Monika Kornacka
Przemysław Grzonka

Społeczeństwo informacyjne a zagrożenie wolności jednostki

Pojęcie wolności

Aby mówić o zagrożeniach dla wolności jednostki stwarzanych przez społeczeństwo informacyjne, należy najpierw określić, czym owa wolność jest. Pytanie to nurtuje filozofów i myślicieli od ponad dwóch tysięcy lat. Już w starożytnej Grecji problem ten był dyskutowany i debaty trwają po dziś dzień. Ich skutkiem jest duża ilość mniej lub bardziej udanych prób definicji tego pojęcia[1], zaś jego rozumienie i zakres zmieniały się diametralnie. Dowodził tego Benjamin Constant, charakteryzując różnice na tym polu między starożytnością a czasami nowożytnymi[2]. Część autorów, wśród których wymienić można Edmunda Burke'a, w ogóle uznała, iż jest to pojęcie niedefiniowalne[3]. Dlatego też prześledzenie całej historii ewolucji rozumienia wolności bądź stworzenie kompletnego katalogu, choćby tylko ważniejszych i bardziej wpływowych koncepcji, przekracza zdecydowanie ramy tej pracy, a taka próba spowodowałaby jedynie całkowite rozmycie podstawowego problemu.

Najogólniejszą definicją wolności podawaną m.in. przez „Nową Encyklopedię Powszechną" PWN jest „brak zewnętrznego przymusu"[4]. Stanowi to uproszczenie myśli angielskiego myśliciela Johna Locke'a, który pisał: „Wolność sprowadza się bowiem do niezależności od przymusu i gwałtu ze strony innych. Nie jest to możliwe tam, gdzie nie ma prawa. Nie jest więc to, jak się nam mówi, wolnością, gdyby każdy robił to, co mu się podoba. Któż bowiem miałby być wolny, gdyby inny był w stanie go tyranizować? Być wolnym, to znaczy dysponować i swobodnie, zgodnie z własnym sumieniem, kierować własną osobą, działaniem, majątkiem, całą swą własnością z przyzwoleniem prawa, któremu się podlega, nie być więc poddanym czyjejś arbitralnej woli, ale kierować się bez przeszkód własną wolą"[5].

Podobnego spojrzenia na sprawę u Friedricha von Hayek'a dopatruje się Miłowit Kuniński, stwierdzając, iż ten, „analizując naturę wolności wskazywał na przymus jako jej przeciwieństwo. Przymus nie oznacza bynajmniej braku możliwości podejmowania wolnej decyzji, lecz polega na manipulowaniu druga osobą, na uczynieniu jej narzędziem realizacji celów tego, kto kontroluje sytuację, kto w ten sposób określa cele pośród których dana

[1] Dla przykładu *Słownik Języka Polskiego PWN* (wydanie Warszawa 1989) podaje trzy definicje wolności, *Nowa Encyklopedia Powszechna PWN* (wydanie Warszawa 1997) pięć, zaś Wikipedia w wersji polskojęzycznej aż czternaście.

[2] M. Kuniński, *Wolność i demokracja*, http://www.omp.org.pl/index.php?module=subjects&func=viewpage&pageid=309, z dnia 07.01.2010

[3] B. Szlachta, *Problem wolności w ujęciu konserwatysty*, http://www.omp.org.pl/index.php?module=subjects&func=viewpage&pageid=698, z dnia 07.01.2010

[4] *Wolność*, w: *Nowa Encyklopedia Powszechna PWN: T.6: SZ,* Warszawa 1997, Wydawnictwo Naukowe PWN, s. 881.

[5] J. Locke, *Traktat drugi. Esej dotyczący prawdziwych początków, zakresu i celu rządu obywatelskiego*, [w:] *Dwa traktaty o rządzie*, (tłum., wstęp i komentarz Zbigniew Rau), Wydawnictwo Naukowe PWN, Warszawa 1992 s. 201.

osoba ma wybierać. Komu narzuca się alternatywy wyboru zostaje pozbawiony wolności i spełnia wolę drugiego w jego interesie"[6]. Jest to bardzo ważne z punktu widzenia tej pracy spostrzeżenie, które pojawi się, gdy będą omawiane problemy np. z ograniczeniem pluralizmu źródeł pochodzenia informacji, kreowania rzeczywistości czy też lansowania określonych postaw i wzorów kulturowych.

Innym z podstawowych obecnie sposobów podejścia do pojęcia wolności jest koncepcja rozróżnienia między wolnością negatywną a wolnością pozytywną, opisana m. in. przez Isaiaha Berlina w eseju „Dwie koncepcje wolności"[7]. Różnicę między nimi M. Kuniński sprowadza do odpowiedzi na następujące dwa pytania:

1. *Wolność negatywna: „Jak daleko sięga obszar, w granicach którego podmiot osoba czy grupa osób ma lub powinien mieć całkowitą swobodę działania wedle własnej woli, bez wtrącania się innych osób?". Berlin w charakterystyczny dla siebie metaforyczny sposób nadaje temu pytaniu także inną postać: ile drzwi stoi przed mną otworem, jakie są przeszkody, które napotykam? W sensie negatywnym wolność tego rodzaju polega na braku przymusu. Uświadomiwszy sobie, iż pojmowanie wolności jako realizacji pragnień bez ingerencji ze stronny innych osób, może oznaczać osiąganie wolności także przez wygaszenie pragnień, Berlin modyfikuje koncepcję wolności przez jej obiektywizację, uznanie, iż polega ona na braku przeszkód na drodze realizacji pragnień („ile drzwi stoi przede mną otworem").*
2. *wolność pozytywna: „Co lub kto jest źródłem władzy lub ingerencji, która może przesądzić, że ktoś ma zrobić raczej to niż tamto, być taki a nie inny?", czy kieruję sobą sam, czy też czynią to inni.*

Wolność negatywna oznacza decydowanie i działanie swobodne w ramach prawa. Wolność pozytywną Berlin rozumie jako bycie panem samego siebie, nie zaś czyimś niewolnikiem czy też niewolnikiem natury lub uczuć[8].

Ta pierwsza może być również określona jako „wolność od" (władzy, przymusu, ingerencji innych etc.) i przez to jest właściwie tożsama z tą, o której pisał Locke. Została ona wyrażona w art. IV „Deklaracji Praw Człowieka i Obywatela" z 26 sierpnia 1789 roku, mówiącej, iż: „Wolność polega na czynieniu tego wszystkiego, co nie szkodzi drugiemu. W ten sposób nie ma innych granic dla używania praw naturalnych człowieka, jak te, które zapewniają używanie tychże praw innym członkom społeczeństwa. Te granice może określić tylko Ustawa"[9]. Jest to tradycyjny sposób pojmowania wolności[10].

Ta druga zaś określana jest jako „wolność do" (wyboru, działania – np. udziału w wyborach etc.). Została ona sformułowana w XIX wieku przez myślicieli takich jak Leonard Hobhouse, na bazie m. in. dzieł Johna Stuarta Milla[11]. Jej odzwierciedleniem są zapisy pozytywne wielu aktów prawnych (np. „Powszechnej Deklaracji Praw Człowieka" z 10 grudnia 1948 roku czy „Konstytucji Rzeczypospolitej Polskiej" z 2 kwietnia 1997 roku), stwierdzające, że prawem człowieka jest dostęp do określonej kategorii dóbr materialnych i niematerialnych (np. prawo do informacji) i gwarantujące jej bezpieczeństwo socjalne.

---

6 M. Kuniński, *op. cit.*

7 *Wolność: Isaiaha Berlina głos w dyskusji*, http://www.racjonalista.pl/kk.php/s,2343, z dnia 07.01.2010.

8 M. Kuniński, *op. cit.*

9 *Deklaracja Praw Człowieka i Obywatela z 26 sierpnia 1789 roku,* http://www.biblioteka.pluru.pl/index.php?option=com_content&view=article&id=106:deklaracja-praw-czowieka-i-obywatela-z-1789-r&catid=45:francja&Itemid=65, z dnia 07.01.2010.

10 R. Lis, *Relacje między wolnością a demokracją.Liberalny punkt widzenia*, [w:] *Aktualność wolności. Wybór tekstów*, wybór i wstęp Bronisław Misztal i Marek Przychodzeń, Fundacja ALETHEIA, Warszawa 2005, s. 267.

11 Ibidem.

Przy analizowaniu zagrożeń stwarzanych dla wolności jednostki przez społeczeństwo informacyjne na pewno należy mieć na uwadze je obie, mimo iż ta dychotomia bywa czasem krytykowana[12].

Zagrożenia prawa do prywatności

Warunkiem, by dany system polityczny uznano za demokratyczny, jest m.in. przestrzeganie właściwych temu systemowi swobód i praw obywatelskich. Rozwój społeczeństwa informacyjnego, wzmożona produkcja i obieg informacji sprawiają, iż często narusza się podstawowe prawa człowieka i obywatela zagwarantowane w konstytucji, bądź w innych aktach prawnych; zwłaszcza zaś prawo do prywatności i prawo do ochrony danych osobowych.

Państwo zawsze dążyło do kontrolowania swych obywateli poprzez gromadzenie o nich informacji. Jednakże dopiero rozwój nowoczesnych technik pozwolił na łączenie tych rozproszonych danych w jeden zbiór oraz na swobodny ich przepływ między instytucjami. „Jeden z najstarszych skomputeryzowanych systemów ewidencji ludności zainstalowany został w 1955 roku w RPA, gdzie niemożliwym był inny sposób obserwacji zatrudnienia i zamieszkania czarnej ludności przez władze państwa. W 1987 roku, obywatele Niemiec, jako pierwsi w Europie, zostali zaopatrzeni w odczytywane przez komputer dowody tożsamości. Podobną właściwość mają wszystkie paszporty wydawane od 1988 roku na obszarze Wspólnoty Europejskiej[13]". Rozwój systemów służących do gromadzenia i przechowywania danych osobowych spowodował równoczesny rozwój prawodawstwa regulującego wspomniany obszar. W 1973 roku, jako pierwszy, uchwalił akty prawne regulujące funkcjonowanie banków danych Parlament Szwedzki. Dziś w większości krajów obowiązują podobne ustawy[14]. Dane osobowe są również chronione na gruncie prawa międzynarodowego[15].

Przepisy te powstały po to, by zagwarantować obywatelom prawo do prywatności, które może być naruszone w każdej z czterech faz procesu przetwarzania danych (zbierania, opracowywania, udostępniania oraz usuwania). Określają one:

- Rodzaj gromadzonych danych personalnych,
- Podmioty, którym dane personalne mogą być udostępnione,
- Warunki dostępu do danych personalnych,
- Cel gromadzenia i wykorzystywania danych personalnych,
- Środki ochrony danych personalnych,
- Podmioty odpowiedzialne za stan danych personalnych (ich całość i nienaruszalność),
- Zasady przepływu danych personalnych,
- Zasady postępowania w przypadku nieprawidłowego wykorzystania danych personalnych[16].

---

[12] M. Szyszkowska, *O wolności,* http://www.racjonalista.pl/kk.php/s,4415/q,O.wolnosci, z dnia 07.01.2010.

[13] A. Pawłowska, *Prawo do informacji czy prawo do prywatności?,* [w:] *Rewolucja informacyjna i społeczeństwo,* (red L. Zacher), Fundacja Edukacyjna TRANSFORMACJE, Warszawa 1997, s. 107.

[14] Chronologicznie: w USA od 1974, w Niemczech od 1876, w Kanadzie od 1977, we Francji od 1978, w Danii, Norwegii, Wielkiej Brytanii od 1984, Irlandii i Australii od 1988 roku.

[15] m.in. w art. 8 *Europejskiej Konwencji Praw Człowieka* oraz w wydanych w 1973 roku rezolucjach 22 i 29 Rady Europejskiej w sprawie ochrony sfery prywatności osób fizycznych ze względu na wykorzystanie elektronicznych banków danych w sektorze prywatnym.

[16] A. Pawłowska, *Prawo…, op. cit.*, s. 108.

Ustawy o prywatności gwarantują osobom prywatnym:
- Dostęp do zgromadzonych o nich danych oraz dostęp do informacji o podmiotach, którym dane te są udostępnione,
- Możliwość sprostowania danych nieprawdziwych,
- Możliwość zablokowania danych nieprawdziwych oraz tych, których prawdziwość zainteresowany kwestionuje (a niemożliwym jest udowodnienie ich prawdziwości),
- Możliwość usunięcia zgromadzonych danych, jeśli ich zbieranie było niedozwolone lub jeśli zachodzą przesłanki usprawiedliwiające zablokowanie,
- Prawo wystąpienia o odszkodowanie za straty majątkowe lub osobiste poniesione w wyniku zamieszczenie nieprawdziwych danych.

„W materii gromadzenia, przetwarzania, przechowywania i udostępniania danych personalnych, społeczeństwa informacyjne stoją w obliczu konfliktu dwóch równorzędnych wartości – bezpieczeństwa publicznego oraz prawa do zachowania prywatności. Pełna realizacja jednej z wymienionych wartości uniemożliwia pełna realizacje drugiej. Ochrona prywatności wymaga: zminimalizowania informacji czerpanych zarówno przez informacje rządowe, jak i pozarządowe; nie kumulowania informacji w jeden zbiór; udostępniania informacji wyłącznie osobie lub organizacji do tego uprawnionej. Systemy prawne społeczeństw informacyjnych zmierzają do pogodzenia racji obywatela i państwa”[17].

Użytkownicy Internetu nie chcą, by osoby postronne mogły łatwo poznać treść ich emaili, czy też ustalić ich tożsamość. Dlatego też często korzystają z technik szyfrowania. Jednak policja i inne służby odpowiedzialne za zachowanie bezpieczeństwa państwowego są przeciwne temu, by obywatele mogli kodować informacje. Państwa w wyniku tego sporu wprowadzają, najlepsze ich zdaniem, regulacje. Francja ustanowiła zakaz używania technik szyfryzacji dla osób prywatnych oraz organizacji. Za złamanie przewidziane są kary pieniężne oraz – w skrajnych przypadkach – kara pozbawienia wolności. Władze Stanów Zjednoczonych podejmowały próby wprowadzenia w życie inicjatywy *Clipper chip*, która zakładała legalne kodowanie wiadomości przez obywateli, ale tylko pod warunkiem, że równocześnie zdeponują oni w odpowiednim urzędzie klucz dekodujący, dzięki któremu państwo mogłoby deszyfrować każdy wysyłany przez nich komunikat. Inicjatywa nie znalazła dużego poparcia, w związku z czym nie weszła w życie.

Ponownie państwo staje przed wyborem, którą z wartości realizować – bezpieczeństwo publiczne czy prawo do prywatności. Policja i tajne służby państwowe przekonują, iż zakaz kodowania danych przesyłanych przez Internet jest niezbędny do skutecznej walki z organizacjami przestępczymi. Przeciwnicy takiego rozwiązania nawet jeśli zgadzają się z pewnymi ograniczeniami swej prywatności, nadal żądają by państwo umożliwiło im kodowanie informacji oraz zachowanie w tajemnicy klucza służącego dekodowaniu informacji. „Uważają oni, że ograniczenie prawa do tajemnicy może nastąpić jedynie na podstawie decyzji sędziego wydawanej według kryteriów podobnych do tych, które stosuje się przy decyzjach o podsłuchu lub rewizji mieszkania”[18].

Jednak nawet szyfrując wiadomości, osoby korzystające z Internetu nie są anonimowe, wbrew temu, co uważa większość obywateli. O realności problemu utraty anonimowości przez użytkowników sieci, świadczyć może sprawa wirusa Melissa – pierwszego makrowirusa dla MS Worda posiadającego także funkcjonalność robaka internetowego. Natychmiast po infekcji wirus skanował książkę adresową w MS Outlook i przesyłał własne kopie pod 50 pierwszych adresów. Dokonywał tego bez zgody czy wiedzy użytkownika, jednak wiadomości wyglądały jakby zostały przesłane w jego imieniu. Epidemia została szybko

[17] Ibidem, s. 108-109.

[18] T. Goban-Klass, *Cywilizacja medialna*, WsiP, Warszawa 2005, s. 233.

opanowana. Mimo to wirus zdążył wyrządzić poważne szkody w wielu systemach komputerowych: liderzy branży, tacy jak Microsoft, Intel oraz Lockheed Martin zostali zmuszeni do tymczasowego wyłączenia swoich korporacyjnych systemów pocztowych. W zidentyfikowaniu autora wirusa pomógł zainstalowany w oprogramowaniu Windows tajny mechanizm programowy (Global Unique Identifier – GUID). W ciągu tygodnia amerykańskie organy ścigania (a dokładnie jednostki do zwalczania cyberprzestępczości) dzięki niemu odnalazły i aresztowały jego twórcę (programistę Davida L. Smitha). Nikt nie jest w pełni anonimowy w sieci. Zresztą, nie tylko Internet i komputer daje możliwość inwigilacji. Także za pomocą innych urządzeń możliwe jest np. sprawdzanie, gdzie dokładnie przebywa dana osoba. „We współczesnych przedsiębiorstwach obserwacja personelu staje się obowiązkiem menadżerów. W firmach przewozowych nowa technologia pozwala sprawdzać zarówno kierowcę, jak i jego pojazd. Telefon komórkowy jest często narzędziem kontroli czasu i miejsca pracy, można bowiem lokalizować pracowników za pomocą służbowych telefonów komórkowych. Dokładne dane o miejscu samochodu przysyłane są za pomocą nadajnika GPS, wówczas informacja dociera do biura poprzez pakietową transmisję danych. Usługa „Gdzie oni są?" opiera się na SMS-ach. Telefon wyposażony w opcję „Szef" sam wysyła pod specjalny numer wiadomości tekstowe o miejscu przebywania pracownika, uwzględniając miasto i nazwę ulicy, a niekiedy nawet mapkę"[19].

Pozostaje do rozstrzygnięcia dylemat, czy pracodawcy maja prawo kontrolować w taki sposób swych podwładnych? Czy przyzwalanie na takie postępowanie nie przyczyni się w niedalekiej przyszłości do stworzenia orwellowskiej rzeczywistości, gdzie w imię bezpieczeństwa będziemy musieli zrzec się własnej prywatności? Równie dobrze można spekulować, czy elity wiedzy i władzy będą chciały promować (m.in. poprzez media i inne środki przekazu) ład demokratyczny oraz społeczeństwo obywatelskie, które sprzyjają ochronie prywatności. Możliwe jest wzmocnienie tendencji merytokratycznych (rządy fachowców bez liczenia się ze społeczeństwem) czy technokratycznych (rządy techników, którzy jako twórcy techniki i jedyni, którzy są zdolni skutecznie nią operować – „wiedzą lepiej" i przedkładają kryteria techniczne nad społeczne). Rozwój takich tendencji stanowi rzeczywiste zagrożenie dla demokracji.

Przestępstwa komputerowe

„Żywiołowy rozwój komputeryzacji powoduje jej związki ze wszystkimi dziedzinami życia społecznego, w tym także z przestępczością zorganizowaną"[20]. Bezpieczeństwo w Internecie jest trudne i kosztowne do osiągnięcia. Przyczynia się do tego m.in. to, iż:

- Sieć nie ma właściciela,
- Nie posiada centralnej kontroli,
- Brak standardowej, akceptowanej przez wszystkich użytkowników polityki (w tym także bezpieczeństwa),
- Brak międzynarodowego prawodawstwa w dziedzinie przestępstw komputerowych.

Przestępstwa popełniane w cyberprzestrzeni Karol J. Jakubowski definiuje jako obejmujące wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszeniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośniki i obieg

[19] Ibidem, s. 238.

[20] M. Wawrzak-Chodaczek, *Kształcenie kultury audiowizualnej młodzieży,* Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2000, s. 51.

w komputerze oraz całym systemie połączeń komputerowych, a także sam komputer. Charakterystyczne dla przestępstw komputerowych jest to, iż:

- Są niemożliwe do dokonania poza środowiskiem komputerowym,
- Często są popełniane przy biernym udziale komputerów (poprzez: oszustwa, wyrządzenie szkód w interesach gospodarczych oraz prywatnych),
- Dokonywane są przez profesjonalnych przestępców z wykorzystaniem komputerów służących do wspomagania swojej działalności (poprzez: nadzór interesów, komunikację, produkcję fałszywych dokumentów, zacieranie śladów).

Ogólnie można sklasyfikować cyberprzestępstwa według typów i rodzajów czynów[21]:

Tabela 1.

Typ	Czyn
Przestępstwa przeciw poufności, integralności i dostępności danych oraz systemów komputerowych	– Nielegalny dostęp do systemu komputerowego. – Nielegalne przechowywanie danych. – Nielegalna ingerencja w dane, powodująca ich uszkodzenie, usuniecie, zniszczenie, modyfikację lub zablokowanie. – Nielegalna ingerencja w system powodująca poważne zakłócenia w funkcjonowaniu systemu komputerowego na skutek wprowadzenia, uszkodzenia, usunięcia, pogorszenia, zmiany lub zablokowania danych. – Wytwarzanie, sprzedaż, oferowanie do używania, import, rozpowszechnianie lub upowszechnianie w inny sposób, a także posiadanie: ∗ przyrządów lub narzędzi, w tym programów komputerowych, przeznaczonych lub specjalnie przystosowanych do celów związanych z popełnieniem wyżej wymienionych przestępstw; ∗ haseł, kodów dostępu lub innych podobnych danych, umożliwiających dostęp do systemu komputerowego lub jego części, w zamiarze ich użycia w celu popełnienia któregokolwiek z powyżej wymienionych przestępstw.
Przestępstwa związane z użyciem komputera	– Fałszerstwo komputerowe (np. wprowadzenie zmian do elektronicznego zapisu informacji o znaczeniu prawnym przez osobę do tego nieupoważnioną, posługiwanie się cudzym podpisem elektronicznym, nieautoryzowane generowanie danych lub całych dokumentów elektronicznych mających wartość dowodową). – Oszustwo komputerowe, czyli spowodowanie utraty własności, przez wprowadzenie, zmianę, usunięcie lub zablokowanie danych komputerowych albo inna ingerencja w proces przetwarzania danych, w zamiarze przysporzenia sobie lub innej osobie nienależnej korzyści majątkowej.
Przestępstwa komputerowe ze względu na treść informacji stanowiącej jej przedmiot	– Wytwarzanie, rozpowszechnianie, przesyłanie, udostępnianie, a także posiadanie pornografii z udziałem osób do lat 18 w systemie komputerowym lub na nośnikach danych.
Przestępstwo przeciwko własności intelektualnej	– Cyfrowe zwielokrotnianie i rozpowszechnianie utworów lub wykonań artystycznych bez zgody osoby uprawnionej.

Prawo do kopiowania, powielania oraz modyfikowania utworu podlega ochronie prawnej, jednak internauci nie zważają na prawa autorskie i wymieniają się pirackimi plikami.

[21] M. Nowina Konopka, *Społeczeństwo informacyjne a globalizacja,* [w:] *Społeczeństwo informacyjne. Istota, rozwój, wyzwania,* (red. M. Witkowska, K. Cholawo-Sosnowska), Wydawnictwo Akademickie i Profesjonalne, Warszawa 2006, s. 173-174.

Piractwo dotyczy zarówno materialnych, jak i informacyjnych dóbr. Do tych ostatnich można zaliczyć takie, których wartość ocenia się poprzez zawartość i treść: wiadomości, utwory muzyczne, filmy. Dobra te mają wspólne cechy, takie jak łatwość powielania i szybka dezaktualizacja.

Skutki piractwa dla państwa to m.in. zmniejszenie przychodów i zysków firm, których produkty są podrabiane, zahamowanie wzrostu płac i wolniejszy rozwój firm, zmniejszenie płaconych przez firmy podatków, a tym samym mniejsze wpływy do budżetu państwa. Wszystko to prowadzi do spowolnienia wzrostu gospodarczego państwa. Dla twórców do najbardziej uciążliwych implikacji piractwa należą m.in. uzyskiwanie mniejszych wynagrodzeń oraz demobilizacja, która jest następstwem braku skutecznej ochrony praw autorskich. Nabywcy zaś ponoszą ryzyko zakupu wadliwego, rezygnują ze świadczeń dodatkowych, tj. np. z gwarancji czy pomocy technicznej oraz ryzykują konsekwencjami prawnymi w przypadku udowodnienia przestępstwa[22].

Z drugiej jednak strony rozmaite systemy zabezpieczania przed kopiowaniem naruszają prawo do swobodnego użytkowania swojej własności. Wprowadzanie nadmiernych obostrzeń również godzi w wolność. Trudno bowiem inaczej nazwać sytuację, w której np. nabywcy płyty usiłuje się zakazać i uniemożliwić wgranie jej do przenośnego odtwarzacza mp3 lub skopiowanie w celu odtwarzania np. w samochodzie.

Zupełnie innym problemem jest malware (od mal – coś złego, ware – artykuły, rzeczy). Pod tym terminem kryją się wszystkie zagrożenia, takie jak np. wirusy, robaki komputerowe czy konie trojańskie, a także phishing.

Wirus to mały program, który nie uruchamia się na ogół sam. Robi to niczego nieświadomy użytkownik komputera. Wirus może dotrzeć do komputera za pośrednictwem wszelkich nośników informacji (np. dysków, taśm a także 2P2, czy IM jak GG), a także z dokumentem Office'a bądź e-mailem.

Robaki komputerowe rozmnażają się samodzielnie, bez udziału człowieka. Ich niebezpieczeństwo nie kryje się, jak w przypadku wirusów, w niszczeniu danych, ale w szybkim ich rozmnażaniu. Może to prowadzić do np. blokowania serwerów internetowych. Wirusy różnią się od robaków także tym, iż infekują nośniki danych i RAM, zaś robaki aktywnie rozprzestrzenia się pocztą, protokołami sieciowymi.

Trojany (konie trojańskie) niezauważone przez użytkownika instalują się samodzielnie na dysku komputera. „Najczęściej zadaniem Trojanów jest pełnienie roli szpiega, który monitoruje zasoby inwigilowanego komputera, aktywność internauty w sieci i następnie co jakiś czas przesyła dane na ten temat pod określony adres „zleceniodawcy" – szpiega, będącego osoba fizyczną. […] W efekcie niezależnie od woli właściciela komputera osoba z zewnątrz może swobodnie na nim pracować, uruchamiając zainstalowane na nim programy, przeglądając, zmieniając lub niszcząc zbiory, a także bez kłopotu przechwytując hasła. Co gorsze, komputer może stać się w rękach hakera marionetką atakująca inne komputery – nawet zaprzyjaźnionych osób"[23].

Do komputerowych przestępstw możemy zaliczyć również:

- Podsłuch (eavesdropping) – dane są przesyłane bez zakłóceń, ale naruszona jest ich poufałość,
- Phishing (scamming) – zdobywanie przez użytkowników sieci danych innych internautów, pozwalających np. na oczyszczanie ich kont z pieniędzy,
- Spoofing – osoba może podszyć się pod inną tożsamość,

[22] Ibidem, s. 175.

[23] W. Gogołek, *Technologie informacyjne mediów*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2005, s. 232.

– Penetracja (tampering) – dane są przechwytywane, modyfikowane i przesyłane do adresata,
– Denial of Service (DoS/DDoS) – odmowa wykonania usługi, atakowany serwer zablokowany dużą ilością żądań. Haker wyzwala masowy atak na cel, korzystając z zaanektowanych (niewystarczająco zabezpieczonych) komputerów, tzw. Zombie. DDoS (Distributed Denial of Service) – tworzy automaty programowe „żołnierzy", które instalują się na przypadkowo wybranych komputerach i stamtąd dokonują zwielokrotniony atak (z wielu komputerów jednocześnie) na komputer ofiary,
– Port scan – uruchamianie usług na wielu portach i wykorzystywanie luk (związanych z usługą) w bezpieczeństwie,
– Naśladowanie (impersonation) – dane docierają do osoby podszywającej się pod adresata,
– Misrepresentation – osoba lub organizacja może podawać fałszywą informację o prowadzonej działalności czy swojej ofercie[24].

Jedną z najczęściej używanych usług internetowych jest poczta elektroniczna. Z jej popularnością związane są jednak także zagrożenia. Niemal każdy internauta wysyłający i odbierający emaile spotkał się z tzw. spamem. Są to olbrzymie ilości maili natarczywie oferujących produkty i usługi. Stanowią ponad połowę elektronicznej korespondencji i przynoszą wielomiliardowe straty. Największym generatorem spamów jest USA (niecałe 23%), dalej Korea Południowa (niecałe 22%) oraz Chiny (niecałe 13%). Polska jest na 11 miejscu z wynikiem nieco ponad 2%[25].

Cyberprzemoc

„Przez cyberprzemoc (cyberbullying) rozumie się różne formy nękania za pomocą Internetu i narzędzi elektronicznych: e-mailów, witryn, czatów, gier online czy for dyskusyjnych w Internecie. To także dręczenie przy wykorzystaniu komunikatorów (jak np. Gadu-Gadu) czy złośliwych SMS-ów"[26]. Cyberprzemoc charakteryzuje się świadomym, wrogim i powtarzającym się działaniem na szkodę ofiary. Ogólnie można wyróżnić następujące przypadki cyberprzemocy:
– Rozsyłanie bądź zamieszczanie w sieci kompromitujących materiałów (m.in. filmów czy zdjęć) dotyczących danej osoby,
– Podszywanie się pod kogoś w Internecie (m.in. włamanie się na konta pocztowe i konta komunikatorów w celu rozsyłania – w imieniu właściciela – kompromitujących wiadomości),
– Rozsyłanie niepowołanym osobom otrzymanych wiadomości jako zapisu prywatnej rozmowy czy kopii e-maila bądź zamieszczanie ich w takim miejscu, że potencjalnie każdy może je zobaczyć,
– Tworzenie kompromitujących i ośmieszających stron internetowych,
– Bezpośrednie nękanie ofiary drogą elektroniczną (np. grożenie, straszenie czy obrażanie),
– Grooming (uwodzenie dzieci przez osoby dorosłe za pośrednictwem Internetu. Zazwyczaj używa się do tego celu czatów i różnego rodzaju komunikatorów. Dorosły nakłania nieletniego do rozmów o seksie, oglądania pornografii, itp., co

[24] Ibidem, s. 243.

[25] Dane na rok 2005.

[26] P. T. Nowakowski, *Przemoc w sieci. Przyczynek do dalszych analiz*, [w:] *Internet – między edukacją, bezpieczeństwem a zdrowiem* (red. Mirosław Kowalski), Maternus Media, Tychy 2008, s. 57.

częstokroć jest przyczynkiem do dalszego molestowania. Niejednokrotnie udaje rówieśnika ofiary i stara się wzbudzić jej zaufanie, by nakłonić do spotkania w świecie rzeczywistym).

Następstwa przemocy w sieci mogą być przeróżne. Ich cechą wspólną jest to, iż najczęściej osoby dotknięte cyberbullyingiem doświadczają problemów w funkcjonowaniu również poza siecią.

Zagrożenia dla tożsamości jednostki i jej relacji z otoczeniem społecznym

Następną grupą zagrożeń są te godzące w tożsamość, indywidualność, samodzielność i niezależność, a także w relacje z innymi, w więzi społeczne oraz w sposób funkcjonowania w społeczeństwie.

Jako podstawowe zagrożenie należy wymienić ubożenie jednostek jako indywidualności. Następuje standaryzacja wzorców widoczna w zachowaniach ludzi i języku, jakim się posługują. Zaczynają naśladować wzorce płynące z mediów – głównie telewizji i Internetu – od celebrytów, showmanów, sportowców lub bohaterów filmów czy seriali, takie jak sposób bycia, wyrażania się, ubiór czy fryzura. Tworzone przez nich wzorce zaczynają być postrzegane jako „obowiązujące" w społeczeństwie, nie pozostawiając miejsca dla innych.

Jednocześnie mamy do czynienia ze stymulacją aspiracji (materialnych, konsumpcyjnych, intelektualnych, seksualnych) przez media, jednak bez możliwości ich praktycznej realizacji przez przeciętnego odbiorcę, co może prowadzić do frustracji, buntu, przestępstw etc[27]. Wybitnym przykładem jest stworzenie stereotypu, iż atrakcyjne fizycznie są jedynie jednostki szczupłe, które to przekonanie doprowadziło u wielu osób do wystąpienia takich chorób jak anoreksja czy bulimia. To samo można powiedzieć o propagowaniu łatwego, konsumpcyjnego stylu życia. Prowadzi to do pogłębiającej się komercjalizacji kultury, czego skutki są trudne do wyobrażenia i przewidzenia, choć już teraz można przewidywać, że będą ponadgeneracyjne. Lech W. Zacher rozważa w tym kontekście możliwość zdominowania kultury przez nową „kulturę techno" wynikającą z coraz to większych zmian w środkach wyrazu, kryteriach estetycznych, formach i treściach. Postrzega ją jednak negatywnie, jako „umasowienie chłamu kulturalnego"[28].

Łączy się z tym orientacja na konsumpcję rozrywki, przy czym ta rozrywka to z reguły kultura masowa, najczęściej bardzo niskiej jakości. Wywołuje ona bierność u jednostek. Rodzi też pytanie o to czy człowiek to jedynie *homo ludens*, dla którego rozrywka jest jedynym celem, czy jednak jest kimś więcej i czy rzeczywiście potrzebuje aż takiej ilości rozrywki, jaką oferują media[29].

W połączeniu z wszechobecnością mass mediów kreujących i upowszechniających te wzorce, sprawia to, iż nie ma już często miejsca na indywidualność oraz oryginalność. Mało która jednostka jest na tyle silna psychicznie, by oprzeć się takiej presji. Te zaś, którym się to udaje i świadomie lub nie, odrzucają te wzorce, stają się wyalienowane ze społeczeństwa, żyją poza głównym jego nurtem i stopniowo coraz bardziej tracą z nim kontakt. Stają przed dylematem wyboru: oglądać gwiazdy tańczące na lodzie, popularną aktualnie telenowelę bądź udzielać się w modnym portalu społecznościowym w Internecie, mimo że nie są zainteresowane takimi formami aktywności (i dzięki temu pozostawać w kon-

[27] L. W. Zacher, *Telewizja jako społecznie ryzykowne medium i forma przekazu informacji i wartości*, [w:] *Rewolucja informacyjna i społeczeństwo* (red. Z. Zacher), Fundacja Edukacyjna TRANSFORMACJE, Warszawa 1997, s. 128.

[28] Idem, *Zagrożenia w cywilizacji informacyjnej…*, [w:] *op.cit*., s. 175.

[29] Idem, *Telewizja…, op. cit*., s. 127.

takcie i relacjach z dominującą grupą, która się tym interesuje) lub nie oglądać, jednocześnie pozbawiając się kompetencji kulturowych i możliwości komunikowania się z ludźmi, dla których programy i portale tego typu stanowią sedno życia i znajdują się w centrum zainteresowań.

Wszystkie te zjawiska są szczególnie widoczne wśród młodzieży, co szeroko opisuje Stanisław Juszczyk[30], ponieważ ona najczęściej ma większe kompetencje w korzystaniu z nowoczesnych środków komunikowania od pokolenia swoich rodziców i częściej z nich korzysta. Do tego dochodzi afirmacja agresji oraz banalizacja śmierci i przemocy – oszacowano, iż dziecko spędzające dużo czasu przed telewizorem przed piętnastym rokiem życia ma okazję zobaczenia od 13 do 32 tysięcy morderstw[31], co w nieunikniony sposób oddziałuje na jego rozwój. Maria Nowina Konopka podaje następujące wady korzystania przez młode osoby z technik wirtualnej rzeczywistości[32]:

- wyobcowanie ze środowiska rzeczywistego,
- utrata umiejętności komunikowania się w grupie,
- utrata empatii,
- obniżenie poziomu wrażliwości,
- obniżenie poziomu uczuciowości,
- spadek zainteresowania nauką szkolną,
- trudności z koncentracją,
- utrata inicjatywy,
- przytępienie wyobraźni i zachowań estetycznych,
- zanik zdrowych form wypoczynku na rzecz całkowitego poświęcenia czasu wolnego grom komputerowym.

Poważnym zagrożeniem z punktu widzenia funkcjonowania człowieka jako członka społeczeństwa jest „dehumanizacja stosunków międzyludzkich, następująca w wyniku rozwoju teleedukacji i telepracy, preferencji kontaktów przez telefon (videotelefon), automatyzacji zarządzania itp."[33], o której pisze Lech W. Zacher. Zmiany w społeczeństwie następują na skutek tworzenia się nowych więzi międzyludzkich, powstających w wyniku zmiany sposobu komunikowania. Coraz częściej bezpośredni kontakt osobisty zastępowany jest kontaktem za pośrednictwem nowych środków komunikowania: telefonów, faksów, poczty elektronicznej, komunikatorów internetowych, for dyskusyjnych etc., co prowadzi do powstania nowych społeczności sieciowych, w miejsce istniejących dotychczas. Mamy coraz większe trudności w komunikowaniu się z najbliższymi, choć jednocześnie tak łatwo jest nawiązywać kontakty z osobami z całego świata. „Świat on line" zastępuje świat fizyczny[34]. Stanisław Juszczyk pisze, że może to prowadzić do swoistego paradoksu socjologicznego: człowiek posiada wiedzę o tym, co wydarzyło się w najodleglejszych częściach świata, jednocześnie jest zupełnie nieświadom tego, co dzieje się w jego najbliższym otoczeniu i nie zauważa swojej pogłębiającej się samotności[35]. Maria Nowina Konopka stwierdza zaś, iż „obecne wspólnoty to efemerydy, w których komunikacja wewnątrzgrupowa nie przeważa nad wymianą informacji i nie odgrywa roli integratora"[36]. Nie da się jednak

[30] S. Juszczyk, *Człowiek w świecie elektronicznych mediów – szanse i zagrożenia*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2000, s. 95 i nast.

[31] Ibidem, s. 109.

[32] M. Nowina Konopka, *Społeczeństwo…, op. cit.*, s. 183.

[33] L. W. Zacher, *Zagrożenia…, op. cit.*, s. 175176.

[34] Ibidem.

[35] S. Juszczyk, *Człowiek…, op. cit.*, s. 73.

[36] M. Nowina Konopka, *Społeczeństwo…, op. cit.*, s. 190.

w dłuższej perspektywie uciec przed tym procesem poprzez odrzucenie nowych sposobów komunikowania. Doprowadziłoby to człowieka jedynie do alienacji od bardzo dużej i stale rosnącej części społeczeństwa z nich korzystających, nie dając w zamian nic, gdyż tradycyjne sposoby komunikowania są coraz mocniej wypierane przez nowe, w związku z czym grupa osób korzystających jedynie bądź głównie z nich z biegiem czasu będzie się coraz bardziej kurczyć.

Prowadzi to do rozwoju takich negatywnych zjawisk, jak napięcia narastające przy intensyfikacji komunikacji, wzrost dywersyfikacji społecznej oraz rosnący dystans społeczny i kulturowy między grupami społecznymi. Należy jednak zaznaczyć, iż wprowadzanie nowych środków komunikacji może zaostrzyć lub złagodzić problemy związane z zachodzącymi w społeczeństwie zmianami, w zależności od tego, w jaki sposób następuje wprowadzenie multimediów i ich rozwój. W zależności od tego mogą one przyczynić się do zintensyfikowania zagrożeń bądź stać się narzędziem umożliwiającym stawienie im czoła. Jednak, jak konstatuje Josep Llampayas, utrzymanie dobrobytu i szans dalszego wzrostu kulturowego i ekonomicznego zależy w znacznej mierze od szybkości wprowadzenia zasobów multimedialnych oraz od skuteczności i masowości ich zastosowań[37].

Wszystko to jednak godzi bezpośrednio w wolność jednostki, zwłaszcza przez kreowanie przymusu społecznego za pomocą lansowania wzorów kulturowych, konsumpcyjnego sposobu życia i zunifikowanych form rozrywki oraz narzucania sposobów komunikowania, pod groźbą wykluczenia społecznego.

Uzależnienia

Wraz z rozwojem technicznym postępuje rozwój różnego rodzaju patologii, wśród których uzależnienia stanowią pokaźna grupę. Internet a także telewizja posiadają status „złodziei czasu", jednak, o ile podczas oglądania telewizji można wykonywać inne czynności, to Internet na to nie pozwala. Uzależnienie od Internetu czy telewizji są przejawami szerszego zjawiska, jakim jest uzależnienie od technologii cyfrowych w ogóle.

Uzależnienie od Internetu, polegające na wielogodzinnym spędzaniu czasu przed komputerem na ogół objawia się w:

- Zmianie rytmu dnia i pory snu,
- Problemach w szkole/pracy,
- Wycofaniu z relacji interpersonalnych,
- Porzuceniu dotychczasowych zainteresowań,
- Utracie łaknienia i zaniedbaniach dotyczących higieny osobistej,
- Poczuciu niepokoju, irytacji podczas prób zaprzestania korzystania z Internetu,
- Braku posłuszeństwa,
- Poczuciu „pochłonięcia" przez Internet,
- Potrzebie wydłużenia czasu spędzanego przy Internecie,
- Utracie kontroli nad korzystaniem z Internetu,
- Traktowaniu Internetu jako ucieczki od problemów codziennych,
- Okłamywaniu bliskich w celu ukrycia swego zaangażowania w Internet,
- Popadaniu w depresję, uczucie lęku, bezradności itp. w czasie spędzanym poza Internetem[38].

[37] Josep B. Llampayas, *Skutki kulturowe nowych środków multimedialnych*, [w:] *Rewolucja informacyjna i społeczeństwo*, (red. L. Zacher), Warszawa 1997, s. 160-161.

[38] M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne,* PWN, Warszawa 2008, s. 150-151.

W skrajnej postaci uzależnienie polega na całkowitym wycofaniu się z realnego świata. Badacze twierdzą, że wszystko to, co bezpiecznie, co szybko i w dużym stopniu zaspokaja przynajmniej podstawowe potrzeby człowieka, uzależnia. Tłumaczy to skalę uzależnień od Internetu – medium zapewniającego anonimowość, możliwość samorealizacji i łatwy kontakt z drugim człowiekiem[39].

„Uzależnienie od Internetu, mimo wielu podobieństw do innych uzależnień dotyczących zarówno przyczyn ich powstania, jak i symptomów, różni się od innych tym, że jego nieodłączną częścią jest kontakt z innymi ludźmi. Specyficzny charakter tych kontaktów sprawia, że – paradoksalnie – w sieci najintensywniej udzielają się towarzysko introwertycy, osoby chorobliwie wręcz nieśmiałe, zagubione, niedowartościowanie, o niskim statusie społecznym. Osoby o takich cechach również najczęściej uzależniają się od Internetu"[40]. Jednostki takie często zdają sobie sprawę ze swoich problemów i najczęściej szukają pomocy w Internecie. Korzystają z dostępnych testów diagnostycznych, porad psychologów, grup terapeutycznych, odpowiednich forów i grup wsparcia. Jednak nie zawsze pozyskane w ten sposób informacje są wiarygodne, często mają pseudonaukowy charakter. Ponadto zazwyczaj nie zwraca się w nich uwagi na niezwykle istotny czynnik, jakim jest okres, w którym symptomy uzależnienia występują. Podstawą do uznawania osoby za uzależnioną jest występowanie objawów przez minimum 12 miesięcy. Wiele przypadków uzależnień zdiagnozowanych przez internetowych specjalistów mija po pewnym czasie i przekształca się z powrotem w nieszkodliwe hobby.

Rozwój nierówności w społeczeństwie

Bardzo istotnym zagrożeniem wolności są pogłębiające się nierówności w społeczeństwie, warunkowane przez tworzenie się i funkcjonowanie społeczeństwa informacyjnego oraz rozwój technologii informacyjnych. Marian Golka przytacza za Paulem DiMaggio i współautorami następującą definicję „cyfrowych nierówności": „nierówność w dostępie do Internetu, intensywności jego wykorzystania, wiedzy o sposobach szukania informacji, jakości podłączenia i wsparcia społecznego, pomagającego w korzystaniu z Internetu, a także nierówności w zdolności do oceny jakości informacji i różnorodności wykorzystania sieci"[41]. Definicję tę można śmiało rozszerzyć na inne nowe media i technologie informacyjne.

Rozwój społeczeństw informacyjnych, wbrew początkowym optymistycznym założeniom, nie przyczynia się do wytworzenia egalitarnych struktur społecznych, ale przeciwnie, do zwiększenia się różnic, kreując nieznane dotąd narzędzia tworzenia nowych ich obszarów. Krystyna Doktorowicz[42] podaje tu takie kategorie jak: *informacyjnie biedni* i *informacyjnie bogaci*, *informacyjnie wyedukowani* i *informatyczni analfabeci*. Za Rayem Thomasem przytacza cztery czynniki warunkujące pogłębianie się istniejących i tworzenie nowych nierówności w społeczeństwie informacyjnym:

1. Technologie informacyjne są produktem kapitalizmu i jako takie są przedmiotem obrotu rynkowego, natomiast nie stosuje się ich do realizacji utopii społeczeństwa egalitarnego.

[39] Ibidem.

[40] A. Czajkowska, *Internetoholizm*, [w:] *W cyberprzestrzeni* (red. W. Godzic), RaBID, Kraków 1999, s. 53.

[41] M. Golka, *Bariery…*, *op. cit.*, s. 138.

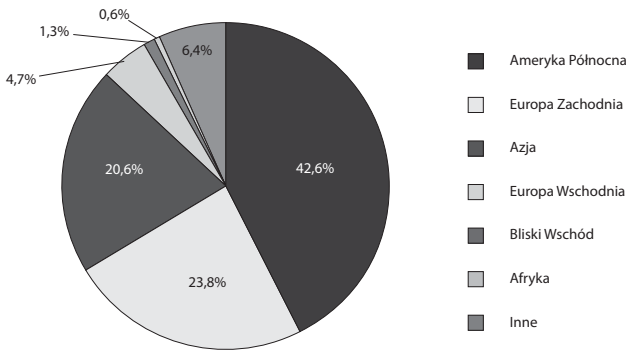
[42] K. Doktorowicz, *Społeczeństwo informacyjne – podziały i nierówności,* [w:] *Rewolucja informacyjna i społeczeństwo* (red. L. W. Zacher), Warszawa 1997, s. 296.

2. Tempo rozwoju technologii informacyjnych wskazuje na to, że społeczna i kulturalna luka między różnymi poziomami ich zastosowania będzie się powiększała, w szczególności między tymi, którzy mają do tych technologii dostęp, a tymi, którzy go nie posiadają.
3. Nowe technologie informacyjne będą budowane ponad już istniejącymi, co oznacza, że ubodzy staną się jeszcze biedniejsi, ponieważ nie będzie ich stać na ciągłą przebudowę stale modernizującej się infrastruktury, zaś bogaci, nadążający za zmianami będą jeszcze bogatsi.
4. Społeczeństwa zamożniejsze i lepiej wykształcone są lepiej od społeczeństw ubogich przystosowane do wykorzystania technologii informacyjnych.

Proces wzrostu rozwarstwienia jest dodatkowo wspomagany przez istnienie monopolu wielkich korporacji z najbogatszych krajów świata, takich jak Microsoft, Apple czy IBM, w dziedzinie rozwoju technologii informacyjnych, które narzucają standardy technologiczne. Kolejnym czynnikiem jest duże, stale zwiększające się tempo tego rozwoju sprawiające, że rozwiązania technologiczne bardzo szybko starzeją się i są zastępowane przez nowe, zanim jeszcze społeczeństwom i jednostkom biedniejszym udało się je przyswoić i wdrożyć. Z tego powodu muszą być one permanentnie zacofane i stan ten stale się pogłębia.

Sytuacja ta znajduje odbicie w przytaczanych przez Mariana Golkę danych odnośnie różnic w dostępie do Internetu między kontynentami. W 2000 roku 42,6% użytkowników sieci pochodziło z Ameryki Północnej, 23,8% z Europy Zachodniej, 20,6% z Azji, 4,7% z Europy Wschodniej, 1,3% z Bliskiego Wschodu i jedynie 0,6% z Afryki. Dostęp do Internetu w połowie 2005 roku miało ok. 65% populacji Ameryki Północnej, ok. 52% Europy Zachodniej i ok. 44% populacji Azji[43]. W Polsce w tym samym czasie było to 30%, podczas gdy w 2007 roku 41%[44]. W czerwcu 2009 roku ponad 50% polskich gospodarstw domowych posiadało szerokopasmowy dostęp do Internetu[45].

Wykres 1. Miejsce pochodzenia użytkowników internetu w 2000 roku.



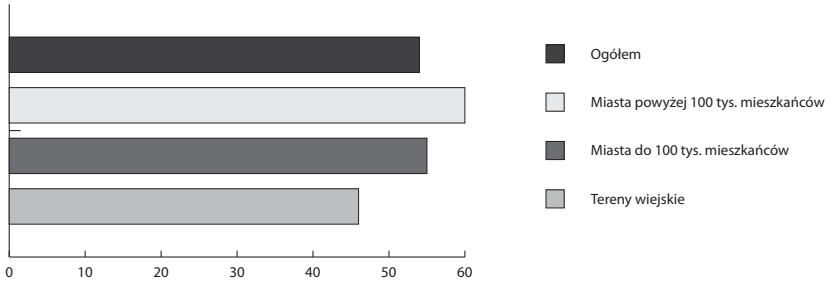
[43] M. Golka, *Bariery…, op. cit.*, s. 138.

[44] Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce. Wyniki badań statystycznych z lat 20042007*, Warszawa 2008, s. 61, http://www.stat.gov.pl/cps/rde/xbcr/gus/PUBL_NTS_spoleczenstwo_informacyjne_w_Polsce_2004_2007.pdf, z dnia 10.01.2010.

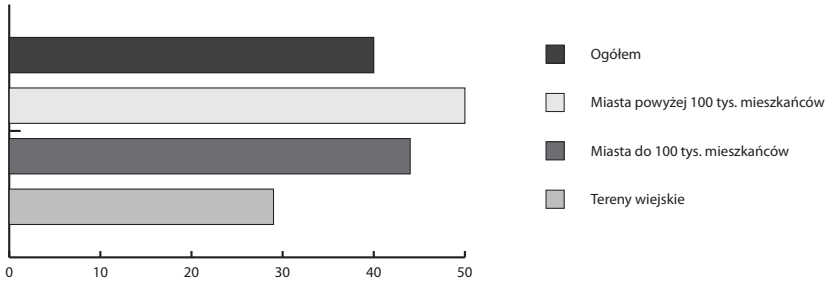
[45] Urząd Komunikacji Elektronicznej, *Zmiany na rynku usług szerokopasmowych, czerwiec 2008 – czerwiec 2009*, http://www.uke.gov.pl/uke/index.jsp?place=Lead02&news_cat_id=19&news_id=4943&layout=1&page=text, z dnia 10.01.2010.

Różnice widać również przy porównaniu możliwości dostępu do Internetu w dużych miastach, małych miastach i na wsiach. Dla przykładu w Polsce w 2007 roku w komputery wyposażone było 54% gospodarstw domowych, przy czym w dużych miastach (powyżej 100 tys. mieszkańców) było to 60%, w mniejszych miastach (do 100 tys. mieszkańców) 55%, a na obszarach wiejskich 46%[46]. W tym samym roku dostęp do Internetu posiadało 41% gospodarstw domowych w naszym kraju – w dużych miastach 50%, w mniejszych miastach 44%, a na obszarach wiejskich 29%[47]. Różnice występują również między poszczególnymi województwami, powiatami, a nawet dzielnicami w obrębie miast. Tomasz GobanKlas uważa, iż taki stan rzecz prowadzi do „upośledzenia", zwłaszcza dzieci z obszarów mniej rozwiniętych, co poważnie ogranicza szanse rozwoju tych regionów[48].

Wykres 2. Gospodarstwa domowe wyposażone w komputery w Polsce w 2007 roku.



Wykres 3. Gospodarstwa domowe z dostępem do internetu w Polsce w 2007 roku.



Bardzo poważnym ograniczeniem wolności, powodującym zróżnicowanie w dostępie do informacji i możliwości komunikowania jest dominacja kulturowa języka angielskiego i alfabetu łacińskiego, widoczna zwłaszcza w Internecie, o czym pisze Marian Golka[49]. Według podanych przez niego danych obecnie 31% użytkowników sieci używa języka angielskiego, a na drugim miejscu jest chiński – 16%. Tymczasem spośród niecałych 6,8 miliarda ludzi żyjących obecnie na świecie[50] jako pierwszego języka chińskiego używa ok. 1,2 miliarda, a angielskiego ok. 328 miliony i został on o milion wyprzedzony przez ję-

[46] Główny Urząd Statystyczny, *Społeczeństwo…, op. cit.*, s. 53, http://www.stat.gov.pl/cps/rde/xbcr/gus/PUBL_NTS_spoleczenstwo_informacyjne_w_Polsce_2004_2007.pdf, z dnia 10.01.2010.

[47] Główny Urząd Statystyczny, *Społeczeństwo…, op. cit.*, s. 61, http://www.stat.gov.pl/cps/rde/xbcr/gus/PUBL_NTS_spoleczenstwo_informacyjne_w_Polsce_2004_2007.pdf, z dnia 10.01.2010.

[48] T. GobanKlas, *Cywilizacja…, op. cit.*, s. 226.

[49] M. Golka, *Bariery…, op. cit.*, s. 139.

[50] Dane U.S. Census Bureau, http://www.census.gov/ipc/www/popclockworld.html, z dnia 10.01.2010.

zyk hiszpański[51]. Uznaje się, że ¾ stron internetowych jest sformułowana w języku angielskim. Przez wiele lat brakowało klawiatur z oznaczeniami innymi niż łacińskie, choć obecnie coraz częściej się pojawiają. Tymczasem na świecie istnieje prawie sześć tysięcy języków, ale jedynie około sto kilkadziesiąt posiada swoje pismo i swoją literaturę. Pismo zresztą często jest niealfabetyczne (oparte na piktogramach lub ideogramach) albo alfabet wzorowany jest na łacińskim, z lepszym lub gorszym skutkiem. Wszystko to sprawia, że większość ludzkości nie ma możliwości korzystania z ogromnej części zasobów Internetu, z uwagi na brak kompetencji językowych.

Następnym zagrożeniem jest pojawienie się tzw. „analfabetyzmu komputerowego". Tomasz GobanKlas analizując je, stwierdza, iż obsługa nowych mediów jest dużo trudniejsza niż tradycyjnych i wymaga o wiele większych kompetencji, stąd jedynie niektórzy są w stanie je w pełni wykorzystać[52]. Powoduje to narastanie różnic społecznych, szczególnie co do poziomu poinformowania. Ci, którzy sobie nie radzą z obsługą nowoczesnych urządzeń i nie potrafią wykorzystywać nowoczesnych technologii, mają ograniczone możliwości dostępu do informacji i w ogóle uczestnictwa w życiu społeczeństwa informacyjnego. Jak pisze Maria Nowina Konopka, „funkcjonowanie w społeczeństwie informacyjnym generuje stałą konieczność podnoszenia poziomu własnych kompetencji"[53]. Do tego autorka zauważa, iż nie wystarczy zdobycie informacji, gdyż te nie są równoznaczne z wiedzą. Do przekształcenia jednych w drugą potrzeba „procesu myślowego, refleksji ukierunkowanej na możliwości weryfikacji i przetworzenia. Informacja nie stanowi potencjału człowieka, który nie potrafi jej wykorzysta, spożytkować. Jedynie umiejętności połączenia wielu różnych danych, wykorzystanie ich w codziennym życiu, skonfrontowanie z innego rodzaju informacjami umożliwia zaklasyfikowanie danej informacji jako tej, która poszerza wiedzę jej posiadacza"[54]. Za Umberto Eco przytacza podział struktury społeczeństwa na trzy klasy:

- najniższą – do której przynależą osoby niepotrafiące posługiwać się komputerem, a więc nastawione na korzystanie z informacji w sposób bierny,
- średnią – składającą się z osób korzystających na co dzień z sieci komputerowej, ale niemających umiejętności programistycznych,
- najwyższą – stanowiącą zbiór osób, które opanowały umiejętność współpracy z komputerem i pełnego korzystania z jego możliwości, potrafią więc nie tylko odbierać informacje i korzystać z nich, ale także je tworzyć[55].

Oczywistą jest tu konstatacja, że ludzie należący do klasy najniższej będą wraz z rozwojem społeczeństwa informacyjnego coraz bardziej nieprzystosowani we wszystkich dziedzinach życia, zwłaszcza zaś jeśli chodzi o dostęp do informacji i konkurencyjność na rynku pracy, co w konsekwencji będzie prowadziło do wykluczenia. Jednocześnie wzrastać będzie uprzywilejowanie klasy najwyższej, której członkowie wieść będą prym w społeczeństwie. Można zaryzykować tezę, iż brak umiejętności korzystania z komputera i nowoczesnych technologii będzie w XXI wieku bardziej dotkliwy niż brak umiejętności czytania i pisania w wieku XX.

Zasygnalizowane tutaj ważkie problemy związane z nierównościami w dostępie do informacji i nowych technologii oraz z umiejętnościami ich wykorzystania, stawiają pod du-

---

[51] *Ethnologue: Languages of the World* (red. M. Paul Lewis), Dallas 2009, http://www.ethnologue.org/ethno_docs/distribution.asp?by=size, z dnia 10.01.2010.

[52] T. GobanKlas, *Cywilizacja…, op. cit.*, s. 259260.

[53] M. Nowina Konopka, *Społeczeństwo…, op. cit.,* s. 184.

[54] *Ibidem*.

[55] Ibidem, s. 185.

żym znakiem zapytania zarówno wolność jednostki do swobodnego dostępu do informacji i uczestniczenia w życiu społeczeństwa informacyjnego, jak i wolność od narzucania jej dominującej kultury, języka czy standardu technologicznego. Jeśli nie będzie się im przeciwdziałać, to oba te obszary wolności będą poważnie zagrożone.

Manipulowanie informacją

Ostatnią grupą zagrożeń dla wolności jednostki są problemy związane z wolnym, swobodnym dostępem do rzetelnej, prawdziwej informacji. Sposób działania mediów w społeczeństwie informacyjnym powoduje wystąpienie dużych wątpliwości, co do tego czy rzeczywiście otrzymywane z mediów informacje są rzetelne, czy też jesteśmy za ich pośrednictwem manipulowani.

Marian Golka stawia tezę, iż współcześnie „mamy do czynienia z niedoinformowaniem, przeinformowaniem albo z informowaniem o sprawach nieważnych i drugorzędnych czy wręcz szkodliwych, jak również ze świadomym dezinformowaniem – czyli kłamstwem lub manipulowaniem”[56]. Za Herbertem Schillerem podaje sposoby manipulowania przez media amerykańskie, polegające na stwarzaniu:

- mitu indywidualizmu i osobistego wyboru,
- mitu neutralności mediów w podawaniu informacji,
- mitu niezmienności natury ludzkiej w kwestii informacji, których rzekomo człowiek potrzebuje,
- mitu braku konfliktu społecznego,
- mitu pluralizmu środków komunikowania[57].

Z kolei Stanisław Juszczyk przytacza za Adamem Lepą najczęściej stosowane sposoby manipulowania za pomocą następujących rodzajów informacji:

- Opatrywanie informacji, które powinny być bezstronne, komentarzem redakcyjnym,
- Podawanie informacji niepełnych lub usunięcie fragmentu informacji,
- Podawanie informacji nieprawdziwych,
- Podawanie informacji wieloznacznych, by utrudnić ich zrozumienie,
- Podawanie informacji mało istotnych jako pierwszych, co sugeruje ich ważność,
- Podawanie informacji ważnych jako informacji bez znaczenia,
- Narzucanie punktowego spojrzenia na problemy, niepokazywanie ich w całościowym wymiarze,
- Przekazywanie informacji w nadmiarze, w celu spowodowania dezinformacyjnego chaosu[58].

Dalej stwierdza on, iż każdego dnia jesteśmy zalewani potokiem różnych informacji, jednak ich pozorna różnorodność jest często złudzeniem wywołanym przez ich obfitość, co stwarza iluzję wolnego wyboru informacji, ponieważ pozornie docierają one do nas z wielu źródeł. Celem socjotechnicznego działania jest tu właśnie wywołanie wrażenia, że skoro wszystkie media przekazują to samo i tak samo, to znaczy, że jest to prawda, w myśl zasady, że kłamstwo powtarzane tysiąc razy staje się prawdą. Powszechny zalew informacjami działa unifikująco na sposób myślenia ludzi, na czym bazują mass media wykorzystując skłonność do zachowań stadnych, uczestniczenia w grupie większościowej i myślenia

[56] M. Golka, *Bariery…, op. cit*., s. 112.

[57] Ibidem, s. 122.

[58] S. Juszczyk, *Człowiek…, op. cit*., s. 66.

w kategoriach: „rację ma większość". Dzięki temu można sterować ludźmi za pomocą presji tzw. opinii publicznej.

System manipulowania opiera się głównie na selekcji informacji i przypisywaniu im odpowiedniej ważności, przez co nawet jeśli nie uda się narzucić odbiorcy sposobu myślenia o danym fakcie, to zwykle przynajmniej można go skłonić, by myślał właśnie o danym fakcie, a nie o innym, zgodnie z teorią agendasetting. Wykorzystuje się tu efekty pierwszeństwa przekazu informacji (tę, którą poznamy pierwszą, uznajemy za prawdziwą oraz podstawową i do niej odnosimy inne, otrzymane później), lub odwrotny efekt końca/świeżości (najlepiej pamiętamy to, co dotarło do nas jako ostatnie, więc na tym się opieramy).

Mass media, a zwłaszcza telewizja, ze względu na ich siłę perswazyjną, powszechność oraz atrakcyjność wizualnego przekazu, kreują „nierzeczywistą rzeczywistość"[59] – fikcyjny świat medialny. To nieustanna inscenizacja i reżyseria (nawet, gdy mamy do czynienia z przekazami „na żywo") to upolitycznienie i ideologizacja. Niebezpieczeństwo polega na tym, iż dla wielu ten wyreżyserowany świat staje się realnym, którego problemami żyją. W wyniku sprzężenia zwrotnego zaczynają wierzyć, że najważniejsze rzeczywiście jest to, co np. powiedział Kuba Wojewódzki w ostatnim odcinku „Mam talent!". A stąd już tylko mały krok do „społecznego zidiocenia".

Jedyną formą obrony przed manipulacją jest weryfikowanie podawanych nam informacji w oparciu o inne, pochodzące z alternatywnych, zaufanych źródeł. Tu jednak stajemy wobec sytuacji, że dowolne informacje pochodzące ze środków masowego przekazu (bądź innych), w tym te mające za zadanie prostować inne informacje, również mogą być zmanipulowane, choć niekoniecznie w ten sam sposób, przez tę samą grupę interesów. Oznacza to, że właściwie nigdy nie możemy być do końca pewni czy informacja, którą posiedliśmy, jest prawdziwa. Sytuację dodatkowo utrudnia fakt, iż sami dziennikarze, mimo iż zobowiązani wymogami prawa i etyki zawodowej do zachowywania najwyższej staranności i rzetelności przy gromadzeniu faktów, częstokroć z różnych powodów (brak czasu, brak możliwości, lenistwo) zaniedbują ich weryfikację i mało przejmują się wiarygodnością. Dobrze ilustruje to cytowana przez Mariana Golkę wypowiedź Ryszarda Kapuścińskiego: „dziennikarstwo bardziej przypomina dziś działalność rozrywkową niż informacyjną. Informuje się o wydarzeniach, nie dochodząc jednocześnie do ich źródeł, do prawdziwych przyczyn. Nawet te wiadomości o bieżących wydarzeniach, wyrwane są z szerszego kontekstu. A wydarzenie wyrwane z szerszego kontekstu może mieć zupełnie inną wymowę i znaczenie niż ma w rzeczywistości. W ten sposób, zamiast informować, dziennikarze wprowadzają w błąd"[60]. Jedynym pewnym sposobem na weryfikację, jaki autor znajduje, jest więc bezpośrednia, osobista obserwacja, co jednak od dawna jest niemożliwe, bo dawno wyszliśmy poza horyzont lokalny i życie we wspólnocie[61].

Bardzo istotny jest tu również problem pluralizmu mediów, który w dobie zaawansowanej koncentracji na rynkach medialnych jest często mocno ograniczony lub wręcz pozorny. Wielkie koncerny medialne (Murdocha, Blacka, Turnera, Bertelsmanna, Marinho, Berlusconiego lub w warunkach polskich „Agora"[62]) kontrolują jednocześnie wiele tytułów prasowych, stacji radiowych, telewizyjnych oraz witryn internetowych i mają bezpośredni wpływ na informacje w nich podawane. Często profile poszczególnych mediów znajdujących się posiadaniu danego koncernu się od siebie różnią, nawet diametralnie, więc przeciętny odbiorca nie ma w świadomości faktu, iż w istocie należą do jednego wydawcy

[59] L. W. Zacher, *Telewizja…*, *op. cit*., s. 128.

[60] M. Golka, *Bariery…, op. cit*., s. 115

[61] Ibidem, s. 118.

[62] Ibidem, s. 116.

i mogą realizować jedną, określoną politykę informacyjną. Potęguje to fałszywe wrażenie pluralizmu rzekomo niezależnych od siebie źródeł informacji, jakie do nas docierają.

Zakończenie

Wolność jest wartością przyrodzoną człowiekowi. Jej ograniczanie lub odbieranie jest równoznaczne z łamaniem najbardziej fundamentalnych z praw człowieka, wyrażonych w aktach prawa m. in. „Deklaracji Praw Człowieka i Obywatela" z 26 sierpnia 1789 roku, „Powszechnej Deklaracji Praw Człowieka" z 10 grudnia 1948 roku. Niestety, w dobie zaawansowanego rozwoju technologii komunikacyjnych i społeczeństwa informacyjnego, zdarza się, iż te podstawowe prawa są naruszane bądź łamane. Współczesna technika częstokroć umożliwia oraz ułatwia ten proceder, zarówno osobom prywatnym, jak i korporacjom. Również organy władzy państwowej, które w systemie demokracji liberalnej powinny reprezentować interesy obywateli, gwarantować ich prawa i być wzorem działalności dla innych podmiotów, nieraz wykorzystują dostępne rozwiązania technologiczne do nieuprawnionego inwigilowania obywateli. Poprzez niedbalstwo lub złą wolę urzędników dopuszczają do wycieków ważnych danych osobowych. W dodatku, z uwagi na tempo rozwoju technologicznego, prawodawcy nie nadążają z tworzeniem uregulowań odpowiadających rzeczywistości i zapewniających ochronę podstawowych praw, takich jak wolność.

Systemy prawne społeczeństw informacyjnych muszą zmierzać do pogodzenia racji obywatela i państwa. Poza tym konieczne jest wypracowanie takich nowych, oddolnych mechanizmów społecznych, by podstawowe prawa człowieka były respektowane i gwarantowane w tej nowej rzeczywistości. Nie jest możliwym wprawdzie osiągnięcie pełnej harmonii, ale należy intensyfikować starania. W innym przypadku grozi nam to, iż mimo niewątpliwych zdobyczy społeczeństwa informacyjnego, zaprzepaszczona zostanie ogromna część dotychczasowego dorobku ludzkości.