ANTROPOLOGICZNY ASPEKT BEZPIECZEŃSTWA INFORMACYJNEGO UŻYTKOWNIKÓW NOWOCZESNYCH ŚRODKÓW KOMUNIKACJI. CZĘŚĆ II

Stanisław W. Ptaszek

Wojskowa Akademia Techniczna

Streszczenie. Poniższa publikacja stanowi kontynuację poprzedniej: *Antropologiczny aspekt bezpieczeństwa informacyjnego użytkowników nowoczesnych środków komunikacji*. W części pierwszej przedstawiłem podstawowe pojęcia z zakresu bezpieczeństwa, w tym bezpieczeństwa teleinformatycznego, komunikacji, nowoczesnej telekomunikacji[1]. W rekomendacjach wyjaśniłem zjawisko cyberprzestępczości oraz dałem wskazówki, jak mu przeciwdziałać. W drugiej części skupiam się na bezpieczeństwie w wymiarze personalnym w ramach instytucji prywatnych i państwowych. Szczególną uwagę zwracam na tematy aktualne, takie jak bezpieczeństwo dzieci i umowę ACTA. Ponadto podkreślam rolę kierunku i zakresu rozwoju ewolucji cyberprzestrzeni, głównie telefonii i internetu.

W części pierwszej wyjaśniłem zasadnicze pojęcia i terminy, ponadto wskazałem podstawowe zagrożenia, a także dokonałem diagnozy co do kierunku i siły zagrożeń. W rekomendacjach wskazałem, że cyberprzestępczość nie zniknie – jest zarówno produktem ery internetowej, jak i częścią ogólnego krajobrazu przestępczego. Dlatego też za nierealistyczne uważam myślenie, że „można wygrać tę wojnę". Zamiast tego powinniśmy znaleźć sposób na zmniejszenie ryzyka. Ważnym aspektem jest kształcenie społeczeństwa w tym kierunku, tak by wszyscy mogli w pełni bezpiecznie wykorzystywać możliwości, jakie dają środki masowej komunikacji i informacji, w tym Internet. Jeśli w codziennym życiu kierujemy się zasadą ograniczonego zaufania, to ową zasadę powinniśmy stosować do świata online. W wychowaniu dzieci należy stosować metody oparte o tzw. zdrowy rozsądek, za pomocą których uczymy i ostrzegamy dzieci o potencjalnych zagrożeniach, jakie niesie Internet. Jeżeli nam się to uda, dzisiejsze dzieci będą lepiej przygotowane do tego, aby zapewnić ochronę sobie i swoim własnym dzieciom. Problem w zapewnieniu bezpieczeństwa teleinformacyjnego obywateli polega również na tym, iż ingerencja państwa wiąże się z groźbą naruszenia praw człowieka, w tym prawa do prywatności. Istniejące technologie informatyczne zapewniają dość wysoki stopień bezpieczeństwa, ale one same są bezskuteczne. Nie można ignorować tego aspektu bezpieczeństwa, który wiąże

[1] Część pierwsza zawarta jest w S. Ptaszek, *Antropologiczny aspekt bezpieczeństwa informacyjnego użytkowników nowoczesnych środków komunikacji*, cz. I, (w:) „Studia Bezpieczeństwa Narodowego", nr 2/2011 WAT. Warszawa 20011, s. 239-261.

się z człowiekiem, z jego łatwowiernością, brakiem asertywności itp. Żadne najdoskonalsze zabezpieczenia nie będą skuteczne, jeśli będziemy stosować kradzione programy i przestarzałe antywirusowe zabezpieczenia.

W obecnej części zamierzam przedstawić najbardziej aktualne oraz przewidywane zagrożenia wynikające między innymi z zawrotnego postępu technicznego w telekomunikacji oraz wpływu na to zjawisko globalizacji. Nigdy w historii ludzkości informacja, jej prawdziwość, szybkość i racjonalność nie miała tak dużego wpływu na sytuację polityczną, ekonomiczną, militarną miliardów ludzi na całym świecie. Głównie chciałbym skupić się na bezpieczeństwie teleinformacyjnym w wymiarze personalnym, czyli indywidualnym[2]. Istota bezpieczeństwa informacyjnego polega na zapewnieniu nienaruszalności podstawowych praw człowieka. Ponadto zamierzam prześledzić społeczno-ekonomiczne skutki korzystania z Internetu przez firmy, a w tych ramach, jak realizowane jest prawo do wolności i bezpieczeństwa. Według mnie zbyt często w sprzeczności jest bezpieczeństwo personalne z bezpieczeństwem instytucjonalnym systemów teleinformacyjnych. Chciałbym zdiagnozować współczesne formy przestępczości komputerowej cyberprzestępczości, a także zagrożenia i bezpieczeństwo w Internecie dzieci i młodzieży. Ustosunkować się do ACTA, jako prawa mającego na celu ochronę własności intelektualnej i praw autorskich, i tego, jak jego postanowienia mają się do prawa człowieka do wolności i rozwoju.

„Będzie lekki, odporny na zniszczenia. Ma służyć do komunikacji, zabawy, załatwiania codziennych spraw, nawet kontroli własnego zdrowia. W pełni się od niego uzależnimy. I nie będzie to tylko telefon", takie wnioski można wynieść po zakończonym w Barcelonie w 2012 World Mobile Congress[3]. Według najnowszych trendów, obecna komórka (zwane pogardliwie „przenośnymi słuchawkami do dzwonienia") przemieni się w smartfon, który dzięki wielu programom każdy będzie mógł skonfigurować zgodnie ze swymi życzeniami. Zasadniczym zagrożeniem tej niewątpliwie pięknej przyszłości jest uzależnienie, ludzie określani jako „hyperconnected" to ci użytkownicy sieci, którzy kilka razy na godzinę przeglądają swój profil społecznościowy i pocztę. Innym, co prawda technicznym, zagrożeniem mobilnej telekomunikacji, ale generującym następne, jest tłok i pewien chaos w oprogramowaniu. Może to być przyczyną personalnego poczucia zagubienia, a dla nieuczciwych polem przestępstw.

[2] Różnice w koncepcjach bezpieczeństwa personalnego i bezpieczeństwa strukturalnego odnoszącego się do instytucji przedstawia w swych publikacjach R. Rosa m.in. w *Filozofia bezpieczeństwa*, wyd. Bellona, Warszawa 1997.

[3] Bardzo ciekawe wiadomości o przyszłości telekomunikacji przedstawił P. Stasiak, *Komórka już nigdy nie będzie telefonem*, (w:) „Polityka" nr 11(2850) z 14.03. 2012, s. 46.

Istota i antropologiczny wymiar bezpieczeństwa personalnego w dobie cyfryzacji państwa

Aksjologia filozoficzna znacznie wcześniej niż wszystkie nauki uznała bezpieczeństwo i jego poczucie za jedną z najważniejszych wartości, jaką ludzkość ceni, a każdy człowiek musi szanować i przestrzegać. Dlatego wszystko, co czynimy jako ludzie, musi służyć człowiekowi. Obecne czasy to czas techniki, a tym samym społeczeństwa cyfrowego, znacznie różnego od wszystkiego, co było przedtem.

Organy państwa powinny służyć jego bezpieczeństwu politycznemu, jako instytucji, ponadto realizować „proces zapewnienia spójności celów w obszarze bezpieczeństwa narodowego z wartościami i normami społecznymi opartych na nich normami prawnymi"[4]. Najistotniejsze w realizacji funkcji bezpieczeństwa jest to, aby przebiegała w zgodzie z wartościami, w tym moralnymi, i prawem.

„Dla nas, dzieci sieci – pisze Piotr Czerski – najważniejszą wartością jest wolność: słowa, dostępu do informacji, kultury. Potrzebujemy systemu, który by spełniał nasze oczekiwania" i należałoby tu koniecznie dodać bezpiecznego, jest to swego rodzaju manifest społeczeństwa cyfrowego[5]. Należy do powyższej deklaracji – manifestu młodego człowieka – dodać, iż system ów przede wszystkim ma spełniać warunek bezpieczeństwa, a nie stać się tylko jednym z pragnień. Myślę, że ogólnie myśl jest trafna i oddaje istotę myślenia, odczuć i działania młodych ludzi nazywających się cyfrowymi.

Świat komunikacji analogowej, czyli elektroniki tradycyjnej, był światem reglamentującym informacje, ograniczającym komunikację. Kto miał środki łączności (przykład stanu wojennego), ten miał informację, co dawało władzę polityczną i gospodarczą. Dysponentów informacji było niewielu, panowała nierówność, gdyż poza owymi dysponentami pozostali musieli polegać na udostępnianej informacji i wierzyć jej. Tę nierówność wyrównała i w pewnym sensie zniosła komunikacja cyfrowa, w tym sieć, dając ok. dwóm miliardom ludzi (na tyle szacuje się ilość użytkowników sieci) możliwość korzystania z informacji w sposób globalny.

Carne Ross uważa, że stary paradygmat Kuhna w dzisiejszych czasach powinien podkreślać siłę nowych systemów i metod politycznych – uwzględniających np. poglądy przeciwników ACTA czy ruchu Wall Ocupation – mogących wyleczyć

[4] Cytat pochodzi z rozprawy naukowej dotyczącej szeroko pojętego instytucjonalnego bezpieczeństwa politycznego pastwa. S. Zalweski, *Bezpieczeństwo polityczne państwa. Studium funkcjonalności instytucji*, Wydawnictwo Akademii Podlaskiej, Siedlce 2010, s. 91.

[5] Bardzo ciekawy, przemyślany i trafny głos młodego człowieka, jak sam się określa dziecka sieci, Piotra Czerskiego, zamieszczony w tygodniku „Polityka" nr 10 (2849), 03-13.03.2012, s. 64-65.

choroby obecnej ekonomii. Ponadto powinien zaoferować lepsze metody organizacji politycznej i ekonomicznej i lepiej rozumieć ludzkie społeczności[6].

W świecie komunikacji cyfrowej wcześniej reglamentowana informacja nie tylko nie straciła na swym znaczeniu, ale ciągle zyskuje. Stała się niemal najważniejszym narzędziem komunikacji zarówno w świecie polityki jak i gospodarki. W związku z tym rośnie rola bezpieczeństwa informacyjnego, gdyż nigdy w historii ludzkości informacje nie miały tak dużego wpływu na miliardy ludzi na całym świecie. Szczególnie widoczne i spektakularne znaczenie informacji jawi się jako polityczne, w tym militarne i ekonomiczne. Informacja może być przyczyną kryzysów politycznych, np. rewolucja arabska, a także powstania nieuczciwych fortun prywatnych, a w wymiarze państwowym może nieść zagrożenie obronności. W wymiarze jednostki może prowadzić do autokracji lub do destrukcji.

Pewną nadzieją jest to, iż do głosu dochodzi pokoleniowe cyfrowe, w przeciwieństwie do społeczeństwa analogowego dorastające z siecią. Według Piotra Czerskiego sieć jest specyficznym rodzajem procesu, zmieniającego ludzi i przez tych ludzi zmienianego, który kształtuje „cyfrowy" sposób postrzegania siebie, najbliższej rzeczywistości całego świata. Zdaniem niego należy traktować obecne młode pokolenie jako pokolenie otwarte, pokolenie dialogu, które tę zdolność zyskało dzięki sieci i posiadaniu codziennego dostępu do kultury. Moim zdaniem istnieją pewne przesłanki, iż tezy Rossa o zdolności samoregulacyjnej sieci się spełnią. Powstanie w przyszłości system – może globalny – stworzony nie dla rządu, ale dla dobra jednostki i grup społecznych, którego będą nie tylko adresatem, ale przede wszystkim twórcą.

Bezpieczeństwo informacyjne, jego istota, polega na zapewnieniu nienaruszalności podstawowych praw człowieka, jak: wolność, prywatność, rozwój czy tolerancja poglądów i zachowań. Przypomnijmy prawa powszechnie gwarantowane, przynależne każdemu człowiekowi z racji urodzenia, a zawarte w demokratycznych konstytucjach i Deklaracji Praw Człowieka ONZ. Tak więc wszyscy uczestnicy społeczeństwa informacyjnego winni postrzegać bezpieczeństwo jako coś, co im się bezwzględnie należy. Bezpieczeństwo i wolność jednostki i ludzkości musi mieć priorytet, nawet kosztem spowolnienia postępu technicznego. Powinna istnieć tu zasada prymatu moralności nad polityką, ekonomią, a zwłaszcza techniką i jej postępem. Konieczna jest popularyzacja i stosowanie zasad aksjologii filozoficznej. Według aksjologii najwyższą wartością – wg religijnych aksjologii Bóg – jest człowiek i wszystko, co mu w rozumny sposób służy, dlatego musi istnieć prymat aksjologii antropologicznej przed techniką, polityką i ekonomią. Problem w zapewnieniu bezpieczeństwa teleinformacyjnego obywateli polega również na tym, iż ingerencja państwa wiąże się z groźbą naruszenia praw człowieka,

[6] Carne Ross is the author of *The Leaderless Revolution: How ordinary people will take power and change politics in the 21st century* – published in the UK by Simon & Schuster 2011, and in the US by Blue Rider Press (Penguin USA) in 2011 (e-book) – wolne tłumaczenie autora tej publikacji.

w tym do prywatności. Świat analogowy był elitarny, a dla przeciętnego człowieka ograniczony, ale stosunkowo bezpieczny. Świat informacji cyfrowej jest znacznie bardziej dostępny, stał się egalitarny, a ceną za to jest zmniejszenie bezpieczeństwa zarówno instytucjonalnego jak i personalnego.

Zmniejszenie bezpieczeństwa uczestników komunikacji cyfrowej wiąże się po pierwsze z jej fizyczno-techniczną istotą, np. łatwiej podsłuchiwać technikę cyfrową niż analogową, a i ona sama doskonali i upowszechnia metody podsłuchu samej siebie: po drugie jej dostępność powoduje, że wśród użytkowników znajdują się miliardy ludzi i miliony instytucji pragnących ją wykorzystać w sposób nie zawsze moralny. Informacja to towar, towar to pieniądz, pieniądz to władza. Tak więc istotą komunikacji opartej na technice cyfrowej jest jej wrażliwość na najróżnorodniejsze zagrożenia i niebezpieczeństwa. Postęp w informatyce nic nie traci ze swego szalonego tempa, dotyczy to również nowoczesnych środków komunikacji. Powstają coraz nowocześniejsze systemy kontroli, a nawet inwigilacji użytkowników. Dzięki rozwojowi kryptologii i coraz dostępniejszym środkom szpiegowskim nikt dziś nie może czuć się pewien, że go ktoś prywatnie czy służbowo nie podsłuchuje, nie kontroluje jego prywatnej i służbowej korespondencji.

Społeczno-ekonomiczne skutki korzystania z Internetu przez firmy a wolność i bezpieczeństwo

Według różnych sondaży skutki używania mediów społecznościowych przez małe i duże firmy to: utrata prywatności i danych – ok. 75%, zarażenie złośliwymi kodami – ok. 79%, spadek aktywności pracowników – ok. 60%, uszczerbek na reputacji oraz problemy z wydajnością – ok. 30%. W związku z powyższym, aby zapobiegać niechcianemu ujawnianiu informacji, coraz więcej firm i instytucji wprowadza różne procedury i systemy bezpieczeństwa. Procedury mogą polegać na tym, iż w całej strukturze organizacji każdy bezpośredni przełożony ma bieżący wgląd w każdą operację (monitorowane i rejestrowane jest każde „kliknięcie") podwładnego. Ponadto, w zależności od szczebla organizacji i zaufania do pracownika, zamykane/blokowane są pewne strony internetowe i adresy. Systemy bezpieczeństwa, których jest mnóstwo i ciągle się doskonalą, stanowią kompilację elektroniki, kryptologii i co nie mniej ważne, psychologii walki elektronicznej[7]. Nie uwzględniają w znikomym stopniu lub wcale etycznego aspektu pracy. Zdaniem etyków każdy pracownik powinien w sposób bezpieczny – a jeżeli to konieczne poufny – poinformować o nielegalnych i nieetycznych praktykach wewnątrz instytucji. Dobrym rozwiązaniem mogą być tzw. linie ds. etyki. Spadek produktywności próbuje się powstrzymać, blokując dostęp do pewnych stron lub całkowity do Internetu.

[7] Usługę taką proponuje wiele elektronicznych agencji zajmujących się bezpieczeństwem, np. Agencja Wdrażania Systemów Bezpieczeństwa HEKTOR.

Jest to częsta praktyka przypominająca „wylanie dziecka z kąpielą". Działanie takie często powoduje regres intelektualny pracowników i ich frustrację, co w konsekwencji pociąga za sobą co najmniej stagnację, a nawet regres firmy.

Bezpieczeństwo personalne a bezpieczeństwo instytucjonalne systemów teleinformacyjnych to inny nie mniej ważny problem. Ministerstwo Edukacji Narodowej zamierza rozbudować System Informacji Oświatowej (SIO). Pozwoli on dokładnie sprawdzić, czy wszystkie dzieci uczęszczają do szkoły, gdyż według ustawy o systemie oświaty edukacja obowiązkowa jest do szesnastego roku życia. W systemie znajdą się takie dane jak PESEL i adresy zamieszkania dzieci, również tych, które wymagają nauczania w trybie indywidualnym oraz dzieci znajdujących się w trudnej sytuacji materialnej i wychowawczej. Pytanie brzmi, czy dla kilkuset dzieci konieczny jest system z powszechnie dostępnymi danymi zawierający tzw. dane wrażliwe: PESEL, imiona rodziców i adresy. Dane te, jako powszechnie dostępne i przechowywane, będą mogły być wykorzystane w przyszłości do różnych niemoralnych celów. Z podobnych względów społeczeństwo polskie, a szczególnie jego młoda część, nie zgadza się na przyjęcie przez ratyfikację międzynarodowego prawa powszechnie znanego jako ACTA. Umiędzynarodawia ono prawnie, czyli czyni z globalnej cyberprzestrzeni obszar swej jurysdykcji i to w sposób dość restrykcyjny. Pozwala organom ścigania innych państw na wgląd w dane niemal wszystkich obywateli, w tym tzw. dane wrażliwe. W obronie prywatności polskich obywateli stanął Generalny Inspektor Ochrony Danych Osobowych, który oficjalnie zarekomendował niepodpisywanie traktatu. Uznał on, iż ACTA niesie wiele zagrożeń praw i wolności określonych w Konstytucji. Na przykład policja formalnie musiałaby przekazywać dane osobowe polskich obywateli, bez gwarancji, że będą one odpowiednio chronione.

Państwo i jego instytucje bezpieczeństwa elektronicznego

Obecne państwo, mając na uwadze swoje bezpieczeństwo, ciągle rozszerza krąg instytucji mających prawne możliwości dostępu do danych wrażliwych i śledzenia elektronicznego wszystkich obywateli[8]. Instytucje takie jak Agencja Bezpieczeństwa Wewnętrznego czy Wojskowe Służby Informacyjne, mając dostęp do owych danych, mogą, chroniąc państwo, wykorzystywać ową wiedzę do kontroli i wpływu na polityków, urzędników, biznesmenów czy zwykłych ludzi. Rozwój metod detektywistycznych umożliwia wpływanie na polityków, biznes i innych z pominięciem obowiązujących procedur prawnych, czyniąc ze służb ochronnych niebezpieczne narzędzie przestępcze, gdyż są to instytucje dobrze zorganizowane i zatrudniające ludzi dobrze znających się na swej profesji, ale niekoniecznie moralnych.

[8] W 2011 roku możliwość niemal nieograniczonego dostępu do informacji decyzją sejmu i senatu otrzymała kolejna instytucja – Najwyższa Izba Kontroli.

Metoda ustanawiania przez polityków i urzędników coraz to nowych podmiotów o szerszych prawnych kompetencjach mających dbać o bezpieczeństwo państwa, a tym samym jego obywateli, jest drogą niebezpieczną i nieefektywną. Niebezpieczną zarówno dla państwa jak i obywateli, gdyż zbyt duże możliwości tych instytucji czynią je trudnymi do kontroli, co może generować patologię[9]. Zbyt duża ilość takich instytucji powoduje ich nieefektywność, gdyż często zdarza się, że ich działania się nakładają, wielokrotnie działania według staropolskiego powiedzenia: „nie wie lewica, co robi prawica" mogą stać się nieświadomie przedmiotem gry politycznej lub szpiegowskiej.

Innym rodzajem zagrożeń istniejącym w telekomunikacji jest zjawisko **cyberprzemocy**, które jest tylko jedną z form **cyberprzestępczości**. Przestępcy do swego procederu wykorzystują Internet i telefony komórkowe, na przykład ok. 70% polskich nastolatków posiada własny profil na portalach internetowych. Najpoważniejsze przestępstwa skierowane do dzieci to próby szantażu, zastraszania, wcielanie się w inną osobę (tzw. podszywanie się), publikowanie lub rozsyłanie ośmieszających i obrażających zdjęć, filmów itp. Najbardziej na te formę przemocy narażeni są najmniej doświadczeni internauci i użytkownicy telefonów komórkowych.

Zagrożenia i bezpieczeństwo w Internecie dzieci i młodzieży. W ostatniej dekadzie na świecie i w Polsce rozpowszechniło się zjawisko nazwane sekstingiem (ang. sex i texting, esemesowanie), czyli przesyłanie roznegliżowanych, erotycznych zdjęć drogą elektroniczną[10]. Dane są niepokojące, gdyż nawet co piąty nastolatek – najmłodsi mieli 8-10 lat – rozsyła swoje nagie zdjęcia przez telefon lub Internet. Młodzi ludzie jako przyczynę swego zachowania podają m.in. „nikt mnie nawet nie dotknął, od tego, że patrzy, niczego mi nie ubędzie". Niektórzy handlują swymi zdjęciami za pieniądze, za doładowanie telefonu itp., nie zdają sobie sprawy z ewentualnych konsekwencji prawnych, a przede wszystkim moralnych. Owe fotografie mogą w przyszłości stać się doskonałym narzędziem szantażu lub zniszczyć ich życie.

Niewątpliwie Internet może być i jest wspaniałym narzędziem edukacji. Dzieci i młodzież w wieku od dziewięciu do szesnastu lat w 81% wykorzystują go do nauki szkolnej. Umożliwia dostęp do szerokiego spektrum wiedzy, chociaż co do jej poziomu można mieć pewne zastrzeżenia, Wikipedia uczciwie informuje o tym, aby jej treści nie traktować jako pewnych. Wyrównuje poziom wiedzy wsi i miast oraz krajów mniej i bardziej rozwiniętych. Internet dla ok. 60% jest komunikatorem, a dla ok. 40% jest miejscem publikacji swych dzieł. Mimo to rośnie zaniepokojenie rodziców, badaczy problemem uzależnienia dzieci od Internetu oraz podobieństwa tego zjawiska do uzależnienia nikotynowego

[9] W czasach prezydentury Ronalda Reagana amerykańska agencja CIA wymknęła się spod społecznej kontroli, prowadząc własną politykę w stosunku do Afganistanu, a przede wszystkim do Contras, którym nielegalnie dostarczała broń. Dopiero specjalna komisja Kongresu wyjaśniła sprawę, winnych ukarała, a CIA odebrała wiele prerogatyw.

[10] Bardzo ciekawy i wnikliwy artykuł na ten temat zamieściła red. Agata Grabau: *Seksting, nastoletnia pornografia*, (w:) „Przegląd Tygodniowy" nr 10 (636) z 11.03.2012, s. 18-22.

i alkoholowego czy narkotycznego. Dla ok. 74% dzieci z grupy od dziewięciu do szesnastu lat Internet to gry, a dla ok. 80% to możliwość oglądania filmów i klipów[11]. Ponadto ok. 38% dzieci publikuje i dzieli się zdjęciami, czasami pornograficznymi, ulegając zjawisku sekstingu, pewna część uległa bloomingowi, czyli uwiedzeniu.

Przeprowadzone przez Unię w ramach programu EU Kids Online badania zagrożeń, jakie niesie ze sobą Internet dla dzieci, wskazują na wiele niepokojących zjawisk[12]. W październiku w ramach programu EU Kids Online opublikowano raport o zagrożeniach i bezpieczeństwie w Internecie dzieci w Europie. W Polsce badaniami takimi kierowała dr Lucyna Kirwil z Wyższej Szkoły Psychologii Społecznej w Warszawie. Celem projektu EU Kids Online jest: „poszerzenie wiedzy o doświadczeniach i zwyczajach dzieci i rodziców w zakresie bezpiecznego korzystania z Internetu i nowych technologii w sieci oraz przekazanie informacji do wykorzystania w promocji środowiska bezpiecznego Internetu dla dzieci"[13].

Wyniki tych badań pokazały, że w populacji polskich dzieci w wieku od 9 do 16 lat co czwarte dziecko kontaktuje się z nieznajomymi online, prawie co siódme dziecko widziało w Internecie materiały związane z seksem, co dziesiąte dziecko przeżywało negatywne emocje (niepokój lub przykrość), korzystając z Internetu, prawie co dwunaste dziecko spotkało się twarzą w twarz z nieznajomym poznanym w Internecie, co siedemnaste dziecko było ofiarą cyberagresji (było napastowane w Internecie).

Ponadto: prawie co czwarte dziecko w wieku 11-16 lat miało w Internecie kontakt z treściami, które mogą szkodzić jego kształtującemu się systemowi wartości, prawie co siódme dziecko w wieku 11-16 lat otrzymało w Internecie wiadomości o podtekście seksualnym[14]. Badania owych zagrożeń Internetu i środków służących bezpieczeństwu będą kontynuowane, gdyż zjawisko to jest dynamiczne i ulega ciągłym przemianom.

Współczesne formy przestępczości komputerowej/cyberprzestępczości pojawiły się wraz z rozwojem komputeryzacji oraz telefonów komórkowych i od tej pory towarzyszą im nieustannie. Funkcjonuje bardzo dużo definicji przestępczości komputerowej. W szerokim rozumieniu przestępczość komputerowa obejmuje wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych. Należy zaznaczyć, iż będą to zarówno czyny popełniane przy użyciu elektronicznych systemów przetwarzania danych (komputer jako narzędzie do popełnienia przestępstwa), jak

[11] L. Kirwil, *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo – część 2. Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców*, Warszawa 2011: SWPS-EU.

[12] Idem, *Raport o wynikach badań europejskich i polskich dzieci*, na www. Eukidsonline.net, s. 47.

[13] Ibidem.

[14] Ibidem, s. 44.

i skierowane przeciwko takiemu systemowi. W dobie elektronizacji, a dziś w epoce cyfrowej, niewątpliwie zjawisko piractwa istnieje. Jest obecnie coraz trudniej definiowalne, ponieważ jest w sposób naturalny bardzo dynamiczne i jak żadne do tej pory globalne. Ponadto określenie owego zjawiska utrudniają sami użytkownicy sieci, np. ich wiek (od trzylatków do stulatków), wykształcenie, w tym wiedza informatyczna (od „naciskaczy klawiatury", przez programistów do najwybitniejszych hakerów), poziom zamożności (od biedoty indyjskiej czy afrykańskiej do multimilionerów).

Carne Ross w swej książce *Rewolucja bez liderów* uważa, że internauci, jako społeczeństwo sieciowe, nie potrzebują żadnych odgórnych regulacji, są w stanie sami się kontrolować, jakość swych działań, dzięki temu budować zaufanie do siebie i swoich produktów[15]. Moim zdaniem stwierdzenie takie jest mocno życzeniowe, gdyby tak było, cyberświat byłby piękniejszy. Jednak rzeczywistość w tym względzie bardzo się różni od oczekiwań. Tymczasem cyberprzestrzeń, w tym sieć, jest pełna patologii, cyberprzestępstw, kłamstwa, wulgaryzmów. Dwa najważniejsze w wymiarze globalnym portale społecznościowe są wypełnione zjawiskami typu infekowanie swych użytkowników złośliwym kodami, np. ok. 73% Facebook i 41% Twitter, naruszenie prywatności – 73% Facebook i 51% Twitter. Pewną prawną próbą eliminowania tych zjawisk ma być ACTA, ale w obecnym kształcie – znacznie ograniczająca wolność i wprowadzająca cenzurę – nie ma szans na powszechną akceptację.

ACTA jako ochrona własności intelektualnej i praw autorskich a bezpieczeństwo użytkownika sieci, jego prawo do wolności i rozwoju

ACTA to według wielu restrykcyjne międzynarodowe prawo, mające chronić prawa autorskie i patentowe. Szczególnie USA, Japonii, Korei[16]. Prace nad umową chroniącą prawa autorskie i patentowe rozpoczęły się w USA pod koniec lat dziewięćdziesiątych, a przy jej powstawaniu pracowały amerykańskie stowarzyszenie PhRMA reprezentujące przemysł farmaceutyczny i MPAA skupiające branżę filmową.

---

[15] Carne Ross, *The Leaderless Revolution: How ordinary people will take power and change politics in the 21st century* – wolne tłumaczenie autora tej publikacji.

[16] Stany Zjednoczone u swego zarania zadbały o ochronę praw własności w Konstytucji USA, ale tylko własnych obywateli, natomiast szeroko kopiowały dzieła zagranicznych twórców dzieł literackich, szeroko bezprawnie wykorzystywali nowe techniki i technologie oraz stosowali nieuczciwy drenaż mózgów, by stać się w ten sposób się potęgą gospodarczą i kulturalną. Obecnie prawo własności w USA regulują ustawy SOPA i PIPA, ACTA ma być międzynarodowym narzędziem chroniącym interesy amerykańskie. Japonia dopiero w latach sześćdziesiątych, kiedy jej myśl techniczna, dzięki kopiowaniu/piractwu stała się konkurencyjna, rozpoczęła proces ochrony patentowej, który zakończyła całkowicie dopiero w latach siedemdziesiątych. Obecnie zarówno USA i Japonia chcą przewodzić w międzynarodowym prawodawstwie ochrony własności intelektualnej, pytanie brzmi: czy mają do tego moralne prawo? Amerykanie zastosowali swą XIX-wieczną, liberalną maksymę (w dowolnej interpretacji): „Pierwszy milion ukradnij, a później możesz zarabiać legalnie".

Bill Clinton podpisał dokument, złośliwie zwany „aktem Myszki Miki", w 1998 roku. Gwarantuje on, że np. wspomniana Myszka jest wyłączną własnością Disney Company do 2023 roku, mimo że obecnie poza amerykańskim pomysłem Myszki, cała reszta jest azjatycka, filmy z Hongkongu, gadżety z Chin itp.

Należy przyznać, że istnieje poważny problem piractwa patentowego i własności autorskiej, ale obrona tych praw nie może odbywać się kosztem słabszych. W przypadku ACTA jest ona postrzegana jako jeden ze sposobów ratowania amerykańskiej gospodarki i prestiżu światowego lidera innowacyjności. W przyszłości restrykcyjne stosowanie ACTA będzie skutkowało monopolem, a ten zawsze wykorzystuje się do podnoszenia cen według swych kryteriów. Zmniejszenie, a w niektórych dziedzinach zanik piractwa, przynieść by mogła właśnie liberalizacja prawa patentowego i autorskiego. Doskonale to widać na rynku farmaceutyków, gdzie często różnica między ceną oryginału a podróbki jest niewielka, ludzie wolą nie ryzykować i kupują oryginały, piractwo jest marginesem.

ACTA budzi sprzeciw, gdyż po pierwsze przyczyni się do regresu szeroko pojętej kultury masowej, w tym popkultury. Sieć internetowa stałaby się polem walki między stronami i bez możliwości dostępu do kultury. Dla milionów ludzi korzystanie z nielegalnych lub półlegalnych źródeł jest jedyną możliwością uczestnictwa w kulturze. Z innej strony są wyspecjalizowane elektroniczne organizacje „monitorujące" sieć, często o charakterze szpiegowsko-rewindykacyjnym, tzw. wywiadownie, mające reprezentować szeroko pojętych posiadaczy praw autorskich. Należy zaznaczyć, iż tylko ponad połowa twórców jest właścicielami swych praw, pozostałe wykupili biznesmeni oraz kompanie medialne i gospodarcze, szczególnie amerykańskie, z takich dziedzin jak np. filmy (scenariusze), gry komputerowe, które są w 80-90% własnością korporacji, a nie twórców, od których często w sposób nieuczciwy je nabyto.

Porozumienie ACTA jest – według jego fundatorów – wymierzone przeciwko wszystkim przejawom naruszania cudzej własności intelektualnej. Największe kontrowersje wzbudzają jednak przepisy dotyczące wykroczeń w środowisku cyfrowym, głównie z wykorzystaniem sieci komputerowych. Free Software Foundation i Free Knowledge Institute wyrażają opinie, że regulacje te naruszają konstytucyjną wolność słowa, ograniczają swobodny rozwój innowacyjnych rozwiązań, w tym oprogramowania typu open-source. Twierdzą one, iż prawo będzie korzystne tylko dla dużych korporacji, posiadających prawa do znanych marek, patentów czy wytworów kultury. Umowę skrytykowała organizacja Reporterzy bez Granic, a także piętnastu laureatów Nagrody Sacharowa oraz uczestnicy wielotysięcznych manifestacji.

Obecna dyskusja i batalia w ochronie własności intelektualnej w historii ludzkości nie jest niczym nowym i cyklicznie się powtarza, od swego początku (wcześniej walczono o własność literacką) miała charakter polityczny. Obecnie ów charakter kładzie się wielkim cieniem na ACTA, przyjęcie tego „porozumienia" (raczej dyktatu najbardziej rozwiniętych państw) oznacza ograniczenie, spowolnienie, a nawet regres

kulturalny i technologiczny pozostałych państw, a należy zauważyć, iż zjawisko to będzie dotyczyć ok. 75% ludzkości.

W starożytności autorzy prosili korzystających z ich wytworów o przypisywanie im autorstwa wykorzystywanych dzieł. I tak np. Andronikos w *Metafizyce* uważał, że według Arystotelesa jego dzieła pochodzą z tego świata, ten świat opisują i dla tego świata są bezwzględnie przynależne. Plometeusze, budując bibliotekę w Babilonie, budowali ją dla ludu, chętnego zgłębiać wiedzę. A że w gromadzeniu najwspanialszych dzieł ówczesnego rozumu ludzkiego wykorzystywali nie zawsze moralne metody kopiowania, to dziś rzecz inna. Starożytni mędrcy i ich następcy uważali, że ich dzieła należą do ludzkości, a studiowanie tych dzieł poczytywali sobie za satysfakcję. Wydłużenie do siedemdziesięciu lat ochrony praw autorskich to skrajna nieodpowiedzialność zarówno prawodawców jak samych autorów i ich spadkobierców. Jest to wielki błąd cywilizacyjny, który przyniesie olbrzymie wielkie straty i opóźnienia w tzw. wielkiej kulturze. Doskonale to widać np. na spuściźnie Jamesa Joyce'a. W 2011 roku minął czas „ochronny", czyli można bezpłatnie wykorzystywać jego – na swe czasy epokową – twórczość, np. *Finnegans Wake*[17]. Od wielu dziesięcioleci czekano na ten czas i co się stało? Zamiast powszechnego zainteresowania, tysięcy publikacji, inscenizacji teatralnych, mamy bardzo nikłe zainteresowanie jego wielką sztuką, która jest tylko współczesna, ale nieaktualna. Myślę, że sam Joyce tą sytuacją byłby zasmucony, nie mówiąc już o stratach, jakie odnieśli czytelnicy czy widzowie, których nie było stać na korzystanie z jego twórczości. Zjawisko wszelkiego rodzaju piractwa jest niemoralne, zarówno komputerowego jak np. podróbek produktów markowych. Powinno być różnymi sposobami zmniejszane, ale musi zaistnieć pewien konsensus. Twórcy, a w rzeczywistości wielkie kompanie medialne, powinni żądać za swe wytwory/produkty wynagrodzenia stosownie do możliwości finansowych nabywcy. Nie może być tak, że jakiś produkt ma tę samą cenę (najczęściej wyrażoną w dolarach amerykańskich) w USA, Chinach czy w Afryce. Gdzie stosownie do dochodu na statystycznego mieszkańca USA kosztuje jedną setną, w Chinach jedną dziesiątą, a w Afryce jedną trzecią. W tych realiach naturalne jest, że zarówno Chińczykowi jak Afrykańczykowi piractwo się opłaci, a nawet jest koniecznością. Działające i nowo powołane organizacje „monitorujące" Internet będą mogły prowadzić inwigilację i wprowadzać środki policyjne.

Najlepszym podsumowaniem powyższych rozważań będzie kilkanaście praktycznych rekomendacji.

[17] James Joyce w 1933 roku napisał poemat fantastyczno-groteskowy *Finnegans Wake*, który do obecnej chwili nie został w pełni odczytany. Na świecie kilku pasjonatów próbuje (mają swobodny dostęp, gdyż okres ochronny minął) go odczytać, publikacje tych prób spotkają się ze znikomym zainteresowaniem, m.in. z tego powodu, że każdy twórca i każde dzieło ma swój czas. Czas, kiedy jest adekwatne czasom i te czasy kształtuje, później jest piękną, ale historią.

Wnioski:

* Niewątpliwie istotne i ważne wartości techniczne, ekonomiczne, polityczne i wszelkie inne nowoczesnych środków komunikacji muszą być podporządkowane dobru człowieka.
* Tworzenie i wykorzystywane cyberprzestrzeni musi wynikać z podstawowych wartości aksjologii antropologicznej, tj. szacunku dla życia, wolności pokoju i rozwoju.
* Bezpieczeństwo człowieka, korzystającego z cyberprzestrzeni, musi mieć priorytet, nawet kosztem wielu ograniczeń i spowolnienia postępu technicznego.
* Zjawisko whistleblowingu zamiast być tępione, powinno być wykorzystywane, jako jedno z narzędzi monitoringu instytucji, do jej doskonalenia.
* Każdy pracownik powinien mieć możliwość w sposób bezpieczny, a jeżeli to konieczne poufny poinformować o nielegalnych i nieetycznych praktykach wewnątrz instytucji, dobrym rozwiązaniem mogą być tzw. linie ds. etyki.
* Na wszystkich pracodawcach powinien ciążyć obowiązek permanentnej edukacji w zakresie zachowań pracowników zgodnych z zasadami etycznymi, aby znali i chcieli przestrzegać zasad „etycznej firmy".
* Internet niewątpliwie jest ważnym narzędziem, które umożliwia nastolatkom poszerzenie wiedzy szkolnej, kontaktów, a nawet publikowanie swych wytworów, rozwija umiejętności kontaktów i wymiany myśli.
* Rośnie uzależnienie dzieci od Internetu, zjawisko to wymaga przemyślanego przeciwdziałania rodziców, szkoły i specjalistów.
* Istnieje pilna potrzeba podnoszenia poziomu świadomości dzieci, ale przede wszystkim rodziców w zakresie zagrożeń, jakie niesie ze sobą Internet.
* Może najważniejsza uwaga: „do efektywnego, nawet najlepszego programu należy dodać: 1) ochronę i pomoc świadomie udzielane przez rodziców, 2) umiejętne korzystanie z Internetu przez dziecko ze świadomością, że: Internet to więcej niż zabawa. To moje życie"[18].
* Przyjęcie ACTA w obecnej wersji umożliwi w imieniu prawa działanie – nie zawsze moralne, np. szpiegowskie, różnym organizacjom „monitorującym" Internet.
* Zjawisko wszelkiego piractwa powinno być zmniejszane, ale musi zaistnieć istotny konsensus, twórcy powinni żądać za swe dzieła wynagrodzenia stosownie do możliwości finansowych nabywcy.
* Żaden internauta lub nadawca nie będzie mógł się czuć bezpiecznie i komfortowo, gdyż instytucje powołane przez ACTA mają prawo działać nawet prewencyjnie i prowadzić działania niekoniecznie moralne, np. prowokację[19].

[18] L. Kirwil, *Raport o wynikach badań europejskich i polskich dzieci*, op. cit., s. 47.

[19] Jeżeli ktoś włamie się na naszą stronę lub portal operatora, to w naszym interesie będzie, aby to udowodnić. Pomoże to uniknąć wszelkich problemów związanych z dochodzeniem (może nawet

LITERATURA:

1. P. Aftal, *Internet a dzieci: uzależnienia i inne niebezpieczeństwa*, przeł. B. Nicewicz, Pruszyński i S-ka, Warszawa 2003.
2. R. Carne, *The Leaderless Revolution: How ordinary people will take power and change politics in the 21st century,* published in the UK by Simon & Schuster, 2011, and in the US by Blue Rider.
3. M. Castells, *Galaktyka Internetu. Refleksje nad internetowym biznesem i społeczeństwem*, Poznań 2003.
4. M. Goliński, *Polska jako społeczeństwo informacyjne – ocena infrastruktury technicznej*, (w:) *Rozwój społeczeństwa informacyjnego – teoria i praktyka*, t. 1, Wyd. AGH, Kraków 2003.
5. A. Grzywak, *Internet w społeczeństwie informacyjnym*, wyd. WSB. Dąbrowa Górnicza 2003.
6. A.J. Kennedy, *Internet*, Optimums Pascal S.A., wyd. I, 1999.
7. K. Krzysztofek, M.S. Szczepański, *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2002.
8. L. Kirwil, *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo* – część 2. Częściowy raport z badań EU Kids Online. II przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców, SWPS–EU, Warszawa 2011.
9. M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Wyd. Polski Instytut Spraw Międzynarodowych, Warszawa 2009, Aneks. *Konwencja o cyberprzestępczości.*
10. M. Ossowska, *Normy moralne, Próba systematyzacji*, wyd. III, PWN, Warszawa 1985.
11. K. Paradowski, *Internet – korzyści i zagrożenia*, Wyd. Centrum Edukacji Społeczeństwa, Warszawa 2000.
12. Praca zbiorowa pod redakcją Andrzeja Janowskiego i Ireny Namysłowskiej, *Bez niedomówień do rodziców. O problemach dzieciństwa i dorastania*, Instytut Psychiatrii i Neurologii i ELMA BOOKS, Warszawa 1998.
13. B. Siemieniecki, W. Lewandowski, *Internet w szkole*, Wydawnictwo Adam Marszałek, Toruń 1998, Wydanie II.
14. B. Szmajdziński, *Syndrom uzależnienia od Internetu*, wydawnictwo Studio-Impuls, Warszawa 2007.
15. R. Rosa, *Filozofia bezpieczeństwa*, wyd. Bellona, Warszawa 1997.
16. R. Tadeusiewicz, *Społeczność Internetu*, Wyd. Exit, Warszawa 2003.

międzynarodowym – można być deportowanym), ewentualnymi zarzutami, umorzeniem lub karą.

The anthropological aspects of informational security and users of contemporary means of communication. Part II

Abstract. This article continues the divagations raised by me in my previous article: *Anthropological aspect of informational security and users of contemporary means of communication*. In the first part, the basic concepts of informatics, communications and modern telecommunications were defined. In the recommendations described by me, pertaining to problems of cybercrime, I've explained what are the possible countermeasures diminishing the threats. In a second part I focus on the current themes, such as: children's safety in the internet and ACTA agreement. This of course does not include all the issues raised in the article. Hence, I also direct my attention to the direction of the evolution of cyberspace, especially when it comes to telephone and internet developments.