STUDIA NAD BEZPIECZEŃSTWEM

Nr 5 **ss. 5–22** **2020**

ISSN 2543–7321

Przyjęto: 15.01.2020
Zaakceptowano: 15.01.2020

Oryginalna praca badawcza DOI: 10.34858/SNB.1.2020.001

Joanna Grubicka
Akademia Pomorska w Słupsku
ORCID: 0000-0001-7934-6044
e-mail: joanna.grubicka@apsl.edu.pl

WIRTUALNA RZECZYWISTOŚĆ – OKSYMORON KULTUROWY INSTRUMENTARIUM WOLNOŚCI

VIRTUAL REALITY – A CULTURAL OXYMORON INSTRUMENT OF FREEDOM

Zarys treści: W przedstawionym artykule podejmuję się interpretacji pojęcia wolności i jej aspektów, które w praktyce wyrażane są przez wolność słowa w Internecie. Na podstawie aktualnie obserwowanych zjawisk i bieżących wydarzeń wskazane zostały zagrożenia wynikające z powszechnej dostępności do publikacji opinii w sieci. W podanych przykładach zaprezentowano zarówno praktykę dokonywanych regulacji, jak i manipulacji w tym zakresie. Przedstawiony artykuł nie aspiruje do całościowej eksplikacji wpływu nowych technologii na funkcjonowanie społeczeństw w wymiarze holistycznym, stanowi raczej próbę egzegezy jednego z jej obszarów – dotyczącą ewoluowania interakcji międzyludzkich pod wypływem nowych technologii. Niniejsza praca próbuje udzielić odpowiedź na pytanie, czy możliwe je sformułowanie się i funkcjonowanie społeczności wirtualnych, analogicznych do społeczności w świecie rzeczywistym? Czy zatem Internet powinien być przestrzenią nieograniczonej niczym wolności? Autorka konfrontuje ze sobą różnorodne aspekty zagrożeń wolności w Internecie, by uzyskany obszar był kompleksowy i obiektywny, daleki od jednostronności i schematycznych uproszczeń. Internet jest bowiem z założenia egalitarnym narzędziem komunikacji, przestrzenią swobodnego tworzenia i przepływu treści, dla których ograniczeniem jest tylko technologia oraz ludzka wyobraźnia, której granic wyznaczyć nie sposób. Wolność zatem zdaje się być nie tylko immanentną, ale wręcz konstytutywną cechą tej wirtualnej przestrzeni, w której funkcjonuje Internet. Przedmiotowy artykuł wskazuje na potrzebę konsolidacji wysiłków ekspertów w wielu zakresach: bezpieczeństwa, psychologii, prawa nad swobodą wolności społeczeństwa w przestrzeni bezpieczeństwa.

Słowa kluczowe: wirtualna rzeczywistość, cyberprzestrzeń, cyfrowa rewolucja, wolność cyfrowa

Key words: virtual reality, cyberspace, digital revolution, digital freedom

Wprowadzenie

W historii ludzkich wynalazków wielokrotnie zdarzało się, że postęp technologiczny pociągał za sobą szersze zmiany o charakterze kulturowym. Internet nie jest w tym względzie wyjątkiem. Aspekt owych zmian staje się stopniowym zacieraniem granic pomiędzy twórcą i odbiorcą treści oraz procesem, szerokiego spektrum wolności człowieka. Niektóre rodzaje aktywności, do niedawna o charakterze elitarnym, nabierają charakteru wyraźnie egalitarnego, pozwalając szerokiej rzeszy jednostek ludzkich na realizację celów, których osiągnięcie w innych okolicznościach byłoby znacznie utrudnione, jeśli nie niemożliwe. Wydaje się, że Web 2.0 w zakresie wolności pozytywnej oferuje znacznie więcej możliwości niż realia życia społecznego poza siecią WWW[1]. Internet dostarcza narzędzi, które w znacznym stopniu ułatwiają realizację wolności, w komunikowaniu się, wyrażaniu myśli, przekazywaniu idei, poglądów, ale łatwość rozpowszechniania informacji stwarza też pole do nadużyć i przekraczania granic godności drugiego człowieka. Do niedawna wydawało się, że globalna sieć stanowi pole zupełnie nieuregulowane i nieobwarowane żadnymi zasadami. Ten stan rzeczy powoli się zmienia i prawodawcy oraz sądy zaczynają wyznaczać granice postępowania w sieci. Osoby zamieszczające treści w Internecie muszą to czynić z zachowaniem minimum ostrożności, aby nie naruszyć granic wolności słowa, szczególnie w zakresie szeroko rozumianego bezpieczeństwa publicznego, przestępstw, moralności, porządku publicznego, dóbr osobistych innych osób oraz informacji tajnych i poufnych. Złożoność świata można analizować w kontekście zmian kulturowych i cywilizacyjnych, których omówić tu nie sposób, ale sięgając do analiz dokonanych przez M. Mead[2] opisującej proces rozwoju i socjalizacji w różnych kulturach, pierwotnych i współczesnych, można przeobrażenia kulturowe współczesnego świata sprowadzić w aspekcie konsekwencyjnym do odwrócenia tradycyjnych zasad wychowania i socjalizacji (starsi uczą się od młodszych – kultura prefiguratywna). Złożona i zmienna przestrzeń życiowa człowieka jest zatem wyznaczana czynnikami społeczno-kulturowymi, wpływającymi na rozwój i jakość autokreacji, co szczególnie dotyczy młodego pokolenia. Coraz częściej zauważa się niepokojącą powierzchowność, lakoniczność, płytkość i kruchość relacji między ludźmi, które znajdują swe umocowanie w utrzymywaniu kontaktów na zasadzie chwilowości i przypadkowości, a nie bliskości spotkań „twarzą w twarz".

Stewart Brand, twórca The WELL™: „Chcieliśmy stworzyć przestrzeń, w której moglibyśmy realizować własne pomysły, eksperymentować. Nie mieliśmy wówczas pieniędzy ani wpływów, ale zdawaliśmy sobie sprawę z szansy, jaka się przed nami pojawiła (…). Każdy mógł tam powiedzieć wszystko". Najwięcej kontrowersji wiąże się z filozoficznym ujęciem wolności człowieka, łączonej tradycyjnie z pojęciem wolnej woli. W rozważaniach dotyczących wolności przyjmuje się rozróżnienie dwóch

[1] M. Szpunar, *Przestrzeń Internetu – nowy wymiar przestrzeni społecznej*, [w:] *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, A. Siwik, L. Haber (red.), Kraków 2008a, s. 225–234.

[2] M. Mead, *Kultura i tożsamość. Studium dystansu międzypokoleniowego*, Warszawa 2000, s. 25.

pojęć: wolności od czegoś, tj. od czynników ograniczających swobodę wyboru, oraz wolności do czegoś, pojmowanej jako działanie oparte na poznaniu i wykorzystaniu konieczności przyrodniczych i społecznych. W obydwu tych znaczeniach wolność nie jest pojęciem absolutnym i – jak każda sfera ludzkiej aktywności – podlega ograniczeniom. W sieci można spotkać wypowiedzi czy wpisy, które wprost nie są może obrażające, ale zdecydowanie niesmaczne i wulgarne. Co ciekawe – budzenie kontrowersji w sieci nieparlamentarnym językiem nikogo już dziś nie dziwi. Bez żadnego problemu w serwisach takich jak YouTube zamieszczać można filmiki, gdzie co drugie słowo to przekleństwo lub obrażanie innych ludzi. Dodatkowo – cieszą się one niemałą popularnością. Wolność globalnej sieci wyraża się jednak nie tylko w zasadzie nieograniczonej możliwości korzystania z jej zasobów czy wyrażania siebie i własnych poglądów (z wyjątkiem zapisów w regulaminach poszczególnych usług, np. portali, czy przepisów prawa karnego), ale przede wszystkim w braku centralnego ośrodka, jakim może być podmiot/instytucja nadzoru i kontroli nad jej całością. Wskazany przymiot wymieniany jest także jako jedna z cech szczególnych cyberprzestrzeni. Do pozostałych zalicza się m.in.: płynność, wirtualność, nieprzewidywalność, alternację (w warstwie programowej i informacyjnej), interaktywność, brak możliwości wytyczenia granic, powszechną dostępność czy uniwersalność. Pojęcie wolności jest terminem wieloznacznym i niejednakowo rozumianym w różnorodnych kontekstach i w stosunku do różnych dziedzin życia. Rzeczywistość wirtualną można rozważać z pominięciem jej aktualnych technologicznych realizacji, a dzięki temu, opierając się na modelach po części fikcyjnych, po części już istniejących, stworzyć rodzaj typologii VR, oddzielając ją jednak od typologii samego zjawiska wirtualności.

Internet jest pierwszym globalnym medium, którego użytkownicy są nie tylko odbiorcami, ale także twórcami treści. Rzeczywistość wirtualną można wykorzystywać w wielu dziedzinach życia publicznego i gospodarczego: w medycynie, rozrywce, do kontroli ruchu drogowego, jako narzędzie w pracy zawodowej czy w różnych gałęziach przemysłu. Cyberprzestrzeń pełni przez to funkcję edukacyjną, usługową, rozrywkową, społeczną, ekonomiczną czy kulturotwórczą, ale również i militarną. W tym kontekście zasadne jest postawienie kwestii wolności nie tylko w sensie swobody odbiorcy, ale także – a może przede wszystkim – swobody nadawcy zamieszczanych tam treści. Skoro każdy ma prawo w sieci zaistnieć, czy to oznacza, że może w niej swobodnie umieszczać wszystko, co zechce? W pierwszym odruchu być może skłonni bylibyśmy powiedzieć, że tak, ale nawet bardzo pobieżna refleksja powoduje wątpliwości wobec tak kategorycznego stwierdzenia. Wolność jest bez wątpienia wartością pozytywną, jedną z najważniejszych, wręcz konstytuującą ludzką egzystencję, ale czy jest wartością bezwzględną? Praktyka życia codziennego wskazuje, że nie sposób na to pytanie odpowiedzieć twierdząco. Natychmiast jednak rodzi się pytanie, kto i na jakich zasadach miałby ograniczać wolność w Internecie? Wolność człowieka żyjącego w społeczeństwie podlega wielorakim ograniczeniom, choćby tylko wynikającym z norm współżycia. Jakkolwiek granice norm społecznych nie są sztywne i – zwłaszcza współcześnie – są na różne sposoby przesuwane, najczęściej pod hasłem poszerzania obszaru wolności jednostki, to samo istnienie tych

norm nie jest kwestionowane[3]. Wręcz przeciwnie, one także są istotną i bezwzględnie konieczną wartością w życiu każdej społeczności, a zatem mają wymiar globalny. Mamy zatem – w pewnym uproszczeniu – sytuację współistnienia i współzależności dwóch istotnych wartości: wolność jednostki z jednej, a normy życia społecznego z drugiej strony. I właśnie przez taki pryzmat spojrzeć należy na zagadnienie swobody w Internecie.

Wybrane zagrożenia w społecznej przestrzeni rozwoju człowieka

Rewolucja informatyczna spowodowała, że współczesny świat stał się dualny i symultaniczny – realny i wirtualny zarazem. Warunki i formy tych przestrzeni stworzyły środowisko, w którym kształtuje się i rozwija społeczeństwo informacyjne. Paradoks przestrzenny globalnej sieci implikuje konieczność głębszych rozważań w zakresie idei wolności cyfrowej w bezpiecznej przestrzeni bezpieczeństwa. Natomiast inkongruencja idei wolności wyraża się w wyznaczających ją dwóch punktach: od i do. W aspekcie wirtualnej sieci – wolność do przejawiać się będzie zarówno w dostępie do istniejących w niej legalnych zasobów informacyjnych, jak i swobody korzystania z nich w dowolny sposób oraz wyrażania własnych przekonań czy poglądów. Z kolei parametr od winien być determinowany zarówno przez wolność od ograniczeń w dostępie do zasobów, jak również związanych z cenzurą, jak i zagrożeń. Dynamizm rozwoju implikuje jednak nie tylko pozytywne zmiany, ale również nowe wyzwania i zagrożenia. Zagrożenia te mają dwojaki charakter: są to istniejące negatywne zjawiska przenoszone do sieci ze świata realnego, jak i powstaniu nowych kategorii niebezpiecznych zachowań i przestępstw.

Generalna klasyfikacja zagrożeń cyfrowych implikowana jest przez:

- działalność człowieka/użytkownika: celową (np. cyberprzestępcy) oraz niecelową (np. niefrasobliwi użytkownicy);
- brak bezpośredniego powiązania z celową działalnością człowieka (zawodność systemów, błędy w oprogramowaniu);
- naturalne środowisko (np. katastrofa naturalna powodująca awarię zasilania);
- hybrydowość zdarzeń.

Z kolei podział zagrożeń w atrybucie informacji funkcjonujących w środowisku cyfrowym będzie wynikał z funkcji celu, tj.: zakłócenia, kradzieży, przechwycenia, uszkodzenia, manipulacji, przejęcia kontroli, modyfikacji lub zniszczenia (informacji i/lub systemów). Narzędziami wykorzystywanymi do osiągnięcia wskazanych celów są odpowiednio przygotowane, złośliwe programy – wirusy lub robaki komputerowe. Wśród nich wyróżnia się m.in.:

- bomby logiczne – uśpiona forma złośliwego oprogramowania aktywująca się z chwilą spełnienia określonych warunków (np. określonego dnia);

[3] M. Szpunar, *Internet a wolność (od) wypowiedzi*, [w:] *Media – między władzą a społeczeństwem*, M. Szpunar (red.), Rzeszów 2007, s. 101–114.

- konie trojańskie – oprogramowanie, które podszywając się pod przydatne lub interesujące dla użytkownika aplikacje, dodatkowo posiada niepożądaną, ukrytą funkcjonalność;
- hoaxy – programy, które wyświetlają nieprawdziwą informację o tym, że w komputerze znajduje się wirus;
- spyware – oprogramowanie, którego celem jest szpiegowanie użytkowników, np. rejestrowanie odwiedzanych stron czy haseł wpisywanych na klawiaturze bez ich wiedzy, a następnie przesyłające pozyskane dane do atakującego;
- phishing – polega na podstępnym zdobywaniu loginów i haseł poprzez podszywanie się pod godną zaufania instytucję lub osobę.

Wspólnym mianownikiem większości wskazanych form złośliwego oprogramowania jest konieczność interakcji i reakcji użytkownika (np. kliknięcie w link), zaś istotą i celem – infekcja systemu (urządzenia) oraz osiągnięcie zamierzonego skutku (np. kradzieży danych).

Należy zauważyć, że coraz częściej wykorzystywane są metody ataku niewymagające specjalistycznej wiedzy z dziedziny programowania. Należą do nich cyfrowe fałszerstwa i wyłudzenia, które można podzielić na następujące podkategorie:

- dokonane za pomocą złośliwego oprogramowania;
- dokonane za pomocą fałszywych komunikatów (e-maile);
- hybrydowe (fałszywe maile zawierające złośliwe programy lub link do takiego rodzaju programów).

Druga i trzecia ze wskazanych form polega na spreparowaniu wiadomości e-mail, w której atakujący podszywa się pod określoną instytucję lub podmiot (np. operatora pocztowego lub dostawcę usług internetowych), umieszczając w treści odnośnik do strony lub załącznik z plikiem sugerującym np. fakturę. W rzeczywistości załącznik zawiera złośliwy program, który infekuje urządzenie użytkownika.

Zagrożenia o charakterze społecznym wiążą się przede wszystkim z pojawianiem się w sieci szkodliwych i nielegalnych treści, podejmowaniem przez użytkowników ryzykownych zachowań czy niebezpiecznych kontaktów. Dotyczą takich zjawisk, jak: cyberprzemoc, grooming, seksting, hejting, pornografia dziecięca, treści rasistowskich, zachęcające do samobójstw i innych. Wartymi wskazania w tym miejscu są również zagrożenia nazywane ukierunkowanymi atakami typu APT (ang. *Advanced Persistent Threat*), które łączą różnego typu narzędzia programistyczne czy socjotechniczne. Przygotowania do tego rodzaju ataków mogą trwać wiele tygodni i zazwyczaj przeprowadzają je zorganizowane grupy dysponujące znacznymi środkami finansowymi oraz czasem niezbędnym do zinfiltrowania konkretnego celu (organizacji, instytucji, firmy), a następnie przeprowadzenia precyzyjnego działania.

Otwarte zasoby Internetu ułatwiają dostęp do rozmaitych treści, również tych nielegalnych, jak i treści, które nie są nielegalne w świetle prawa, ale należą do kategorii szkodliwe. Za treści szkodliwe uważa się takie, które mogą wywołać negatywne emocje u odbiorcy i które mogą mieć wpływ na jego sferę emocjonalną i społeczną

oraz zachowanie. Wśród nich są m.in. treści obrazujące przemoc, obrażenia fizyczne, prezentujące drastyczne sceny, okrucieństwo wobec zwierząt, treści nawołujące do podejmowania działań autodestrukcyjnych, treści dyskryminacyjne oraz pornograficzne. Prawie jedna czwarta polskich młodych internautów miała kontakt z „treściami potencjalnie zagrażającymi rozwojowi społecznemu dzieci, tworzonymi przez innych użytkowników", potencjalnie zagrażającymi rozwojowi społecznemu dzieci, tworzonymi przez innych użytkowników Internetu[4]. Nie tylko szkodliwość treści może mieć wpływ na rozwój człowieka. Paradoksalnie również ich atrakcyjność. Interesujące, atrakcyjne treści i aplikacje, z którymi użytkownicy stykają się w sieci, mogą powodować utratę kontroli nad czasem i intensywnością korzystania z Internetu, komputera, gier komputerowych, portali społecznościowych i innych wirtualnych aktywności. Może to wpłynąć na ograniczenie lub rezygnację z innych czynności dnia codziennego, a także prowadzić do zaniedbywania rodziny, obowiązków, nauki szkolnej czy hobby i/lub unikania kontaktu z rówieśnikami. Badania polskich nastolatków wykazały, iż przebywali oni w sieci dłużej, niż pierwotnie planowali (83,3%), a ponad połowa odczuwała poirytowanie, gdy Internet przestał działać lub nie miała do niego dostępu (64,2%). Dodatkowo co piaty nastolatek rezygnował ze snu, co trzeci z obowiązków, aby móc korzystać z Internetu (29,8%)[5].

Obecnie istnieje prawo wyboru między realną przestrzenią społeczną a przestrzenią alternatywną, jaką jest cyberprzestrzeń[6]. Jeżeli przestrzeń rzeczywista jest jak najbardziej realna, to cyberprzestrzeń jest wirtualna. Jeżeli rzeczywista przestrzeń jest ograniczona terytorialnie, spotkania mogą odbywać się w określonej szerokości geograficznej, w określonej strefie czasowej, to w cyberprzestrzeni nie ma ograniczeń czasowych. W każdej jednostce czasu można kontaktować się z ludźmi na całym świecie, a tym samym cyberprzestrzeń staje się nową przestrzenią relacji interpersonalnych czy społecznych. Anonimowość w cyberprzestrzeni powoduje, że nie mając tych barier, ma się do czynienia z niskim poziomem stresogenności tej wirtualnej rzeczywistości. Jeżeli kontakty przez te bariery stają w rzeczywistości elitarne, ograniczone do pewnego grona osób, to w cyberprzestrzeni mają charakter alitarny[7]. To decyduje o tym, że cyberprzestrzeń staje się coraz bardziej atrakcyjną przestrzenią społeczną.

Cyberprzestrzeń coraz częściej jest także możliwością ucieczki od problemów w świecie realnym. Unikając niewygodnych dialogów, pytań, komentarzy lub kontaktów w rzeczywistości, internauci są w stanie ukryć się w sieci i stworzyć tam przestrzeń odpowiadającą ich aktualnym potrzebom lub dającą anonimowość i względne poczucie bezpieczeństwa.

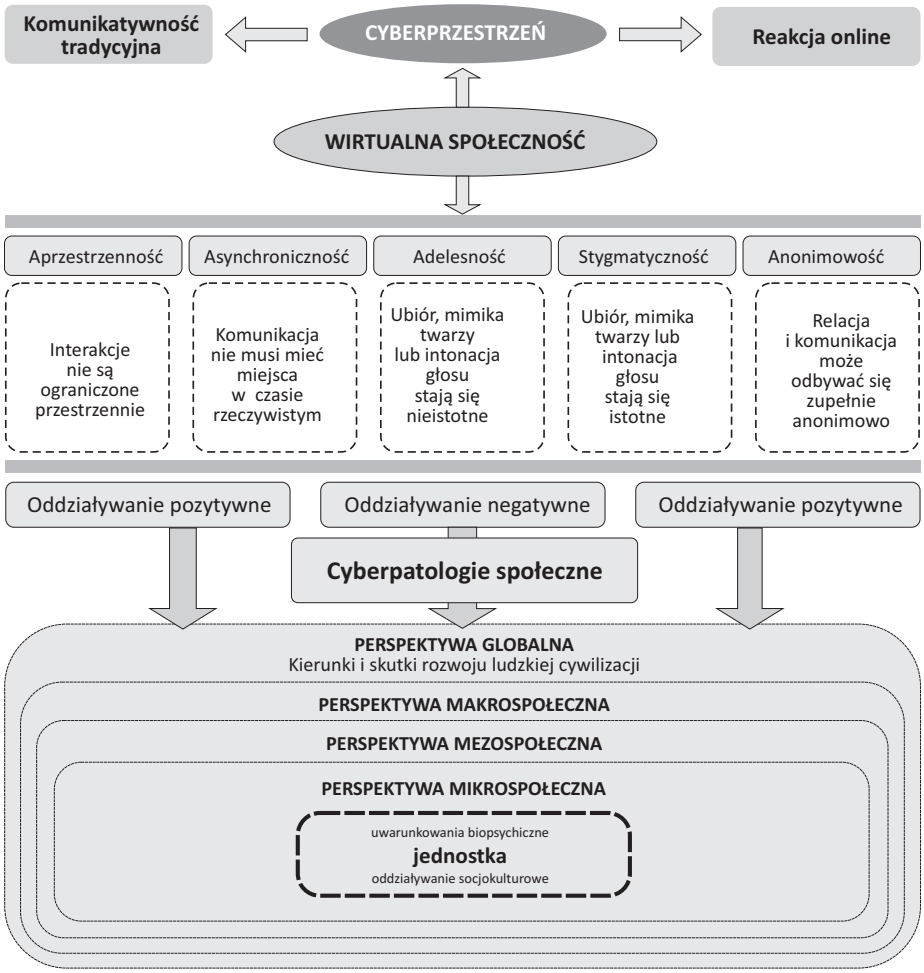
---

[4] L. Kirwil*, Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo – część 2. Częściowy raport z badań EU Kids online przeprowadzonych wśród dzieci 9–16 i ich rodziców*, Warszawa 2011, s. 42–44.

[5] Raport *Nastolatki 3.0*., Warszawa 2016.

[6] M. Szpunar, *Granice wolności słowa w Internecie*, [w:] *Nowe media i komunikacja wizualna*, P. Francuz, S. Jędrzejewski (red.), Lublin 2010, s. 107–125.

[7] J. Grubicka*, Restricting freedom on the internet in a public security space, East Journal of security studies No 2,* Słupsk–Harkov 2017, s. 135–145.



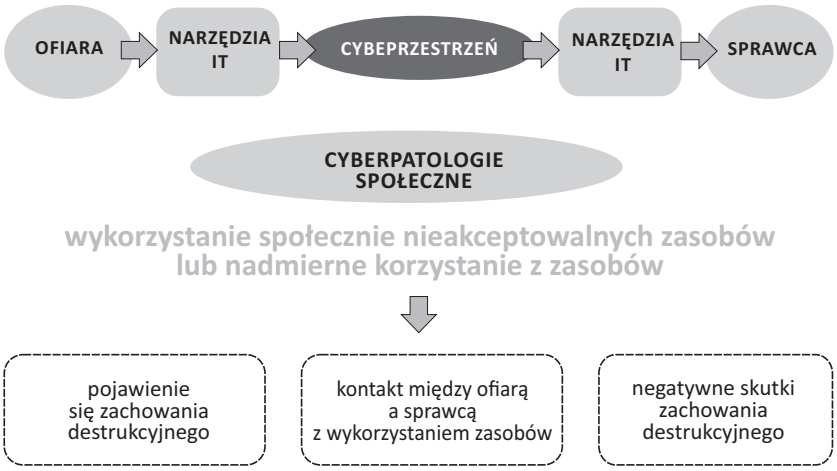
Ryc. 1. Zależność wirtualnej społeczności o przypisanych cechach w perspektywie analiz patologii społecznych
Fig. 1. The dependence of the virtual community with assigned features in the perspective of analyzes social pathologies
Źródło: opracowanie własne.

Użytkownicy cyberprzestrzeni, uczestniczący w różnego rodzaju społecznościach wirtualnych zaczynają wierzyć, że nie jest to jedynie symulacja kontaktu z drugim człowiekiem czy też grupą, a właściwie forma komunikacji międzyludzkiej. Według W. Burszty prowadzi to do zjawiska społecznej samotności, trudności w definiowaniu własnej tożsamości, a także umiejętności komunikowania się z innymi *face to face* (z ang. twarzą w twarz). Z obserwacji internetowego życia społecznego wynika, że aktywność jego członków jest początkiem interakcji kontynuowanej w rzeczywistości lub na odwrót, rzeczywistość ta przenoszona jest i kontynuowana w przestrzeni

wirtualnej. Pokazuje to, że wirtualna społeczność nie jest do końca odrębną rzeczywistością, a tylko jednym ze sposobów na przebieg interakcji, która może wpływać na inne aspekty ludzkiego życia. Szczególnie, że do relacji online jej uczestnicy wnoszą swój statut społeczno-ekonomiczny, płeć, wiek, środowisko kulturowe, związki offline.

M. Smith wymienia pięć podstawowych cech, które określają wirtualną społeczność, a przy tym nie są osiągalne w komunikacji tradycyjnej[8]. Są to m.in.: aprzestrzenność, asynchroniczność, acielesność, stygmatyczność, anonimowość. Zależność wirtualnej społeczności o przypisanych cechach w perspektywie analiz patologii społecznych zestawiono na ryc. 1.

Wykorzystanie społeczne nieakceptowalnych zasobów lub nadmierne korzystanie z narzędzi IT skutkujące negatywnymi efektami zachowania destrukcyjnego przedstawiono na ryc. 2.



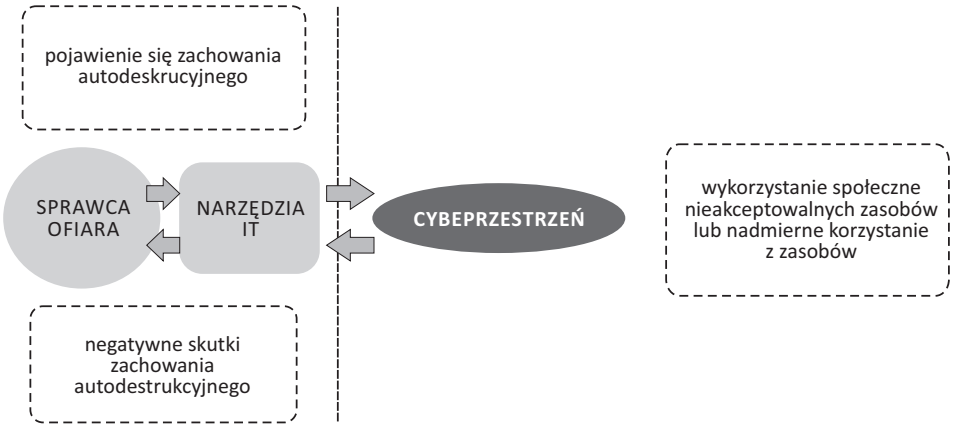
Ryc. 2. Model zachowania destrukcyjnego
Fig. 2. Model of destructive behavior
Źródło: opracowanie własne[9].

Przykładami zachowań destrukcyjnych przedmiotów społecznych zarówno podmiotów personalnych, jak i strukturalnych w cyberprzestrzeni są: cyberprzestępczość, cyberprzemoc, cyberseks, uzależnienie od Internetu (siecioholizm) i telefonu (fonoholizm). Warto zwrócić uwagę na fakt, że jednostka, małe grupy społeczne bądź większe zbiorowości poprzez narzędzia IT mogą być ofiarą, jak i sprawcą zachowań patologicznych. Podmiot referencyjny działań podejmowanych przez otoczenie społeczne w zakresie zapewnienia im bezpieczeństwa i ochrony przed zjawiskami patologicznymi, ale i podmiotem sprawczym tychże działań. Wyrządzanie krzywdy samemu sobie, autodestrukcja wydaje się czynnością pozbawioną logiki, typową dla szaleństwa.

[8] *Ibidem*, s. 200.
[9] J. Grubicka, D. Zbroszczyk, *Cyberaptologie jako zagrożenie dla bezpieczeństwa publicznego*, [w:] „Doctrina", Studia społeczno-polityczne 2019, nr 16, Siedlce, s. 47–59.

Zdaniem Z. Freuda, każda jednostka nosi w sobie impuls, popychający ku życiu i wszystkiemu, zwanym „popędem życia", ale również zupełnie przeciwny, skłaniający ku śmierci i destrukcji, który określił jako „popęd śmierci". Jest również czynnikiem powodującym rozwój symptomów oraz zachowań autodestrukcyjnych u niektórych osób. Jednak tylko w niektórych przypadkach zachowania te się zakorzeniają i przeistaczają w stałe cechy osobowości. Zwykle dzieje się tak, jeżeli istnieją duże pokłady stłumionego gniewu. Agresywne impulsy w cyberprzestrzeni są skierowane do innej osoby, lecz z jakiegoś powodu wyrażenie ich jest niemożliwe. Czasem dzieje się tak, ponieważ skierowane są do ukochanej osoby lub ze strachu przed konsekwencjami wypowiedzenia ich na głos.W tych przypadkach agresja kieruje się na własną osobę.

Właśnie wtedy człowiek uczy się, jak zachowywać się jak swój największy wróg i rozwijają się autodestrukcyjne osobowości. Przykładami zachowań autodestrukcyjnych przedmiotów społecznych w cyberprzestrzeni są: uzależnienie od gier komputerowych, od Internetu czy od telefonu. Model zachowania autodestrukcyjnego w wirtualnej przestrzeni przedstawia ryc. 3.



Ryc. 3. Model zachowania autodestrukcyjnego
Fig. 3. Model of self-destructive behavior
Źródło: opracowanie własne.

Myśli autodestrukcyjne obejmują wszelkie myśli nakierowane na zdewaluowanie osoby, zapobieganie jej postępowi lub podważanie ich osiągnięć. W umyśle osoby autodestrukcyjnej takie myśli pojawiają się w sposób prawie automatyczny. Osoby ze skłonnościami do autodestrukcji często zachowują się wrogo lub wręcz krzywdząco wobec innych. Tworzą niepotrzebne konflikty, zachowują się w sposób bezmyślny, nieuprzejmy, są zazdrośni, plotkują itd. Drugą osobę postrzegają jako źródło kłótni. Inni ludzie powodują u nich frustrację, ponieważ więzi opierają się na porównaniach, w których z takiego czy innego powodu zawsze to oni przegrywają. Po takich konfliktach zazwyczaj wpadają w etap głębokiego użalania się nad samym sobą. Atakują, lecz kiedy ktoś odpowie na ten ich atak, zachowują się jak ofiary niesprawiedliwości.

Obrażają, ale kiedy ktoś ich obrazi, czują żal nad samymi sobą. Nie przyznają, że był to owoc ziarna zasianego przez nich[10].

Internet sprzyja kontaktom interpersonalnym, jednakże kontakty w sieci niosą za sobą pewne ryzyko, szczególnie w przypadkach wykorzystania sieci do nawiązywania relacji z osobami nieznanymi bezpośrednio w świecie offline. Warto zauważyć, że właśnie taką aktywność – kontaktowania się online z osobami nieznanymi osobiście – deklaruje aż 25% młodych internatów[11], a wielu przyznaje się do osobistego spotkania w świecie realnym z wcześniej nieznanymi osobami, a poznanymi w sieci. Do grupy niebezpiecznych kontaktów należy zaliczyć również zjawisko uwodzenia dzieci w Internecie, polegające na wytworzeniu relacji za pośrednictwem Internetu między osobą dorosłą a osobą małoletnią (poniżej 15 r.ż.) w celu jego uwiedzenia i wykorzystania. Niebezpieczne kontakty to również kontakty mające na celu wciągnięcie nastolatka do różnego rodzaju sekt, grup, społeczności i subkultur, np. o radykalnych poglądach, propagujących zachowania np. agresywne, samookaleczanie, restrykcyjną dietę czy stosowanie substancji psychoaktywnych. Kontakty takie podejmują również osoby zainteresowane pozyskaniem danych osobowych i innych poufnych informacji, wykorzystywanych później w celach przestępczych.

Budowanie i utrzymywanie potencjalnie niebezpiecznych kontaktów z nieznajomymi nie jest domeną wyłącznie młodych ludzi, ale to właśnie oni, ze względu na brak doświadczenia oraz często mniejsze z uwagi na wiek kompetencje w zakresie właściwej oceny sytuacji, rozumienia i przewidywania skutków podejmowanych działań w kontraście z otwartością, chęcią nawiązania znajomości, zaufaniem, są bardziej narażeni na poważne konsekwencje.

Internet to miejsce eksperymentowania, również z własną tożsamością i podejmowania ryzykownych zachowań. Jakie zachowania podejmują użytkownicy sieci? Są to m.in.: poszukiwanie informacji na temat narkotyków i innych substancji psychoaktywnych lub aktywności szkodliwych dla zdrowia czy podejmowanie niebezpiecznych kontaktów, w tym z nieznajomymi osobami dorosłymi, które mogą przejawiać skłonności pedofilskie czy z jednostkami/grupami nakłaniającymi do zachowań ryzykownych lub niezgodnych z prawem. Do grupy zachowań ryzykownych można włączyć seksting (w tym seksting kamerkowy) – czyli zjawisko przesyłania treści (zdjęć, filmików) o charakterze erotycznym, głównie swoich nagich lub półnagich zdjęć, za pomocą Internetu i telefonu komórkowego. Seksting może również przyjmować formę seks-komunikacji na żywo, za pośrednictwem komunikatorów z wykorzystaniem kamerki wideo w urządzeniu. Z badań wynika, iż co czwarty polski nastolatek otrzymał intymne zdjęcia, 7% nastolatków wysłało intymne zdjęcia, a ok. 30% nastolatków „zna osobę", która wysyła intymne zdjęcia[12]. Ponadto nastolatki nadużywają/

[10] J. Grubicka*, Social are of the internet in the context of values and personal sofety threats in cyberspace*, International Journal of Pedagogy Innovation and New Technologies 2020, nr 7(1), Warszawa 2020, s. 16–30.

[11] L. Kirwil, *op.cit*., s. 42–44.

[12] Raport *Ogólnopolskie badanie Nastolatki wobec Internetu realizowane przez Pedagogium WSNS we współpracy z Rzecznikiem Praw Dziecka oraz Naukową i Akademicką Siecią Komputerową*, Warszawa 2014.

dysfunkcyjnie korzystają z Internetu (13%)[13], uprawiają hazard online oraz przede wszystkim nie chronią swojej prywatności poprzez udostępnianie szerokiemu gronu odbiorców zbyt wielu informacji o sobie, publikowanie licznych zdjęć i przyjmowanie do grona znajomych przypadkowych osób. Owa „otwartość" bywa przyczynkiem do podejmowania przez innych użytkowników agresji elektronicznej i działań o charakterze przemocy. Są to m.in. wyzywanie, straszenie, prześladowanie, oczernianie, poniżanie kogoś w Internecie przy użyciu nowych technologii. Doświadczenia związane z różnymi formami cyberprzemocy, tj. przerabianiem i publikowaniem ośmieszających zdjęć i filmów, upublicznieniem sekretów ofiar, uporczywym, wulgarnym i złośliwym komentowaniem wpisów oraz celowym ignorowaniem aktywności online ofiary potwierdziło wielu młodych internautów[14].

Jaka przyszłość czeka Internet? Nowoczesne technologie, zmieniające się w niezwykle szybkim tempie sprawią, iż techniczne korzystanie z sieci stanie się jeszcze łatwiejsze. Być może do pracy z komputerem, o ile będzie adekwatnym używanie takiej nazwy, wystarczy komunikowanie głosowe. Z całą pewnością sieć stanie się jeszcze bogatszym źródłem wiedzy, informacji, rozrywki i platformą komunikacji. Taka perspektywa jest całkiem realna i być może zupełnie bliska. Jedno się nie zmieni – korzystanie z Internetu jest i będzie kwestią odpowiedzialności, potrzebna jest i będzie refleksja nad tym, z jakich materiałów warto, a z jakich nie należy korzystać.

Prawo i wolność społeczeństwa informacyjnego w Internecie

Do fundamentalnych praw społeczeństwa informacyjnego należą: swobodny dostęp do globalnej infrastruktury informacyjnej, prawo własności, wiarygodność informacji oraz prawo do ochrony prywatności[15]. Gwarancja tych praw oraz ich ochrona jest dla współczesnych państw dużym wyzwaniem. Narodowe unormowania legislacyjne dotyczące Internetu są ograniczone terytorialnie. Immanentną cechą Internetu jest jego globalny zasięg, umożliwiający umieszczanie w jego zasobach dowolnych komunikatów. Problemem współczesnych państw staje się zatem przeciwdziałanie publikowaniu w sieci określonych treści. Często zwraca się uwagę na to, że Internet – jakkolwiek kojarzony na ogół z wolnością wypowiedzi – może również stać się narzędziem inwigilacji i nadzoru nad obywatelami. Daje bowiem różnym firmom i instytucjom duże możliwości śledzenia użytkowników, zbierania wiadomości i sporządzania baz danych o potencjalnych klientach. Również instytucje państwowe w coraz większym stopniu interesują się tym, co dzieje się

[13] K. Makaruk, S. Wójcik, *EU NET ADB, Badanie nadużywania internetu przez młodzież w Polsce*, Warszawa 2012.

[14] Por. *EU NET ADB Badanie nadużywania Internetu przez młodzież w Polsce*, Fundacja Dzieci Niczyje, Warszawa 2012, s. 7; Ł. Wojtasik, *Przemoc rówieśnicza a media elektroniczne,* „Dziecko Krzywdzone. Teoria, badania, praktyka" 2009, nr 1(26), s. 2; J. Pyżalski, *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Kraków 2012, s. 215–219; *Raport Nastolatki 3.0.*, Warszawa 2019.

[15] Y. Benkler, *Bogactwo sieci, Jak produkcja społeczna zmienia rynki i wolność*, Warszawa 2008, s. 476.

w sieci[16]. Można zatem zaryzykować twierdzenie, że cyberprzestrzeń powiększa sferę nie tylko wolności, ale i kontroli. Represje wobec niepokornych blogerów czy blokowanie dostępu do niepożądanych witryn stały się praktyką nagminnie stosowaną w niektórych krajach wrogo nastawionych do wolności w sieci, np. w Chinach. Państwa autorytarne mogą korzystać z funkcji filtrowania i monitorowania przekazu. Istnieje przekonanie, że odpowiedni dostęp do narzędzi internetowych zapewni wszędzie większą wolność. Przykład Chin wskazuje jednak na coś innego. Chiny, bardziej niż jakikolwiek inny kraj, udowadniają, że możliwy jest powszechny dostęp do Internetu przy jednoczesnym zachowaniu kontroli jego wykorzystania[17]. Zasadniczą kwestią w tym zakresie jest wyważenie racji pomiędzy bezpieczeństwem państw i społeczeństw a wolnością jednostki i jej prawem do swobodnej wymiany informacji. Człowiek, mając do czynienia z coraz większym postępem technologicznym, traci czujność i zbytnio ufa technologii. Szczególnie niebezpieczne jest to w przypadku ochrony informacji, gdzie ich znaczna większość przesyłana jest za pośrednictwem Internetu[18].

Biorąc pod uwagę fakt rzeczywistych zagrożeń wirtualnej sieci oraz coraz większych, realnych strat związanych z ich skutkami, od ponad dwóch dekad podejmuje się wysiłki zmierzające do unormowania cyfrowego świata – tak na poziomie państw, organizacji, jak i w szerokiej przestrzeni międzynarodowej. Nie podlega dyskusji fakt, że w obecnym kształcie nie istnieje już możliwość powrotu do czasów początków sieci, która była miejscem tylko i d e i i służyła głównie wymianie myśli użytkowników, urzeczywistniając marzenie o globalnej komunikacji. Dziś jest osnową funkcjonowania każdego obszaru i sfery – tak państwowej, jak i prywatnej. Sednem staje się wyzwanie znalezienia równowagi pomiędzy zachowaniem wolności sieci a jej bezpieczeństwem – w każdym ze wspomnianych wcześniej poziomów i w każdym obszarze. Najlepszym przykładem podejmowanych działań w tym zakresie są w szczególności: Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń, Dyrektywa w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii czy – w przestrzeni międzynarodowej – amerykańska międzynarodowa strategia dla cyberprzestrzeni. Wspólnym mianownikiem podejmowanych działań jest jasno określony cel: utrzymanie i rozwój bezpieczeństwa sieci z zapewnieniem wolności Internetu – rozumianej generalnie jako rozwój społeczeństwa opartego na ochronie podstawowych praw i wolności (w szczególności wolności słowa) z jednoczesną, efektywną ochroną danych i prywatności oraz zapewnienie wolnego przepływu informacji, m.in. zapobieganie cenzurze). Parafrazując słowa A. de Tocqueville'a, można stwierdzić, że wolność sieci kończy się tam, gdzie zaczyna się jej bezpieczeństwo.

[16] M. Podgórski, *Wirtualne społeczności i ich mieszkańcy. Próba etnografii*, [w:] *Wielka sieć. E-seje z socjologii Internetu*, J. Kurczewski (red), Warszawa 2006, s. 105–106.

[17] Y. Benkler, *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność*, Warszawa 2008, s. 159.

[18] J. Grubicka, *Konwergencja technologiczna a system bezpieczeństwa informacji*, [w:] *Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use*, W. Filipkowski (red.), Gdynia 2015, s. 86–99.

Nie sposób bowiem zapewnić bezpieczeństwa bez ingerencji w wewnętrzną strukturę i sposób funkcjonowania danej sfery. Jednocześnie nie sposób zapewnić wolności bez jej ochrony, co w przypadku świata cyfrowego, z uwagi na jego szczególną specyfikę (również od strony *stricte* technicznej), doprowadziłoby w konsekwencji albo do anarchii, albo do przejęcia kontroli przez silniejszych.

Zagrożeniem dla tak pojmowanej wolności stają się jednak innego rodzaju działania, które pozwoliłyby dostawcom usług internetowych na ustanawianie różnych warunków dostępu dla użytkowników, z prawem wprowadzania dodatkowych opłat za tzw. usługi specjalne włącznie. Wyzwaniem natomiast – regulacje z obszaru *post mortem*, ponieważ tylko od wiedzy i uprzedniego działania użytkowników zależy, czy ich spadkobiercy będą w stanie nie tylko odziedziczyć cyfrowe aktywa, ale także mieć możliwość zakończenia spraw w świecie cyfrowym, takich jak: korzystanie z usług, serwisów czy usunięcie kont. Kwestie tego rodzaju, mimo że wrażliwe, pozostają niezwykle istotne: obecnie większość tak prozaicznych spraw, jak chociażby rachunki, realizuje się za pośrednictwem sieci (powiadomienie na e-mail, dokonanie opłaty za pośrednictwem bankowości elektronicznej itp.). Z dotychczasowych rozważań wysnuć można wniosek, że tak jak cyberprzestrzeń posiada określone warstwy, tak i paradygmat wolności sieci w tych warstwach będzie się przejawiać. Na poziomie informacyjnym będzie dotyczyć: otwartego, równego i nieograniczonego dostępu do ich zasobów dla wszystkich użytkowników. Kwestia ta ma znaczenie również w kontekście tzw. wolnego oprogramowania, którego idea, jak i realizacja zakłada możliwość uruchamiania, kopiowania, rozpowszechniania, analizowania oraz zmianę i poprawianie przez użytkowników. Zgodnie z definicją wolnego oprogramowania opublikowaną przez Free Software Foundation[19] użytkownikowi przysługują następujące wolności, które jednocześnie stanowią podstawowe założenia, aby oprogramowanie można było określać mianem wolnego:

- wolność 0: uruchamiania programu w dowolnym celu;
- wolność 1: analizowania programu oraz dostosowywania go do swoich potrzeb;
- wolność 2: rozpowszechniania kopii programu;
- wolność 3: udoskonalania programu i publicznego rozpowszechniania własnych ulepszeń, dzięki czemu może z nich skorzystać cała społeczność[20].

Program jest wolnym oprogramowaniem, jeśli zapewnia użytkownikom wszystkie te wolności. W przeciwnym wypadku jest „niewolnym".

Wskazane założenia pozwalają lepiej zrozumieć kontekst korzystania z usług sieciowych typu *Software as a Service* (SaaS), których istotą jest oferowanie określonych usług lub programów przez usługodawcę, uruchamianych na jego urządzeniach. W praktyce oznacza to, że użytkownik korzysta z narzędzi/programów oferowanych przez usługodawcę za pośrednictwem przeglądarki internetowej, nie ma zatem

[19] *What is free software?*, http://www.fsf.org/ [dostęp: 9.01.2019].
[20] *Wolne oprogramowanie*, Wikipedia, https://pl.wikipedia.org/wiki/Wolne_oprogramowanie [dostęp: 9.11.2017].

potrzeby instalowania oddzielnego oprogramowania na własnym urządzeniu, np. pakiet aplikacji Google, aby wykorzystywać w pełni ich funkcjonalność. Mimo wygody w korzystaniu z tego rodzaju usług, jak stwierdził jednoznacznie Richard M. Stallman: „Nie mamy żadnej kontroli, korzystając z usługi w sieci, pozbawiamy się wolności. I to zarówno w zakresie powierzanych usługodawcom danych, ale także tej wolności, które daje użytkownikom prawdziwie wolne oprogramowanie”[21]. Poza brakiem kontroli nad danymi, również w gestii usługodawcy pozostaje sposób i zakres korzystania przez użytkowników z udostępnianego oprogramowania, ponieważ *de facto* używany jest komputer usługodawcy. Przede wszystkim nie należy wychodzić z założenia, że Internet to miejsce, gdzie każdy może pisać, co chce i zaniechać dochodzenia swoich praw. Personalia autora obrażającego nas wpisu można ustalić, nawet jeśli posługuje się on anonimowym pseudonimem. Nie zawsze jednak można namierzyć sprawcę po numerze IP – ponieważ może on korzystać z komputera publicznego. Jedną z opcji jest możliwość zgłoszenia się do administratora portalu z informacją o naruszeniu naszego dobrego imienia na łamach serwisu. Jeśli administrator określonej strony odmawia pomocy, mamy możliwość udania się do Generalnego Inspektora Ochrony Danych Osobowych z prośbą o ujawnienie danych. W dalszej kolejności z pomocą może nam przyjść Prokuratura. Mamy oczywiście możliwość również wkroczenia na drogę cywilną w celu ustalenia, kim jest nadawca znieważających nas przekazów, jednak może się to okazać stosunkowo kosztowne i łatwiejsza będzie droga związana z postępowaniem karnym. Walka o dobre imię może być trudna i czasochłonna, ale warto ją podjąć.

Nie sposób rozważać wolności sieci tylko w powszechnie znanej jej postaci, ponieważ posiada ona równoległą warstwę określaną mianem Deep Webu (ukryta sieć/głęboka sieć). Z określeniem tym wiążą się także nazwy: Dark Netu/Dark Webu. Dark Web oznacza witryny ukrywające adresy IP serwerów, z których korzystają, co m.in. powoduje, że nie jest możliwe znalezienie takich witryn za pośrednictwem standardowych wyszukiwarek. Wykorzystywanym najczęściej do tego narzędziem szyfrującym pozwalającym ukryć adresy, ale również użytkowników końcowych, jest The Onion Router (TOR)[22]. Pomimo kontrowersji, jakie wzbudzają tego typu narzędzia, w szczególności w zakresie nielegalnej zawartości lub przestępczej działalności, rozwiązania dające możliwość anonimizacji aktywności służą również legalnym (zwykłym) użytkownikom, którzy nie chcą być śledzeni przez narzędzia wykorzystywane przez dostawców usług cyfrowych, np. przeglądarki. Klasycznym już przykładem możliwości śledzenia aktywności użytkowników są tzw. ciasteczka cookies, które co do zasady powinny jedynie wspomagać działania samej aplikacji. Śledzenie wyszukiwanych treści, odwiedzanych witryn, pobieranych plików czy kupowanych przedmiotów, co pozwala na tzw. profilowanie użytkownika (zainteresowania, przyzwyczajenia czy nawet miejsce zamieszkania).

[21] *Richard M. Stallman odwiedził Polskę. Król hakerów twierdzi, że w Sieci pozbawiamy się wolności*, http://gadzetomania.pl/3758,richard-m-stallman-odwiedzil-polske-krol-hakerow-twierdz-ze-w-sieci-pozbawiamy-sie-wolnosci [dostęp: 11.09.2017].

[22] Do maskowania adresu IP można – poza węzłami TOR-a – skorzystać np. z *web proxy*.

W klasycznym, szerszym ujęciu bezpieczeństwo definiowane jest jako stan wolny od zagrożeń. W kontekście bezpieczeństwa informacyjnego jest to stan wolny od zagrożeń, takich jak: sabotaż, szpiegostwo, dywersja, ale również przekazywanie informacji nieuprawnionym podmiotom.

W zakres tej definicji wchodzi także wszelka działalność służąca zabezpieczaniu zasobów informacyjnych – wytwarzanych, gromadzonych, przetwarzanych, przechowywanych i przekazywanych w sieciach komunikacyjnych oraz nośnikach informacji (komputery, serwery, bazy danych), a w szczególności systemy oraz metody zabezpieczeń. Bezpieczeństwo zasobów – w znaczeniu technicznym – określają dwa modele zarządzania: restrykcyjne (to, co nie jest dozwolone, jest zabronione) oraz liberalne (to, co nie jest zabronione, jest dozwolone).

Wskazywane wcześniej dokumenty o charakterze strategicznym i normatywnym zakładają stworzenie określonych stref odpowiedzialności za bezpieczeństwo samej sieci i tym samym danych w niej funkcjonujących, tj. Internet, intranet, ekstranet itp., jak i za poszczególne elementy i obszary. Za przykład może posłużyć nałożenie w drodze przyjętej Dyrektywy NIS[23] określonych obowiązków w obszarze bezpieczeństwa na operatorów usług kluczowych, tj. sektorów krytycznych, takich jak prywatne lub publiczne: finanse, energetyka, transport, opieka zdrowotna, oraz dostawców usług cyfrowych (wyszukiwarki, platformy handlowe, usługi przetwarzania w chmurze). W pierwszym zbiorze mieszczą się podmioty, które – zgodnie z art. 5 Dyrektywy – spełniają łącznie następujące przesłanki:

- świadczą usługę, mającą kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;
- świadczenie tej usługi zależy od sieci i systemów informatycznych – incydent miałby istotny skutek zakłócający dla świadczenia tej usługi.

Ponadto każde z państw członkowskich Unii Europejskiej jest zobowiązane do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, określającej cele strategiczne oraz odpowiednie środki i regulacje mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych oraz obejmujące minimum wskazane w Dyrektywie sektory i usługi. Ponadto określone zostały kwestie, które bezwzględnie muszą uwzględniać krajowe strategie w zakresie bezpieczeństwa sieci i systemów informatycznych, mianowicie:

- priorytety i cele bezpieczeństwa sieci i systemów informatycznych;
- ramy zarządzania służące realizacji przyjętych celów – w tym role i zakresy;
- obowiązki organów i instytucji rządowych oraz pozostałych, właściwych podmiotów (każde z państw zobligowane zostało do wyznaczenia organu lub organów do ochrony bezpieczeństwa cybernetycznego);
- środki w zakresie gotowości, reagowania oraz przywracania funkcjonowania do stanu normalnego, w tym także w zakresie współpracy pomiędzy sektorami publicznym i prywatnym;

[23] Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci…, *op.cit.*

- w zakresie przyjętych strategii krajowych: wytyczne dla programów edukacyjnych, informacyjnych oraz szkoleniowych oraz wytyczne dla planów badawczo-rozwojowych;
- plany oceny ryzyk służący ich określaniu;
- wykaz podmiotów zaangażowanych we wdrażanie strategii[24].

W obszarze współpracy międzynarodowej Dyrektywa NIS w art. 13 przewiduje możliwość zawierania umów międzynarodowych „zgodnie z art. 218 TFUE, z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając i organizując ich udział w niektórych działaniach grupy współpracy. Takie umowy muszą uwzględniać potrzebę zapewnienia odpowiedniej ochrony danych"[25]. W odniesieniu do globalnego zasięgu sieci istotne znaczenie ma również zapis art. 18 ust. 2. Jurysdykcja i terytorialność, który stanowi, że: dostawca usług cyfrowych, który nie posiada jednostki organizacyjnej w Unii, ale oferuje usługi w zakresie:

- internetowej platformy handlowej;
- wyszukiwarki internetowej;
- przetwarzania w chmurze;
- wyznacza przedstawiciela w Unii, który musi posiadać jednostkę organizacyjną w jednym z tych państw członkowskich, w których oferowane są usługi.

W zakresie jurysdykcji oznacza to, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną.

Podniesienia w tym miejscu wymaga również kwestia istoty istnienia sieci rozumianej jako globalnego medium oraz środowiska funkcjonowania społeczeństwa informacyjnego: jej osią, punktem centralnym i zarazem punktem odniesienia jest i pozostanie użytkownik, jednak mimo jego kluczowej roli niewiele miejsca i uwagi poświęca się mu w dokumentach, które zdają się kłaść nacisk na wszystkie z wymienionych wcześnie warstw cyberprzestrzeni. Rzeczona odpowiedzialność, ale przede wszystkim świadomość mechanizmów i cyfrowych zagrożeń użytkowników ponad wszelką wątpliwość przyczyniłyby się do szybszego i pełniejszego osiągnięcia wytyczonych celów w tym obszarze.

Zakończenie

Najbardziej ogólną i raczej powszechnie przyjętą granicą wolności jednego człowieka jest wolność drugiego. Korzystając z dobrodziejstw wolności słowa, prawa do posiadania własnych poglądów i dóbr, prawa do poszanowania osobistej godności, nie można zapominać, że te same prawa przysługują innym, a zatem wszelkie

[24] Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa w sieci…, *op.cit*.

[25] *Ibidem*.

działania jednostki nie mogą ograniczać i naruszać praw innych ludzi. Nie ma żadnych powodów, by te normy postępowania w realnej rzeczywistości nie odnosiły się w tym samym stopniu do przestrzeni wirtualnej w Internecie. W końcu jest to tylko narzędzie i choć bez wątpienia wpłynęło ono na życie społeczne, to mimo wszystko człowiek jest jego twórcą, a nie tworzywem. Rozpowszechnianie w Internecie treści prawnie zakazanych (pedofilia, nawoływanie do przestępstw, propagowanie faszyzmu czy komunizmu, przygotowywanie działań o charakterze terrorystycznym) jest i powinno być karane. Administratorzy portali, na których takie treści są zamieszczane, muszą mieć bezwzględne prawo, a nawet obowiązek ich usuwania. Odrębną i niezwykle istotną kwestią jest powszechnie występujący w Internecie brak odpowiedzialności za słowo, zwłaszcza w anonimowych wulgarnych „postach", świadomie wymierzonych w godność osoby, dobre imię grupy społecznej bądź organizacji, której dotyczą. Wydaje się, że nie byłoby naruszeniem wolności wypowiedzi, gdyby udało się praktycznie wdrożyć zasadę, że wpisy i komentarze w Internecie nie mogą funkcjonować anonimowo, że technicznym warunkiem ukazania się treści w Internecie jest zarejestrowanie się i podanie swych danych osobowych (w formie ukrytej dla ogółu odbiorców). Ogólnie rzecz ujmując, powinna obowiązywać zasada – tyle wolności, ile odpowiedzialności. Ograniczenia zawsze jednak winny mieć charakter zindywidualizowany, odnoszący się do konkretnej osoby czy grupy osób podejmujących sprzeczne ze społecznymi normami działania. W żadnym natomiast przypadku nie mogą to być ograniczenia wprowadzane na drodze administracyjnych decyzji władzy i dotyczące społeczeństwa. Takie formy działania są przejawem totalitaryzmu i żadnymi względami nie mogą być usprawiedliwione. Z pewnością długo jeszcze potrwa wypracowanie konsensualnej, wspólnej wizji bezpiecznej i zarazem wolnej przestrzeni cyfrowej. Internet sprawia, że trudniej jest reżimom autorytarnym kontrolować ludność, tak samo niespotykana otwartość i wolność środowiska usieciowionego wymaga nowych sposobów ochrony społeczeństw otwartych przed jednostkami i grupami działającymi destrukcyjnie. Warunkiem skutecznego egzekwowania ograniczeń jest współpraca międzynarodowa.

Bibliografia

Benkler Y., *Bogactwo sieci, Jak produkcja społeczna zmienia rynki i wolność*, Warszawa 2008.

Grubicka J., Motyka R., *Człowiek jako ważne ogniwo zapewnienia bezpieczeństwa informatycznego jednostce administracyjnej*. *Bezpieczeństwo w administracji i biznesie we współczesnym świecie*, cz. II, Gdynia 2011.

Grubicka J., *Konwergencja technologiczna a system bezpieczeństwa informacji*, [w:] *Nowoczesne technologie na rzecz bezpieczeństwa. Zagadnienia dual-use*, W. Filipkowski (red.), Gdynia 2015.

Grubicka J., *Social are of the internet in the context of values and personal sofety threats in cyberspace*, International Journal of Pedagogy Innovation and New Technologies 2020, nr 7(1), Warszawa.

Grubicka J., *Restricting freedom on the internet in a public security space*, East Journal of security studies No 2, Słupsk–Harkov 2017.

Grubicka J., Zbroszczyk D., *Cyberaptologie jako zagrożenie dla bezpieczeństwa publicznego*, [w:] „Doctrina" Studia społeczno-polityczne 2019, nr 16, Siedlce 2019.
Burszta W.J., *Internetowa Polis w trzech krótkich odsłonach*, [w:] *Ekran, Mit, Rzeczywistość*, W.J. Burszta, Warszawa 2003.
Kirwil L., *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo – część 2. Częściowy raport z badań EU Kids online przeprowadzonych wśród dzieci 9–16 i ich rodziców*, Warszawa 2011.
Kulesza J., *Ius internet. Między prawem a etyką*, Warszawa 2012.
Makaruk K., Wójcik S., *EU NET ADB, Badanie nadużywania internetu przez młodzież w Polsce*, Warszawa 2012.
Mead M., *Kultura i tożsamość. Studium dystansu międzypokoleniowego*, Warszawa 2000.
Pyżalski J., *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*, Impuls, Kraków 2012.
Podgórski M., *Wirtualne społeczności i ich mieszkańcy. Próba etnografii,* [w:] *Wielka sieć. E-seje z socjologii Internetu*, J. Kurczewski (red.), Warszawa 2006.
Szpunar M., *Internet a wolność (od) wypowiedzi*, [w:] *Media – między władzą a społeczeństwem*, Rzeszów 2007.
Szpunar M., *Granice wolności słowa w Internecie*, [w:] *Nowe media komunikacja wizualna*, P. Francuz, S. Jędrzejewski (red.), Lublin 2010.
Szpunar M., *Przestrzeń Internetu – nowy wymiar przestrzeni społecznej*, [w:] *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, A. Siwik, L. Haber (red.), Kraków 2008.

Summary

Freedom seems to be not only an immanent, but even a constitutive feature of the virtual space in which the Internet functions. Based on current observations and current events, threats resulting from the general ability to publish opinions on the Internet have been indicated. This article does not aspire to be a comprehensive explication of the impact of new technologies on the functioning of societies in a holistic dimension, it is rather an attempt at exegesis of one of its areas - concerning the evolution of human interactions under the influence of new technologies. The author addresses various aspects of threats to freedom on the Internet so that the obtained understanding is comprehensive and objective, far from being a one-sided and schematic simplification. The Internet is by definition an egalitarian communication tool, a space for free creation and flow of content, limited only by technology and human imagination, the boundaries of which cannot be defined. The article indicates the need to consolidate the efforts of experts from many areas: security; psychology; law, as it appertains to freedom of society in the security space.