BRONISŁAW SITEK
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide de Gasperi w Józefowie
bronislaw.sitek@gmail.com

ZASADY ETYCZNE STOSOWANE W CYBERPRZESTRZENI

ETHICAL PRINCIPLES APPLIED IN CYBERSPACE

ABSTRACT

Cyberspace is a global phenomenon and is not controlled by any country or international body. The lack of control does not mean anarchy. Hence, the Internet regulations as well as the ethical principles adapted to cyberspace, which is composed of the technologies and network, are developed. For each of these areas similarly, although a different ethical principles were constructed. The codes of ethics were developed for information technology. And for the networks, that means for ordinary users, a specific ethical Decalogue were created. The construction of ethical norms for cyberspace is an important task that requires deep thought.

Keywords: *information technology, networks, Internet law, ethics, cyberspace*

STRESZCZENIE

Cyberprzestrzeń ma charakter globalny i nie jest kontrolowana przez jakiekolwiek państwo bądź instytucję międzynarodową. Brak kontroli nie oznacza jednak anarchii. Stąd rozwija się prawo internetowe, a także zasady etyczne dostosowane do cyberprzestrzeni, na którą składają się technologie i sieci informatyczne. Dla każdego z tych obszarów zbudowano podobne, chociaż też różniące się zasady etyczne. Dla technologii informacyjnych stworzono kodeksy etyczne. Z kolei dla sieci informatycznych, czyli dla zwykłych użytkowników, stworzono swoisty dekalog etyczny. Budowa norm etycznych dla cyberprzestrzeni jest ważnym zadaniem, wymagającym głębokiego przemyślenia.

Słowa kluczowe: *technologie informatyczne, sieci informatyczne, prawo internetowe, etyka, cyberprzestrzeń*

WPROWADZENIE

Rozwój nowych technologii, zwłaszcza w obszarze informatycznym, wymaga dość pogłębionej refleksji nad celami nowych badań, a także nad granicą, której człowiek nie powinien przekraczać. Ta wstępna uwaga ma swój sens w świetle tego, że współczesne badania w dużej mierze są inspirowane (i finansowane) potrzebami ekonomicznymi czy po prostu inwestycjami kapitałowymi, które chcą w ten sposób zwiększyć swój stan posiadania. Jeszcze 100 lat temu badania naukowe były inspirowane głównie potrzebą rozwiązania istotnych problemów człowieka bądź społeczeństwa. W tym właśnie duchu należy widzieć badania takich naukowców, jak L. Pasteur (wynalazca szczepionki na wściekliznę), A. Fleming oraz H.W. Florey i E.B. Chain (odkrycie penicyliny) oraz F.G. Banting (odkrycie insuliny). Człowiek czuł się odtwórcą czy badaczem praw, które istniały w naturze, przykładem czego jest I. Newton, który odkrył – a nie stworzył – zasady dynamiki, oraz A. Einstein, który zbudował słynną teorię względności. Naukowcy aż do przełomu XIX i XX wieku starali się naturę odkrywać bądź poprawiać, zwłaszcza w obszarze zdrowia człowieka, nie zaś tworzyć nową rzeczywistość.

Wyniki badań naukowych tamtego okresu najczęściej nie wzbudzały obaw społecznych co do ich zgodności z moralnością czy szeroko rozumianą etyką. To nastawienie do badań naukowych, postępu i rozwoju nowych technologii oraz technik zmieniło się wraz z technologiami zaawansowanymi. Człowiek nie zajmuje się już odkrywaniem praw natury bądź też jej poprawianiem, lecz tworzeniem nowej rzeczywistości. Kończy się pewna epoka oparta na biblijnym nakazie czynienia sobie ziemi poddaną (Rdz. 1,28). W tej koncepcji człowiek miał być tylko użytkownikiem ziemi, miał prawo do korzystania z niej i pobierania pożytków. Nie jest jednak kreatorem, jest nim bowiem Bóg. Nowa epoka charakteryzuje się tym, że człowiek przechodzi od roli użytkownika do roli twórcy. Taka zmiana podejścia człowieka do materii ożywionej i nieożywionej jest możliwa właśnie dzięki zaawansowanym technologiom, zwłaszcza w obszarze technologii informatycznych. Pozwalają one na stworzenie nowej wirtualnej rzeczywistości, która z jednej strony głęboko przenika dotychczasowe życie jednostki i społeczeństwa, z drugiej zaś daje nowe, dotychczas niespotykane możliwości.

Przedmiotem niniejszego opracowania jest analiza treści zasad etycznych, jakie już funkcjonują w cyberprzestrzeni. Jest to bowiem rzeczywi-

stość globalna i rozproszona jednocześnie, trudna do skontrolowania. Chociaż podejmowane są w tym zakresie liczne próby. Między innymi Rosja, Chiny, a także ostatnio i Unia Europejska ustami komisarz E. Bieńkowskiej zapowiedziały stworzenie własnych systemów satelitarnych (GPS). Poza zapowiedziami, jak na razie nie udało się żadnemu państwu wprowadzić kontroli nad funkcjonowaniem cyberprzestrzeni.

W tej perspektywie jawi się jedyna możliwość, tj. formułowanie zasad odpowiedzialnej etyki, którą winni posługiwać się tak twórcy poszczególnych elementów cyberprzestrzeni, jak i użytkownicy poszczególnych instrumentów cyberprzestrzeni. Można powiedzieć, że normy etyczne są jednym z instrumentów, które pozwolą na jej uporządkowanie.

POJĘCIE CYBERPRZESTRZENI

Jednym z pojęć, które w ostatnich czasach zdobyło największą popularność, jest słowo „cyberprzestrzeń". Jednocześnie dla przeciętnego człowieka to pojęcie owiane jest nimbem tajemniczości. Niewiele osób zapytanych na ulicy o jego znaczenie byłoby w stanie je zdefiniować. Tymczasem można zaleźć liczne definicje tego pojęcia w profesjonalnym piśmiennictwie, w politykach sektorowych poszczególnych państw, korporacji oraz organizacji międzynarodowych, a także w aktach normatywnych krajowych, unijnych i międzynarodowych.

Twórcą pojęcia „cyberprzestrzeń" (*cyberspace*) jest William Gibson, który w 1982 roku użył go po raz pierwszy w powieści pt. „Burning Chrom". W powieści pt. „Neuromancer" zaprosił czytelników do cyberprzestrzeni, którą określał jako halucynacja doświadczana każdego dnia przez miliardy uczestników we wszystkich krajach. Cyberprzestrzeń według niego to graficzne odwzorowanie danych pobieranych z dysków wszystkich komputerów świata (zob. J. Wasilewski, s. 226).

Pojęcie „cyberprzestrzeń" jest pochodną wcześniej używanego terminu „cybernetyka" (*cybernetics*). Po raz pierwszy termin ten został sformułowany przez Norberta Wienera w 1948 roku. Według niego zadaniem cybernetyki było zbudowanie komunikacji pomiędzy światem ożywionym, zwłaszcza zwierząt, do których zaliczał człowieka, a światem maszyn. W ten sposób powstało nowe środowisko składające się z inteligentnych istot żywych i maszyn. Oba światy wzajemnie się przenikają i nie są rozdzielne (zob. J. Wasilewski, s. 226).

Dalszy rozwój koncepcji cyberprzestrzeni powiązany był z progresem technologii teleinformatycznych, służących do zwiększenia efektywności komunikacji w wielu obszarach życia, zwłaszcza w wojsku, w służbach specjalnych, w administracji publicznej oraz w wielkich korporacjach. Powstałe urządzenia teleinformatyczne stały się częścią państwowej, a także korporacyjnej infrastruktury krytycznej. Istotnym elementem tej infrastruktury stały się komputery i sieci, które służyły nie tylko do przekazywania informacji, ale również do zawierania czynności cywilnoprawnych, podejmowania decyzji administracyjnych, gromadzenia bądź archiwizowania danych (bazy danych). Negatywną stroną nowej przestrzeni aktywności człowieka było stworzenie nowych form przestępczości (zob. J. Wasilewski, s. 226; odnośnie do cyberprzestępczości zob. J. Wójcik, s. 99–116).

Według K. Dobrzenieckiego cyberprzestrzeń jest rodzajem kontrolowanego chaosu. Nie ma właściciela ani jednego centralnego ośrodka decyzyjnego. Pomimo tych ujemnych cech rzeczywistość ta funkcjonuje i szybko się rozwija. Próba podporządkowania cyberprzestrzeni przepisom praw napotyka opór wirtualnej społeczności oraz przeszkody natury technicznej, raczej trudne do przezwyciężenia. Stąd rodzą się pytania, w szczególności o relację twórców i użytkowników wirtualnej rzeczywistości do przepisów prawa, zasad etycznych czy obyczajności. Rodzi się bowiem nowy wymiar wolności i praw jednostki, który wymyka się spod klasycznych ograniczeń, jakie istnieją w świecie realnym (K. Dobrzeniecki, s. 15 i nast.).

Pojęcie „cyberprzestrzeń" definiowane jest w licznych dokumentach zawierających wytyczne dla polityki państwa. I tak, w „Rządowym programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016"[1] pojęcie to zostało zdefiniowane w następujący sposób: „Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Dodatkowo zaś zostało zdefiniowane pojęcie „cyberprzestrzeń RP", przez które rozumie się „cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe)".

[1] Tekst Programu znajduje się na stronie internetowej: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [data dostępu: 3.11.2016].

Z kolei w ekspertyzie dotyczącej rekomendowanego, optymalnego strategicznego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, opracowanej przez NASK na zlecenie Ministerstwa Administracji i Cyfryzacji, przez cyberprzestrzeń rozumie się przestrzeń, którą tworzą urządzenia i programy informatyczne komunikujące się pomiędzy sobą i z użytkownikami[2].

W kolejnym dokumencie – „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej" – przyjętym przez rząd Polski w 2015 roku cyberprzestrzeń zdefiniowano jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami"[3].

Ustawowa zaś definicja cyberprzestrzeni znajduje się w art. 2.1b ustawy z 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. 2002 nr 156 poz. 1301). Według tej ustawy przez cyberprzestrzeń „[...] rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2014 r. poz. 1114), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami".

Polskie definicje nie obiegają od tych, które stosuje się w doktrynie bądź polityce chociażby USA. Departament Obrony USA tak zdefiniował pojęcie „cyberprzestrzeń": jest to „globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę

[2] Tekst ekspertyzy pt. *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa, wrzesień 2015, znajduje się pod adresem internetowym: https://mac.gov.pl/files/nask_rekomendacja.pdf [data dostępu: 3.11.2016].

[3] Dokument znajduje się na stronie internetowej BBN pod adresem: https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [data dostępu: 4.11.2016].

technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery" (zob. J. Wasileski, s. 227).

Ciekawostką jest to, że pojęcie „cyberprzestrzeń" nie zostało zdefiniowane w „Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" z 2013 roku[4]. Komisja przyjmuje znaczenie tego pojęcia jako coś oczywistego.

Słusznie stawia się akcent w powyższych dokumentach na bezpieczeństwo w cyberprzestrzeni, jednak głównie z zastosowaniem przepisów prawa, polityk okołounijnych bądź też poprzez rozbudowę zasobów przemysłowych i technologicznych wykorzystywanych na potrzeby bezpieczeństwa cybernetycznego. Nie ulega wątpliwości, że są to ważne i konieczne działania. Nie można jednak wszystkich zdarzeń, jakie mają miejsce w cyberprzestrzeni, uregulować przepisami prawa lub też rozwiązaniami technologicznymi. Konieczne jest również zdefiniowanie norm etycznych, które mogą być stosowane tam, gdzie nie dostaje prawo lub nowe technologie.

CZY W CYBERPRZESTRZENI JEST POTRZEBNA ETYKA?

Inspirowany przez biznes, a także potrzeby polityczne dynamiczny rozwój cyberprzestrzeni wymusza stosowanie nie tylko instrumentów prawnych, technicznych, ale i pozanormatywnych, tzw. miękkich (*soft law*). Już na samym początku należy zauważyć, że nieco inne treści będzie zawierała etyka dotycząca obszaru technologii informacyjnych (IT – *Information Technology*), a inaczej będą one wyglądały w systemach informacyjnych (IS – *Information System*). Pogłębiona analiza zasad etycznych winna obejmować również kwestie związane z problematyką rygoryzmu moralnego vs. relatywizm moralny, uniwersalizm vs. indywidualizm, oraz monizm vs. pluralizm, np. wielokulturowość. Tych kwestii jednak nie da się rozstrzygnąć w tak krótkim opracowaniu (zob. X. Wu, S. Rogerson, N.B. Fairweather).

Normy etyczne są niezbędne do zbudowania etosu zachowań akceptowanych w sieci. Wydaje się, że konieczne jest nawet zbudowanie swoistego dekalogu norm moralnych czy etycznych dla uczestników cyberprzestrzeni, w tym dla programistów. Właśnie te normy etyczne powinny być też elementem składowym procesu edukacji nowych pokoleń informatyków.

[4] JOIN(2013) 1 final.

Specyfiką tejże etyki jest to, że normy etyczne są definiowane już nie przez religię, ośrodki polityczne, kulturę, lecz przez uczestników cyberprzestrzeni, do których należy zaliczyć:

- projektantów,
- programistów,
- użytkowników,
- administratorów sieci komputerowych, baz danych i opiekunów komputerowych,
- a przede wszystkim wielkie korporacje działające na rynku elektronicznym.

Etyka dla IT

Technologie informatyczne tworzone są przez profesjonalistów. Dla ich użytku tworzone są akty wewnętrzne korporacji oraz przedsiębiorstw w formie kodeksów. Wzorcowe kodeksy etyczne, będące zbiorem zasad postępowania dla twórców narzędzi wykorzystywanych w cyberprzestrzeni, powstały przede wszystkim w USA, zwłaszcza w wielkich korporacjach przemysłu elektronicznego. Najbardziej znany jest kodeks IEEE – Institute of Electrical and Electronics Engineers, który jest częścią Strategii Rozwoju tejże firmy. Upływ czasu oraz pojawianie się nowych technologii IT sprawia, że jest on ciągle aktualizowany. Ostatnia jego wersja jest datowana na 2 lipca 2016 roku.

Podstawowym przesłaniem kodeksu etycznego IEEE jest to, aby pracownicy zobowiązali się do zachowywania najwyższych standardów etycznych oraz profesjonalnych. Do najważniejszych zasad etycznych tego kodeksu należą takie normy, jak:

- pracownicy firmy winni składać oświadczenia, że są świadomi znaczenia technologii w podnoszeniu jakości życia na świecie oraz że akceptują zobowiązania, jakie płyną z wykonywanego zawodu. W ten sposób pracownicy zobowiązują się do akceptowania odpowiedzialności za nowe produkty przez nich wytwarzane. Mogą one bowiem zagrażać bezpieczeństwu, zdrowiu, dobru publicznemu albo środowisku naturalnemu,
- pracownicy firmy zobowiązują się do unikania realnych lub możliwych konfliktów, a powstałe już konflikty zobowiązują się rozwiązywać bezpośrednio z osobami, między którymi ten konflikt powstał,
- pracownicy firmy winni cechować się takimi wartościami, jak uczciwość i profesjonalizm w obchodzeniu się z bazami danych,

- pracownicy tej firmy powinni odrzucać wszelkie formy nieuczciwości, winni podnosić swój poziom wiedzy i kompetencji dotyczących nowych technologii, aplikacji, ale też winni się uczyć o negatywnych i pozytywnych skutkach programów oraz aplikacji,
- pracownicy akceptują rzeczową krytykę współpracowników i przełożonych o swojej pracy; uznają i poprawiają własne błędy,
- pracownicy zobowiązują się do równego traktowania uczestników cyberprzestrzeni, niezależnie od rasy, religii, płci, niepełnosprawności, wieku czy narodowości,
- pracownicy unikają świadomego wyrządzania szkód innym osobom, ich własności czy reputacji,
- pracownicy mają być solidarni, a więc winni pomagać kolegom w ich profesjonalnym rozwoju oraz w przestrzeganiu norm prawnych i zasad etyki,
- pracownicy nie mogą używać komputera w celu szkodzenia innym użytkownikom cyberprzestrzeni oraz nie mogą zakłócać innym pracy na komputerze.

Typowo polski jest Kodeks Etyki z 2011 roku, który został zredagowany i przyjęty przez Polskie Stowarzyszenie Informatyków. Jest to kodeks skierowany do pracowników i osób przynależących do Stowarzyszenia. W pkt 1 podkreślono rolę służebną informatyków wobec klientów. W pkt 3 jest mowa o obowiązku doskonalenia wiedzy przez informatyków. W pkt 6 zobowiązani są do zachowania integralności systemów komputerowych, które obsługują. Stąd też muszą swojemu klientowi przedstawiać rzetelną informację o tym, co robią, i muszą zrobić tak, aby system informacyjny działał sprawnie. Informatycy skupieni w Polskim Stowarzyszeniu Informatyków nie mogą też naruszać zasad uczciwej konkurencji, czyli nie mogą np. podejmować pracy w firmach, które ze sobą konkurują[5].

Etyka dla SI

Etyka dla użytkowników systemów informacyjnych musi mieć charakter ogólny, nie tak jak to jest w przypadku etyki korporacyjnej bądź zawodowej. Najbardziej znany obecnie zbiór takich zasad powstał w 1992 roku w Wa-

[5] Tekst Kodeksu Etyki Polskiego Stowarzyszenia Informatyków znajduje się na stronie internetowej pod adresem: http://www.pti.org.pl/index.php/KZI-Kodeks-zawodowy-informatykow-PTI-29-maja-2011-r2 [data dostępu: 4.11.2016].

szyngtonie i został utworzony przez Instytut Etyki Komputerowej (*Computer Ethics Institute*). Instytut ten powstał w 1985 roku, wydał on 10 przykazań, jakimi powinni posługiwać się użytkownicy komputerów czy cyberprzestrzeni. Układ przykazań nie jest przypadkowy, bowiem wzorowany jest na biblijnym Dekalogu, zresztą jak również niektóre treści. Przykazania te były później przyjmowane w piśmiennictwie, niekiedy też były krytykowane.

Te 10 przykazań zostało zdefiniowane od strony negatywnej, tak jak Dekalog. Są to następujące przykazania[6]:

1. Nie używaj komputera w celu szkodzenia innym. Zakaz ten nie ogranicza się do szkód fizycznych, ale dotyczy głównie szkód wyrządzonych innym użytkownikom komputerów poprzez uszkodzenie ich plików, napisanie aplikacji, która będzie wykradała dane z innych komputerów, nieuprawnione kopiowanie danych, wejście w komputer bez zgody właściciela. Do tej kategorii zachowań nieetycznych zalicza się również zaangażowanie w hakerstwo, spamowanie, wyłudzanie informacji, cyberprzemoc.
2. Nie zakłócaj pracy innym na komputerze. Takie działanie materializuje się m.in. poprzez używanie komputera lub oprogramowania w taki sposób, aby zakłócać prace innych. Przykładem może być wpuszczanie do sieci wirusów komputerowych, które zaburzają normalną pracę innych użytkowników cyberprzestrzeni. Takie zaburzenia mogą przybierać różną formę. Może to być zablokowanie pamięci operacyjnej, przez co komputery zainfekowane nie mogą normalnie pracować lub pracują powoli, może to być też użycie programów normalnie funkcjonujących, ale są też wykorzystywane do przeprowadzenia ataku na inne komputery bądź na systemy informatyczne instytucji publicznych lub nawet państwa.
3. Nie podglądaj treści na komputerze innych ludzi. Nie jest moralnie i prawnie dopuszczalne czytanie cudzych listów, w tym maili oraz SMS-ów. Jest to też naruszenie praw człowieka do prywatności. Ograniczeniem tego przykazania będzie kontrola komputera i jego zawartości przez uprawnione do tego służby, w razie nadużycia stosowania urządzeń elektronicznych, np. gromadzenie na dysku pornografii dzie-

[6] Wykaz tych przykazań oraz objaśnienia ich znaczeń w dużej mierze zostały opracowane na podstawie hasła *Ten Commandments of Computer Ethics,* [w:] en.wikipedia.org. Adres: https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics [data dostępu: 4.11.2016].

cięcej. Zajmują się tym wyspecjalizowane instytucje śledzące aktywność użytkowników cyberprzestrzeni, którzy dopuszczają się czynów o charakterze kryminalnym lub terrorystycznym. Także pracodawca jest uprawniony do kontroli zawartości komputerów, na których pracują pracownicy w jego firmie.

4. Nie używaj komputera do kradzieży informacji wrażliwych lub poufnych. Chodzi o informacje, które dotyczą pracowników, pracodawcy, pacjentów ze szpitala lub tym podobnych. Podobnie należy traktować włamanie się do banku danych bądź też nielegalny transfer danych. Praktyki te są coraz częstsze z powodu postępu technologicznego.
5. Nie używaj komputera do tworzenia lub rozpowszechniania fałszywych informacji przez Internet lub maile. Nieetyczne jest zatem uczestniczenie w procesie rozpowszechniania fałszywych i zniesławiających informacji dotyczących osób lub firm. Dość częstą praktyką w Internecie jest rozpowszechnianie fałszywych informacji o odkryciach naukowych oraz o produktach (nieprawdziwa reklama). Niektóre państwa celowo tworzą fałszywe opisy wydarzeń historycznych tylko po to, aby zmienić historiografię. Do realizacji tego celu wykorzystuje się fakt, że prawdziwe zdarzenia są opisane w publikacjach drukowanych, do których, zwłaszcza młode pokolenie, już nie sięga. Czytane czy wręcz kopiowane są informacje znajdujące się w Internecie, często zmanipulowane czy wręcz nieprawdziwe. Brak konfrontacji tekstów drukowanych z wirtualnymi sprawia, że młode pokolenie wychowywane jest już na bazie informacji nieprawdziwych i zmanipulowanych, które przyjmuje jako prawdziwe.
6. Nie kopiuj ani nie używaj oprogramowania, za które nie zapłaciłeś. Każdy programista ma prawa autorskie do programu, który napisał. Podobnie zresztą jak twórca innego dzieła intelektualnego. Respektowane też muszą być prawa własności intelektualnej zakładu pracy, w którym programista pracuje i dla którego tworzy oprogramowania. Stąd nielegalne używanie kopii programów komputerowych jest uznawane za bezprawne i nieetyczne.
7. Nie korzystaj z zasobów komputera innych bez ich zgody lub bez adekwatnej zapłaty. Za nieetyczny uznaje się nieuprawniony dostęp do cudzego komputera, jego zasobów lub udostępnianie danych nielegalnie uzyskanych innym użytkownikom sieci. Jest to forma naruszenia

ich prawa do prywatności. Takie zachowanie materializuje się poprzez nieuprawnione wejście w posiadanie hasła do cudzego komputera lub jego poszczególnych zasobów. Nieetyczne jest również uprawnione korzystanie z zasobów cudzego komputera lub baz danych, ale bez zapłaty. Przykładem może być korzystanie z prywatnych zasobów naukowych, do których jest otwarty dostęp, ale za odpłatnością. Niespełnienie tego wymogu jest również działaniem nieetycznym.

8. Nie zawłaszczaj cudzej własności intelektualnej. Program jest własnością jego wytwórcy lub organizacji, dla której wytwórca pracuje. Zatem kopiowanie programu i rozprowadzenie go w formie odpłatnej lub nieodpłatnej pod własnym imieniem uznawane jest za zachowanie nieetyczne.
9. Nie zapominaj o skutkach społecznych programu, który napisałeś, lub programu, który zaprojektowałeś. Programy komputerowe są używane przez miliony użytkowników w różnym wieku, poczynając od małych dzieci, a kończąc na osobach starszych. Są to w szczególności gry komputerowe, animacje, programy edukacyjne, które mają znaczący wpływ na ich użytkowników. Stąd twórcy programów komputerowych winni czuć się moralnie odpowiedzialni za konsekwencje społeczne, jakie swoim działaniem mogą wywołać. Programiści zatem powinni uwzględniać specyfikę grupy docelowych odbiorców ich produktów nie tylko pod względem treści, możliwości percepcyjnych, ale również pod kątem ich systemu wartości i wrażliwości. Świadome pisanie programów negatywnie oddziaływających na odbiorców jest uważane za nieetyczne, podobnie zresztą jak to jest w przypadku reklam.
10. Zawsze używaj komputera w taki sposób, aby zapewnić respektowanie praw innych użytkowników. Obecnie komputer stał się podstawowym narzędziem komunikowania się w cyberprzestrzeni. Do tego służy nie tylko poczta elektroniczna, ale również portale społecznościowe czy czat. Normy etyczne obowiązujące w tego rodzaju komunikacji w cyberprzestrzeni w dużej mierze są takie same, jakie obowiązują w komunikacji, która ma miejsce w realnym świecie. Zatem komunikujący się ze sobą, niezależnie od środka, winni: nie stosować języka wulgarnego, nie umieszczać nieodpowiedzialnie negatywnych znaków obok nazwiska innych osób, np. negatywnych emotikonów, nie naruszać prawa innych do prywatności poprzez rozpowszech-

nianie informacji prawdziwych, ale zniesławiających, np. informacji o romansie, w końcu nie należy składać fałszywych deklaracji, np. dotyczących statusu cywilnego czy wykształcenia. Komunikacja przez Internet powinna też respektować czas innych użytkowników.

Etyka a prawo komputerowe

Jedną z szybciej rozwijających się gałęzi prawa jest prawo komputerowe. Jego zadaniem jest regulacja zasad korzystania z własności programów oraz danych znajdujących się w bazach danych. Kluczową zatem kwestią jest własność, która odpowiada nowemu rodzajowi przedmiotów niematerialnych tworzonych i funkcjonujących w cyberprzestrzeni. Ponadto prawo komputerowe tworzy zasady bezpieczeństwa, zwłaszcza chroni prawo do prywatności i integralności. Określa zasady dostępu do komputera, sieci informatycznej oraz usług informatycznych.

W przepisach prawa przewiduje się ochronę, w szczególności reguluje zachowanie ludzi, którzy używają komputerów i sieci. Przepisy prawa dotyczą zwłaszcza:

- ochrony praw autorskich dotyczących programów bądź projektów programów,
- ochrony komputera i sieci przed działaniami kryminalnymi,
- ochrony haseł i danych zawartych w komputerach,
- ochrony dostępu do programów i usług internetowych,
- ochrony baz danych zawierających dane o osobach, dane technologiczne czy inne (zob. A. Junker, M. Benecke, s. 35 i nast.).

Prawo określa tylko ogólne zasady poruszania się w cyberprzestrzeni, stąd nie zawsze w sposób odpowiedni może zagwarantować należyty poziom kontroli działań w komputerze i w Internecie. Ponadto prawo komputerowe rozwija się dość powoli i nie nadąża za postępem technicznym w tej dziedzinie i rozwojem cyberspołeczności.

Nie jest tajemnicą, że sędziowie, prawnicy, politycy, pracownicy administracji publicznej lub policjanci nie zawsze rozumieją zasady korzystania z urządzeń technicznych związanych z cyberprzestrzenią, nierzadko nie rozumieją poleceń komputerowych. Wielu użytkowników cyberprzestrzeni nie rozumie, w jaki sposób komputer i korzystanie z niego może podlegać przepisom prawnym. Należy dysponować specjalną wiedzą. Na jej

zdobycie konieczne jest dużo czasu. Wszyscy musimy mieć czas na adoptowanie się do nowej sytuacji i powstanie kultury bycia w cyberprzestrzeni. Pomocne w tym są właśnie zasady etyki, które tworzone są przez samą cyberspołeczność.

PODSUMOWANIE

Postęp techniczny w ostatnich 30 latach nabrał tempa dotąd niespotykanego w dziejach ludzkości. Jednym z obszarów prawie całkowicie nowych, stworzonych przez człowieka jest cyberprzestrzeń. Ma ona charakter globalny i nie jest kontrolowana przez jakiekolwiek państwo. Tworzy się nowa społeczność, do niedawna jeszcze określana jako wirtualna. Brak kontroli nie oznacza anarchii. Stąd dość dynamicznie rozwija się prawo internetowe, a także zasady etyczne typowe dla cyberprzestrzeni.

Na cyberprzestrzeń składają się technologie i sieci informatyczne. Dla każdego z tych obszarów zbudowano podobne, ale jednak znacząco różniące się zasady etyczne. Dla technologii informacyjnych tworzone są kodeksy etyczne. Wzorcowe kodeksy etyczne dla informatyków powstały w USA. Z tych wzorców czerpią również polscy informatycy skupieni w Polskim Towarzystwie Informatyków. Z kolei dla sieci informatycznych, czyli dla zwykłych użytkowników, stworzono swoisty dekalog etyczny.

Budowa norm etycznych dla cyberprzestrzeni jest ważnym zadaniem, wymagającym przemyślenia. Niemniej jednak można powiedzieć, że nie odbiegają one zasadniczo od norm etycznych stosowanych w świecie realnym. Czymże jest bowiem zakaz kradzieży dóbr intelektualnych, zakaz zniesławiania w sieci, zatrudnianie profesjonalistów, czymże jest uczciwość i szacunek dla drugiej osoby, jak nie wartościami często przytaczanymi z prawa rzymskiego i nauki katolickiej.

Bibliografia

Dobrzeniecki K. (2004). *Prawo a etos cyberprzestrzeni*. Toruń.

Junker A., Benecke M. (2000). *Computerrecht*. Baden-Baden 2000.

Wasilewski J. (2013). *Zarys definicji cyberprzestrzeni*. „Przegląd Bezpieczeństwa Wewnętrznego", 5/9/2013.

Wójcik J. (2009). *Cyberprzestrzeń i jej główne zagrożenia: cyberprzestępczość i cyberterroryzm*, [w:] Lisiecki M. i in., *Bezpieczeństwo wewnętrzne Rzeczpospolitej Polskiej na tle innych państw Unii Europejskiej*. Józefów.

Źródła internetowe

http://www.pti.org.pl/index.php/KZI-Kodeks-zawodowy-informatykow-PTI-29-maja-2011-r2 [data dostępu: 4.11.2016].

https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics [data dostępu: 4.11.2016].

https://mac.gov.pl/files/nask_rekomendacja.pdf [data dostępu: 3.11.2016].

https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html [data dostępu: 4.11.2016].

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [data dostępu: 3.11.2016].

Wu X., Rogerson S., Fairweather N.B., *Ethical Considerations on Information System Development: Perspectives on a Practical Moral Framework*, http://rccs.southernct.edu/category/ethicomp-99/ [data dostępu: 4.11.2016].