych (ICT), w tym występujące zagrożenia, które mogą stać się ich udziałem dla rozwijającej się gospodarki w Polsce.

Cel: diagnoza i ocena administracji rządowej w budowaniu gospodarki, której istotnym elementem jest wykorzystywanie postępu w zakresie zaawansowanych technologii.

Metoda badawcza: indywidualnych przypadków oraz badania dokumentów.

Główne wyniki badań: częsta praktyka przenoszenia odpowiedzialności za bezpieczeństwo danych i informacji na podmioty prywatne, ułatwienia w uzyskaniu kwalifikacji pracowników ochrony osób i mienia, w tym prowadzenie działalności gospodarczej oraz wciąż niski poziom umiejętności korzystania z narzędzi teleinformatycznych, wymaga dalszych przemyślanych i ukierunkowanych działań ze strony państwa.

Implikacje praktyczne: stwierdzono, że systematycznie dochodzi do naruszenia zasad bezpieczeństwa informacji, które mogą nieść za sobą negatywne konsekwencje wizerunkowe oraz finansowe. Budowanie nowoczesnego społeczeństwa informacyjnego opartego na wiedzy, wymaga zmiany świadomości konsumentów oraz pożądanych zmian legislacyjnych.

Kategoria artykułu: badawczy.

Słowa kluczowe: społeczeństwo informacyjne, innowacje, bezpieczeństwo teleinformatyczne.

Kody JEL: O380, O390, Z00

Wstęp

W ostatnim wieku nie pojawiła się najprawdopodobniej druga równie silna idea wszechświatowej wspólnoty, z jaką mieliśmy do czynienia w odniesieniu do Internetu w początkowej fazie jego istnienia. Dotychczasowa przestrzeń, której synonimem była sztucznie ukształtowana całość społeczna wraz z hierarchicznie rozrastającymi się wspólnotami − na których czele stać miała ponadlokalna władza − została uzupełniona o przestrzeń trzeciego wymiaru; obok stabilnej i trwałej przestrzeni – na którą składać się miały beton i stal, tworzące tkankę struktury oraz autostrady i sieci kolejowe, postrzegane jako system jej powią-

zań – nałożyła się przestrzeń trzeciego rodzaju, globalna sieć informatyczna. Jak zauważa Zygmunt Bauman obok przestrzeni: „...która została sztucznie skonstruowana pod względem terytorialnym, urbanistycznym i architektonicznym..." nastaje czas cyberprzestrzeni. Następnie za Paulo Virilio poddaje w wątpliwość znaczenie podziału: „...na tu i tam", wynikającego z możliwości błyskawicznego przekazywania treści, bez ograniczeń natury fizycznej i czasowej (Bauman 2000, s. 24).

Wraz z poszerzeniem kanałów komunikowania się i wymiany informacji, czynnikami współwystępującymi – obok cyberprzestrzeni – są rewolucje w mikroelektronice i inżynierii genetycznej, definiowane jako nowy paradygmat technologiczny, nazywany informacjonalizmem (Bendyk 2004). Z kolei Manuel Castells konstatuje, iż technologie informacyjne nie mogą być postrzegane w kategoriach prostych narzędzi, ale są ustawicznym procesem, którego cechą jest dynamiczny rozwój. Na paradygmat technologii informacyjnej − będący podstawą społeczeństwa informacyjnego − składa się pięć cech: a) informacja będąca kluczowym elementem funkcjonowania technologii, b) wszechobecność nowych technologii, które są integralną częścią ludzkiej egzystencji, bowiem bezpośrednio wpływają na jej kształtowanie, c) działanie zgodne z logiką sieci wszystkich współpracujących z nią komponentów (systemy, zbiory relacji), d) elastyczność polegająca nie tylko na odwracalności procesów, ale również możliwości modyfikowania instytucji i organizacji będących jej elementem jako odpowiedź na dokonujące się nieustannie zmiany, e) konwergencja technik i technologii prowadząca do wyodrębnienia się wysoce zintegrowanych systemów − w miejsce dotychczas funkcjonujących w obrębie zbliżonych branż – których funkcjonowanie upodobnia się do siebie, powodując wzrost złożoności systemów i niemożność funkcjonowania jednego elementu bez udziału pozostałych (Bendyk 2004; Castells 2007; Mazurkiewicz 2011; Pietruszka-Ortyl 2012).

Sieć dotychczas postrzegana w kategoriach powszechnej szczęśliwości i bezinteresowności coraz częściej nabiera wymiarów rynkowych, obrasta funkcjami oraz instytucjami ekonomicznymi. Internet coraz częściej zaczyna być postrzegany jako wszechświatowe imperium, w którym wielkie firmy, portale oraz szeroko rozumiana administracja zachowują się wobec siebie merkantylnie i agresywnie; żywa jest wciąż pamięć o otwartym oprogramowaniu – uwarunkowanym kulturowo i wynikającym z genezy Internetu − z dostępnym kodem źródłowym, jako kluczowym czynniku rozwoju sieci. Kulturze techno-merytokratycznej (Castells 2003)[1] – wyrażającej się w postrzeganiu postępu naukowo-technicznego przez środowiska naukowe i akademickie, które będąc przekonane o ich słuszności, upatrują szansę rozwoju cywilizacyjnego – przeciwstawiane jest coraz częściej wyobrażenie o sprzedaży Internetu po kawałku, co skutkować może ograniczeniami podróży i bezinteresownego błądzenia w sieci. Wyrażeniem buntu wobec tej imperialnej dominacji są „plagi" rozsyłania wirusów i robaków komputerowych lub przeprowadzanie ukierunkowanych ataków na poszczególne elementy infrastruktury sieciowej – organy administracji państwowej, dostar-

[1] Manuel Castels wymienia cztery warstwy kulturowe, które jego zdaniem wpłynęły na powstanie oraz kształtowanie Internetu: kulturę techno-merytokratyczną, kulturę hakerską, kulturę wirtualno-komunitariańską oraz kulturę przedsiębiorczości.

czycieli usług internetowych, bądź też podmioty współuczestniczące w tworzeniu platformy IT[2].

Postęp techniki informatycznej, telekomunikacyjnej i tzw. multimediów sprawia, że otoczenie, w którym żyjemy podlega ciągłym przeobrażeniom, tak więc ewoluowanie Internetu i tworzenie globalnego społeczeństwa informacyjnego − mimo licznych głosów krytyki − wydaje się nieuniknione. Aktualne tendencje światowej gospodarki wskazują, że warunkiem rozwoju gospodarczego jest powszechny dostęp do informacji. Zapewnienie takiego dostępu jest jednym z konstytucyjnych obowiązków państwa. Państwo może jednak wywiązywać się z tego obowiązku dwojako: obierając rolę biernego obserwatora i pozostawiając przemiany społeczne zwykłemu biegowi spraw (wychodząc z założenia, że nieuniknione, globalne zmiany wcześniej czy później muszą nastąpić również w Polsce), lub przyjmując rolę aktywną przez wyznaczenie odpowiednich priorytetów rozwojowych i podjęcie działań zmierzających do przyspieszenia wspomnianych przemian.

Stwarzanie warunków dla zapewnienia bezpośredniego dostępu do informacji, kształtowania świadomości społeczeństwa oraz rozwijania jego potencjału intelektualnego i gospodarczego implikuje konieczność włączenia się struktur państwowych, w budowę ery informacyjnej, przez wykorzystanie nowoczesnych technologii społeczeństwa informacyjnego. Ze względu na proces integracji ze strukturami Unii Europejskiej pojawia się potrzeba dostosowania polskich rozwiązań i standardów do kształtującego się nowoczesnego społeczeństwa opartego na technikach informacyjnych. Istotę tego procesu zauważył również Donald Tusk, który, nawiązując do kwestii odrzucenia ACTA, stwierdził: „Internet stał się przestrzenią, jeśli nie dominującą, to równie istotną dla przestrzeni realnej. Nie zdawaliśmy sobie sprawy, jak głębokiej istoty, wręcz cywilizacyjnej, dotykamy ...".

Pomijając kwestie doniosłości rozwoju globalnej wioski, do dzisiaj jeszcze polski rynek jest za liderami rozwoju usług teleinformatycznych (UKE 2010)[3]. Liczba internautów w naszym kraju jest wciąż mniejsza niż w innych państwach Unii Europejskiej, a dostępna infrastruktura nie zapewnia, w wielu przypadkach, pożądanej przepustowości łącza, umożliwiającego swobodne korzystanie z dostępnych usług, choć sytuacja ulega systematycznej poprawie[4]. Jak podkreśliła Anna Streżyńska w swoim komentarzu do *Raportu pokrycia terytorium Rzeczypospolitej Polskiej istniejącą infrastrukturą telekomunikacyjną zrealizowanymi w 2010 r. i planowanymi w 2011 r. inwestycjami oraz budynkami umożliwiającymi*

[2] Warto tu wymienić ataki przeprowadzone w dniach 21-25 stycznia 2012 r. na witryny administracji państwowej, a w późniejszym okresie również na zasoby innych instytucji, w ramach akcji protestacyjnej przeciwko podpisaniu przez Polskę porozumienia w sprawie zwalczania handlu artykułami podrabianymi i piractwa internetowego ACTA (Anti-Counterfeiting Trade Agreement). W wyniku tych działań rządy m.in.: Polski, Czech, Łotwy i Austrii zdecydowały o zawieszeniu procesu ratyfikacyjnego do czasu wypracowania rozwiązania nowego modelu, który regulowałby prawa własności, równocześnie zapewniając prawo anonimowości i chroniąc wolności w Internecie.

[3] Opublikowany przez Urząd Komunikacji Elektronicznej *Raport o stanie rynku telekomunikacyjnego w Polsce w 2010 roku* sytuuje Polskę na 10. miejscu w Unii Europejskiej w zakresie dostępu do usług szerokopasmowego Internetu, zaś w zakresie penetracji dostępem mobilnym Polska zajmuje 8 pozycję. Ponadto z raportu wynika, że w najbliższej przyszłości procesy rynkowe będą ukierunkowane na konwergencje usług, świadczonych z wykorzystaniem różnorodnych technologii łączności elektronicznej. Na znaczeniu tracić będzie dotychczasowy, tradycyjny podział na połączenia głosowe, przesył obrazu czy transmisję danych.

[4] Urząd Komunikacji Elektronicznej podejmuje liczne działania, w porozumieniu z przedsiębiorcami telekomunikacyjnymi w celu intensyfikacji kompleksowych inwestycji w ramach segmentu „białe plamy".

kolokację[5], proces zbierania informacji, powinien pozwolić na sprawne wkroczenie w świat europejskiej społeczności informatycznej. Dodaje ponadto, iż stałym trendem jest rozwój technologii i poprawa prędkości szerokopasmowych łączy jako istotnego elementu rozwoju i źródła przewagi konkurencyjnej współczesnych krajów i gospodarek. Beneficjentami gospodarki opartej na wiedzy są zarówno podmioty biznesowe, jednostki rządowe i samorządowe, a także klienci indywidualni (UKE 2013).

Dotychczasowe strategie mające za zadanie kształtowanie społeczeństwa informacyjnego w Europie, opierały się w głównej mierze na powielaniu działań zawartych w narodowych eStrategiach[6]. Głównym celem niepodzielnie jest wzmocnienie konkurencyjności europejskiej gospodarki. Ponadto oczekuje się, że będzie ona stymulować wzrost zatrudnienia, wydajność pracy i konkurencyjność produktów unijnych na rynkach światowych oraz że korzystnie wpłynie na całą sferę europejskiego życia społeczno-gospodarczego. Założenia inicjatywy znajdują pełne odzwierciedlenie w ogólnych celach, które przyjęły państwa członkowskie, a mianowicie wprowadzenia mieszkańców Europy w wiek cywilizacji cyfrowej we wszystkich sferach aktywności społeczno-zawodowej oraz tworzenia warunków dla konkurencyjności Europy w stosunku do reszty świata, gotowej do wdrażania i finansowania nowych idei. Procesy te winny być dokonane z uwzględnieniem uwarunkowań społecznych, gospodarczych i kulturalnych krajów unijnych tak, aby tworzyły klimat zaufania, wzmacniały jedność społeczeństw.

Dyskusja w środowiskach specjalistycznych na temat zaawansowania technologicznego polskiej gospodarki po transformacji systemowej rozpoczęła się w latach dziewięćdziesiątych. Przełomem okazała się uchwała Sejmu RP z dnia 14 lipca 2000 roku, w sprawie budowania społeczeństwa informacyjnego diagnozująca, iż „system prawny i polityka rządu nie tworzą dostatecznych warunków rozwoju społeczeństwa informacyjnego”[7]. Delegowano zatem na Radę Ministrów kompetencje w zakresie przygotowania narodowej strategii rozwoju społeczeństwa informacyjnego, czego efektem było przyjęcie w listopadzie 2000 roku przez Radę Ministrów *Stanowiska w sprawie uchwały Sejmu RP z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce*, oraz dokumentu programowego *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce* (KBN 2000), przygotowanego przez Komitet Badań Naukowych we współpracy z Ministerstwem Łączności. Jednocześnie Rada Ministrów zobowiązała się do podjęcia działań mających na celu przyspieszenie rozwoju społeczeństwa informacyjnego w Polsce. Jednym z nich było zobowiązanie ówczesnego Ministerstwa Łączności

[5] Podstawę prawną inwentaryzacji infrastruktury telekomunikacyjnej stanowi ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. Nr 106, poz. 675).

[6] Genezy inicjatywy poszukiwać należy w upoważnieniu, którego Rada Europejska udzieliła w Lizbonie Komisji przygotowującej na szczyt Unii Europejskiej w Feira (19-20 czerwca 2000 roku) plan działania w ramach eEurope 2002. Priorytety opisane w Agendzie Lizbońskiej zostały ujęte w trzech grupach tematycznych. Pierwsza obejmuje zagadnienia związane z niedrogim i bezpiecznym dostępem do Internetu oraz promuje tanie łącza w sektorach nauki i bezpieczeństwa. Kolejny program zakłada inwestycję w czynnik ludzki oraz podnoszenie kwalifikacji. Odbiorcą jego są głównie ludzie młodzi, którym proponuje się pracę w warunkach gospodarki opartej na wiedzy. Ostatnia grupa tematyczna przewiduje wdrażanie technologii informacyjno-komunikacyjnych w wielu obszarach funkcjonowania państwa.

[7] Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce (Monitor Polski” z 2000 r., Nr 22, poz. 448).

do opracowania dokumentu pt. *ePolska − Strategia rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*, na wzór podjętej przez UE inicjatywy eEurope (KBN 2001).

Motywem opracowania polskiego planu rozwoju społeczeństwa informacyjnego – *ePolska*, było zainicjowanie pożądanych zmian społeczno-gospodarczych określających naszą pozycję w nowoczesnej Europie, jak również przygotowanie do integracji z Unią Europejską. Plan działań budowy społeczeństwa informacyjnego zakładał osiągnięcie następujących głównych celów: przygotowania społeczeństwa do szybkich przemian technologicznych, społecznych i gospodarczych, wzrostu innowacyjności gospodarki w celu poprawy jej konkurencyjności, przygotowania społeczeństwa polskiego do wyzwań nowego rynku pracy i nowych metod pracy, czy też stworzeniu warunków dla trwałego i zrównoważonego rozwoju regionalnego.

W toku rozważanych zagadnień istotny jest problem współczesnej percepcji czynników stymulujących wzrost gospodarczy, w drodze dynamicznego rozwoju technologii informacyjnych i komunikacyjnych, które w wymierny sposób, mają służyć dobru kraju i jego mieszkańców. W opracowanym przez rząd dokumencie *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013* (MSWiA 2008), wyznaczono trzy najważniejsze obszary. W pierwszym wymienia się człowieka oraz przyspieszenie rozwoju kapitału intelektualnego i społecznego Polaków. W kolejnym wskazuje się na gospodarkę i następujące komponenty: wzrost efektywności, konkurencyjności i innowacyjności firm również na globalnym rynku, a także ułatwienie komunikacji i współpracy między firmami dzięki wykorzystaniu technologii informacyjnych i komunikacyjnych. Ostatni obszar dotyczy państwa, a w szczególności wzrostu dostępności i efektywności administracji publicznej i sposobu świadczenia usług[8].

W swoim liście Donald Tusk zauważył: „Niezwykle szybkie zmiany, które obserwujemy w tej dziedzinie, dokonały przełomu w gospodarce. Okazuje się że dla przedsiębiorstw szybki Internet jest równie ważny, jak autostrady czy linie energetyczne. Aby polska gospodarka przyciągała inwestorów i najlepszych pracowników, musimy spowodować, by to niezwykłe narzędzie, ten instrument działania, był powszechnie dostępny" (Vall i in. 2011, s. 40). Na poparcie tej tezy prezentowane są wyniki badań znaczenia tego rozwoju dla wzrostu gospodarczego, z których wynika, że technologie informacyjne i komunikacyjne w ostatnich latach odpowiadają za około jedną czwartą wzrostu PKB oraz za 40% wzrostu produktywności w Unii Europejskiej.

[8] *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013* jest dokumentem sektorowym, uwzględniającym priorytety europejskiej polityki w dziedzinie społeczeństwa informacyjnego, które wynikają z założeń Strategii Lizbońskiej oraz inicjatyw *eEurope – społeczeństwo informacyjne dla wszystkich* oraz jej kontynuacji *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia*. Ponadto przygotowana *Strategia* jest spójna z dokumentami określającymi strategiczne kierunki rozwoju Polski do których można zaliczyć: *Strategię Rozwoju Kraju 2007-2015*; *Narodowe Strategiczne Ramy Odniesienia 2007-2013*; *Strategiczny Plan Rządzenia*.

Przypadki naruszenia bezpieczeństwa

Dla zobrazowania problemu można zwrócić szczególną uwagę na kilka przypadków negatywnych konotacji rozwoju społeczeństwa informacyjnego. Pierwszy z nich dotyczy tygodnika „NIE", który ujawnił fakt posiadania 12 twardych dysków z komputerów Ministerstwa Spraw Zagranicznych, zaledwie dzień przed ogłoszeniem − w atmosferze skandalu − końcowego sprawozdania komisji śledczej badającej „sprawę Rywina", a w której niebagatelną rolę w ustalaniu okoliczności sprawy odgrywały również cyfrowe nośniki informacji. Znalazły się na nich dokumenty z lat 1992-2004, w tym 4216 plików z rozszerzeniem doc (Microsoft Word), a także setki innych plików, tabele, arkusze kalkulacyjne, e-maile, kody, klucze i hasła. Wiele z nich zawierało klauzulę „poufne i tajne". Pierwotnie dyski użytkowane były w różnych komórkach Ministerstwa − gabinecie ministra, Departamentach: Polityki Bezpieczeństwa, Ameryki, Azji i Pacyfiku, Afryki i Bliskiego Wschodu, Europy, Prawa Traktatowego, Protokołu Dyplomatycznego, a nawet w księgowości.

Zakres przedmiotowy ujawnionych przez tygodnik „NIE" informacji, znajdujących się na nośnikach danych jest bardzo zróżnicowany. Począwszy od tych, które u czytelnika wzbudzić mogą wesołość, aż po kwestie o znaczeniu strategicznym. Artykuł traktuje o sprawach dotyczących ministra Włodzimierza Cimoszewicza: grupy krwi, numeru paszportu, relacji złożonej ambasadorom o przebiegu wizyty premiera Leszka Millera w Moskwie, otrzymanych nagrodach oraz zakupach garderoby. Szerszej analizie poddany został jeden z dokumentów − nie objęty klauzulą tajności − stanowiący szczegółową relację ze spotkania ambasadorów RP, które odbyło się w dniach 1-4 lipca 2002 roku w Warszawie.

W tym samym artykule opisującym zawartość twardych dysków, które w niekontrolowany sposób „wypłynęły" z MSZ, autor ujawnia również dane dotyczące pracowników Biura Ochrony Rządu: numery rejestracyjne i rodzaje pojazdów ścisłego kierownictwa, wykaz osób zajmujących się ochroną najważniejszych obiektów administracji rządowej, ich adresy, numery telefonów i pozwoleń na broń. Artykuły zamieszczane w tygodniku „NIE" wskazują, że na dyskach MSZ znajdują się ponadto dane dotyczące spraw o charakterze międzynarodowym. Odczytać z nich można informacje i analizy w sprawie globalnego bezpieczeństwa energetycznego. Według analityków rządowych, stoimy u progu mocarstwowej rozgrywki o władzę nad złożami ropy naftowej i gazu ziemnego.

Kilka godzin po ujawnieniu skandalu minister Cimoszewicz złożył dymisję. Na zwołanej godzinę później konferencji prasowej wziął na siebie polityczną odpowiedzialność za utratę dysków nie wykluczając, że ujawnienie ich może wyrządzić szkodę interesom politycznym naszego kraju. Premier Leszek Miller nie przyjął dymisji, podając w uzasadnieniu, że Włodzimierz Cimoszewicz gwarantuje pozytywne sfinansowanie wszystkich prac poprzedzających członkostwo Polski w UE. Rozgorzała publiczna debata na temat konsekwencji, które może nieść za sobą wyciek informacji. Zauważalny wyraźnie był ich ambiwalentny ton. W opinii jednych, incydent mógł oznaczać prawdziwą katastrofę i paraliż zarówno dyplomacji, służb specjalnych, jak i innych organów administracji rządowej. Ministerstwo Spraw Zagranicznych rutynowo bowiem otrzymuje informacje z innych ministerstw i agen-

cji wywiadowczych, np. analizy sytuacji i tajne informacje[9]. Tezę powyższą zdawała się potwierdzać wypowiedź szefa ABW Andrzeja Barcikowskiego. W udzielonym wywiadzie zaprezentował on pogląd, iż znaczenie dysków było na pewno duże. Innego zdania był urzędnik zajmujący się sprawami europejskimi w MSZ, wyrażając wątpliwość, czy na tego typu dyskach mogą być dane istotne z punktu widzenia interesów państwa. Zaskakująca z uwagi na okoliczności wydaje się ocena bezpieczeństwa informacji przetwarzanych na komputerach w resorcie MSZ: „MSZ stosuje szereg środków mających na celu ochronę przed penetracją wewnętrznej sieci informatycznej zarówno w sferze dostępnego oprogramowania, jak również środków organizacyjnych. Korzystamy w tym zakresie z nowoczesnych dostępnych rozwiązań"[10].

Rezultatem ujawnienia nieprawidłowości w MSW była szeroka debata w mediach na temat bezpieczeństwa danych agregowanych w formie cyfrowej. W przypadku informacji spełniających ustawowe znamiona tajemnicy państwowej, winny być one przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie[11]. W raporcie zatytułowanym *ABW − rok po reformie* czytamy: „Wśród urzędników polskich instytucji wciąż jeszcze zdecydowanie zbyt niski jest poziom świadomości istniejących zagrożeń związanych z dostępem do informacji o newralgicznym znaczeniu dla interesów RP. Co prawda w kulturze urzędniczej coraz silniej zakorzeniają się pożądane zasady postępowania, niemniej jednak − pomimo kilkuletniego już okresu obowiązywania stosownych przepisów − nadal nie są one w pełni przestrzegane (...) Zdarzają się przy tym przypadki nieuprawnionego kopiowania ważnych dokumentów lub wywożenia ich za granicę i przechowywania w miejscach absolutnie do tego nieprzystosowanych, np. pokoju hotelowym. Istotna jest także kwestia poprawy poziomu funkcjonowania systemów zabezpieczeń technicznej i fizycznej ochrony obiektów, które są szczególnie narażone na możliwość penetracji przez osoby nieuprawnione do dostępu do informacji niejawnych" (Góra 2004, s. 3).

Liczne przykłady pokazują, że politycy, urzędnicy czy też osoby pełniące funkcje administratorów w innych podmiotach, lekceważą obowiązek chronienia zużytych twardych dysków, a pracownicy traktują je bardziej w kategoriach kawałka metalu nie mając pojęcia, że ma on taką samą wartość jak dokument[12].

[9] W ostatnich latach rządy wielu krajów zachodnich (Wielka Brytania, Grecja, USA), zostały dotknięte aferami związanymi ze skradzionymi bądź zagubionymi komputerami. Oficer brytyjskiego wywiadu MI6 zostawił w londyńskiej taksówce laptopa z zawartością supertajnych raportów antyterrorystycznych. Taksówkarz odniósł komputer na policję. Z kolei, gdy w 2000 roku kontrola w Departamencie Stanu USA ustaliła, iż z ministerstwa zaginęło kilkadziesiąt laptopów, pracę stracił szef wewnętrznej służby bezpieczeństwa.

[10] Wypowiedź rzecznika prasowego Ministerstwa Spraw Zagranicznych Bogusława Majewskiego w kontekście publikacji tygodnika „NIE".

[11] Zgodnie z obowiązującymi ówcześnie przepisami dyski z komputerów należało archiwizować w bezpiecznym miejscu (na terenie tajnej kancelarii) albo zniszczyć.

[12] Jak niebezpieczne jest pozbywanie się twardych dysków dowiedli w 2002 roku dwaj studenci Laboratorium Nauk Komputerowych amerykańskiej uczelni Massachusetts Institute of Techology, którzy za pomocą Internetu za niecałe tysiąc dolarów kupili 158 starych dysków nie nadających się zdaniem poprzednich właścicieli do użytku. Studentom udało się uruchomić 129 z nich. Na dyskach odkryli oni m.in. raporty medyczne, szczegółowe informacje finansowe firm i osób prywatnych oraz kilka gigabajtów prywatnych e-maili i materiałów pornograficznych. Na dyskach były także informacje pozwalające podszyć się pod kogoś innego. Z jednego z nich odzyskali 5 tysięcy numerów kart kredytowych.

Dwa dni po ujawnieniu przez „NIE" informacji o posiadaniu 12 twardych dysków MSZ, szef ABW Andrzej Barcikowski poinformował w Sejmie o zatrzymaniu dwóch osób, które według wszelkiego prawdopodobieństwa zamieszane były w ich kradzież z magazynu Ministerstwa. Pierwszy, będąc pracownikiem technicznym i nie zdając sobie sprawy z zawartości dysków, dokonał ich wymontowania, po czym zaniósł do punktu skupującego zużyty sprzęt komputerowy i sprzedał w cenie 10 zł za sztukę. Druga zatrzymana osoba to student Politechniki, który usiłował sprzedać je kilku redakcjom; ostatecznie zakupu dokonała redakcja tygodnika „NIE". Prowadząca postępowanie Agencja Bezpieczeństwa Wewnętrznego wykluczyła, aby sprawa miała jakikolwiek podtekst wywiadowczy czy polityczny. Jednak, zdarzenie to wywołało ironiczne komentarze w Europie, czego przykładem są liczne tytuły prasowe[13].

Kolejną egzemplifikacją zagrożeń wynikających z rozwoju społeczeństwa informacyjnego jest przypadek umieszczenia w 2005 r. w Internecie listy katalogowej z zasobów archiwalnych centrali MSW, powszechnie określanej listą Wildsteina. Obejmowała ona dwieście czterdzieści tysięcy nazwisk osób, których teczki przechowywane są w Instytucie Pamięci Narodowej. Baza zawierająca osobowy indeks archiwów została skopiowana z komputerów Instytutu przez dziennikarza „Rzeczpospolitej" Bronisława Wildsteina, motywującego swoje postępowanie względami praktycznymi, a więc chęcią ułatwienia publicystom występowania do IPN o odtajnienie danych konkretnych osób. Należałoby zadać więc pytanie, co wniosła ta sprawa do ówczesnego dyskursu obejmującego sferę lustracji? Z pewnością, z jednej strony stanowi doskonały materiał empiryczny dla badań nad powyższym zagadnieniem. Z drugiej zaś, obrazuje dychotomiczną strukturę nie tylko elit politycznych, ale również świata mediów czy społeczeństwa. Niezwykle szybko po umieszczeniu wykazu osób na serwerze znajdującym się poza granicami Polski rozgorzała dyskusja na temat problematyki lustracyjnej, w tym jej wymiaru etycznego. Mimo zamieszczenia na stronie internetowej www.fajne.info./lista/ tzw. disclaimera (zaprzeczenia) o treści: „Uwaga! Jeśli zaczniesz uważać kogoś za kapusia tylko dlatego ze jest na poniższej liście to jesteś głupi/głupia. Są tu rozmaite nazwiska, tajnych współpracowników, zawodowych ubeków, kandydatów na współpracowników oraz osób pokrzywdzonych…", nie uniknięto pytań, czy taka formuła lustracji stanowi wartość, dla której mogą cierpieć niewinne osoby.

Powstałych dylematów nie rozwiązały także sprostowania Andrzeja Friszke, członka kolegium IPN, który wyjaśnił, iż na liście znajdują się różne osoby: funkcjonariusze SB, współpracownicy, tajni agenci oraz osoby typowane przez peerelowskie służby na tajnych współpracowników. Często nie były one świadome tego faktu, sama zaś struktura dokumentu uniemożliwia ich selekcję. Liczący ponad 4 tysiące stron wykaz zawiera wyłącznie imię,

[13] Przykłady ważniejszych tytułów prasowych odnoszących się do ujawnionego w Polsce „wycieku" informacji niejawnych: „Le Monde" (Francja): *Polski minister spraw zagranicznych obnażony*; „Berliner Morgenpost" (Niemcy): *Nowa afera zachwiała polskim niestabilnym rządem*; „ORF" (Austria): *Afera danych - minister spraw zagranicznych prosi o dymisję*; „SME" (Słowacja): *Polska straciła tajne informacje i także prawie ministra*; „Financial Times" (Wielka Brytania): *Rozgrywka Urbana*; „Die Presse" (Austria): *Rząd stoi przed upadkiem*; „Kathimerini" (Grecja): *Przeciek tajnych dokumentów*; „Kommiersant" (Rosja): *Polskiemu MSZ nie pozostało już nic do ukrycia*.

nazwisko oraz sygnaturę, pod jaką teczka jest przechowywana w archiwach instytutu[14]. Wyniesienie listy, przekazanie jej innym dziennikarzom, a następnie umieszczenie w sieci spotkało się ze skrajnymi komentarzami − od bezwarunkowej aprobaty po zdecydowane potępienie. Stanowisko swoje wyraziła również Rada Etyki Mediów twierdząc, że ujawnienie indeksu nazwisk zatruło atmosferę społeczną wokół lustracji oraz w znacznej mierze naruszyło autorytet Instytutu Pamięci Narodowej[15]. W wydanym oświadczeniu zaapelowała do środowiska mediów o kontynuowanie misji kontrolnej w taki jednak sposób, by wspomóc działania IPN na rzecz pożądanego przebiegu odtajnienia dokumentów. Przypomniała również o pojawiających się dylematach, gdzie jawność życia politycznego, oglądalność, słuchalność i poczytność winna być rozpatrywana przez aksjomat odpowiedzialności i rozwagi oraz minimalizowania kosztów społecznych. Rada zdezawuowała instrumentalne traktowanie mediów przez niektóre osoby czy środowiska, karcąc jednocześnie „Gazetę Wyborczą" za enuncjacje prasowe opatrzone tytułami: *Ubecka lista krąży po Polsce* czy *Barbarzyństwo Wildsteina*, które w jej ocenie niosą dezinformację oraz potęgują klimat wzajemnych podejrzeń. Dyskurs o potencjalnym zagrożeniu dla istotnych interesów państwa zaostrzyła informacja o pojawieniu się na liście nazwisk osób – oficerów Wojskowych Służb Specjalnych, których teczki z klauzulą „tajne" i „ściśle tajne" zostały przekazane IPN.

Praktyka życia codziennego stanowi kolejny impuls do rozważań na temat negatywnych skutków rozwoju społeczeństwa informacyjnego, jak chociażby włamania do komputerów lekarzy Porozumienia Zielonogórskiego przez Lubelski Oddział Narodowego Funduszu Zdrowia czy próba sprzedaży tajnych danych przez oficera WSI nadzorującego pracę supertajnego natowskiego systemu komputerowego „Kronos". Ostatnią głośną egzemplifikacją tych zagrożeń – w kontekście już wspomnianego w artykule porozumienia ACTA – jest włamanie na początku 2012 roku do służbowego laptopa wiceministra Administracji i Cyfryzacji przez członków społeczności hakerskiej „Anonymous"[16]. Niezwłocznie po dokonaniu kradzieży prywatnych i służbowych danych, zamieścili w Internecie ostrzeżenie, iż jeśli Polska podpisze ACTA, ujawnią dane na temat osób z rządu[17]. Z kolei przez długi czas społeczność międzynarodowa była informowana o umieszczanych na portalu „WikiLeaks" materiałach, zawierających niejawne dokumenty rządowe: raporty z obszarów objętych walkami i incydentami z udziałem wojsk koalicji w Afganistanie, Iraku, czy treści depesz opracowywanych i przesyłanych przez amerykańskie placówki dyplomatyczne. Przekaz

[14] Pierwotnie uważano, iż cyfra „0" identyfikuje pracownika służby bezpieczeństwa, natomiast „00" osobę zakwalifikowaną jako tajny współpracownik lub kandydat na to stanowisko. W późniejszym czasie IPN oznajmił, że liczba zer nie ma żadnego znaczenia i na jej podstawie nie należy dokonywać żadnych interpretacji. Pojawiły się również w Internecie zmodyfikowane listy, np. strona prawicowego tygodnika „Głos" zawierała informacje dotyczące jednostek, z których pochodzą konkretne teczki, a także rodzaj bazy archiwalnej obejmującej akta osobowe (etatowi funkcjonariusze) i akta tajnych współpracowników i kandydatów.

[15] Rada Etyki Mediów jest organem kolegialnym, kadencyjnym, liczącym trzynaście osób. Do najważniejszych jej zadań należy wypowiadanie się na temat ważnych lub budzących wątpliwości etycznych zjawisk w mediach.

[16] W wyniku przeprowadzonego ataku hakerzy spowodowali wyłączenie najważniejszych stron administracji rządowej m.in.: Sejmu, Ministerstwa Finansów, Policji, Biura Ochrony Rządu, Ministerstwa Obrony Narodowej, a także witrynę Platformy Obywatelskiej. Ponadto intruzom udał się przejąć serwer na którym umieszczona była strona Kancelarii Prezesa Rady Ministrów – http://www.kprm.gov.pl oraz podmienić jego treść.

[17] Zob. szerzej: *Hakerzy szukali informacji w laptopie ministra informacji o ACTA?,* http://www.wprost.pl/ar/289422/Hakerzy-szukali-w-laptopie-ministra-informacji-o-ACTA/; *Skradziono dane z laptopa wiceministra cyfryzacji,* http://www.rp.pl/artykul/796372.html [dostęp:25.04.2012].

medialny zdominowały informacje o zagrożeniu prywatności zarówno obywateli, jak też najważniejszych polityków w Europie i na świecie, przez wykorzystywanie przez amerykańskie służby programu „PRISM", umożliwiającego dostęp do tekstowych, dźwiękowych i wizualnych materiałów, przesyłanych za pośrednictwem największych portali internetowych. Prawdziwą falę oburzenia wywołały jednak informacje, iż służby specjalne agregują dziennie kilka milionów zdjęć internatów − korzystających z takich portali społecznościowych, jak Facebook, Twitter czy Google+ − kontrolują adresy e-mail, ściągnięte pliki, numery telefonów oraz treści i materiały wymieniane na czatach, by budować w ten sposób kompletne profile osób, a być może i dowiązywać je do posiadanych w bazach odcisków palców.

Podsumowanie

Rozwój techniki komputerowej spowodował − zdaniem Zygmunta Baumana − nienasycone pragnienie informacji, której zasób w cyberprzestrzeni wydaje się nieskończony; powoduje on zarazem „...abstrakcyjną pokusę kontrolowania informacji, której w istocie nie sposób zaspokoić" (Bauman 2005, s. 45). Linda Groff stwierdza z kolei, że żadne z państw należących do współzależnego świata nie może być całkiem odporne na rewolucję informacyjną (Groff 1997). Podążając zatem za tymi poglądami, nie tyle istotne wydaje się pytanie, czy cyberprzestrzeń należy kontrolować, ale jaki powinien być jej zakres (Romiszewska 2004); dochodzi tutaj do polaryzacji poglądów, gdzie z jednej strony dominuje chęć zapewnienia nieskrępowanej ograniczeniami przestrzeni do wypowiadania swoich myśli, poglądów, wreszcie korzystania z udostępnionych zasobów, z drugiej zaś strony, twierdzi się, że owa swoboda winna być ograniczona stosownymi regulacjami prawnymi. Jeszcze inaczej konstatuje M. Castells zauważając, że „Internet jest szczególnie podatny na wzmacnianie sprzecznych tendencji (…). Nie jest ani utopią, ani dystopią, lecz wyraża nas samych". Dalej wyraża przekonanie o nieuchronności konfliktów w obszarze wolności i prywatności, pojawiających się w interakcji państwa, biznesu, a komunikacją opartą na sieci (Castells 2003).

Niepomierny wzrost wrażliwości na strategiczne znaczenie danych, informacji i wiedzy, które jeszcze niedawno pełniły role pomocnicze, powoduje konieczność dokonania analizy tego rodzaju zagrożeń, bowiem tworzenie struktur formalnych *bona fide* – zaliczyć do nich można Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL w strukturze ABW, Centrum Operacji Cybernetycznych MON oraz komórki organizacyjne wsparcia zwalczania cyberprzestępczości w Policji − nie spowoduje, iż problem straci choć trochę na aktualności. Przedstawiciele każdego kraju, odpowiedzialni za procesy decyzyjne, powinni dopasować politykę czy kwestie rozwojowe do intensywności i rodzaju tych przeobrażeń, uwarunkowanych zróżnicowanymi systemami polityczno-ekonomicznymi, stopniem rozwoju, jak również kulturą i historycznymi doświadczeniami.

W tym właśnie obszarze powinny ujawnić się coraz mocniej, odpowiedzialne działania ze strony osób odpowiedzialnych za administrowanie czy też przechowywanie wrażliwych

danych, rozumianych jako bezpieczeństwo informacji[18]. W przedmowie do Białej Księgi Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej Prezydent Bronisław Komorowski zauważa: „Ostatnie dwie dekady przyniosły wiele dynamicznych zmian w strategicznym środowisku bezpieczeństwa Polski. Globalizacja i rewolucja informacyjna przyczyniły się do powiązania świata coraz ściślejszymi sieciami wzajemnych zależności (...) Mamy do czynienia z erupcją zagrożeń w cyberprzestrzeni. Powoduje to konieczność nowego podejścia do bezpieczeństwa narodowego"[19]; zagrożenia teleinformatyczne nie dotyczą jedynie wybranych państw, bowiem model funkcjonowania sieci decyduje o ich globalnym, transnarodowym charakterze (Liedel 2011).

Zarówno na gruncie europejskim, krajowym, coraz więcej podmiotów − usytuowanych zarówno w strukturze administracji publicznej, jak również sektorze prywatnym − realizuje zadania w obszarze zapewnienia bezpieczeństwa informacyjnego; nie są one jednak w stanie zapewnić kompleksowej ochrony − może z wyłączeniem elementów infrastruktury krytycznej oraz najważniejszych organów i instytucji ważnych dla bezpieczeństwa, obronności czy gospodarki państwa – wszystkim podmiotom współtworzącym sieć globalnych więzi. Dlatego też coraz powszechniejszą praktyką jest korzystanie z usług *outsourcingowych*; rolę tę nierzadko przejmują podmioty odpowiedzialne za ochronę osób i mienia, a do zakresu ich odpowiedzialności − pomijając oczywiście te najbardziej powszechne − należy chociażby prognozowanie obecnych i potencjalnych zagrożeń, sporządzanie planów ochrony obiektów, w ramach których mogą zostać wydzielone strefy ochronne, związane przykładowo z dostępem do danych wrażliwych (np. obejmujących ochronę danych osobowych, informacji niejawnych itp.)[20].

Przygotowywana przez Ministerstwo Sprawiedliwości, a następnie uchwalona ustawa regulująca wykonywanie niektórych zawodów w pierwszej transzy przewidywała ułatwienia w dostępie do 49 zawodów, w tym również dla osób wykonujących zadania związane z ochroną fizyczną oraz zabezpieczeniem technicznym. Zastąpiono dotychczasowy egzamin państwowy, przeprowadzany przez komisje powoływane przez komendantów wojewódzkich policji wpisem na listę kwalifikowanych pracowników ochrony, przy spełnieniu jednocześnie formalnych wymogów[21]. Konieczne jest legitymowanie się dokumentem potwierdzającym specjalistyczne przygotowanie teoretyczne i praktyczne w zakresie wyszkolenia strzeleckiego, samoobrony, technik interwencyjnych oraz znajomości przepisów prawa związanych z wykonywaniem ochrony osób i mienia. O ile zmiany powyższe można postrzegać jako znaczące w kontekście podejmowania zatrudnienia w obszarze ochrony

[18] W opinii Krzysztofa Lidermana, ochrona informacji obejmuje szerokie spektrum działań, włączając w to formy werbalne, które mają na celu niedopuszczenie do nieuprawnionego ujawnienia, zmiany, zniszczenia lub utraty informacji, co może spowodować szkody dla kogoś lub czegoś.

[19] Pełny tekst dokumentu dostępny jest na stronie http://www.abw.gov.pl/ftp/pdf/Biala_Ksiega_e-book_24.05.2013.pdf, [dostęp: 25.05.2012].

[20] Podstawę prawną działania firm i pracowników ochrony określa ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. z 1997 r. Nr 114, poz. 740 z późn. zm.).

[21] Wśród nich wymienić należy m.in.: wiek, pełną zdolność do czynności prawnych, niekaralność, zdolność fizyczną i psychiczną oraz nienaganną opinię wydaną przez komendanta komisariatu policji oraz została dopuszczona do posiadania broni w trybie innych przepisów.

osób i mienia, czy wchodzenia ludzi młodych na rynek pracy[22], nie sposób jednak pominąć pewnych zagrożeń, które regulacja ta ze sobą niesie. Konieczna będzie tutaj weryfikacja podmiotów prowadzących szkolenia teoretyczne i praktyczne, pod kątem jakości realizacji tych zadań.

Nie mniej istotna wydaje się również kwestia wdrożenia skutecznej polityki prewencyjnej czy profilaktyki, bowiem jak wynika z opracowanego przez Ministerstwo Administracji i Cyfryzacji pod koniec 2013 r. raportu – będącego analizą i podsumowaniem wdrożonej Strategi rozwoju społeczeństwa informacyjnego w Polsce w latach 2008-2013 – społeczeństwo polskie notuje wciąż niski poziom umiejętności korzystania z narzędzi teleinformatycznych (18%), przy średniej dla trzech liderów UE wynoszącej 39% (MAC 2013).

Bibliografia

Bauman Z. (2005), *Życie na przemiał,* Wydawnictwo Literackie, Kraków.

Bauman Z. (2000), *Globalizacja,* PIW, Warszawa.

Bendyk E. (2004), *Antymatrix. Człowiek w labiryncie sieci,* W.A.B., Warszawa.

Castells, M. (2003), *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem,* Dom Wydawniczy Rebis, Poznań.

Castells M. (2007), *Społeczeństwo sieci,* Wydawnictwo Naukowe PWN, Warszawa.

Cylka T. (2004), *Tajne przez poufne, „*Głos Wielkopolski".

Groff L. (1997), *Rewolucja informacyjna: globalne trendy restrukturyzacyjne, wizje i decyzje*, (w:) *Problemy społeczeństwa informacyjnego*, Transformacje, Warszawa.

Góra J. (2004), *Twarde prawo, niedbalstwo jeszcze twardsze, „*Gazeta Prawna", nr 69.

Komitet Badań Naukowych (KBN) (2001), *ePolska − Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*, Warszawa.

Komitet Badań Naukowych dla Rady Ministrów (KBN) (2000), Raport *Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce,* Warszawa.

Liedel K. (2011), *Bezpieczeństwo informacyjne państwa*, (w:) *Transsektorowe obszary bezpieczeństwa narodowego*, Difin, Warszawa.

Mazurkiewicz A. (2011), *Paradygmaty zarządzania we współczesnym przedsiębiorstwie: wybrane aspekty,* (w:) *Nierówności społeczne a wzrost gospodarczy,* Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów.

Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) (2008), *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013,* Warszawa.

Ministerstwo Administracji i Cyfryzacji (MAC) (2013), *Społeczeństwo informacyjne w liczbach*, Warszawa.

Pietruszka-Ortyl A. (2012), *Praca oparta na wiedzy,* (w:) *Zachowania organizacyjne w kontekście zarządzania wiedzą,* Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków.

[22] W chwili obecnej brak jest oficjalnej statystyki obejmującej liczbę osób wykonujących zadania związane z ochroną osób i mienia, jednak na podstawie danych przedstawionych przez organizację branżową – Polską Izbę Ochrony, należy szacować ich liczbę na około trzysta tysięcy pracowników ochrony zatrudnionych w ponad pięciu tysiącach koncesjonowanych przedsiębiorstwach.

Rawicz J., (2004), *Raport pod dyktando: nie było grupy trzymającej władzę, Rywin działał sam*, „Gazeta Wyborcza".

Romiszewska B. (2004), *Internet – enklawa wolności czy wirtualne więzienie?*, (w:) *Kulturowe instrumentarium wolności*, Wydawnictwo Naukowe INPiD UAM, Poznań.

Rozenek A. (2004), *Cimoszewicz obnażony, „*NIE", nr 15.

Silicki K. (2009), *Unia Europejska a bezpieczeństwo teleinformatyczne – inicjatywy i wyzwania,* (w:) *Bezpieczeństwo teleinformatyczne państwa,* Polski Instytut Spraw Międzynarodowych, Warszawa.

Urząd Komunikacji Elektronicznej (UKE) (2010), *Raport o stanie rynku telekomunikacyjnego w Polsce w 2010 roku*, Warszawa.

Urząd Komunikacji Elektronicznej (UKE) (2011), *Raport pokrycia terytorium Rzeczypospolitej Polskiej istniejącą infrastrukturą telekomunikacyjną zrealizowanymi w 2010 r. i planowanymi w 2011 r. inwestycjami oraz budynkami umożliwiającymi kolokację*, Warszawa.

Wroński P. (2004), *Sekrety MSZ sprzedane, „*Gazeta Wyborcza".

Wroński P. (2004), *Ujawnienie dysków to katastrofa, „*Gazeta Wyborcza".

Vall M., Majorek M., Walecka-Rynduch A. (2011) *Współczesna przestrzeń polityczna. Ewolucja czy rewolucja?*, Krakowskie Towarzystwo Edukacyjne, Kraków.

Antinomy of the Information Society – Opportunities and Threats

Summary

In his article, the author touched the problems of the information society whose development is currently perceived as a guarantor of development of the knowledge-based economy. He characterised the most important components of innovative information and communication technologies (ICT), inclusive of the occurring threats that may become their destiny for the developing economy in Poland.

Objective: diagnosis and assessment of the governmental administration in building the economy whose important element is use of progress as regards advanced technologies.

Research method: individual cases and documents examination.

Main research findings: a frequent practice of transfer of responsibility for data and information security onto private entities, facilitation in acquisition of qualification by workers of persons and property protection, including carrying out economic activity as well as still the low level of skills to make use of ICT tools require further well-judged measures on the side of the state.

Practical implications: it is stated that there systematically takes place breach of the information security rules that may entail negative image and financial consequences. Building the modern information, knowledge-based society requires alteration of consumers' awareness and desired legislative amendments.

Article category: research.

Key words: information society, innovations, teleinformation security.

JEL codes: O380, O390, Z00

Антиномия информационного общества – шансы и угрозы

Резюме

В статье затронули проблематику информационного общества, развитие которого в настоящее время воспринимается в качестве гаранта развития экономики, основанной на знаниях. Дана характеристика основных составных частей инновационных информационных и коммуникационных технологий (ICT), в том числе выступающих угроз, которые могут стать их участью для развивающейся экономики в Польше.

Цель: диагноз и оценка госадминистрации в формировании экономики, существенным элементом которой является использование прогресса в области современных технологий.

Исследовательский метод: изучение индивидуальных случаев и документов.

Основные результаты исследований: частая практика переноса ответственности за безопасность данных и информации на частных субъектов, упрощение обретения квалификации работниками охраны лиц и имущества, в том числе проведение экономической деятельности, а также по-прежнему низкий уровень пользования телеинформатическими инструментами требуют дальнейших обдуманных и целенаправленных действий со стороны государства.

Практические импликации: констатировали, что систематически выступают нарушения принципов безопасности информации, которые могут вести к негативным последствиям для имиджа и финансов. Формирование современного информационного общества, основанного на знаниях, требует изменения сознательности потребителей и желательных законодательных изменений.

Категория статьи: исследовательская.

Ключевые слова: информационное общество, инновации, телеинформатическая безопасность.

Коды JEL: O380, O390, Z00

Artykuł nadesłany do redakcji w lipcu 2014 r.

Afiliacja:

dr Dariusz Skalski
Państwowa Wyższa Szkoła Zawodowa w Wałczu
Instytut Kultury Fizycznej
ul. Bydgoska 50
78-600 Wałcz
tel.: 67 250 01 87
e-mail: dariusz@pwsz.eu