W kierunku wolności ponowożytnych. Środowisko internetowe a kwestia wolności

Autor: **Paweł Nowakowski**

W artykule tym[1] zamierzam przedstawić i uzasadnić trzy tezy, wśród których najważniejsze znaczenie przypisuję drugiej z nich. Wszystkie one są komplementarne, w tym sensie, że druga wynika niejako z pierwszej, zaś trzecia opiera się na przyjęciu zasadności drugiej i ma względem niej charakter swego rodzaju subtezy. Punktem wyjścia dla rozważań, źródłem których jest ten artykuł (a wcześniej referat na konferencji, której ta praca zbiorowa stanowi zwieńczenie) jest paradygmat wskazujący na dwa rodzaje wolności. Wątpliwości części społeczności uczonych odnośnie trafności i zasadności tego podziału sprawiają, że przyjęte przeze mnie stanowisko wyjściowe jest dość kontrowersyjne. Na kartach tego artykułu nie będę poruszał problematyki sporów i interpretacji filozoficznych odnoszących się do tej problematyki. Ograniczę się do przedstawienia tego, w jaki sposób pojmuję te dwa typy wolności w odniesieniu do bezpośredniego przedmiotu swoich rozważań. Dopiero wówczas przejdę do przedstawiania i uzasadniania swoich tez. Dodatkowo, wspomnieć należy, że trzecie twierdzenie również opiera się na pewnym punkcie odniesienia, którym jest zasada preferencji czasowej. Jednakże, w celu zachowania spójności wywodu oraz dlatego, że prawdziwość tej teorii nie jest szeroko kwestionowana, zarysuję jej podstawy nie w uwagach wstępnych, lecz we właściwej dla przedstawienia trzeciej tezy części artykułu. Jej uzasadnienie zostanie przedstawione metodą dedukcyjną.

Istotą paradygmatu, do którego nawiązuję, jest rozróżnienie, które w pewnym uproszczeniu obrazuje się czasami wyróżniając wolność *od* i wolność *do* jako dwa różne sposoby ujmowania tego podstawowego pojęcia (zob. np. Swift 2010). Uważam, że pomimo wspomnianych kontrowersji, przy odpowiednim zdefiniowaniu tych kategorii, mogą być one użyteczne, choćby tylko jako narzędzia metodologiczne. I tak wolność *do* definiuję tu jako możliwości i brak ograniczeń (poza pewnymi, obiektywnymi, jak np. pewne nakłady finansowe)

[1] Jest to rozdział pracy zbiorowej „Społeczeństwo sieciowe – między wolnością a zniewoleniem" pod redakcją Mariusza Baranowskiego i Bartosza Miki (Poznań 2012).

odnośnie realizacji swoich celów i szans przy wykorzystywaniu owoców postępu technologicznego. Z kolei wolność *od* jest to wolność podmiotu od gromadzenia, przechowywania, wykorzystywania i udostępniania przez inne podmioty dotyczących go informacji lub, wykorzystując słowa Ireny Lipowicz (2011: 5): „wolność od ingerencji innych w naszą autonomię informacyjną". Żaden z tych rodzajów wolności nie może być absolutny, co wynika z faktu, że człowiek żyje w społeczeństwie, podlegając przez to pewnym regułom (etycznym, prawnym) odnośnie kształtu tego życia, które to reguły normują zakres obu typów wolności. W tak rozumianej dystynkcji, wolność *od* pozostaje możliwie pełna, gdy, używając stwierdzenia Roberta Nozicka (1999: 205): „Moje prawo własności do mojego noża pozwala mi pozostawić go, wszędzie gdzie chcę, ale nie w twojej piersi".

Artykuł ten nie jest pierwszą publikacją na temat związany z Internetem, w której nawiązuje się do rozróżnienia na te dwa rodzaje wolności. Inga Oleksiuk (2004) zwracała uwagę na konflikt między wolnością do wypowiedzi u jednych, a wolnością od kontaktu z subiektywnie postrzeganymi jako nieprzyzwoite treściami. Z kolei Dominika Kotowicz (2006: 294–295) wspominała o „wolności od monopolistycznej kontroli", rozumianej jednak w kontekście pluralizmu kanałów komunikacji w Internecie. W sposób podobny, jak w niniejszym artykule, rozumiał rozróżnienie tej podstawowej wartości Janusz Morbitzer (2011: 60-61). Jednak wolność *od* została przez niego przedstawiona jako totalna samowola. Podejście swoje zaczerpnął on dwóch innych autorów, którzy pisali o tej kategorii w kontekście środowiska internetowego, Józefa Klocha i Roberta Geislera. Morbitzer wspominał również o wolności od Internetu jako „samego narzędzia" (Tamże: 60-61).

Moja pierwsza teza koresponduje ze stwierdzeniami kilku autorów, które chciałbym w tym miejscu przytoczyć. Wojciech Lis (2010: 177) napisał: „Nowoczesne komputery, coraz doskonalsze programy służące do ich obsługi, Internet, sieci komórkowe, telewizja satelitarna, monitoring z pewnością **ułatwiają** codzienne życie, ale jednocześnie stanowią poważne **zagrożenie** dla wolności i praw człowieka, zwłaszcza dla jego prywatności". Cytowana wyżej Lipowicz (2011: 8) stwierdziła zaś: „(...) rozwój technologii informacyjnych stwarza nowe **zagrożenia** nie tylko dla bezpieczeństwa zewnętrznego i wewnętrznego ale i dla wolności człowieka (...)". Natomiast Kotowicz (2006: 298)

ujęła ten problem następująco: „Wolność dostępu do informacji, jaką zapewnia internet, posiada dwie wykluczające się implikacje: z jednej strony **łatwość** zdobycia pożądanych wiadomości, z drugiej **niebezpieczeństwo** [podkreślenia we wszystkich trzech cytatach moje] wykorzystania danych przez osoby lub grupy do tego niepowołane". Chciałbym zradykalizować te wypowiedzi. Nie będzie specjalnie oryginalnym stwierdzenie, że wolność *do*, tak ją rozumiem, ma charakter dynamiczny, a zwrot jej wektora biegnie w jednym kierunku, powodując systematyczne zwiększanie tego typu wolności w środowisku internetowym. Uważam jednak, że również wolność *od* jest w tych realiach wartością dynamiczną, tyle że jej wektor skierowany jest w kierunku przeciwnym. Skutkuje to systematycznym zmniejszaniem się tego rodzaju wolności. Sądzić należy, że występuje ścisła korelacja między tymi zjawiskami – a więc jednoczesnym powiększaniem się wolności *do* i kurczeniem się wolności *od*. W podobnym tonie wypowiedział się Wolfgang Sander-Bauermann, badacz specjalizujący się w wyszukiwarkach internetowych, stwierdzając: „Ceną, jaką płacimy za korzystanie z usługi, są dane zbierane na temat każdego użytkownika" (cyt. za Reppesgaard 2009: 24).

Wspomniana korelacja jest widoczna na trzech płaszczyznach. P i e r w s z a z nich związana jest z coraz to większą, celową, przekraczającą granice konieczności, wynikające z obsługi internauty czy wykonywania zadań służbowych, ingerencją w wolność *od* przez inne podmioty. Istnienie d r u g i e j płaszczyzny wynika z utworzenia narzędzi, które implikują wspomnianą korelację z samej swej istoty. Natomiast t r z e c i a jest wynikiem rezygnacji z wolności *od* przez samych jej dysponentów.

Płaszczyzna p i e r w s z a dotyczy rządu i podległych mu instytucji oraz podmiotów nie-rządowych (czyli głównie prywatnych). Znana jest ona, rzec można, powszechnie. Zacznę tu od uwagi, że nie trzeba dowodzić oczywistej tezy, iż Internet stwarza możliwość zwiększenia wolności *do*. Pozwala oszczędzać czas, wielce ułatwia realizację różnych celów i zwiększa paletę możliwości, jakie otwierają się dzięki niemu przed podmiotem. Wystarczy zatem wskazać na podłoże, na którym dochodzi do kurczenia się wolności *od*. Wspomnianą korelację dostrzega się automatycznie. Przykładów, którymi można się posłużyć jest bardzo wiele. Najpierw podam kilka dotyczących rządu i podległych mu instytucji.

Dobrym przykładem jest brytyjska ustawa Regulation of Investigatory Power Acts (RIPA). Na jej mocy przyznano znacznej liczbie instytucji prawo uzyskania danych od operatorów internetowych, w sytuacji, gdyby bezpieczeństwo narodowe wymagałoby dostępu do tych informacji. Do czego wykorzystano ten instrument prawny? Między innymi do inwigilacji rodzin trojga uczniów, aby znaleźć odpowiedź na pytanie, czy uczniowie ci zamieszkują rejon odpowiadający szkole, w której się uczą. (Kulesza 2010: 85) Jak można stwierdzić, wykupując dostęp do Internetu, rodziny te naraziły się na elektroniczną inwigilację. Inny przykład stanowi przyjęcie w 2002 roku przez państwa grupy G8 aktu „Zasady dostępu do danych istotnych dla ochrony bezpieczeństwa publicznego". Dokument ten wytyczał strategię dążącą do zobowiązania komercyjnych usługodawców do współpracy ze służbami specjalnymi. Jak zauważył Krzysztof D. Szatrawski (2008: 138): „Usługi wymienione w tym akcie obejmują wszelkie rodzaje połączeń sieciowych, zaś udostępnione w ten sposób dane w powiązaniu z dostępem do Internetu pozwolą na monitorowanie dowolnego użytkownika w czasie rzeczywistym oraz wykorzystanie zarchiwizowanych danych o aktywności wszystkich użytkowników w dowolny sposób, na przykład w celu określenia zainteresowań, szybkości reakcji, zdolności poznawczych i kreatywności każdego obywatela. Wizja totalnie kontrolowanego społeczeństwa staje się w świetle tego dokumentu niebezpiecznie realna". Warto też zwrócić uwagę na bazę MATRIX (Multistate Anti-Terrorism Information Exchange). Początkowo funkcjonowała ona w firmie o nazwie Seisint Inc. na Florydzie, jednak po zamachach w Nowym Jorku w 2001 roku przekształciła się w podporządkowany służbom specjalnym organ o charakterze szpiegowskim. Baza ta łączyła informacje o aktywności w czasie rzeczywistym użytkowników Internetu (zakupy, wyszukiwane informacje, zainteresowania) z danymi znajdującymi się w państwowej bazie danych (Tamże: 133). W ten sposób konstruowano „podstawę do opracowania kompletnego portretu psychologicznego każdego obywatela" (Tamże). Można też powiedzieć parę słów o Rzeczpospolitej. Polskie służby państwowe mają legalny dostęp do treści objętych tajemnicą komunikowania się. Wystarczającym powodem dla uzyskania przez nie dostępu do tego rodzaju danych jest zamiar zapobieżenia lub wykrycia przestępstw, na co literalnie wskazują ustawy. „Funkcjonariuszom CBA, SKW [Służba Kontrwywiadu Wojskowego – przyp. P.N.] i ABW są udostępniane dane objęte tajemnicą komunikowania się w celu realizacji ich wszystkich

ustawowych zadań” (Lipowicz 2011: 9, 11, 13; szerzej na temat zakresu danych legalnie dostępnych aparatowi państwa zob. tamże: 9–13).

Więcej i bardziej różnorodne przykłady można podać odnośnie firm prywatnych. W środowisku internetowym najczęściej przetwarza się dane z portali społecznościowych i wyszukiwarek (Lewiński 2011: 56) Operatorzy wyszukiwarek mają bardzo duże możliwości o charakterze inwigilacyjnym (Fisher 2011). Istotną rolę mają tu pliki *cookie* (ang. *cookie*– ciasteczko). Mają one służyć personalizacji usług. Celem przetwarzania danych użytkowników przez operatorów wyszukiwarek ma być zwiększenie jakości świadczonych przez nich usług. Im więcej danych znajdzie się w posiadaniu operatora i im dłużej będą przez niego przechowywane, tym bardziej zindywidualizowane będą wyniki wyszukiwania informacji za pośrednictwem wyszukiwarki. Pliki *cookie* dzielą się na sieciowe i *flash*. Te pierwsze powstają w wyniku funkcjonowania wyszukiwarki, i przypisuje się je danemu użytkownikowi komputera. Warto dodać, że istnieje możliwość modyfikacji przeglądarki internetowej, tak aby nie przyjmowała plików *cookie*. Jednak dokonanie takich ustawień nie pozostaje bez znaczenia, jeśli chodzi o poprawne działanie usług. Pliki *flash cookies* mają za zadanie kopiować „ciasteczka” sieciowe, tym samym utrudniając ich kasowanie. Dzięki nim można także pozostawać w posiadaniu informacji o preferencjach danego internauty, wykorzystując np. treść fraz wpisanych w wyszukiwarkach. Kluczowa jest jednak kwestia, czy poprzez te działania można zidentyfikować konkretnego użytkownika (tamże: 66–67). Jak stwierdził organ UE, Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych: „Choć w większości przypadków bezpośrednia identyfikacja adresów IP przez wyszukiwarki nie jest możliwa, (...) dokonać [jej] może osoba trzecia. (...) [W] większości przypadków (...) dane konieczne do identyfikacji użytkownika(-ów) adresu IP są dostępne” (cyt. za: tamże: 66) W związku z tym pojawia się problem z zachowaniem tzw. „prawa do zostania zapomnianym” (Tamże: 64–66), które zalicza się w przyjętej przeze mnie siatce pojęć do zakresu wolności *od*. *Cookies* ułatwiają korzystanie z Internetu, personalizują je. Jednak mogą być w nich zawarte informacje o numerach kart kredytowych, loginach, hasłach, o stronach internetowych, które się odwiedzało, o kupowanych produktach (Lis 2010: 179; za: tamże). *Cookies* służą prywatnym podmiotom także do wybierania zindywidualizowanych reklam, jakie użytkownik ujrzy na swoim monitorze. W tym celu Google kupił firmę

DoubleClick, przodującą w dziedzinie internetowych banerów reklamowych. Dzięki niej śledzi (za pośrednictwem „ciasteczek") ruchy 80% internautów, i przesyła na ich monitory odpowiadające ich profilom reklamy. W podobnych celach Google zbiera dane na temat użytkowników należącej do niego poczty elektronicznej. Również portale społecznościowe zbierają dane o użytkownikach w celu pogrupowania ich pod kątem reklam, które ujrzą oni na swych monitorach (Poulet 2011: 54–55, 61, 66). Nieco ironicznie można zapytać, co stoi na przeszkodzie, by nie czytać internetowych rozmów i korespondencji, i nie podsyłać reklam, np. lodówek, kiedy ktoś żaliłby się swojemu rozmówcy, że jego chłodziarka się popsuła. Albo reklam agencji marketingowych i PR, gdyby ktoś rozważał start w wyborach, np. na Prezydenta RP.

Zupełnie innych przykładów dostarczyła firma Amazon. Użytkownicy, którzy postanowili skorzystać z usług tej firmy, nie sprawdziwszy uprzednio wystarczająco dokładnie ofert konkurencji, widzieli na ekranach wyższe ceny za te same produkty, niż ci, którzy postanowili poświęcić więcej czasu na poszukiwanie w sieci tańszych ofert. Różnice cen dochodziły do 10 dolarów (za Kulesza 2010: 93). Poza tym, dzięki wykorzystywanemu oprogramowaniu, klienci Amazon byli poddawaniu ocenie pod względem gustu, aby na tej podstawie zaoferować im górną cenę, którą, według obliczeń, mogliby zapłacić za dany produkt. Jeśli ktoś kupił za pośrednictwem tej firmy album muzyczny danego wykonawcy, to, w przypadku, gdyby za jakiś czas chciał kupić inną jego płytę, musiałby, oczywiście nie wiedząc o tym, zapłacić za nią odpowiednio drożej, niż ktoś inny, kto np. odwiedził sklep pierwszy raz (Szatrawski 2008: 130).

Na szczególną uwagę zasługują również zagrożenia *desktop search*, dzięki którym operator wyszukiwarki wchodzi w posiadanie informacji dotyczących treści dokumentów, które użytkownik utworzył lub przeglądał (Fischer 2011: 70) Jak pisał Bogdan Fischer (tamże): „Dalej idące serwisy typu *cloud* (np. Google Documents – edytor tekstu, Flickr – zdjęcia, planowany system operacyjny Chrome OS) zmierzają w kierunku umieszczania wszelkich osobistych informacji na serwerach firm oferujących reklamę behawioralną".

Przejdę teraz do omówienia d r u g i e j ze wskazanych płaszczyzn. Część z wyżej wskazanych przykładów można by powtórzyć dla zobrazowania także tego podłoża. Chodzi tu w szczególności o pliki *cookie* i korzystanie z

wyszukiwarek w ogóle. Zdaniem Kotowicz (2006: 279) komunikowanie się za pośrednictwem środków elektronicznych pociąga za sobą realne niebezpieczeństwo dostępu do treści przez wszystkich, którzy mają ku temu sposobność i potrafią to zrobić. W życiu generalnie nie można czuć się w pełni bezpiecznie, gdyż zawsze istnieje jakieś prawdopodobieństwo zakłócenia bezpieczeństwa jednostki, chodzi tu jednak o wspomnianą korelację: ułatwienie komunikacji obrazuje zwiększenie się wolności *do*, zaś jednoczesne wystawienie się na „pastwę" tych, którzy „mają sposobność i potrafią" oznacza (choćby potencjalne) pomniejszenie wolności *od*. Można bez przesady powiedzieć, że są to przykłady narzędzi, które implikują wspomnianą korelację z samej swej istoty. Przykładami dla tej płaszczyzny mogą być też programy do identyfikacji twarzy oraz usługa Google Street View. Joanna Kulesza (2010: 87) zwróciła uwagę, że „[n]ajwiększe zagrożenie stanowi światowa <<armia>> fotografów-amatorów (...). Szeregi tej armii zasilają aktywni, skrupulatni użytkownicy portali społecznościowych, którzy tworząc swoje <<siatki>> znajomych, pozwalają dotrzeć do praktycznie każdej osoby na ziemi (...)". Dzięki używanym przez te osoby programom do identyfikacji twarzy możliwe jest ustalenie tożsamości sfotografowanych osób, widniejących nawet na drugim planie fotografii. Usługę taką proponuje Google za pośrednictwem swojego programu o nazwie Picassa. Użytkownicy są zachęcani przez tę firmę do zaznaczania w Internecie, jakie osoby są widoczne na zdjęciu. Pozwala to na odnalezienie przez Picassę wszelkich zdjęć tej osoby, jakie przesłano do sieci (Tamże). Dostępne są też inne tego typu programy, które rozpoznają twarz, aby następnie skojarzyć fotografię z informacjami, które udostępnione są za pośrednictwem serwisu Facebook lub Nasza Klasa. Dzięki temu można wejść w posiadanie takich danych na czyjś temat, jak np. jego miejsce zamieszkania, zatrudnienie, wykształcenie, zainteresowania, grupa jego znajomych (Tamże: 88). Jak z pewną dozą ironii zauważa Kulesza (2010: 88): „W połączeniu z metadanymi, w które opatrywane są cyfrowe fotografie, nietrudno będzie ustalić, gdzie w tym roku na wakacjach przebywała większość znajomych, których fotografie w Picassie podpiszemy". Widać tu wzrost wolności *do*. Przejawia się on w zwiększonej możliwości „chwalenia" się swoimi zdjęciami przed innymi, możliwości dowartościowania się poprzez kreację swojego wizerunku w Internecie, imponowanie innym. Z drugiej strony pojawia się jednak zmniejszenie wolności *od* – od zidentyfikowanym przez obcą osobę czyjejś tożsamości i, w zależności od zakresu i charakteru

działalności w Internecie, szeregu innych informacji, możliwych do odkrycia na podstawie czyjegoś nazwiska – np. wszelkich zdjęć, na których uwieczniono wizerunek tej osoby i które umieszczono w sieci.

Połączenie różnych dostępnych środków umożliwia sporządzenie całościowego, szerokiego profilu danego użytkownika. Można posunąć się do stopnia, że przy posłużeniu się Google Maps lub Zumi.pl, wejdzie się w posiadanie takich informacji na temat konkretnego użytkownika, jak zdjęcie jego domu i okolicy. Za przykład może tu służyć osoba Toma Owada, który w 2006 roku wykorzystał dostęp do imion, nazwisk i miast zamieszkania klientów firmy Amazon, aby zestawić je z adresami znalezionymi w internetowej „książce" telefonicznej Yahoo! People Search. Dzięki temu, wykorzystując tym razem usługę Google Maps, wskazał zdjęcia domów konkretnych klientów w dużym powiększeniu. Warto dodać, że wybrał nabywców takich książek, jak np. „Rok 1984" czy „Fahrenheit 451" (Tamże: 88–89).

Szczególną uwagę zwraca, od niedawna dostępna również w Polsce, usługa Google Street View. Dzięki niej można wirtualnie podróżować ulicami, widok których dostępny jest w zakresie 360 stopni. Jest to możliwe dzięki wcześniejszemu sfotografowaniu ulic (wraz z całą właściwą im sferą publiczną) z wysokości 3–4 metrów (Spiecker gen. Döhmann 2011: 74). Jak słusznie zwraca uwagę Indra Spiecker gen. Döhmann (Tamże): „Należy przy odniesieniu do osoby odróżnić okazjonalną fotografię ludzi i przedmiotów oraz celowy zapis widoków budynków". Anonimizację („rozmazanie" twarzy oraz tablic rejestracyjnych) zapewnia się dopiero przed udostępnieniem zdjęć w Internecie, po obróbce fotografii pierwotnych. Według Google, opublikowano 20 milionów zdjęć[2], co oznacza, że przy marginesie błędu wynoszącym 0,5%, naruszono podstawowe prawa ok. 100 tysięcy osób. Co ważne, gromadzenie przez Google danych o właścicielach, przechodniach, użytkownikach, którzy znaleźli się na zdjęciach, nie ma bezpośrednio z nimi związanego powodu. Dzięki tej usłudze można znacznie obniżyć koszty (czas, pieniądze) realizacji celów. Pozwala to na oszczędności i nowe inwestycje. To z kolei implikuje powszechne korzystanie z Google Street View. Zachodzi niebezpieczeństwo zwiększenia efektywności działalności

[2]Należy zwrócić uwagę, że dane te podaję za autorką artykułu, na który się powołuję. Od tego czasu zdjęć tych zapewne zdecydowanie przybyło.

przestępczej przez np. możliwość łatwiejszego przygotowania się do jej popełniania. Zwiększają się też możliwości nękania (Tamże: 83, 86, 87). Zakładana przeze mnie korelacja jest tu bardzo dobrze widoczna.

Pozostaje omówienie t r z e c i e j z wymienionych płaszczyzn założonej na początku artykułu korelacji. Chodzi tu, dla przypomnienia, o rezygnację ze swojej wolności *od* przez samych jej dysponentów. Charakteryzując sytuację w Polsce Lipowicz (2011: 4) pisała: „Nowe pokolenie traktuje już wolność polityczną jako rzecz oczywistą, o która trzeba zabiegać raczej w innych krajach, a codzienne troski koncentrują się wokół bezpieczeństwa – finansowego i socjalnego. Ochrona prywatności i ustrojowe, ogólniejsze cele ochrony danych, w tym ochrona godności człowieka, wydają się drugoplanowe. Beztroskie <<dzielenie się prywatnością>> w portalach społecznościowych wydaje się wręcz atrybutem wolności", dodając (Tamże: 7–8): „Po co nam wolność skoro mamy bezpieczeństwo? Iluzoryczność poczucia zbędności przestrzeni indywidualnej wolności w życiu społecznym, a więc i prywatności, jest ściśle związana z nową iluzją bezpieczeństwa". Podobnie wypowiadał się Paweł Fajgelski (2011: 37), zwracając uwagę na pochopność i lekkomyślność w kontekście dysponowania, zauważając też jednak, że mamy do czynienia z „uzależnianiem świadczenia usług od zgody na przetwarzanie danych w celach marketingowych" (Tamże: 38).

Bardzo ważną kwestię, doskonale obrazującą trzecią płaszczyznę stanowi tzw. personalizacja usług, o której częściowo była już mowa. Chodzi tu o dostosowanie przez usługodawców treści, danych i usług do poszczególnych osób korzystających z ich oferty. W zamian za udostępnienie dodatkowych danych gwarantuje się użytkownikowi możliwość udziału w konkursach i promocjach, dostęp do określonych usług lub informacji. Dzięki temu korzystanie z oferty staje się efektywniejsze (Mazurek, Zając, Rakocy: 155, 156). Należy mieć na uwadze, że oferta wywiera na (potencjalnego) klienta określone bodźce. Danej firmie nie jest obojętna jego decyzja, odnośnie tego, czy zawrze on tą transakcję, czy nie. Dlatego, a tym bardziej mając świadomość o stosowaniu wyspecjalizowanych technik marketingowych, można się spodziewać, że owe bodźce będą coraz bardziej skuteczne. Dziesięć lat temu Ryszard Tadeusiewicz (2002: 135–136) zwrócił uwagę na to, że sprzeciw internautów wobec praktyk sprowadzających się do ich inwigilacji, spowodowany był przede wszystkim tym, iż nie wiedzieli oni o tym procederze. W momencie przedstawienia im oferty,

zgodnie z którą, w zamian za udostępnienie tych samych informacji na swój temat, otrzymywaliby gratyfikację, np. w postaci możliwości udziału w konkursach, odzew użytkowników Internetu był znacznie bardziej pozytywny. Podsumowując, autor ten stwierdził (Tamże: 136), że: „(...) [co prawda] niektórzy ludzie są skłonni rezygnować z przysługującego im prawa do prywatności (także w Internecie), chociaż nie bezinteresownie... Dotyczy to jednak raczej mniejszości. Zdecydowana większość uważa swoją strefę prywatną za wartość po prostu nienaruszalną". Jednakże w świetle powyższych przykładów, pochodzących ze znacznie bardziej aktualnych publikacji, trudno utrzymać owo zastrzeżenie autora. Zdaje się, że mamy do czynienia z innym zjawiskiem.

Owa trzecia płaszczyzna okazuje się kluczowe dla drugiej tezy tego artykułu. Kondycja obecnego społeczeństwa, którego podstawową cechą jest prawie że wszechobecność Internetu, pozwala na wysunięcie stwierdzenia odnośnie dominującego typu wolności w tym społeczeństwie. Nawiązując do dokonanego przez francuskiego liberała, Benjamina Constanta (1992) słynnego rozróżnienia na wolność starożytnych i wolność nowożytnych, proponuję uznać wolność czasów nam współczesnych jako **wolność ponowożytnych,** zastrzegając, że niekoniecznie uważam ją za związaną z nurtem postmodernistycznym.

Istotą wolności ponowożytnych jest preferowanie niepolitycznie rozumianej wolności *do* (rozumianej tak, jak zdefiniowałem ją na początku artykułu) kosztem wolności *od*. W przeciwieństwie do podmiotu kierującego się nowożytnym, oświeceniowym postrzeganiem wartości wolności, podmiot współczesny ceni wartość niezależności znacznie mniej niż jego poprzednik. Nie jest to bynajmniej paradoksalne cofnięcie się do wartości wolności rozumianej na sposób starożytny. Podmiot współczesny nadal dysponuje pewnym, wciąż nie małym, zakresem wolności *od*. Nie zanika ona. Dopóki podmiot godzi się, pośrednio czy bezpośrednio, na włączanie innych podmiotów do grona dysponentów prywatnych czy nawet wrażliwych danych na swój temat, dopóty jasne być musi, że ma się on czego zrzekać (wolności *od*). Wolność *do* staje się – nawet jeśli nie *de nomine*, to *de facto* – **bardziej cenna** niż wolność *od*. Świadomi zagrożeń godzimy się na coraz większe uszczuplanie naszej wolności *od*. Jakie są tego powody? Po pierwsze, trudno jest nam zrezygnować z niezwykłej dogodności, jaką daje Internet i współczesne społeczeństwo. Aby się nią cieszyć musimy

sprzedać naszą wolność *od*, która coraz częściej staje się cenna jako towar, jako nasza siła nabywcza. Możemy ją wymienić na szerszą wolność *do*, i czynimy to. Po drugie, wiemy, że tak też czynią inni – i zwykle (jak dotąd) kłopoty z tego powodu nie są zbyt częste, ani zbyt uciążliwe. Współczesny człowiek jest zdania, ze ciągle jeszcze warto, zaś ci, którzy zachowują zdanie odmienne często godzą się na uszczuplanie swej wolności *od*, wybierając „mniejsze zło" - czyli nie wykluczając się z pełnego udziału w społeczeństwie.

W związku z powyższym pozostaje trzecia teza tego artykułu, która brzmi następująco: podmiot jest tym bardziej skłonny do poświęcenia wolności *od* dla zwiększenia wolności *do*, im wyższa jest jego preferencja czasowa. Zasada preferencji czasowej została sformułowana przez Williama Stanleya Jevonsa, a rozwinięta przez Eugena Böhm-Bawerka. Dalszym rozwojem tej teorii zajęli się: Knut Wicksell, Frank Albert Fetter i Irving Fisher (Mises 2007: 415, 416). Treść tej zasady można przedstawić następująco: „Działający podmiot dąży zawsze do tego, żeby mniej zadowalający stan rzeczy zastąpić bardziej zadowalającym (...). Ponadto zawsze bierze pod uwagę, kiedy plany na przyszłość będą zrealizowane, czyli zastanawia się nad tym, ile czasu potrzeba na ich urzeczywistnienie, oraz nad tym, jak długo określone dobro będzie istniało i służyło. A zatem przedkłada dobra wcześniejsze nad dobra późniejsze oraz dobra trwalsze nad dobra mniej trwałe. " (Hoppe 2006: 32). Zasada preferencji czasowej stoi u podstawy tego, że podmiot decyduje się poświęcić dobro możliwe do uzyskania w krótkim czasie na rzecz dobra, które ma być dostępne później, jedynie pod warunkiem, że upatruje w tym większej satysfakcji, niż ta, jaką odniósłby, wybrawszy wcześniejszy dostęp do dobra. Ludzie różnią się pod względem stopy preferencji czasowej (może się ona zmieniać w czasie także w odniesieniu do tej samej osoby), co wynika z oceny satysfakcji, jaką niesie ze sobą konsumpcja teraźniejsza w stosunku do późniejszej. Można zatem mówić o wyższej i niższej preferencji czasowej, co oznacza, kolejno, mniejszą i większą skłonność do przedkładania dóbr możliwych do uzyskania później, lecz zarazem dających większą satysfakcję, nad dobra możliwe do uzyskania wcześniej, jednak zapewniające mniejszy stopień satysfakcji. Dla ludzi z wysoką preferencją czasową liczy się tylko teraźniejszość i to, co nastąpi zaraz po niej. Oczekują efektów swoich działań od razu, albo z jedynie minimalną zwłoką. Z kolei osoby charakteryzujące się niską stopą tej preferencji zorientowane są na przyszłość,

dlatego natychmiastowa konsumpcja cieszy się o wiele mniejszym zainteresowaniem z ich strony (Hoppe 2006: 32–38; cyt. za: tamże, 38; Mises 2007: 410, 412).

Dla podejmowanych przeze mnie rozważań ważne znaczenie ma fakt rzadkości czasu. By posłużyć się słowami Hansa-Hermanna Hoppego: „wybieranie, preferowanie pewnej rzeczy czy stanu nad inny, w oczywisty sposób pociąga za sobą to, że nie wszystkiego, nie wszystkich możliwych przyjemności, można doświadczać w tym samym czasie. Coś, co jest uważane za mniej wartościowe musi zostać poświęcone po to, aby osiągnąć coś innego, co jest uważane za bardziej wartościowe" (Hoppe 2010: 19). Ponadto, „czas zużyty dla osiągnięcia celu A powoduje, że mniej czasu zostaje na osiągnięcie innych celów. A im więcej czasu zabiera osiągnięcie pożądanego rezultatu, tym wyższe będą koszty obejmujące czekanie i, aby je usprawiedliwić, tym większe musi być oczekiwane zadowolenie" (tamże, 20).

Teoria preferencji czasowej została wykorzystana nie tylko w ekonomii, lecz również w myśli politycznej – tu należy wskazać na Hoppego (zob. Hoppe 2006) – czy politologii (Hoppe wyróżnił publikacje Banfielda [1974] i Smitha [1988]. Zob. Hoppe 2006: 38).

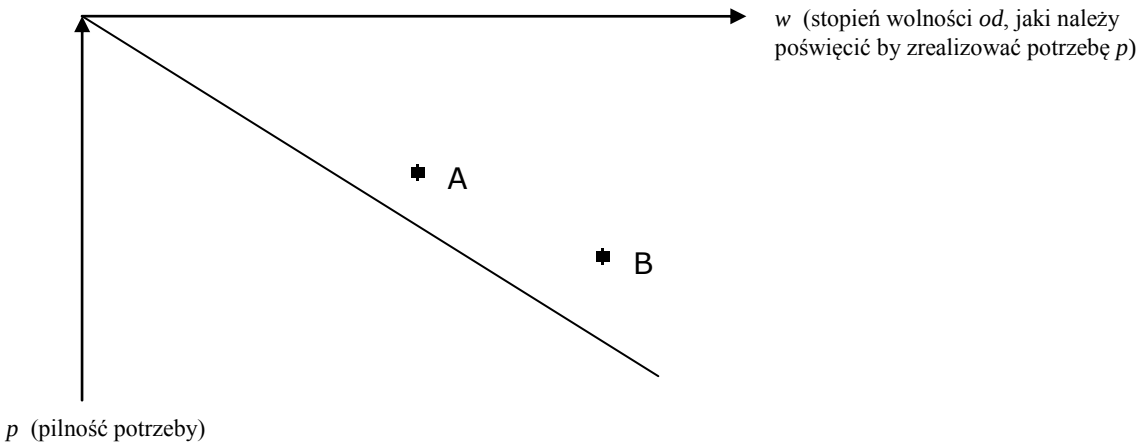
Jakie argumenty przemawiają na rzecz zasadności postawionej wyżej tezy? Zgodnie z tym, co zostało powiedziane wcześniej, człowiek nie został pozbawiony możliwości wyboru sposobu zagospodarowania swojej wolności *od*. Dlatego też, w dużej liczbie przypadków, wybiera pomiędzy poświęceniem części swej wolności *od* na rzecz zwiększenia wolności *do* a zachowaniem dotychczas posiadanego poziomu wolności *od* i tym samym rezygnacji ze zwiększenia swej wolności *do*. Nie ulega wątpliwości, że korzystanie z Internetu pozwala realizować te same cele w znacznie szybszym czasie. Tak jest przykładowo w przypadku komunikowania się za pomocą poczty elektronicznej, dokonywania przelewów internetowych, robienia zakupów, poszukiwania wszelkich informacji. Podobnie jest w przypadku korzystania z usług personalizacji, które pozwalają zaoszczędzić czas, a poza tym gwarantują czasami dodatkowe dobra, takie jak możliwość dostępu do dodatkowych usług lub udziału w konkursach. *Ceteris paribus*, oznacza to zmniejszenie kosztów przy osiąganiu tych samych celów. Jednak problem polega na tym, że *ceteris* nie są omawianych przypadkach *paribus*.

Pojawia się bowiem dodatkowy koszt, czyli wspomniana utrata części wolności *od*.

Gdyby działający podmiot zdecydował się zrealizować wspomniane cele w sposób „tradycyjny", nie narażałby się na utratę swojej wolności *od*, czy też, jak w przypadku personalizacji, wprost nie wymieniałby jej na udogodnienia (większy zakres wolności *do*). Dlatego podejmując decyzję, czy skorzystać, jeśli jest to jeszcze możliwe, z tradycyjnych metod zaspokajania potrzeb czy posłużyć się w ich zaspokajaniu Internetem, podmiot staje w obliczu dokonania rachunku oczekiwanych zysków i strat w związku z ewentualnym podjęciem i zaniechaniem określonego działania. W zależności od tego, czy szybsze osiągnięcie celu jest dla niego ważniejsze, niż zachowanie tej części wolności *od*, która musiałaby zostać poświęcona, aby cel ten został zrealizowany szybciej, czy też zachowanie dotychczasowego stopnia tej wolności ceni wyżej, niż szybszą realizację celu, zdecyduje się na odpowiednie działanie. Może być tak, i zapewne tak się też dzieje, że ten sam podmiot wybiera jedną alternatywę, albo drugą, w zależności od pilności potrzeby i stopnia wolności *od*, którego poświęcenia wymaga realizacja danej potrzeby. Pewnego razu może uznać, że warunki skorzystania z pośrednictwa Internetu są dla niego opłacalne, innego razu odmówić zawarcia tej „transakcji", wybierając metody tradycyjne, albo, w przypadku ich nieistnienia, w ogóle zaniechać realizacji potrzeby. Co jednak nastąpiłoby w przypadku, kiedy w obliczu takiej alternatywy stanęłoby dwoje ludzi, identycznie oceniających pilność swojej potrzeby i koszt w postaci poświęcenia części wolności *od*, którym obarczona byłaby realizacja tej potrzeby? Czy zawsze w tego rodzaju sytuacji postąpiliby jednakowo?

Otóż zgodnie z teorią preferencji czasowej należy odpowiedzieć, że decyzja każdego z tych podmiotów zostałaby dokonana w związku z właściwą każdemu z nich stopą preferencji czasowej. Gdyby oboje mieli identyczną stopę, ich decyzje byłyby, *ceteris paribus*, zawsze jednakowe. Gdyby jednak różnili się pod tym względem, ich decyzje byłyby jednakowe tylko do pewnego stopnia. Obrazuje to

Wykres 1.



W miarę, jak zmniejsza się pilność potrzeby (*p*), przy jednoczesnym wzroście stopnia wolności *od*, jaki należy poświęcić, by zrealizować potrzebę p (*w*), przy porównywaniu gotowości podmiotów A i B do podjęcia działania, dojdziemy do momentu, w którym jeden z nich (na wykresie założono, że będzie to podmiot A) uzna, że pilność potrzeby p jest mniejsza, niż koszt, jakiego wymaga jej realizacja – *w*. A będzie uważał, że możliwe przyszłe niedogodności, które wiązałyby się z poświęceniem przez niego danej części swojej wolności *od*, nie są warte (szybszej) realizacji potrzeby na danym rodzaju pilności. Dlatego zdecyduje się na zrealizowanie swojej potrzeby w sposób tradycyjny, zamiast przy użyciu Internetu, albo w ogóle zaniecha jej realizacji. Z kolei podmiot B uzna, że nadal warto poświęcić dany stopień wolności *od*, aby zrealizować konkretną potrzebę za pomocą Internetu. A wykaże się większym zorientowaniem na przyszłość, niż B. Będzie to oznaczać, że, *ceteris paribus*, podmiot A charakteryzuje się niższą preferencją czasową od pomiotu B.

Nie jest rzeczą łatwą definiowanie procesów tak współczesnych, jak te, które były przedmiotem rozważań w niniejszym artykule. Niektórzy, jak Michel Foucault (zob. 2002) byli w tym zakresie do tego stopnia sceptyczni, że twierdzili nawet, iż nie da się zgłębić istoty współczesnego sobie *archiwum*. Zdaje się jednak, że udało się to choćby wspomnianemu Constantowi, nie jest to więc niemożliwe. Dlatego uważam, że można i należy próbować. Jedną z takich prób podjęto w tym artykule.

BIBLIOGRAFIA:

Constant, Benjamin. 1992. O wolności starożytnych i nowożytnych. W: Arka, nr 42 (1992). S.74-82

Fajgelski, Paweł. 2011. Zgoda udzielana na przetwarzanie danych osobowych udzielana w Internecie. W: G. Szpor (red.). Internet. Ochrona wolności, własności i bezpieczeństwa. Warszawa: Wydawnictwo. C. H. Beck. S. 37-45.

Fisher, Bogdan. 2011. Prawo użytkowników wyszukiwarek internetowych do poszanowania ich autonomii informacyjnej. W: G. Szpor (red.). Internet. Ochrona wolności, własności i bezpieczeństwa. Warszawa: Wydawnictwo. C. H. Beck. S. 63-73.

Foucault, Michel. 2002. Archeologia wiedzy. Warszawa: De Agostini: „Altaya".

Hoppe, Hans-Herman. 2006. Demokracja – bóg który zawiódł. Warszawa: Fijor Publishing.

Hoppe, Hans-Herman. 2010. A Theory of Socialism and Capitalism. Auburn, Alabama: Ludwig von Mises Institute.

Kotowicz, Dominika. 2006. Internet – szanse i zagrożenia dla demokracji. W: D. Batorski (red.), M. Marody (red.), A. Nowak (red.). Społeczna przestrzeń Internetu. Warszawa: Academica. S. 283-305.

Kulesza, Joanna. 2010. Ius Internet. Między prawem a etyką. Warszawa: Wydawnictwa Akademickie i Profesjonalne.

Lewiński, Andrzej. 2011. Identyfikacja osób w Internecie w świetle orzecznictwa i przepisów o ochronie danych osobowych. W: G. Szpor (red.). Internet. Ochrona wolności, własności i bezpieczeństwa. Warszawa: Wydawnictwo. C. H. Beck. S. 55-63.

Lipowicz, Irena. 2011. Nowe wyzwania w zakresie ochrony danych osobowych. W: Internet. Ochrona wolności, własności i bezpieczeństwa. Warszawa: Wydawnictwo. C. H. Beck. S. 3-16.

Lis, Wojciech. 2010. Prawo do prywatności a rozwój nowych technologii informatycznych. Szanse I zagrożenia. W: J. Mucha (red.). Nie tylko internet.

Nowe media, przyroda i „technologie społeczne” a praktyki kulturowe. Kraków: Nomos.

Mazurek Paweł, Zając Jan M., Rakocy Kamil. 2007. Między inwigilacją a uwodzeniem. Użytkownicy internetu wobec praktyk gromadzenia i przetwarzania danych. W: Studia Socjologiczne 2007.S. 31-55.

Mises, Ludwig von. 2007. Ludzkie działanie. Warszawa: Instytut Ludwiga von Misesa.

Morbitzer, Janusz. 2011. Aksjologiczne konteksty Internetu. W: M. Szpunar (red.) Paradoksy Internetu. Konteksty społeczno-kulturowe. Warszawa: Wydawnictwo Adam Marszałek. S. 54-73.

Nozick, Robert. 1999. Anarchia, państwo, utopia. Warszawa: Aletheia.

Oleksiuk, Inga. 2004. Wolność wypowiedzi i wolność od wypowiedzi. W: R. Paradowski (red.). Kulturowe instrumentarium wolności. Poznań: Wydawnictwo Naukowe INPiD UAM

Poulet, Bernard. 2011. Śmierć gazet i przyszłość informacji. Wołowiec: Wydawnictwo Czarne.

Reppesgaard, Lars. 2009. Imperium Google. Warszawa: Wrocławska Drukarnia Naukowa.

Spiecker gen. Döhmann, Indra. 2011. Prywatny pomiar świata jako problem prawa ochrony danych. O obchodzeniu się z informacją przestrzenną na przykładzie Google Street View W: G. Szpor (red.). Internet. Ochrona wolności, własności i bezpieczeństwa. Warszawa: Wydawnictwo. C. H. Beck. S. 73-92.

Swift, Adam. 2010. Wprowadzenie do filozofii politycznej. Kraków: Wydawnictwo WAM.

Szatrawski, Krzysztof Dariusz. 2008. Kulturowe konsekwencje rewolucji informatycznej – między indywidualną wolnością a społeczną kontrolą. W: Szkice Humanistyczne T.8, nr 1 (2008). S.125-138.

Tadeusiewicz, Ryszard. 2002. Społeczność Internetu. Warszawa: Akademicka Oficyna Wydawnicza Exit.