# ANTROPOLOGICZNY ASPEKT BEZPIECZEŃSTWA INFORMACYJNEGO UŻYTKOWNIKÓW NOWOCZESNYCH ŚRODKÓW KOMUNIKACJI. CZ. I

**Stanisław W. Ptaszek**

Wojskowa Akademia Techniczna

**Streszczenie.** Według Arystotelesa podstawą przetrwania i rozwoju jednostki jest wspólnota, która wymaga komunikacji, pierwotnie tylko werbalnej, a dziś multimedialnej. Zatem podstawowy askpekt ludzkiego bezpieczeństwa koresponduje bezpośrednio z ludzką umiejętnością porozumiewania się. W historii rozwoju cywilizacji człowieka przemiana sposobu komunikowania się przeszła różnego rodzaju przemiany, od form prostych do bardziej złożonych i wielowymiarowego systemu dominującego obecnie. Artykuł wskazuje na antropologiczny aspekt zabezpieczenia owej komunikacji przed podstawowymi zagrożeniami. Prezentuje podstawowe pojęcia z tego zakresu, takie jak społeczeństwo i bezpieczeństwo teleinformacyjne, oraz określa formy cyberprzestępczości. W rekomendacjach wyjaśnia cyberprzestępczość, ale też daje wskazówki, jak owym zagrożeniom przeciwdziałać. Ponieważ kultura ludzka ciągle ewoluuje, najbardziej adekwatnym opisem, który połączy elementy uniwersalne z przemianami partykularnymi, wydaje się być analiza filozoficzna.

Potrzeba bezpieczeństwa i poczucie jej spełnienia zarówno w wymiarze jednostkowym i jak gatunkowym należą do podstawowych potrzeb człowieka. Jednak obserwacje przeprowadzone zarówno wśród internautów jak i innych użytkowników nowoczesnych środków komunikacji wskazują na zjawisko niepokojące.

Stajemy się – często mimo woli – członkami społeczeństwa informacyjnego. Samo określenie na początku swego powstania – ukute już w latach 70. XX wieku przez przedstawicieli Klubu Rzymskiego – używane było przede wszystkim jako kategoria socjologiczna. Pełniejszy wymiar zyskało w USA w latach 80., a w Europie w latach 90. XX wieku. W tym czasie za przyczyną gwałtownego rozwoju technik informatycznych nabrało ono znaczenia cywilizacyjnego. Wielowymiarowość zjawiska i polityki bezpieczeństwa, w tym teleinformatycznego, państw dobrze ukazuje strategia cyberprzestrzeni USA, według której można wyróżnić pięć poziomów jej realizacji: poziom użytkowników indywidualnych (których w Stanach szacuje się na ok. 150 mln), poziom podmiotów gospodarczych, poziom państwowy i poziom

międzynarodowy[1]. Najbardziej interesujący poziom to poziom indywidualnych użytkowników, których nie sposób wyizolować od pozostałych, a jednocześnie stanowią ważną część tego systemu.

W najbliższej przyszłości rozszerzy się zakres np. *e-governmentu*, co zobliguje obywateli do uczestnictwa życiu politycznym, społecznym i administracyjnym poprzez korzystanie z nowoczesnych technik informacyjno-komunikacyjnych, np. wszelkie wybory, sprawy administracyjne i finansowe. Uczestnicząc w życiu Unii, korzystać będziemy z powstałego w 2001 roku programu e-Europa, który niesie wiele możliwości informacyjnych i udogodnień administracyjnych. Należy także wspomnieć jeszcze o bardzo dynamicznie rozwijającym się handlu internetowym i usługach w e-Biznes czy e-Bank. Coraz więcej uczelni wprowadza jako formę uzupełniania wiedzy program e-Uczelnia, obligując studentów do interaktywnego uczestnictwa w wykładach, seminariach i życiu akademickim. Natomiast nauczaniem na odległość zajmuje się e-learning, e-educations, specjalistyczne programy wykorzystujące internet, intranet, extranet, łączność satelitarną, interaktywne media. Zaletą jest, iż uczący się ma możliwość indywidualnego wpływu na materiał, tempo i jakość wiedzy, a rolą nauczyciela jest wskazywać kierunki, zakres i kontrolować postępy w nauczaniu.

Ze względu na zakres, wielowymiarowość i dynamikę problemu poniższe opracowanie muszę zawęzić do użytkowników komputerów, internetu, w tym bankowości, handlu, ogłoszeń, portali społecznościowych i innych nowoczesnych środków łączności, np. telefonii satelitarnej, iPodów czy iPhonów[2].

Jednak owe środki poza olbrzymi możliwościami niosą niestety równie wiele zagrożeń, od ekonomicznych, np. oszustwa finansowe, okradanie kont, przez psychiczne, np. uzależnienia od gier, „czatów", do moralnych, np. oszustwa matrymonialne. Właśnie tymi zagrożeniami bezpieczeństwa psychicznego, prawnego czy ekonomicznego pragnę zająć się w tym artykule.

Antropologiczny aspekt bezpieczeństwa informacyjnego użytkowników nowoczesnych środków komunikacji spróbuję nakreślić poprzez:

- próbę określenia podstawowych wyzwań i zagrożeń bezpieczeństwa w wymiarze indywidualnym grożących ze strony nowoczesnych środków komunikacji,
- diagnozę stanu istniejących jak i przyszłych zagrożeń w aspekcie społecznym i politycznym,

[1] M. Madej, *Rewolucja informatyczna*, (w:) M. Madej, M. Tretlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, wyd. Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 37.

[2] Pragnę podziękować autorom książki *Bezpieczeństwo teleinformatyczne państwa*, po pierwsze za twórczą inspirację i baczniejsze zwrócenie uwagi na ten problem, po drugie za wskazanie zakresu tematu, źródeł literatury i dokumentów normujących działanie internetu w wymiarze indywidualnym i prawnym. Patrz M. Madej, M. Tretlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, wyd. Polski Instytut Spraw Międzynarodowych, Warszawa 2009.

- przybliżenie wybranych terminów i pojęć funkcjonujących w tym przedmiocie (często w ogóle niezrozumiałych),
- udzielenie ogólnych i konkretnych rad mogących przyczynić się do podniesienia poziomu bezpieczeństwa,
- próbę analizy wiktymologicznej strony zjawiska, w jaki sposób sami jako użytkownicy narażamy się na ataki i stajemy się ofiarami, niemal na własne życzenie,
- z ubolewaniem przyznam, że zjawisko „dzieci w sieci" jedynie zasygnalizuję. Nie czuję się w pełni kompetentny do dokonania głębszej analizy,
- zamieszczenie w aneksie fragmentu dokumentu najbardziej przydatnego z punktu widzenia zwykłego użytkownika – Konwencji Rady Europy o cyberprzestępczości.

Jak już wspomniałem, bez względu na naszą wolę stajemy się coraz bardziej członkami społeczeństwa informacyjnego. W literaturze przedmiotu można spotkać ponad 20 definicji **społeczeństwa informacyjnego**, jednak żadna z nich nie obejmuje całości zjawiska, myślę, że nie może go zdefiniować w całości, gdyż jest zbyt szerokie, a przy tym dynamicznie zmienne[3]. Z konieczności przedstawię definicję, która na użytek niniejszych rozważań ujmuje dużą część istoty tego zjawiska, a którą podają K. Krzysztofek i M. Szczepański: „społeczeństwo, w którym informacja jest intensywnie wykorzystywana w życiu ekonomicznym, społecznym, kulturalnym i politycznym, to społeczeństwo, które posiada bogate środki komunikacji i przetwarzania informacji, będące podstawą tworzenia większości dochodu narodowego oraz zapewniające źródło utrzymania większości ludzi…"[4]

Każdego dnia mamy do czynienia z dalszym i coraz dynamiczniejszym rozwojem społeczeństwa informacyjnego w dwu płaszczyznach; pierwsza poszerza o następne kraje i regiony globu, stąd mówimy o globalizacji sieci informatycznych i nazywamy świat „globalną wioską". Druga płaszczyzna to wymiar indywidualny, niemal każdy dzień przynosi nowe możliwości wykorzystania nowych środków informacji, które coraz bardziej stają się nieodzowne zarówno w życiu zawodowym jak rodzinnym i indywidualnym.

Inne definicje zwracają uwagę na konkurencyjność zarówno w przemyśle, jak i w usługach lub możliwość zwykłych kontaktów rodzinnych i przyjacielskich. Ponieważ corocznie relatywnie tanieją i stają się coraz dostępniejsze, to dla wielkiej diaspory chińskiej czy indyjskiej stanowią wielkie udogodnienie i możliwości kontaktów rodzinnych i biznesowych.

Dla Unii Europejskiej społeczeństwo informatyczne „to strategia rozwoju poszczególnych gospodarek narodowych, która może zlikwidować konsekwencje

[3] Jerzy S. Nowak w *Społęczeństwie informacyjnym – geneza i definicje*: www.silesia.org.pl/Nowak_Jerzy_Społeczeństwo prezentuje 22 definicje społeczeństwa informacyjnego.

[4] Wg K. Krzysztofek, M.S. Szczepański, *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2002, s. 170.

zapóźnienia ekonomicznego tych gospodarek i całej Europy w stosunku do Stanów Zjednoczonych i Azji"[5]. Główne zasady odnoszące się do społeczeństwa informacyjnego: powszechny dostęp wszystkich ludzi do podstawowego zakresu techniki komunikacyjnej i informacyjnej, otwarta sieć, czyli nieskrępowany dostęp do sieci wszystkich operatorów i usługodawców, zdolność wzajemnego łączenia się i przetwarzania danych, kompatybilność i zdolność współpracy wszelkiej techniki umożliwiająca pełny kontakt bez względu na miejsce przepływu, są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i w usługach[6]. Jedno z pierwszych opracowań Komitetu Badań Naukowych dla Rady Ministrów z 2000 roku określało „społeczeństwo informatyczne jako ogół ludzi, mających powszechne i łatwe możliwości komunikowania się oraz dostęp do potrzebnych im informacji, poprawiających warunki życia, wykonywania pracy oraz wypełniania powinności obywatelskich[7]. Swoją definicję Społeczeństwa Informacyjnego podaje polski Urząd Komitetu Integracji Europejskiej. Wg UKIE Społeczeństwo Informacyjne to nowy typ społeczeństwa, który ukształtował się w krajach, w których rozwój nowoczesnych technologii teleinformatycznych osiągnął bardzo szybkie tempo. Podstawowymi warunkami, które muszą być spełnione, aby społeczeństwo można było uznać za informacyjne, jest rozbudowana nowoczesna sieć telekomunikacyjna, która swoim zasięgiem obejmowałaby wszystkich obywateli oraz rozbudowane zasoby informacyjne dostępne publicznie. Ważnym aspektem jest również kształcenie społeczeństwa w kierunku dalszego rozwoju, tak by wszyscy mogli w pełni wykorzystywać możliwości, jakie dają środki masowej komunikacji i informacji.

Cele społeczeństwa informacyjnego wg UKIE to: internet jako środek komunikacji obywatelskiej i informacji publicznej, powszechny dostęp do informacji, edukacja[8].

Internet to doskonałe narzędzie, jest stosunkowo nowym zjawiskiem, ludzie dopiero zaczynają zdawać sobie sprawę, w jaki sposób może poprawić ich życie. Niestety wielu internautów pozostaje w błogiej nieświadomości potencjalnych zagrożeń. W ciągu ostatnich 10-15 lat obserwuje się bardzo dynamiczny rozwój, od witryn informacyjnych, przez portale społecznościowe, do e-Bankowości, od stosunkowo prostych dwuwymiarowych gier, do interaktywnych trójwymiarowych gier i e-mailowych widokonferencji dostępnych na całym świecie w rzeczywistym czasie.

---

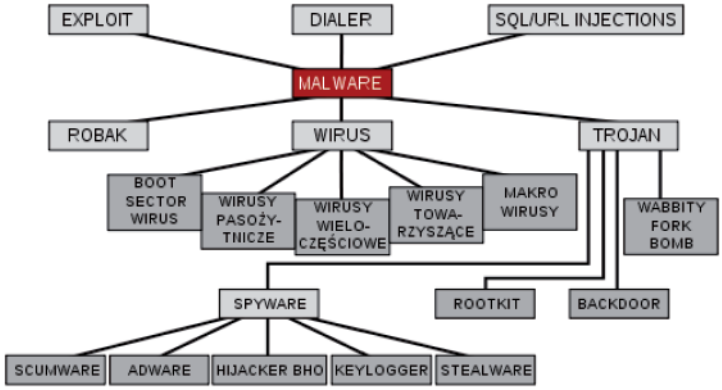
[5] Program eEuropa+ powstał jako narzędzie przyspieszenia reform i modernizacji gospodarek krajów Unii Europejskiej.

[6] J. Nowak, *Społeczeństwo informatyczne*, Rozdz. II. *Definicje podstawowe*, s. 23-24.

[7] M. Madej, M. Trelikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, wyd. Polski Instytut Spraw Międzynarodowych, Warszawa 2009, s. 163.

[8] Szerzej na stronach internetowych UKIE i KBN i Rady Ministrów, można znaleźć tam strategię, propozycje i rozwiązania dotyczące informatycznej integracji Polski ze światem. Jednak bardziej dokładne badania tematu wychodzą poza zainteresowanie niniejszego opracowania.

Rola **bezpieczeństwa informacyjnego** wiąże się głównie z szybko rosnącym znaczeniem informacji jako takiej. Nigdy w historii ludzkości informacje często na pozór bez znaczenia nie miały tak dużego wpływu nawet na miliardy ludzi. Szczególnie widoczne i spektakularne jest ich znaczenie ekonomiczne, informacja może być przyczyną powstania nieuczciwych fortun prywatnych lub państwowych, a w wymiarze państwowym nieść zagrożenie obronności, może wpływać na polityczne procesy decyzyjne, zmieniać i kształtować – czasem nimi manipulując – zjawiska społeczne, w wymiarze jednostki może prowadzić do autokracji lub destrukcji. Bezpieczeństwo informacyjne polega na zapewnieniu nienaruszalności podstawowych praw człowieka, jak wolność, prywatność, rozwój czy tolerancja poglądów i zachowań. Tak więc wszyscy uczestnicy społeczeństwa informacyjnego powinni postrzegać bezpieczeństwo jako priorytet, nawet kosztem spowolnienia postępu technicznego. Powinna istnieć tu zasada prymatu moralności nad polityką, ekonomią, a zwłaszcza techniką i jej postępem. Problem w zapewnieniu bezpieczeństwa teleinformacyjnego obywateli polega również na tym, iż ingerencja państwa wiąże się z groźbą naruszenia praw człowieka, w tym do prywatności.




Obecnie co trzeci Polak regularnie korzysta z sieci i dobrze sobie radzi, najczęściej są osoby studiujące lub mające średnie i wyższe wykształcenie oraz średni lub wyższy poziom zarobków. Jednak istnieje grupa ludzi niedostosowanych do wymogów społeczeństwa informacyjnego, którzy są pozbawieni (czasami z własnej woli lub braku możliwości edukacji) szans na zdobywanie wiedzy czy pracy drogą internetową. Wirtualna Polska podaje, że posiada 789 540 blogów, a Onet 1 575 020 blogów, na których Polacy intensywnie wymieniają swe poglądy społeczne i polityczne, każdy uczestnik życia samorządowego czy państwowego posiada swój blog[9]. Dzisiejsi rodzice często nie posiadają wystarczających kompetencji,

[9] Dane na dzień 12.11.2010, szczegóły na stronach poszczególnych portali.

aby edukować swoje dzieci na temat bezpieczeństwa w sieci, ponieważ sami nie do końca są świadomi mocy tej technologii. Współczesne dzieci (ok. 60%) wiedzą, jak obejść rodzicielskie blokady, potrafią korzystać z najnowszych technologii. Zwykle jednak niewiele wiedzą o zagrożeniach, które on niesie. Dzisiejsza przestępczość, nie ta prymitywna, lecz inteligentna (najczęściej wywodząca się ze środowiska informatycznego lub pracująca na jego potrzeby), skoncentrowała się na tym nowym, a jednocześnie bardzo atrakcyjnym sposobie ludzkiej komunikacji, dostrzegając w nim potężne źródło dochodu.

## Podstawowe pojęcia internetu i cyberprzestępczości

**System informatyczny** oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie ze wspólnym programem, wykonuje automatyczne przetwarzanie danych[10]. **Dane informatyczne** oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny[11].

Jednym z najbardziej znanych pojęć jest **haker**. Pojawiło się ono w Stanach Zjednoczonych (jak zdecydowana większość wszystkich terminów) w latach 80. XX wieku[12]. Haker pierwotnie był utożsamiany z osobą o dużej wiedzy informatycznej, która dzięki niej jest w stanie złamać lub obejść zabezpieczenia elektronicznego systemu komputerowego swej „ofiary". Tak zwane pierwsze pokolenie hakerów rzadko miało złe zamiary, motywem było doskonalenie i chęć zaistnienia w grupie, do dziś takie ataki się zdarzają, włamują się do systemu i pozostawiają tam wiadomość, nie czyniąc żadnych szkód. Hakerzy – według Wikipedii – odznaczają się bardzo dobrą orientacją w Internecie, znajomością wielu języków programowania, a także świetną znajomością systemów operacyjnych, w tym zwłaszcza z rodziny Unix (GNU/Linux, BSD itp.). Pomimo że międzynarodowe środowisko hakerów stara się dbać o swój etos i nie uprawiać cyberprzestępczości, to jednak zdarzają się wśród nich hakerzy wandale i frustraci. Inny rodzaj hakerów to **krakerzy**, którzy z osobistych pobudek atakują system i świadomie czynią w nim szkody. Jako **script-kiddies** określani są hakerzy, którzy nie posiadają dużej wiedzy, a do włamań wykorzystują gotowe – często dostępne w internecie – narzędzia. Najczęstszym motywem ich działania jest chęć dołączenia do elity hakerów. **Zombie** to komputer działający w sieci, na którym założono bez wiedzy użytkownika oprogramowanie umożliwiające kontrolę nad

[10] Ibidem, s. 223.

[11] Ibidem.

[12] Do ok. 2003-2005 roku co druki internauta na świecie był Amerykaninem, zjawisko to w sposób naturalny generowało różnego rodzaju formy aktywności, w tym też przestępczej lub nie do końca legalnej.

owym komputerem przez osobę z zewnątrz, co naraża go na utratę danych, a nawet wykorzystanie go wbrew woli użytkownika. Termin **bonet** odnosi się natomiast do grupy komputerów (zombie) połączonych siecią, a sterowanych z zewnątrz bez wiedzy ich użytkowników. Zjawisko **haktywizmu** „związane jest z powstaniem i upowszechnieniem portali społecznościowych, na których miliony ludzi głosi poglądy religijne, polityczne i ideologiczne". Haktywizm powstał jako forma protestu i nieposłuszeństwa obywatelskiego, jako informatyczna forma kontestacji rzeczywistości, był i jest dość skuteczną bronią pacyfistów, ekologów i ruchów niezależnych. Na atakowanych stronach www umieszczano własne komunikaty bądź je podmieniano, nie czyniąc szkód, a jedynym motywem była chęć dotarcia do jak największej liczby odbiorców i zmiana opinii społecznej lub stanu rzeczy, np. ataki na kompanie odpowiedzialne za skażenie środowiska itp. Dzisiejszy haktywizm przyjął formę walki politycznej prowadzonej za pomocą elektroniki przez indywidualnych zwolenników określonych idei, partii czy ruchów. **Cyberteroryzm** zmierza w sposób świadomy do zakłócenia lub eliminacji atakowanego systemu informatycznego, poprzez atak na sieć internetową państwa, instytucji państwowej, kompanii czy banku, co stanowi poważne zagrożenie w wymiarze społecznym i jednostkowym. Z internetu korzystają np. instytucje ratownictwa zdrowotnego, pożarowego, wodnego, ale też banki i inne instytucje finansowe. Oczywiście rządy, banki centralne, wojsko, policja i sądownictwo dysponują podwójnymi sposobami łączności, a ich zabezpieczenia są na najwyższym poziomie. W internecie są dostępne programy, tzw. **exploit**, tworzone w celu wykrywania słabych miejsc i luk w programie aplikacji, co pozwala na uzyskanie nielegalnego dostępu do danej aplikacji, a nawet całego komputera, a to w konsekwencji naraża komputer na paraliż i jego ciągłą infiltrację.

**Koń trojański**, **malware** lub **malicious software** to pojęcia dość znane użytkownikom, wszystkie stanowią zbliżone formy tzw. złośliwego oprogramowania.

CERT Polska dzieli zagrożenia na następujące grupy: złośliwe oprogramowanie (malware, adware, trojany, dialery), gromadzenie informacji (skanowanie, podsłuch, inżynieria społeczna), próby włamań (wykorzystywanie znanych luk systemowych, próby nielegalnego logowania), włamania (na konto zwykłe, uprzywilejowane do aplikacji), atak na dostępność zasobów (sabotaż komputerowy), atak na bezpieczeństwo informacji (nieuprawniony dostęp, nieuprawniona zmiana), oszustwa komputerowe (kradzież tożsamości, *spofing*, *phishing*, naruszenie praw autorskich, nieuprawnione wykorzystywanie zasobów).

## Przestępczość komputerowa w wymiarze jednostkowym

Według badania OBOP z lipca 2009 roku, z negatywnymi aspektami korzystania z internetu zetknęła się ponad połowa jego użytkowników. Są to np. znalezienie w sieci nieprawdziwych informacji, bycie obiektem agresji werbalnej, ofiarą

kradzieży, oszustwa, a nawet śmierć[13]. Można zauważyć, że w czołówce najczęstszych doświadczeń są cztery różne jakościowo zjawiska. Najczęściej jest to **zagrożenie o charakterze technologicznym** – wirusy komputerowe, które mogą współwystępować z innymi sytuacjami, np. kradzieżami, niemniej te pojawiają się sporadycznie. Dalej sytuują się **nieprawdziwe informacje**, które do pewnego stopnia zbieżne są z jednym z najczęściej wskazywanych doświadczeń, czyli z oszustwem, w tej kategorii jednak użytkownicy wymieniali oszustwa raczej o charakterze handlowym, związane z zakupami dokonywanymi przez sieć.

**Problem „nadużywania" internetu**, zbyt długiego przebywania online plasuje się na trzecim miejscu – diagnozuje go u siebie blisko co czwarty internauta. Warto zauważyć, że wiele sytuacji, o które pytano, zdarza się obecnie rzadziej niż rok temu, natomiast spędzanie zbyt dużej ilości czasu w sieci to jedno z tych zjawisk, które występują równie często. Można przypuszczać, że jego powszechność nie będzie malała[14].

**Przestępczość komputerowa/cyberprzestępczość** pojawiła się wraz z rozwojem komputeryzacji i od tej pory towarzyszy mu nieustannie. Funkcjonuje bardzo dużo definicji przestępczości komputerowej. W szerokim rozumieniu przestępczość komputerowa obejmuje wszelkie zachowania przestępne 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, a także w sam komputer. Należy tu zaznaczyć, iż będą to zarówno czyny popełniane przy użyciu elektronicznych systemów przetwarzania danych (komputer jako narzędzie do popełnienia przestępstwa), jak i skierowane przeciwko takiemu systemowi.

W myśl *Kodeksu karnego* za **przestępstwa komputerowe** uważa się: oszustwa związane z wykorzystaniem komputera, fałszerstwa komputerowe, zniszczenie danych lub programów komputerowych, sabotaż komputerowy, wejście do systemu komputerowego przez osobę nieuprawnioną, podsłuch komputerowy, bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych, bezprawne kopiowanie topografii półprzewodników, modyfikacja danych lub programów komputerowych, szpiegostwo komputerowe, używanie komputera bez zezwolenia, używanie prawnie chronionego programu komputerowego bez upoważnienia[15]. W końcowej części artykułu przedstawię

[13] Badanie TNS OBOP zostało przeprowadzone metodą ankiety telefonicznej w dniach 25 września – 3 października na reprezentatywnych grupach Polaków powyżej 18 roku życia (próba podstawowa) oraz Polaków powyżej 18, opracował M. Feliksiak, Warszawa, lipiec 2009, OBOP. BS 106/2009.

[14] Ibidem, s. 3.

[15] A. Adamski, *Prawne aspekty nadużyć popełnionych z wykorzystaniem nowoczesnych technologii przetwarzania informacji*, Materiały z konferencji naukowej, Poznań, 20-22 IV 1994, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 1994.

fragment europejskiej *Konwencji o cyberprzestępczości*, która umożliwia walkę z cyberprzestępczością w wymiarze międzynarodowym, co podnosi bezpieczeństwo obywateli Unii Europejskiej.

## Przejawy zagrożeń prywatności w internecie, formy obrony

Internet to doskonałe narzędzie do zdobywania wiedzy, poznawania świata, kontaktowania się z innymi osobami oraz zawierania znajomości, jednak najeżony jest wieloma niebezpieczeństwami. Zagrożenie prywatności, szczególnie w internecie, nie jest tajemnicą, chętnych na dane jest wielu. Od legalnie zatrudnionych specjalistów ds. marketingu, do oszustów i nadawców spamów, wszyscy chcą uzyskać jak najwięcej informacji o uczestnikach sieci. Jeżeli chodzi o osoby dorosłe, z reguły mają one świadomość, komu można, a komu nie wolno ujawniać informacji osobistych, gorzej sprawa się ma ze świadomością dzieci. Ale i dla dorosłych nie jest już to jednak takie oczywiste czy uświadamiane w trakcie pracy w sieci. Szczególnie w chwilach ekscytacji grą, słuchania i ściągania muzyki łatwo popełniają błędy.

Organizacja Privacy International opublikowała ciekawy ranking dotyczący prywatności i stopnia inwigilacji w poszczególnych krajach, w tym w Polsce – *Leading surveillance societies in the EU and the World 2007*. Polskę zaliczono do kategorii: *systemowe niepowodzenia w zapewnianiu ochrony*[16].

Paweł Górecki na stronie www.newsweek.pl pisał, że anonimowość internautów w sieci jest mitem[17]. Pojawiają się bowiem coraz bardziej wyrafinowane programy pozwalające tropić internautów, tyle że im to wcale nie przeszkadza. „Gdybym dzisiaj, a nie przed sześciu laty tworzył Facebook, w ogóle nie dbałbym o ochronę danych prywatnych. Ludzie przestali jej potrzebować" – mówił przed kilkoma tygodniami Mark Zuckerberg, założyciel popularnego serwisu społecznościowego. **Dane użytkowników – takie jak nazwisko, płeć, miejsce zamieszkania czy lista znajomych – może teraz przeglądać praktycznie każdy.** I co na to internauci? Właściwie nic. Odzywają się wprawdzie pojedyncze głosy oburzenia, ale osób logujących się codziennie do Facebooka nie ubywa. Złość szybko mija, bo prywatność wcale nie znajduje się na szczycie naszej hierarchii wartości.

**Psychologowie twierdzą, że kiedy obok prywatności kładziemy na szali inne wartości, takie jak wygoda czy szybkość dostępu do informacji, zawsze cenimy je wyżej.** „W niemal wszystkich sytuacjach, kiedy trzeba wybierać pomiędzy prywatnością a innymi wartościami, wybieramy te ostatnie. Wolimy karty kredytowe od gotówki, karty magnetyczne od kluczy, wyszukiwarki internetowe, które śledzą nasz każdy krok, od wpisywania adresów samemu" – pisze Helen Nissenbaum, badaczka

[16] www. prywatnosc.pl.

[17] Paweł Górecki, www.newsweek.pl, maj 2010.

z Uniwersytetu Nowojorskiego. Co niestety potwierdza 2010 rok, dane – milionów użytkowników portalu Facebook, bez ich wiedzy i zgody – zostały przekazane firmom zajmującym się reklamą i tworzeniem baz informacji o internautach. Źródłem były gry, m.in. „Farm Ville", „Texas Hold'em Poker" i programy losujące wróżby, a wymagające od użytkownika tzw. Facebook ID. Zważywszy że co miesiąc z ok. pół tysiąca aplikacji korzysta do 50 milionów narażonych na utratę prywatności ludzi, pomimo że Facebook zapowiedział (jedynie) ograniczenie, a nie likwidację wypływu informacji, zjawisko staje się niezwykle groźne dla całego systemu. Podważa bowiem zaufanie do systemu komunikacji, który mógłby być najwspanialszym sposobem wymiany myśli, rozrywki i nauki.

Zagrożenia przybierają wiele form, np. pewne witryny wymagają zarejestrowania w celu uzyskania pełnego dostępu. Niektóre proszą o **podanie nazwiska (lub pseudonimu) oraz adresu e-mail**, inne o podanie kompletu informacji, w tym adresu do korespondencji i numeru telefonu. Internetowe fora społecznościowe oraz komunikatory mogą żądać nawet pod groźbą zerwania współpracy przesłania profili zawierających znacznie więcej informacji osobistych, w tym zdjęć, danych o wieku, płci czy informacji o hobby czy rodzinie. Do tych informacji dostęp może mieć każdy, a w tym także czekający na taką okazję oszust. W trakcie odwiedzin witryny sieci WWW może dojść do przekierowania do strony fałszywej lub wyłudzającej dane, przygotowanej w celu uzyskiwania lub wykradania informacji osobistych. Często **przystępując do konkursów**, **gier**, szczególnie interaktywnych, zostajemy zmuszeni do zarejestrowania się w celu zdobycia nagrody. Z powodu ujawnienia swoich danych osobowych w witrynach sieci WWW możemy otrzymywać spamy i niepożądane wiadomości przez **e-mail**. Duża część tej poczty może mieć charakter marketingowy i niechcianej reklamy. Fałszywe wiadomości e-mail powodują niezamierzone wejście do witryny sieci WWW, która wygląda na znaną, jednak w rzeczywistości jest fałszywą stroną internetową. Naprawdę niebezpieczne wiadomości e-mail to tzw. **niechciany spam**, który może zawierać załączniki z wirusami niebezpieczne dla komputera. Emaile mogą być wysyłane z oprogramowaniem typu „spyware" służącym do wykradania informacji osobistych, finansowych lub haseł. Wiele witryn internetowych służących **udostępnianiu i pobieraniu gier, wiadomości czy muzyki** umożliwiających darmowe ich pobieranie jednocześnie wymaga od użytkownika udostępniania plików w swoim komputerze. W konsekwencji pozwala to hakerom oraz złodziejom tożsamości na uzyskanie dostępu do naszego komputera, ponadto pobierane pliki mogą również zawierać wirusy lub inne destrukcyjne kody. Kradzież tożsamości, a ściślej fałszerstwo tożsamości, to celowe używanie danych personalnych innej osoby, adresu zameldowania, numeru PESEL, najczęściej w celu osiągnięcia korzyści majątkowej. Kradzież tożsamości zwana jest także defraudacją tożsamości, gdyż chodzi o podszywanie się pod czyjeś dane. Komputerowa **kradzież tożsamości**, do niedawna uważana za science fiction, stała się realnym problemem w Polsce,

ok. 7% Polaków – dwukrotnie więcej niż w innych państwach europejskich – padło jego ofiarą. Równie poważne konsekwencje mogą wynikać z braku **wyrobionych nawyków oraz słabych metod zabezpieczeń**, co prawda oprogramowanie anytwirusowe, zabezpieczające komputer, jest w co trzecim komputerze, często są jednak przestarzałe i nieaktualne. Wiele ofiar hakerów przez pewien czas nie zdaje sobie sprawy, że ich dane osobowe zostały wykradzione, co zwiększa rozmiary szkód i wydłuża czas ich naprawienia po wykryciu kradzieży. Niektórzy nigdy sobie tego nie uświadamiają, a ich tożsamość będzie w cyberprzestrzeni „czekała" na wykorzystanie.

Rik Ferguson, starszy doradca ds. bezpieczeństwa w firmie Trend Micro, który prowadzi intensywne badania nad cyberprzestępczością, opracował profil ułatwiający zorientowanie się, czym są cybergangi, jak funkcjonują i dlaczego tak ważna jest ochrona prywatności użytkownika w internecie. Uważa, że „ci przestępcy nie są rewolwerowcami ani bandziorami, nie są także cyfrowymi dowcipnisiami czy dziwakami o przetłuszczonych włosach. Bardzo trudno ich rozpoznać, ponieważ większość z nich wygląda tak jak ty lub ja... Niestety, szary świat przestępczości online zbyt często pozostaje niezauważony". „Większość użytkowników po prostu nie zdaje sobie sprawy, że ich dane osobowe mają realną wartość finansową. Poszczególne informacje są sprzedawane bardzo tanio, ale cała ta działalność ma bardzo duże obroty. Często słyszałem, jak znajomi mówili: „Moje konto i tak jest puste, więc nie mam się czym przejmować". Trzeba sobie uświadomić, że kradzież tożsamości ma konsekwencje znacznie szersze niż to, co się dzieje tu i teraz. Może ona wpływać na sytuację finansową danej osoby przez całe życie. Z pewnością prawdą jest, że w przestępczość online angażuje się coraz więcej amatorów, ale prawdziwe zagrożenie stwarzają dobrze zorganizowane gangi"[18].

Zagrożenia, które czekają na internautów, obejmują zarówno zwykły spam reklamowy, który możemy znaleźć w swoich skrzynkach pocztowych, jak i bardziej wyszukane oszustwa, których celem jest **kradzież danych** dostępu do konta na portalu społecznościowym lub zainfekowanie komputera trojanem. Może to prowadzić do utraty Twoich danych lub pieniędzy, nie wspominając o narażaniu także osób z kręgu Twoich znajomych. Musisz zrozumieć, że gdy padniesz ofiarą tego przestępstwa, narażasz nie tylko siebie, ale także innych ludzi, głównie przyjaciół z portali społecznościowych. **Publikowanie zdjęć**, które nas kompromitują lub są przepełnione erotyką, może za kilka lat znacznie utrudnić nam na przykład znalezienie pracy. Pamiętajmy też, że ideą serwisów społecznościowych jest łączenie grona przyjaciół lub osób o podobnych zainteresowaniach. Liczba znajomych o niczym nie świadczy, więc nie akceptujmy każdego zaproszenia tylko dlatego, że ktoś nam je zaproponował.

[18] źródło, www.trendmicro.pl.

Jeżeli chcesz być bezpieczny w Sieci, powinieneś nie tylko przestrzegać podstawowych zasad bezpieczeństwa, lecz także uświadamiać swoich przyjaciół.

Kolejny rodzaj zagrożenia, który został stworzony z myślą o **bankowości** online, a teraz jest skierowany także przeciwko użytkownikom portali społecznościowych, to narzędzia kradnące hasła. Programy te wstrzykują swoje funkcje do przeglądarki internetowej (najczęściej celem jest Internet Explorer), aby wykraść informacje dotyczące konta, zanim zostaną one wysłane do internetu. Atak **„przy okazji"**: czasami odwiedzenie zainfekowanej strony internetowej wystarczy, aby szkodliwy program został po cichu zainstalowany na komputerze użytkownika. Jeżeli internauta nie ma oprogramowania antywirusowego, takie ataki będą nieuniknione podczas przeglądania stron internetowych, tym bardziej jeżeli korzysta on z przeglądarki zawierającej luki.

W internecie nie jesteśmy anonimowi i nawet przy wielu staraniach, korzystaniu z serwerów pośredniczących, unikaniu wysyłania maili z przypadkowych miejsc, anonimowi nie będziemy. Zawsze jest zagrożenie, że gdzieś popełniliśmy błąd. Wystarczy przecież, że założymy nowe konto w komunikatorze i nasz adres IP zostaje skojarzony z konkretnym numerem oraz mailem (który zazwyczaj jest niezbędny do rejestracji). Komuś może się wydawać, że wystarczy skorzystać z proxy lub programów typu TOR (*The Onion Router*), by anonimowo korzystać z Internetu. Nic bardziej mylnego. Po pierwsze nie zapewniają one bezpieczeństwa dla całego ruchu sieciowego, po drugie udowodniono, że istnieje szansa na zdobycie danych, które teoretycznie powinny być niewidoczne. W 2007 roku Dan Egerstad, szwedzki konsultant ds. bezpieczeństwa, udowodnił, że możliwe jest przejęcie nazw użytkowników i haseł do skrzynek pocztowych osób korzystających właśnie z programu TOR[19]. Niektórzy internauci mogą czuć się niekomfortowo, wiedząc, jak łatwo można dotrzeć do informacji o stronach internetowych, które wcześniej przeglądali w domu czy w pracy. Nie wszyscy chcą, żeby ta wiedza była udostępniana. Rozwiązaniem może być urządzenie o nazwie Stealth Surfer, które ukrywa IP komputera[20]. Na ujawnienie części danych jesteśmy skazani poprzez samo podłączenie komputera do Sieci – podanie daty logowania, preferencje użytkownika, wyniki wyszukiwania oraz wiele innych informacji, bez których nie można mówić o swobodnym poruszaniu się po internecie. Z drugiej jednak strony nie musimy pomagać wielkim korporacjom w zdobywaniu naszych danych osobowych. Nie ma potrzeby uzupełniania wszystkich pól informacyjnych podczas rejestracji w nowym portalu, co może nas i współużytkowników komputera uchronić przed cyberprzestępcami.

[19] Maciej Ziarek, www.kaspersky.pl.

[20] Gadżet podłączany jest do komputera poprzez port USB. Zastosowanie technologii Tor Network Security ukrywa adres IP komputera, do którego podłączyliśmy Stealth Surfera. Przy zakupie otrzymuje się również 4-letni abonament do serwisu Hushmail. Urządzenie działa także w środowisku MojoPac. Stealth Surfer można będzie nabyć w wersjach z 2 GB, 4 GB lub 8 GB pamięci. Cena to, odpowiednio: 179, 225 oraz 279 dolarów.

## Wnioski

- 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 takim kierunku, 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 winniśmy stosować do świata online.
- W wychowaniu dzieci stosować metody oparte na tzw. zdrowym rozsądku, 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 dzieciom.
- Problem w zapewnieniu bezpieczeństwa teleinformacyjnego obywateli polega również na tym, iż ingerencja państwa wiąże się z groźbą naruszenia praw człowieka, w tym do prywatności.
- Istniejące technologie informatyczne zapewniają dość wysoki stopień bezpieczeństwa, ale one same są bezskuteczne. Nie można ignorować tego aspektu bezpieczeństwa, który wiąże się z człowiekiem, z jego łatwowiernością, brakiem asertywności, itp.
- Żadne najdoskonalsze zabezpieczenia nie będą skuteczne, jeśli będziemy stosować kradzione programy i przestarzałe antywirusowe zabezpieczenia.

Poniższa konwencja stanowi wielki krok przede wszystkim w międzynarodowej walce z cyberprzestępczością, a w konsekwencji ma wpływ na poziom bezpieczeństwa obywateli. Dzięki ponadgranicznej współpracy zwiększają się możliwości walki z krajową przestępczością, co przekłada się na podniesienie poziomu bezpieczeństwa również w wymiarze jednostki. Przestępcy utracili w ten sposób pewność bezkarności, anonimowości, a co ważne możność ukrycia się w innym kraju. Definiuje ona podstawowe pojęcia techniczne oraz prawne, zakres kompetencji procesowych i odpowiedzialność państwa. Z konieczności prezentuję najistotniejsze fragmenty, całość dostępna min: MSZ Internetowa Baza Danych.

### KONWENCJA O CYBERPRZESTĘPCZOŚCI

Budapeszt, 23 listopada 2001 roku

Preambuła

Państwa członkowskie Rady Europy i inne Państwa Sygnatariusze niniejszej konwencji, biorąc pod uwagę, że celem Rady Europy jest osiągnięcie większej jedności

między jej członkami; uznając wartość wspierania współpracy z innymi Państwami Sygnatariuszami niniejszej konwencji;

przekonane o potrzebie prowadzenia, jako kwestii priorytetowej, wspólnej polityki kryminalnej mającej na celu ochronę społeczeństwa przed cyberprzestępczością, między innymi poprzez przyjęcie właściwych przepisów prawnych i wspieranie międzynarodowej współpracy;

pamiętając o konieczności zagwarantowania równowagi pomiędzy wdrażaniem przepisów prawnych a poszanowaniem podstawowych praw człowieka, zgodnie z Konwencją Rady Europy z 1950 roku o ochronie praw człowieka i podstawowych wolności oraz Międzynarodowym Paktem Narodów Zjednoczonych z 1966 roku o prawach obywatelskich i politycznych, jak również innymi traktatami odnoszącymi się do praw człowieka, które potwierdzają prawo każdej jednostki do posiadania własnych wolnych opinii, jak również prawo do wolności wypowiedzi, łącznie z wolnością poszukiwania, uzyskiwania i dzielenia się wszelkiego rodzaju informacjami i ideami, bez względu na granice, oraz prawo do poszanowania prywatności;

pamiętając także o prawie do ochrony danych osobowych, przewidzianym np. w Konwencji Rady Europy z 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych; mając na uwadze Konwencję Narodów Zjednoczonych z 1989 roku o prawach dziecka oraz Konwencję Międzynarodowej Organizacji Pracy z 1999 roku o najgorszych warunkach pracy dzieci;
uzgodniły co następuje:

Artykuł 1

**Definicje**

Dla celów niniejszej konwencji:

a) „system informatyczny" oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych;
b) „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny;
c) „dostawca usług" oznacza:
    i. dowolny podmiot prywatny lub publiczny, który umożliwia użytkownikom jego usług komunikowanie się za pomocą systemu informatycznego, oraz
    ii. dowolny inny podmiot, który przetwarza lub przechowuje dane informatyczne w imieniu takich usług komunikacyjnych lub użytkowników takich usług.

**Tytuł 1**

**Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów**

Artykuł 2

**Nielegalny dostęp**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym.

Artykuł 3

**Nielegalne przechwytywanie danych**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego przechwytywania za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym.

Artykuł 4

**Naruszenie integralności danych**

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych.
2. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie 1 musi skutkować poważną szkodą.

Artykuł 5

**Naruszenie integralności systemu**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowa-

dzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych.

Artykuł 6

**Niewłaściwe użycie urządzeń**

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnych i bezprawnych:
   a) produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania:
      i. urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5;
      ii. hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna, z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5; oraz
   b) posiadania jednostki wymienionej powyżej w punktach a. i. lub ii. z zamiarem wykorzystania w celu popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5. Strona może w swoim prawie wprowadzić wymóg, że odpowiedzialność karna dotyczy posiadania większej ilości takich jednostek.

***Tytuł 2***

**Przestępstwa komputerowe**

Artykuł 7

**Fałszerstwo komputerowe**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego wprowadzania, dokonywania zmian, wykasowywania lub usuwania danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to, czy są one możliwe do bezpośredniego odczytania i zrozumiałe. Strona może wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze.

Artykuł 8

**Oszustwo komputerowe**

Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego spowodowania utraty majątku przez inną osobę poprzez:

a) wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych,
b) każdą ingerencję w funkcjonowanie systemu komputerowego, z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.

Artykuł 9

**Przestępstwa związane z pornografią dziecięcą**

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego i bezprawnego:
   a) produkowania pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego;
   b) oferowania lub udostępniania pornografii dziecięcej za pomocą systemu informatycznego;
   c) rozpowszechniania lub transmitowania pornografii dziecięcej za pomocą systemu informatycznego;
   d) pozyskiwania pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby;
   e) posiadania pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych.
2. Dla celów powyższego ustępu 1 pojęcie „pornografia dziecięca" obejmuje materiał pornograficzny, który w sposób widoczny przedstawia:
   a) osobę małoletnią w trakcie czynności wyraźnie seksualnej;
   b) osobę, która wydaje się być nieletnią, w trakcie czynności wyraźnie seksualnej;
   c) realistyczny obraz przedstawiający osobę małoletnią w trakcie czynności wyraźnie seksualnej.
3. Dla celów powyższego ustępu 2, pojęcie „osoba małoletnia" obejmuje wszystkie osoby poniżej 18 roku życia. Strona może wprowadzić wymóg niższej granicy wieku, która nie może być niższa niż 16 lat.
4. Każda ze Stron może zastrzec sobie prawo niestosowania, w całości lub w części, ustępu 1.d. i e. oraz ustępu 2.b. i c.

Artykuł 10

**Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych**

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń prawa autorskiego zdefiniowanego w prawie danej Strony zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Aktu Paryskiego z dnia 24 lipca 1971 roku zmieniającego Konwencję Berneńską o ochronie dzieł literackich i artystycznych, Porozumienia w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o prawach autorskich, z wyłączeniem praw osobistych przewidzianych przez te konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego.

Artykuł 11

**Usiłowanie i pomocnictwo lub podżeganie**

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego pomocnictwa lub podżegania do popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-10 niniejszej konwencji.

Artykuł 12

**Odpowiedzialność osób prawnych**

1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla zagwarantowania poniesienia odpowiedzialności przez osoby prawne za przestępstwa określone zgodnie z niniejszą konwencją, popełnione dla ich korzyści przez dowolną osobę fizyczną, działającą samodzielnie bądź jako część organu osoby prawnej, zajmującą w niej pozycję wiodącą z uwagi na:
   a) uprawnienia do reprezentowania osoby prawnej;
   b) uprawnienia do podejmowania decyzji w imieniu osoby prawnej;
   c) uprawnienia do wykonywania kontroli w ramach osoby prawnej.

Artykuł 13

**Kary i środki**

1. Każda Strona podejmie niezbędne środki prawne lub inne, aby zagwarantować, że przestępstwa określone zgodnie z artykułami 2-11 będą karane za pomocą skutecznych, proporcjonalnych i zniechęcających sankcji, obejmujących pozbawienie wolności.
2. Każda Strona zagwarantuje, że osoby prawne ponoszące odpowiedzialność zgodnie z artykułem 12, podlegać będą skutecznym, proporcjonalnym i znie-

chęcającym sankcjom lub środkom o charakterze karnym lub innym, w tym sankcjom pieniężnym.

Artykuł 14

**Zakres przepisów procesowych**

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które są niezbędne dla ustanowienia uprawnień i procedur przewidzianych w niniejszej części dla celów prowadzenia specjalnych dochodzeń i postępowań karnych.
2. Z wyjątkiem szczególnych, odmiennych regulacji artykułu 21, każda Strona stosuje środki wymienione w ustępie 1 niniejszego artykułu do:
   a) przestępstw określonych zgodnie z artykułami 2-11 niniejszej konwencji;
   b) wszystkich innych przestępstw popełnionych przy użyciu systemu informatycznego; oraz
   c) zbierania dowodów w formie elektronicznej odnoszących się do przestępstw.

Artykuł 21

**Przechwytywanie danych dotyczących treści**

1. Każda Strona przyjmie odpowiednie środki prawne i inne, które mogą być potrzebne, w odniesieniu do grupy poważnych przestępstw, jakie zostaną określone w prawie wewnętrznym, dla nadania właściwym organom uprawnień w zakresie:
   a) gromadzenia lub rejestrowania przy pomocy środków technicznych istniejących na jej terytorium;
   b) zmuszenia dostawcy usług, aby w ramach możliwości technicznych, jakimi dysponuje:
      i. gromadził lub rejestrował przy pomocy środków technicznych istniejących na jej terytorium, lub
      ii. współpracował i udzielał pomocy właściwym organom przy gromadzeniu lub rejestrowaniu,

w czasie rzeczywistym, danych dotyczących treści konkretnych przekazów realizowanych na jej terytorium przy użyciu środków informatycznych.

Artykuł 22

**Jurysdykcja**

1. Każda Strona przyjmie środki prawne lub inne, które mogą być potrzebne dla ustanowienia swojej jurysdykcji w odniesieniu do przestępstw określonych zgodnie z artykułami 2-11 niniejszej konwencji, gdy przestępstwo popełnione jest:
   a) na jej terytorium; lub
   b) na pokładzie statku pływającego pod banderą tej Strony; lub
   c) na pokładzie samolotu zarejestrowanego na podstawie prawa tej Strony; lub

d) przez jednego z jej obywateli, jeżeli przestępstwo jest karalne według prawa miejsca jego popełnienia lub jeśli przestępstwo popełnione zostało poza jurysdykcją terytorialną jakiegokolwiek państwa.

2. Każde państwo może zastrzec sobie prawo do niestosowania lub stosowania tylko w ściśle określonych przypadkach lub warunkach, zasad jurysdykcji, o jakich mowa w ustępie 1.b.-1.d. niniejszego artykułu lub w dowolnej części tego ustępu.

Artykuł 23

**Ogólne zasady współpracy międzynarodowej**

Strony współpracują zgodnie z postanowieniami niniejszego rozdziału oraz z zastosowaniem właściwych instrumentów międzynarodowych o międzynarodowej współ-pracy w sprawach karnych, porozumień uzgodnionych na podstawie jednolitego lub wzajemnego ustawodawstwa oraz ich prawa krajowego, w sposób możliwie jak najszerszy, dla celów ścigania i prowadzenia postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi lub dla celów zbierania dowodów w postaci elektronicznej, odnoszących się do przestępstw.

Artykuł 24

**Ekstradycja**

1a. Niniejszy artykuł stosuje się do ekstradycji między Stronami w związku z przestępstwami określonymi zgodnie z artykułami 2-11 niniejszej konwencji, pod warunkiem, że są one karalne na podstawie prawa obu zainteresowanych Stron karą pozbawienia wolności w wymiarze co najmniej jednego roku lub większą karą.

**Część 2**

**Postanowienia szczegółowe**

Artykuł 31

**Wzajemna pomoc prawna odnosząca się do dostępu do przechowywanych danych informatycznych**

1. Strona może zwrócić się do drugiej Strony z wnioskiem o przeszukanie lub uzyskanie dostępu przy użyciu podobnych metod, zajęcie lub podobne zabezpieczenie albo ujawnienie danych przechowywanych przy użyciu systemu informatycznego, znajdującego się na terytorium Strony wezwanej, w tym także danych zabezpieczonych zgodnie z artykułem 29.

Artykuł 32

**Ponadgraniczny dostęp do przechowywanych danych, za zgodą lub gdy są one publicznie dostępne**

Strona, bez zezwolenia drugiej Strony, może:

a) uzyskać dostęp do przechowywanych danych informatycznych, które są publicznie dostępne (źródło otwarte), niezależnie od geograficznej lokalizacji tych danych, lub
b) uzyskać dostęp lub otrzymać przy pomocy systemu informatycznego znajdującego się na własnym terytorium dane informatyczne przechowywane na terytorium innego państwa, jeżeli Strona uzyska prawnie skuteczną i dobrowolną zgodę osoby upoważnionej do ujawnienia Stronie tych danych przy pomocy tego systemu informatycznego.

Artykuł 34

**Wzajemna pomoc prawna w zakresie przechwytywania danych dotyczących treści**

W zakresie dozwolonym przez obowiązujące traktaty i prawo krajowe, Strony powinny świadczyć sobie pomoc wzajemną w zakresie gromadzenia lub rejestrowania w czasie rzeczywistym danych dotyczących treści określonych przekazów realizowanych przy pomocy systemu informatycznego.

Artykuł 35

**Sieć 24/7**

1. Każda ze Stron wyznaczy punkt kontaktowy dostępny 24 godziny na dobę przez 7 dni w tygodniu, w celu zapewnienia natychmiastowej pomocy dla celów prowadzenia czynności śledczych lub postępowań odnoszących się do przestępstw związanych z systemami i danymi informatycznymi lub dla celów zbierania dowodów w postaci elektronicznej dotyczących przestępstw. Pomoc ta będzie obejmowała ułatwienia lub, jeżeli jest to dopuszczalne przez prawo krajowe lub praktykę, bezpośrednie zastosowanie następujących środków:
   a) zapewnienie doradztwa technicznego;
   b) zabezpieczenie danych zgodnie z artykułami 29 i 30;
   c) gromadzenie dowodów, dostarczanie informacji o prawie oraz lokalizowanie osób podejrzanych.

ROZDZIAŁ IV
POSTANOWIENIA KOŃCOWE

Artykuł 38

**Zakres terytorialny**

1. Każde państwo, w chwili podpisywania lub składania swojego instrumentu ratyfikacyjnego, akceptacji, zatwierdzenia lub przystąpienia, może wskazać terytorium lub terytoria, do których stosować się będzie niniejsza konwencja.

Artykuł 41

**Klauzula federalna**

1. Państwo federalne może zastrzec sobie prawo wykonywania zobowiązań wynikających z Rozdziału II niniejszej konwencji zgodnie z jej podstawowymi zasadami regulującymi stosunki między władzami federalnym a państwami wchodzącymi w skład federacji lub innymi analogicznymi jednostkami terytorialnymi, pod warunkiem, że jest nadal w stanie prowadzić współpracę na podstawie Rozdziału iii.

Artykuł 48

**Notyfikacja**

Sekretarz Generalny Rady Europy notyfikuje państwom członkowskim, państwom niebędącym członkami Rady Europy, które uczestniczyły w opracowywaniu niniejszej konwencji, jak też wszystkim państwom, które przystąpiły do konwencji lub zostały zaproszone do przystąpienia do niej:

Sporządzono w Budapeszcie dnia 23 listopada 2001 roku w językach francuskim i angielskim, przy czym obie wersje językowe są jednakowo autentyczne, w jednym egzemplarzu, który zostanie złożony w archiwum Rady Europy. Sekretarz Generalny Rady Europy przekaże poświadczone kopie każdemu państwu członkowskiemu Rady Europy, państwom niebędącym członkami Rady Europy, które uczestniczyły w opracowywaniu konwencji oraz każdemu państwu zaproszonemu do przystąpienia do konwencji.

BIBLIOGRAFIA:


1. A. Adamski, *Cyberberprzestepczość – aspekty prawne i krymnologiczne*, „Studia Prawnicze" 2005, nr 4(166).
2. P. Aftal, *Internet a dzieci: uzależnienia i inne niebezpieczeństwa*, przeł. B. Nicewicz, wyd. Pruszyński i S-ka, Warszawa 2003.
3. M. Castells, *Galaktyka Internetu. Refleksje nad internetowym biznesem i społeczeństwem*, Poznań 2003.
4. W. Cellary (red.), *Polska w drodze do globalnego społeczeństwa informacyjnego. Raport o rozwoju społecznym*, Wydane przez Program Narodów Zjednoczonych ds. Rozwoju, Warszawa 2002.
5. M. Goliński, *Polska jako społeczeństwo informacyjne – ocena infrastruktury technicznej*, (w:) *Rozwój społeczeństwa informacyjnego – teoria i praktyka*, t. 1, Wyd. AGH, Kraków 2003.
6. A. Grzywak, *Internet w społeczeństwie informacyjnym*, wyd. WSB, Dąbrowa Górnicza 2003.
7. Ch. Jonscher, *Życie okablowane. Kim jesteśmy w epoce przekazu cyfrowego?*, Muza SA, Warszawa 2001.

8. J.A. Kennedy, *Internet*, Optimus Pascal SA, wydanie I, Bielsko-Biała 1999.
9. K. Krzysztofek, M.S. Szczepański, *Zrozumieć rozwój. Od społeczeństw tradycyjnych do informacyjnych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2002.
10. M. Madej, M. Tretlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Wyd. Polski Instytut Spraw Międzynarodowych, Warszawa 2009, *Aneks. Konwencja o cyberprzestępczości*.
11. M. Majta, *Rola informacji w kształtowaniu nowych społeczeństw*, EBIB, Wrocław 2005.
12. K. Paradowski, *Internet, korzyści i zagrożenia*, wyd. Centrum Edukacji Społeczeństwa, Warszawa 2000.
13. J. Raczkowska, T.D. Woyciechowska, *Problemy zagrożenia młodzieży uzależnieniem (diagnoza i terapia)*, Centralny Ośrodek Metodyczny Poradnictwa Wychowawczo-Zawodowego Ministerstwa Edukacji Narodowej, Warszawa 2009.
14. B. Siemieniecki, W. Lewandowski, *Internet w szkole*, Wydawnictwo Adam Marszałek, Wydanie II, Toruń 1998.
15. B. Szmajdziński, *Syndrom Uzależnienia od Internetu*, wydawnictwo Studio-Impuls, Warszawa 2007.
16. R. Tadeusiewicz, *Społeczność Internetu*, Wyd. Exit, Warszawa 2003.
17. P. Wallece, *Psychologia internetu*, Dom Wydawniczy Rebis, wydanie I, Poznań 2001.
18. T. Zasępa, R. Chmura (red.), *Internet i nowe technologie ku społeczeństwu przyszłości*, Edycja Świętego Pawła, Częstochowa 2008.
19. *Bez niedomówień do rodziców. O problemach dzieciństwa i dorastania*, praca zbiorowa pod redakcją A. Janowskiego i I. Namysłowskiej, Instytut Psychiatrii i Neurologii, ELMA BOOKS, Warszawa 1998.
20. *Nauka, nowoczesne technologie i społeczeństwo informacyjne 2007-2013*, Warszawa, wrzesień 2005.

## The Anthropological Aspects of Informational Security for the Users of Contemporary Means of Communication

Abstract. According to Aristotle, human ability of the individual survival and development rests in its communal existence, and is determinedly related to communication process. Hence, primary aspect of human security corresponds directly with the person's ability to communicate. Historically, evolution of the basic communication skill went a long way, looking back at history. At the beginning it was verbal but evolved into a more complex and multidimensional system dominating today. Having this in view, author of the article presents some anthropological characteristic of security in its progressed form. With respect to that, there are presented typical categories of security issues with regards to communication in society, information security and cybercrime. There are also some recommendations given addressing an issue of how to prevent particular dangers. Since anthropology of human culture is evolving the best way to explain different changes is by using the formal philosophical language able to describe in unison many aspects of those changes.