

Instytut Problemów Współczesnej Cywilizacji

XLIII

Prywatność – prawo czy produkt?

Warszawa, maj 2008

ISBN 978-83-89871-13-0

© Copyright by Instytut Problemów Współczesnej Cywilizacji
Warszawa 2008

Adres:

Instytut Problemów
Współczesnej Cywilizacji
ul. Koszykowa 80
02-008 Warszawa
tel. 022-234-70-07
fax 022-234-70-08
e-mail: instytut@ipwc.pw.edu.pl

Opracowanie redakcyjne i skład:

BETEX, ul. Irzykowskiego 2/100, 01-317 Warszawa, tel. 022-665-09-22

Druk:

Wydawnictwo SGGW
ul. Nowoursynowska 166, 02-787 Warszawa, tel. 022-593-55-21

Szanowni Czytelnicy!

Cieszę się, że mogę przekazać Państwu kolejny, już czterdziesty trzeci zeszyt Instytutu. Jest on poświęcony seminarium, które odbyło się w Instytucie 28 maja bieżącego roku, a dotyczyło szeroko rozumianej prywatności.

Pojęcie prywatności wydaje się być dobrze określone. Tymczasem tak nie jest. Prywatność rozpatrywana z różnych punktów widzenia jawi się inaczej. Wiąże się bowiem z wieloma, może nawet wszelkimi, aspektami życia człowieka we współczesnym świecie. Warto więc o niej rozmawiać.

Seminarium zostało zorganizowane przez prof. Tomasza Szapiro, on też przedstawił jego ideę we Wprowadzeniu. Bardzo mu za to dziękuję.

Dziękuję też Panu redaktorowi Markowi Ostrowskiemu, Panu doktorowi Bogumiłowi Kamińskiemu i Panu profesorowi Tomaszowi Szapiro za to, że zgodzili się przygotować i wygłosić ciekawe referaty, a także osobom zabierającym głos w dyskusji.

Mam nadzieję, że treść zeszytu Państwa zainteresuje.

Zapraszam na kolejne seminaria Instytutu – następne poświęcone będzie zbliżonej tematyce.

*Marek Dietrich
Dyrektor Instytutu Problemów
Współczesnej Cywilizacji*

Wprowadzenie

Bardzo serdecznie witam wszystkich Państwa na naszym spotkaniu. Rozpocznę od zagajenia, którego wymagają czekające nas wystąpienia. Temat spotkania jest na tyle innowacyjny, że należy skomentować źródła naszego nim zainteresowania. Prywatność rzadko bywa przedmiotem dyskusji na spotkaniach w interdyscyplinarnych gremiach naukowych. Na świecie prawdziwym zapalnikiem dla tego tematu stały się te badania w dziedzinie sztucznej inteligencji, w których komputerowe przetwarzanie danych prowadzi do nowej wiedzy. Wiedza ta, jak każda wiedza, może być dla ludzi pożyteczna, ale bywa, że im zagraża i prowadzi do krzywdy. Ta świadomość spowodowała, że specjaliści z dziedziny sztucznej inteligencji zaczęli zastanawiać się nie tylko nad algorytmami przetwarzania danych, ale także nad szeregiem powiązanych kwestii, które – jak się okazało – zahaczają i o media, i o prasę, i – przede wszystkim – o prawo.

W lutym tego roku zostałem zaproszony przez profesora Matwina z Uniwersytetu w Ottawie w Kandzie do współpracy dotyczącej analizy ekonomicznych aspektów prywatności. Temat okazał się fascynujący, interdyscyplinarny, bardzo świeży. Pierwsza w Europie konferencja na ten temat odbyła się w marcu, choć na kontynencie amerykańskim temat jest przedmiotem dyskusji od kilku już lat.

Tematy interdyscyplinarne budzą wiele pytań. Instytut jest platformą międzyuczelnianej wymiany poglądów, wiele naszych spotkań dotyczyło różnych aspektów życia uczelni, więc wspomniana okoliczność zaowocowała bardzo naturalnym wnioskiem: skoro prywatność wiąże się z wieloma aspektami życia uczelni i ogólniej – edukacji, to zagadnienie prywatności powinno być badane również od strony edukacyjnej i trzeba rozpocząć wymianę poglądów na ten temat. Jednak temat ten, choć ważny, jest zarazem hermetyczny, gdyż wiedza w tej dziedzinie dopiero powstaje. Dlatego postanowiliśmy rozbić tę problematykę na dwie części. W części pierwszej, dzisiaj, spróbujemy przedstawić kalejdoskop zagadnień związanych z prywatnością, pokazując problem prywatności z wielu stron. Ponieważ Państwo znacie program, więc nie będę ich teraz wyliczał. Natomiast po pewnym czasie, zapewne już po wakacjach, uwzględniając

uwagi Państwa związane z wątkami w dyskusji, wydamy i upowszechnimy Zeszyt Instytutu z materiałami z tego seminarium i zaprojektujemy kolejne spotkanie pod roboczym tytułem *Prywatność i kształcenie*. Kształcenie, gdyż nie tylko chodzi o szkolnictwo wyższe i edukację akademicką, ale i o oświatę pojętą szerzej – prawdopodobnie mechanizmy psychologiczne związane z naruszeniami prywatności sięgają korzeniami już szkoły podstawowej.

Taka jest geneza tego spotkania. Jeśli chodzi o jego porządek, to będziemy referowali w kolejności podanej w programie, a w przerwach technicznych, koniecznych dla uruchamiania naszych prezentacji, powstanie naturalna okazja do zadawania pytań i komentarzy. Po wystąpieniach podsumujemy wszyscy spotkanie, kontynuując rozmowę mniej formalnie w trakcie poczęstunku, na który zapraszamy Państwa serdecznie i który zamknie nasze spotkanie.

Chciałbym podziękować z góry, bo mogę nie mieć okazji później, tym osobom, którym udało się dotrzeć, mimo że miały różne obowiązki i będą musiały w trakcie spotkania nas opuścić. Jeszcze raz bardzo dziękuję i tym goręcej Państwa zapraszam – chyba mogę powiedzieć w imieniu wszystkich – do przerywania nam pytaniami w trakcie spotkania. W szczególności do tych osób, którym nie podziękuję na końcu należy pierwszy prelegent – Pan redaktor Ostrowski, którego przybycie oznaczało pokonanie trudności związanych z Jego zawodowymi obowiązkami jako uczestnika i komentatora wydarzeń o skali międzynarodowej, państwowej. W ten sposób zρέcznie przechodzę do rozpoczęcia części merytorycznej, oddając Panu Redaktorowi głos. Proszę bardzo.

Tomasz Szapiro

SFERA PRYWATNOŚCI – ILE O SOBIE POWINNIŚMY WIEDZIEĆ

Marek Ostrowski

Redaktor tygodnika „Polityka”

e-mail: M.Ostrowski@polityka.com.pl

Z ogromnym zażenowaniem tu przed Państwem występuję, gdyż zawsze dla naukowców żywiłem zarówno estymę, jak i odczuwałem treść, sam nie dostępując tego szczytu. Jedynym właściwie usprawiedliwieniem dla mojej tu obecności jest przekonanie, że nawet laicy mogą coś wnieść do rozważań naukowych, czego przykładem niech będzie rozmowa z moim imiennikiem dr Markiem Ostrowskim z Uniwersytetu Warszawskiego, który się zajmuje fotografią lotniczą i satelitarną. On sam, jeżeli dobrze pamiętam, jest biologiem z wykształcenia i przed wielu laty prezentował mi swoje zdjęcia do późniejszego, bardzo pięknego albumu o Polsce, który wydał w dwóch tomach z imponującymi zdjęciami naszego kraju z góry. Jego komentarz do zdjęć był taki: przeczuwam, że w tych zdjęciach tkwi ogromny potencjał badawczy, interdyscyplinarny dla naukowców z dziedzin, o których sam nie mam pojęcia. Tu, jeśli dobrze pamiętam, trudność polegała na tym, że ani on nie potrafił sformułować problemów badawczych dla tych nauk, ani z kolei ci przyszli, ewentualni klienci jego zdjęć prawdopodobnie nie wiedzieli w ogóle o istnieniu materiału do badań. Dopiero jakieś zetknięcie się tych dwóch światów mogło zaowocować odkryciami czy problemami, których dotąd nie nazwano. Ponieważ pamiętam tę rozmowę, więc tę swoją, jak powiedziałem i estymę, i treść w stosunku do naukowców usiłuję łagodzić przekonaniem, że przecież przypadki czemuś tam służą.

Prywatność istotnie jest, wydaje mi się, takim zagadnieniem coraz bardziej obecnym w rozważaniach współczesnych. Ze względu na wiele czynników, o których za chwilę sobie powiemy. Zacznę od historycznego przykładu jednego z geniuszy ludzkości Wiliama Szekspira; literaturoznawcy są zgodni, że chodzi o największego twórcę w języku angielskim, zatem postać gigantyczną,

biorąc jeszcze pod uwagę dzisiejsze znaczenie języka angielskiego. Życiem tego geniusza interesowała się zawodowo cała armia badaczy, jego bibliografia liczy dziesiątki tysięcy pozycji, a mimo tego szczególnego zainteresowania, nie wiadomo, kiedy się urodził (nie wydawano w czasach elżbietańskich świadectw urodzenia), gdzie się uczył i jaki szkoła miała program, co właściwie robił zanim trafił do Londynu, jaką wyznawał religię, mówi się o sympatiach katolickich w jego rodzinie, czy istotnie miał skłonności homoseksualne, jakby to sugerowały pewne nuty w jego utworach, czy miał kochanki lub kochanków, ale co najistotniejsze – nie wiadomo, czy istotnie był w ogóle autorem monumentalnych dzieł do dziś podziwianych przez świat. Nie jest też znany jego majątek: przypuszczamy, że się dorobił znacznej fortuny. I co? Minęło zaledwie pięć stuleci – o tak znaczących osobach współczesnych wiemy niemal wszystko. Ale problem się pogłębia, bo dotyczy każdego z nas, czyli mówimy o osobach zupełnie innego wymiaru, zwykłych obywatelach, osobach niepretendujących do żadnej sławy, a tym bardziej do geniuszu. Mimo to, dokumentacja życia takich osób jest bardzo szczegółowo sporządzana, nie tylko w księgach stanu cywilnego, gdzie wszyscy jesteśmy zapisani, część z nas nawet w Centralnym Rejestrze Skazanych także jest zapisana. Jest znacznie gorzej, bo ślady naszego bytowania są rozliczne i – najczęściej wbrew naszej woli – skrupulatnie rejestrowane. Rozmowy telefoniczne, cała korespondencja e-mailowa zapewne też. Na to zjawisko trzeba zwrócić uwagę, dlatego że już – o ile wiem – chyba ponad 10% osób zatrudnionych w krajach rozwiniętych pracuje w domu, czy naśladując zwrot angielski – „z domu”, poprzez sieć. Rejestrowane są lektury i znajomości internetowe, nie mówiąc już o zwykłych transakcjach przy użyciu karty bankowej. Operatorzy sieci telefonicznych mają nakaz rejestracji tych połączeń i zachowania rejestru przez jakiś czas. Oczywiście, można zapytać – co z tego, przecież najważniejszą, wyczuwalną zmianą jest po prostu proliferacja tych połączeń sieciowych i tyle. Jednak życie nasze dokumentowane jest poza naszą wiedzą i zapewne, powtarzam, wbrew naszej woli. Kto i na jakich warunkach i w jakich warunkach może żądać informacji o tych zbiorach i rejestrach? Tego dobrze nie wiemy. Wiemy tylko, że służby specjalne odtwarzają te sieci, nawet są jakieś programy techniczne, inżynieryjne, które umożliwiają prowadzenie śledztwa na podstawie odtwarzanej mapy kontaktów osobistych, ich częstotliwości. Z tego można wnioskować, kto, jak i kiedy postępował. Czytałem parę dni temu, że w Niemczech ma powstać nowy ośrodek podsłuchowy i analizujący takie dane. Zapewne chodzi o przechwytywanie całego ruchu telekomunikacyjnego i automatyczną jego analizę zorientowaną na śledzenie zagrożeń. Wszystkie te procesy stanowią bardzo poważne, potencjalne zagrożenie dla prywatności.

Swoje krótkie wystąpienie zbudowałem w ten sposób, że chciałem przedstawić cztery casusy związane z prywatnością, bardzo współczesne, żeby, powiedzmy, zarysować panoramę problemów, jakie w związku z tymi casusami można omawiać. Jestem prawnikiem z wykształcenia, w związku z tym chciałem przypomnieć ramy normatywne, jakie tych zjawisk dotyczą, a w trzecim punkcie nakreślić pole konfliktów i problemów, tak jak je rozumiem, jakie problem prywatności tworzy.

Zacznę od ostatnio bardzo głośnego casusu przestępcy w Austrii – Josefa Fritzla, to był ten mężczyzna, który rozbudował piwnicę swego domu i tam więził swoją córkę, z którą splodził dzieci. Państwo znają z prasy ten bulwersujący, makabryczny przypadek. Chciałem zwrócić uwagę na takie w nim elementy: ten mężczyzna był skazany za gwałt w 1967 roku, nastąpiło zatarcie skazania. Nawiasem mówiąc, gdyby kazuistycznie ten przypadek traktować, to właściwie nie powinienem teraz mówić o tym wyroku, bo zatarcie skazania polega na tym, że przestępca właśnie korzysta z przywileju niewspominania o dawnym przestępstwie. On zgłosił zaginięcie swojej córki Elizabeth, którą, okazuje się wcale nie zaginioną, uwięził w piwnicy, a potem, jak ona rodziła dzieci, to on część tych dzieci sam w jej imieniu podrzucał na próg własnego domu wraz z jakimiś listami, zapewne podrobionymi, sugerującymi, żeby się tymi dziećmi zaopiekować. Władze państwowe zezwalały na adopcję tych dzieci, czyli on stawał się potem adoptowanym ojcem swoich własnych dzieci, a równocześnie w istocie własnych wnuków. Jakaś aberracja kompletna. Ale pytanie rodzi się takie: w Austrii rozległy się głosy, że władze państwowe w tym przypadku nie wypełniały swoich obowiązków, ponieważ nie sprawdzały oświadczeń tego mężczyzny i to w wielu płaszczyznach. Po pierwsze, że nie dość energicznie prowadziły poszukiwania rzekomo zaginionej osoby. Dalej, że nie sprawdzały warunków adopcji, prawda też, że zezwoliły na rozbudowę piwnicy, nie pytając o uzasadnienie. Gdyby na chwilę zapomnieć o makabrycznym aspekcie tej całej brutalnej sprawy, to w gruncie rzeczy można zapytać, ale dlaczego władze państwowe miały to wszystko sprawdzać. Przecież ta poszkodowana – o czym dopiero teraz wiadomo – córka, zgodnie z tym, co sama pisała, domagała się, żeby jej nie szukać, że ona po prostu chce żyć w spokoju. Mamy więc tu sferę prywatności. Dalej, jeżeli pojawia się ktoś do adopcji, to nie ma powodu nie wierzyć, nie przyjmować z dobrą wiarą oświadczeń osób zainteresowanych adopcją, zwłaszcza, że dziadek jest naturalną osobą, właściwą, żeby zostać adoptowanym ojcem, skoro matka dziecka nie chce się tym dzieckiem zajmować. Co do zezwolenia na rozbudowę piwnicy, trudno by państwo za każdym razem badało, czy nie kryje się za podaniem mieszkańca jakiś straszny dramat czy plan przestępczy. Słowem, ten casus, choć tak makabryczny, ujawnia konflikt

pomiędzy ochroną prywatności a interesem ochrony praw dzieci. Okazuje się, że w tym wyjątkowym przypadku, z całą pewnością ingerencja władzy powinna iść w kierunku znacznego zmniejszenia pola prywatności tego przestępcy. Ale tak się nie stało.

Drugi casus, też z tego roku, z kilku ostatnich miesięcy. Mianowicie, Niemiecka Służba Wywiadowcza zakupiła nagraną nielegalnie płytę CD czy DVD z danymi z banku w Liechtensteinie od jakiegoś informatora, który sprzedał tę płytę też innym krajom, w tym podobno Stanom Zjednoczonym. Pozyskano tą drogą czy od innego informatora np. dane o majątku dyrektora Deutsche Post, ogromnej instytucji. Natychmiast postawiono mu zarzut, że dygnitarz część swoich oszczędności trzymał w tym zagranicznym banku w Liechtensteinie z naruszeniem przepisów podatkowych. Inny czy ten sam informator wywiadu – nie wiem, w każdym razie klientom znajdującym się w tym wykradzionym zbiorze oferował zniszczenie danych na dyskietce, jeśli oni mu zapłacą. A dodatkowo, poprzez sprzedaż tych danych władzom państwowym spodziewał się zredukowania wyroku za poprzednie przestępstwa, które popełnił. Cała ta afera dotyczy rachunków bankowych ponad 2 tys. osób. Pojawiają się tu pytania, czy wymiar sprawiedliwości zgłosi się po klientów banku naruszających prawo podatkowe. Widzę tu następujący konflikt dotyczący prywatności. Z jednej strony są kraje, które wprowadziły bardzo daleko idącą tajemnicę bankową, w Liechtensteinie, na przykład, prowadzenie przedsiębiorstwa leży w zakresie uprawnionej tajemnicy adwokackiej. Z tego co wiem, adwokat może zgłosić czyjeś przedsiębiorstwo do rejestracji i nie ma potrzeby w ogóle się tłumaczyć, kto jest właścicielem tego przedsiębiorstwa, a zatem cała księgowość pozostaje zakryta. W niektórych krajach federalnych, kantonach Szwajcarii, odwrotnie – panuje całkowita jawność podatkowa, tzn. obywatel może sobie pójść do Urzędu Skarbowego i przejrzeć dane sąsiada dotyczące nie tylko podatków, które płaci, ale majątku, który posiada. Taka sędzia, Francuzka, z pochodzenia Norweżka, Ewa Joly, która jako sędzia śledcza doprowadziła do ujęcia i skazania dyrektora ogromnego francuskiego koncernu naftowego Elf Aquitaine, podpisała wraz z innymi prawnikami w roku 2001, dobrze nie pamiętam, tzw. Deklarację Paryską. Ci bardzo doświadczeni w walce z korupcją sędziowie sugerują, że w ogóle należy znieść prywatność osób publicznych w zakresie majątku i znieść również tzw. raje podatkowe, gdyż – jej zdaniem – nie ma sensu ani żadnej perspektywy pomyślności walki z korupcją w innych warunkach. Ona te postulaty traktuje w ogóle jako linię progową sukcesu walki z przestępczością na wysokim szczeblu, walki z korupcją. Uważa, że bez zniesienia prywatności osób publicznych nie ma prawdziwej, rzetelnej walki z korupcją, a właściwie tylko mydlimy oczy opinii publicznej, bo jeśli istnieje tak ogromna łatwość

ukrycia majątku, to nie ma w ogóle sensu gadanie o walce ze zorganizowaną przestępczością.

Trzeci *case* dotyczy sfery obyczajowej. Wynotowałem sobie dwa takie orzeczenia z Ameryki, może nie bardzo głośne, ale charakterystyczne. Pierwsze się nazywa *Kyllo versus Stany Zjednoczone*. Otóż, ten *Kyllo* to mężczyzna, który w swoim domu zapewne hodował marihuanę, nie wiem, w każdym razie jakąś roślinę, która służyła do wyrabiania narkotyków i poskarżył się na to, że władze zastosowały z dała czynne urządzenie termiczne, które wykryło podwyższoną temperaturę dachu garażu, gdzie on te rośliny niedozwolone hodował. *Kyllo* twierdził, że doszło w ten sposób do naruszenia jego prywatności, a z kolei przedstawiciel władz Stanów Zjednoczonych twierdził, że to urządzenie służące wykryciu tej podwyższonej temperatury przecież nie penetrowało wnętrza jego domu i żadne istotne szczegóły życia domowego nie mogły być tą drogą zebrane. Mimo to powstał spór, gdyż ten oskarżony posługiwał się tezą, iż nie wyprowadził, że tak powiem, na zewnątrz żadnego powodu do wszczęcia śledztwa, ponieważ ukrywał tę działalność, a skoro ją ukrywał, to powinna się ona mieścić w obrębie prywatności chronionej przez prawo. Inny *case*, to jest sprawa *Lawrence* i inni przeciwko Teksasowi. Otóż, policja na podstawie zawiadomienia o jakimś zamieszaniu związanym prawdopodobnie z użyciem broni w okolicy, gdzie ten *Lawrence* przebywał, wkroczyła do domu i zastała tam *Lawrence'a* z innym mężczyzną w trakcie aktu homoseksualnego, a prawo Teksasu określa, że to jest przestępstwo, nawet jeżeli dwie osoby prywatnie, w zakresie tej swojej prywatności w domu robią takie rzeczy, krótko mówiąc, dwóch mężczyzn nie może przebywać nawet w domu całkowicie zamkniętym i bez obecności osób trzecich, jeśli podejmują tego rodzaju, zboczone, według prawa Teksasu, akty. Jednak Sąd Najwyższy uznał, że to, że istnieje nawet takie rygorystyczne prawo, nie oznacza, że nie można się domagać chronienia prywatności. Chociaż oskarżenie powoływało się na znany fakt, że większość opinii publicznej, obywateli w tym stanie potępia tego rodzaju zachowanie, a zatem, że to jest wystarczająca przesłanka do zniesienia ochrony prywatności, to sąd federalny uznał, że opinia większości nie może decydować o tym, czy to jest materia prywatna czy nie, i w takim razie potwierdził, że to na pewno sfera prywatna.

Ostatni *casus* dotyczy też po trosze dzisiejszej wizyty oficjalnej w Polsce; właśnie to Pan Przewodniczący tutaj mówił o tych moich zajęciach – Francja leży w zakresie moich dziennikarskich obowiązków. Akurat dzisiaj z wizytą do Polski, bardzo krótką zresztą, przyjechał prezydent Francji. Otóż, we Francji obecnie politolodzy mówią o zjawisku *pipolizacji*, tzn. *pipolisation*, tak to po francusku brzmi, chodzi o neologizm utworzony od angielskiego słowa

people, czyli ludzie, co już jest samo w sobie fenomenem, bo Francuzi, mając tak ogromne pojęcie o wielkości swojego języka i również pewną fobię na tle ochrony tego języka i nie zaśmiecania go, sami jednak utworzyli to pojęcie, które miałyby oznaczać metodę uprawiania polityki zastępującą merytoryczną dyskusję o rządach w państwie wydarzeniami czy zainteresowaniami dotyczącymi *people*. Stąd ta pipolizacja: zamiast refleksji o naturze i programie rządów, treścią życia publicznego stają się właśnie takie rozmaite mniej lub ważne incydenty z życia osób na świeczniku. Co to ma wspólnego z prywatnością? Otóż, rozumuje się tak – ponieważ to się staje ważnym zjawiskiem politycznym i społecznym, bo dzięki tej pipolizacji politycy łatwiej zdobywają głosy wyborców, nie dyskutując merytorycznie o programie rządu w danym kraju, a więc nie o budowie dróg, autostrad, nakładach na szkolnictwo, badania i wdrożenia, tylko manipulując wydarzeniami z zakresu tej pipolizacji, to ponieważ politycy posługują się tą metodą, zatem wyborca, zbiorowy wyborca ma prawo wnikać w ich sferę prywatną. Skoro oni takim narzędziem się posługują, to narzędzie to, związane z ich sferą życia prywatnego, powinno podlegać większej kontroli niż w przypadku osób prywatnych nie pchających się do polityki. W istocie, coś z tą pipolizacją jest, gdyż sądownictwo na ogół przyjmuje tezę, iż osoby publiczne w mniejszym stopniu powinny korzystać z ochrony życia prywatnego. W ten sposób jednak powstaje samonakręcający się mechanizm, gdyż np. my dziennikarze chętnie podążamy za tym procesem: prasa chętnie za tym podąża, wzbudza dodatkowe zaciekawienie czytelników, a i sami politycy chętnie z owej pipolizacji korzystają.

Powstaje oczywiście pytanie, gdzie leży jakaś rozsądna granica ochrony prywatności życia osób publicznych. Jakaś granica powinna zostać wytyczona, choćby dlatego, że widzimy, że następuje degradacja samego procesu politycznego, który przecież jest w ogóle u podstaw zdrowego państwa absolutnie pożądanym i koniecznym. Tu przypomnę inny *case* amerykański w sprawie Kalifornia *versus* Greenwood z 1988 roku. W orzeczeniu do tego uzasadnienia amerykański Sąd Najwyższy wspomina o takim procesie: mianowicie dziennikarz jakiegoś tabloidu, czyli popularnego dziennika, z posesji ówczesnego sekretarza Stanu, Henry Kissingera zabrał 5 worków śmieci, po czym przeanalizował dokładnie ich zawartość i z tego zrobił artykuł, opublikował, że tak powiem, wyniki swoich badań. Okazuje się, że ze śmieci można się bardzo wiele dowiedzieć o osobie, która te śmieci wyrzuca. I problem powstał taki, czy śmiecie, to jest nasze własne śmiecie, chociaż przez nas wyrzucone w przestrzeń publiczną, to jest sfera prywatna, czy nie. Otóż, część prawników twierdziła, że to na pewno sfera publiczna, bo my się tych śmieci pozbywamy i nie chcemy nawet wiedzieć, co się dalej z nimi dzieje. Ale byli i tacy, którzy twierdzili, że

człowiek ma prawo oczekiwać, że jego śmieci będą zabrane przez upoważnione przedsiębiorstwo i że to nie będzie przedmiotem niczyjej ciekawości.

Ostatni *case*, o jakim chciałem wspomnieć, ale myślę, że on być może będzie przedmiotem kolejnych referatów, dotyczy rozwoju takich programów komputerowych – czytałem o tym dosłownie parę dni temu – ogłoszono, że jakaś firma sprzedaje programy porządkujące skrzynki kontaktowe i korespondencyjne z klientami korporacyjnymi, i że wobec tego osoba trzecia może pozyskiwać te kontakty w formacie już uporządkowanych pakietów, mimo że osoby, które są na liście tych kontaktów, niejednokrotnie nie mają w ogóle zielonego pojęcia, że są tymi zapisanymi klientami albo często może nawet były, ale przestały nimi być. Oczywiście, technika dalej idzie naprzód i nie wiadomo co dalej dla ochrony prywatności dobrego z tego wyniknie.

Trochę się niestety rozgadałem, bo casusy za bardzo mnie poprowadziły, ale myślę, że one same skłaniają do refleksji. Powiem teraz – już z konieczności bardzo krótko – o ramach normatywnych i o polach konfliktów, jak je postrzegam.

Prywatność jest materią regulowaną na najwyższym szczeblu prawa, tzn. w konstytucji. Chodzi o dwa główne artykuły w polskiej konstytucji dotyczące tego zagadnienia: art. 47 i art. 51. Artykuł 47 z grubsza brzmi, że „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”. I artykuł 51, że „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby”. Widać więc, że taka jest koncepcja prywatności w prawie, że można powiedzieć, że prywatność, to jest po prostu prawo do pozostawienia nas w spokoju, tzn., że my sobie żyjemy jak żyjemy i nikt niech w to nie wnika jak, czyli prawo przewiduje pozostawienie takich suwerennych decyzji autonomii jednostek. Pole konfliktów i problemów widzę takie, że – po pierwsze – z tych *case'ów* wynika, że ciągle nie wiemy, jaki jest właściwie zakres tej prywatności, co to jest życie prywatne, co to jest życie osobiste, co to jest intymność, czyli występuje w pierwszej płaszczyźnie konflikt pomiędzy ochroną prywatności a dostępem czy nawet prawem do informacji, które jest także ważnym prawem. Z jednej strony jest, jak widać, potrzeba ochrony prywatności, z drugiej strony chcemy też coś wiedzieć. Prawda, że trudno stwierdzić, co chcemy właściwie wiedzieć o innych, ale na ogół chcemy wiedzieć. Drugi konflikt, to jest oczywisty konflikt między interesem prywatnym a interesem publicznym. Z jednej strony chronimy prywatność, z drugiej strony wiemy, że np. na przykładzie tego Fritzla, że interes publiczny wymaga wiedzy, wiedzy o ludziach, którzy mogą popełnić przestępstwo, nasilają się potrzeby walki z terroryzmem, to już jest cały osobny rozdział. W Stanach Zjednoczonych

jest ustawa znacznie ograniczająca prawa obywatelskie właśnie na potrzeby tej walki, tzw. *Patriot Act*. W Anglii, jeszcze za pani Thatcher, kiedy wystąpiły te ogromne problemy z angielskimi bandytami, którzy jeździli na mecze piłkarskie, utworzono taką komórkę, która się nazywała *National Criminal Intelligence Services*, NCIS, czyli krajową służbę wywiadu kryminalnego i ona po raz pierwszy w dziejach nowoczesnego państwa prawa otrzymała uprawnienie do gromadzenia wszelkich informacji o potencjalnie groźnych kibicach bez postawienia im żadnego oskarżenia, co jest w nowoczesnym prawie złamaniem kanonu, że możemy zbierać informacje o kimś, dopiero kiedy on o coś jest konkretnie podejrzany, a tutaj zbierano informacje, a nawet tylko podejrzenia i przypuszczenia jedynie na wszelki wypadek.

Trzeci wreszcie konflikt, to konflikt między różnymi interesami prywatnymi. To można powiedzieć tak: czy biznes ma prawo wiedzieć o konsumencie i co, w jakim zakresie, jak może przeprowadzać reklamę i akwizycję. Widzimy, że wszystko idzie raczej w tym kierunku, że my, obywatele będziemy się stawać – na podstawie informacji o sobie zebranych, właściwie nie wiadomo czy w warunkach legalnych, czy nie – przedmiotem manipulacji interesów prywatnych, interesów, które wkraczają w naszą sferę prywatności najdalej, gdyż nachalnie kształtują sposób naszego życia tak publicznego, jak i prywatnego. Dziś, generalnie, prawnicy postulaty formułują takie, że w prawie chcieliby wzmocnić zakaz nadmiernej ingerencji. Ale – moim zdaniem – materia jest płynna, gdyż trudno określić, gdzie są granice prywatności, a proliferacja sieci i proliferacja informacji zbieranych często bez naszej wiedzy i woli naraża prywatność na ingerencję niepożądaną. Właściwie dopiero w Ameryce, na określonych tylko *case'ach*, niektóre, ale przecież nie wszystkie granice prywatności się testuje, sprawdza. W Polsce nie bardzo wiadomo jak robić, ludzie poza tym nie są skłonni do składania skarg. Stąd myślę, że potrzeba rozważań i prawniczych, i ekonomicznych jest duża, gdyż tę sferę płynności może jakoś będzie można zmniejszać, choć, mając na uwadze proliferację danych, to bardzo skomplikowane zadanie. Dziękuję bardzo.

PRZETWARZANIE POUFNYCH DANYCH KLIENTÓW – KORZYŚCI I KOSZTY

Bogumił Kamiński

Szkola Główna Handlowa

e-mail: bkamins@sgh.waw.pl

W moim wystąpieniu skupię się na biznesowym aspekcie problemu przetwarzania poufnych danych klientów. Wskażę, w jaki sposób takie dane są wykorzystywane w celu podnoszenia efektywności funkcjonowania przedsiębiorstw oraz w jaki sposób mogą być one wykorzystywane w przyszłości. Dodatkowo omówię wpływ polskich regulacji prawnych dotyczących ochrony danych osobowych na rachunek korzyści i kosztów ich przetwarzania.

Na wstępie skupię się na problemie zdefiniowania pojęcia danych osobowych. Z biznesowego punktu widzenia najbardziej istotny jest tu prawny (a nie np. ekonomiczny czy etyczny) wymiar tego pojęcia, ponieważ z niego wynikają prawa i obowiązki nakładane na przedsiębiorstwo, które przetwarza dane osobowe. Problem prywatności w polskim systemie prawnym jest regulowany konstytucyjnie. Jednak z punktu widzenia prowadzenia działalności gospodarczej, kluczowe znaczenie ma Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych regulująca funkcjonowanie Głównego Inspektoratu Ochrony Danych Osobowych (GIODO). Kluczowym z punktu widzenia definicji danych osobowych jest Art. 6 § 1 Ustawy: „(...) *W rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. (...)*”. Dodatkowo w ramach powyższej definicji istotnym założeniem ustawowym jest, że kryterium możliwości identyfikacji ograniczone jest racjonalnym poziomem kosztów, które należało by ponieść, aby zidentyfikować osobę, której dane dotyczą. W ramach powyższej definicji należy zwrócić uwagę na fakt, że w momencie dokonania identyfikacji osoby, której dane dotyczą, to ochroną objęte są wszystkie dane. Nie ma tutaj takich wyjątków, że część danych podlega ochronie, a inna część nie jest nią objęta.

W sensie definicji ustawowej kluczowe jest osadzenie danych osobowych w kontekście osoby, której ona dotyczy. Pozbawienie danych osobowych tego kontekstu powoduje, że można uznać, że są one pozbawione charakteru danych osobowych. Spostrzeżenie to ma bardzo istotne implikacje dla analizy danych osobowych. Bardzo często przedsiębiorstwa prywatne oraz instytucje państwowe prezentują dane zagregowane – wyliczone na podstawie danych osobowych, ale właśnie pozbawione kontekstu osób, na podstawie których zostały one wyznaczone. Na przykład firmy telekomunikacyjne raportują tzw. wskaźnik ARPU (ang. *Average Revenue Per User*). Wartość tego wskaźnika – przeciętnego przychodu wyliczonego dla wielomilionowej bazy klienckiej – nie podlega ochronie, jednak nie jest dopuszczalne upublicznienie wartości przychodu pojedynczego klienta. Problem pojawia się w przypadku podawania tego typu zagregowanych wskaźników dla bardzo małych populacji. Weźmy przykład zaczerpnięty ze statystyki publicznej – podawanie średniego dochodu na gospodarstwo domowe. Informacja taka w skali kraju czy województwa jest pozbawiona charakteru informacji osobowej. Jednak udzielenie tej informacji w odniesieniu do gminy, może w szczególnych przypadkach (bardzo małe liczne społeczności, o silnym zróżnicowaniu poziomu dochodów) prowadzić do zagrożenia utraty poufności danych indywidualnych.

* * *

Zanim przejdę do sposobu wykorzystania danych osobowych przez firmy w prowadzeniu działalności gospodarczej, omówię kwestię kosztów i ograniczeń tego wykorzystania. Koszty te można podzielić na trzy kategorie: *informacyjne*, *organizacyjne* oraz *zarządcze*.

Koszt informacyjny powstaje, gdy firma chce przetwarzać czyjeś dane i – po pierwsze – musi uzyskać na to zgodę. Co więcej, to nie jest zgoda nieograniczona, lecz dotyczy przetwarzania danych w konkretnym celu. Na przykład, większość z polskich konsumentów zetknęła się podczas podpisywania umów z zapisem o wyrażeniu zgody na przetwarzanie swoich danych osobowych w celach marketingowych. Konieczność udzielenia tej zgody wynika stąd, że zawierając umowę, w naturalny sposób akceptujemy przetwarzanie naszych danych osobowych w celu w niej wskazanym. W innym przypadku umowa ta nie mogłaby być realizowana przez spółkę (na przykład bank musi być w stanie przetwarzać dane o naszej zdolności kredytowej, jeśli udziela nam kredytu). Zgoda na to, żeby dane osobowe wykorzystywać w celach marketingowych, które oczywiście nie są bezpośrednio związane z wykonaniem umowy, musi być udzielona w sposób jawny. Co więcej, obowiązkiem strony, która przetwarza dane, jest zapewnienie, że ten zakres danych, które ona zbiera, musi być

adekwatny do celu, dla którego one są zbierane. Czyli nie jest tak, że firma może zbierać wszelkie dane, które by chciała.

Drugą kategorią kosztów przetwarzania danych osobowych, to koszty organizacyjne. Jeżeli firma chce zarządzać danymi osobowymi, to ustawa nakłada na nią obowiązki odnośnie sposobu przechowywania i przetwarzania tych danych. Po pierwsze – firma musi zarządzać informacją o zgodach na przetwarzanie danych osobowych, czyli gromadzić i chronić informację o tym, kto i w jakim zakresie wyraził zgodę na wykorzystanie swoich danych. Z drugiej strony – firma ma obowiązek do udzielania informacji osobom, których dane osobowe przechowuje, na temat faktu i zakresu ich wykorzystania. To prowadzi do konieczności tworzenia struktur organizacyjnych będących w stanie takich informacji udzielać, co w oczywisty sposób podnosi koszty przetwarzania danych osobowych.

Ostatnią kategorią kosztów ograniczających swobodę firm w zarządzaniu danymi osobowymi są koszty związane z wymogami zarządczymi. Po pierwsze, firma nie ma prawa przechowywać danych dłużej niż to jest konieczne. Innymi słowy, firma jest zobowiązana do zaprzestania przechowywania danych osobowych klientów, których dane nie są jej już potrzebne. Jest to obowiązek, który podnosi koszty zarządzania. Z drugiej strony, firma ma obowiązek dostosowania środków technicznych i organizacyjnych do potrzeb ochrony danych osobowych. Jeśli firma tego nie zrobi, to może nie otrzymać zgody na przetwarzanie danych osobowych. Warto w tym miejscu odnotować, że każdy rejestr danych osobowych musi być w GIODO zarejestrowany i jest jawny. Na przykład, wchodząc na witrynę internetową GIODO, można sprawdzić, że PKO BP posiada kilkadziesiąt rejestrów danych osobowych. Co więcej, można dokładnie sprawdzić, jaki zakres informacji osobowych jest w nim przechowywany.

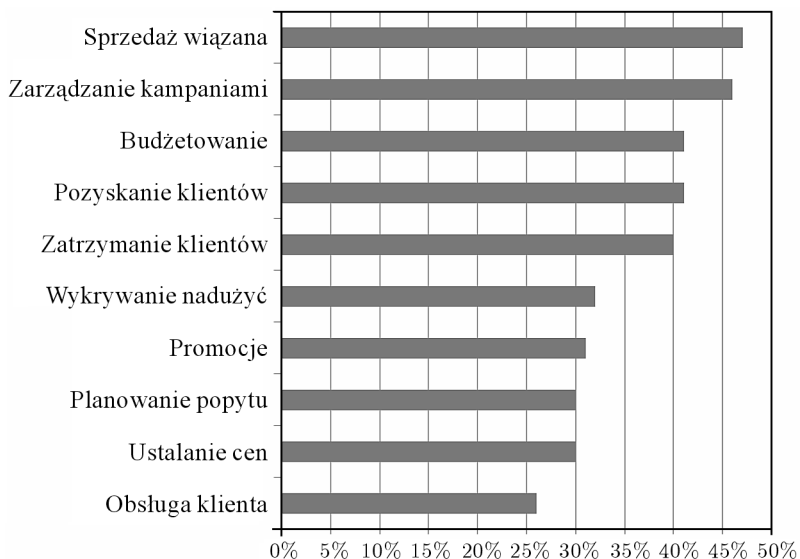
Na zakończenie omawiania zagadnień związanych z przetwarzaniem danych osobowych należy zwrócić uwagę, że nie wszystkie dane można przechowywać i przetwarzać. Ustawa nakłada wiele ograniczeń w tym zakresie. Nie wolno przechowywać danych takich jak: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna lub związkowa, stan zdrowia, kod genetyczny, nałogi lub życie seksualne, skazania, orzeczenia o ukaraniu, mandaty karne. Ograniczenie to nie dotyczy tylko tych instytucji, dla których przetwarzanie tych danych jest niezbędnie konieczne w celu realizacji umów lub zobowiązań (np. szpital może przetwarzać dane o stanie zdrowia, a związek wyznaniowy o przynależności danej osoby do niego). Natomiast w przypadku typowych przedsiębiorstw tych informacji gromadzić nie wolno. To ostatnie ograniczenie jest często dla firm

niewygodne, zwłaszcza że często są to cenne informacje, które mogłyby zostać wykorzystane np. w celach marketingowych.

* * *

Przejdźmy teraz do kwestii wykorzystania danych osobowych w przedsiębiorstwach. W tym zakresie można wyróżnić dwa zasadnicze obszary zastosowań: *operacyjne* i *analityczne*. Operacyjne wykorzystanie danych klientów wiąże się koniecznością jego identyfikacji oraz realizacji zobowiązań umownych. Ten obszar wykorzystania danych osobowych klientów z reguły nie wywołuje wątpliwości i kontrowersji. Inaczej wygląda sytuacja w przypadku zastosowań analitycznych. Firmy wykorzystują dane klientów w celu wyciągnięcia z nich wniosków, których nie wykorzystują bezpośrednio do wykonania umowy z klientem, ale w celu podniesienia efektywności swojego gospodarowania.

W 2007 The Data Warehousing Institute przeprowadził wśród korporacji badanie dotyczące wykorzystania danych w celach prognozowania i analityki. Wyniki przedstawiono na rysunku 1.

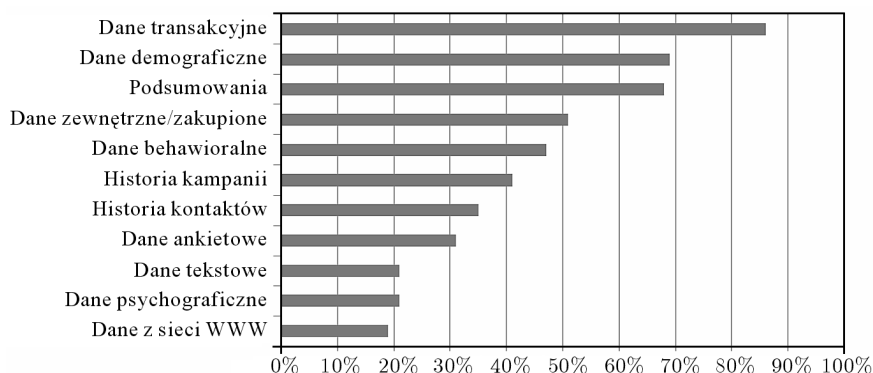


Rys. 1. Estymowany odsetek korporacji wspierających wybrane procesy biznesowe za pomocą analizy danych (źródło: *Predictive Analytics*, TDWI Best Practices Report, 2007)

Zauważmy na przykład, że prawie 50% firm wykorzystuje metody analityczne przy tzw. sprzedaży wiązanej, opracowując strategię zwiększania sprzedaży dla konkretnego klienta. Jest to obszar analityczny, w którym bardzo

intensywnie wykorzystywane są informacje zaliczane do danych osobowych klienta. Analogiczna sytuacja występuje w takich obszarach, jak: zarządzanie kampaniami, pozyskiwanie klientów, zatrzymanie klientów czy promocje. Są to procesy biznesowe, w których wykorzystanie danych osobowych może być traktowane jako ingerencja w prywatność klienta – obszary, w których firma stara się wpływać na zachowanie klienta, wykorzystując dane o nim samym.

Warto zwrócić również uwagę na szczegółowy zakres danych, które w tych analizach są wykorzystywane. Informacja ta przedstawiona jest na rysunku 2.



Rys. 2. Estymowany odsetek korporacji wykorzystujących wybrane typy danych na potrzeby analityczne (źródło: *Predictive Analytics*, TDWI Best Practices Report, 2007)

Prawie 90% firm wykorzystuje w analizach dane o transakcjach zawartych z klientem. Podobnie, bardzo duży odsetek firm wykorzystuje dane demograficzne czy informacje o zachowaniu klientów. I znowu można sobie zadać pytanie, czy klienci są świadomi tego, że takie dane są wykorzystywane do tego, żeby na nich wpływać.

Z powyższych przesłanek wynika, że obszar zastosowań danych klientów do prowadzenia analiz oraz zakres wykorzystywanych danych jest potencjalnie bardzo szeroki. W polskich warunkach biznesowych najszerszej są one wykorzystywane przez firmy telekomunikacyjne i instytucje finansowe.

* * *

Szerokie wykorzystanie danych osobowych klientów przez przedsiębiorstwa komercyjne w naturalny sposób doprowadziło do powstania rynku, na którym dokonuje się nimi obrotu. Powstały firmy, obecne również w Polsce, których jedyną działalnością biznesową jest gromadzenie, analiza i sprzedaż danych

o osobach fizycznych. Największym na świecie przedsiębiorstwem tego typu jest Acxiom Corporation. Jego wartość była oceniana przez rynek giełdowy na około 1 miliarda dolarów amerykańskich w maju 2008 roku. Oprócz sprzedaży samych danych o klientach (tzw. sprzedaż prospektów), firma ta sprzedaje przetworzone informacje o potencjalnych profilach przyszłego zachowania konkretnych osób fizycznych (w swoich procedurach dzieli ona całe społeczeństwo na 70 standardowych grup odznaczających się podobnym charakterem potrzeb). Jest to oczywiście również bardzo cenna informacja. Na przykład, bank może być zainteresowany zakupem informacji tylko o tych klientach, którzy potencjalnie w najbliższym czasie będą dokonywali zakupu mieszkania, co z reguły skutkuje potrzebą zaciągnięcia kredytu hipotecznego. Zakup tej informacji może ułatwić bankowi zaprojektowanie skutecznej kampanii promocyjnej.

Firma Acxiom jest bardzo dobrym przykładem do zilustrowania problemów i zagrożeń związanych z przetwarzaniem danych osobowych. Pierwszym z tych problemów jest *wymiana danych osobowych pomiędzy instytucjami*, a drugim – sam fakt gromadzenia *olbrzymich baz danych przechowujących dane osobowe*. Problemy te zilustruję na przykładzie konkretnych zdarzeń w historii firmy Acxiom.

W 2003 roku Armia Stanów Zjednoczonych, czyli podmiot, który ma większe niż przeciętne uprawnienia do zbierania informacji osobowych, planował wykorzystać dane zbierane przez firmę Acxiom do oceny przewidywania ryzyka ataku terrorystycznego na bazy marynarki wojennej. Aby zachować poufność prowadzonych działań, zakup tych danych odbył się za pośrednictwem specjalnie w tym celu założonej firmy-pośrednika symulującej prowadzenie normalnej działalności gospodarczej. Sytuacja ta została później ujawniona publicznie, czego konsekwencją było pozwanie firmy Acxiom przez organizację *Electronic Programms Information Center* za złamanie zasad przetwarzania danych osobowych. Acxiom, sprzedając dane, ani nie poinformował o tym swoich klientów, ani nie uzyskał od nich zgody na taką sprzedaż. Sytuacja ta ilustruje fundamentalny problem związany z przetwarzaniem danych osobowych: w momencie, gdy dane klienta znajdują się w jakiejś bazie danych, pojawia się ryzyko, że ich wykorzystanie wymknie się spod kontroli osoby udzielającej informacji.

Niewątpliwie jednak potrzebne są mechanizmy, które umożliwiają wymianę danych osobowych między różnymi instytucjami (choćby w opisanych powyżej celach walki z terroryzmem). Rodzi się pytanie, jak dane posiadane przez różne instytucje połączyć w taki sposób, żeby ich sobie nie przekazywać, a zarazem móc je wspólnie analizować. Innymi słowy – w jaki sposób dwie różne instytucje mające dwie rozdzielne bazy informacji o klientach mogą dokonać ich

łącznej analizy przy jednoczesnym zachowaniu warunku, że dane detaliczne zawarte w tych bazach nie są przekazywane na zewnątrz.

Drugi problem, na który pragnę zwrócić uwagę, to kwestia fizycznej ochrony danych osobowych. Często bowiem dużo większe zagrożenie dla prywatności klienta niż analiza jego danych stanowi niekontrolowane przekazanie danych lub ich kradzież. W historii firmy Acxiom ten problem wystąpił w 2003 roku, kiedy to ukradziono jej dane o jednym miliardzie sześciuset milionach klientów. Ktoś się włamał do centralnego serwera danych firmy i skopiował imiona, nazwiska, adresy, daty urodzenia, wielkości dochodów i wiele innych danych osobowych. Warto podkreślić, że zagrożenie stanowił sam fakt zgromadzenia jednego miliarda sześciuset milionów rekordów informacji o klientach w jednej bazie danych, co znacznie zwiększało pokusę ich kradzieży i ją ułatwiło. Co ciekawe, kradzież ta nie została od razu wykryta. Dokonały tego służby specjalne (FBI) na podstawie analizy zapisów na tak zwanych *chatach*. Zidentyfikowały one mianowicie osobę, która w bardzo krótkim czasie była w stanie udzielać rozmówcom bardzo szczegółowych informacji o wielu niezwiązanych ze sobą osobach fizycznych. Można więc powiedzieć, że kradzież odkryto przez przypadek.

I tutaj znowu pojawia się problem – w jaki sposób zapewnić zdolność analizowania bardzo dużych zbiorów danych indywidualnych klientów, ale nie lokalizować ich w jednym miejscu. Jest to o tyle istotne, że w zastosowaniach biznesowych nie jest istotne zebranie wszystkich informacji w jednym miejscu, ale raczej zdolność przeprowadzenia analizy wszystkich danych.

* * *

Problem wymiany danych pomiędzy instytucjami oraz zapewnienie zdolności analizy danych klientów bez konieczności ich gromadzenia w jednym miejscu podjęli w 2000 roku Agrawal i Srikant¹. W pionierskiej pracy, która zapoczątkowała rozwój dziedziny obecnie nazywanej *privacy preserving data mining*². W dziedzinie tej bada się problem opracowania takich sposobów analizy danych, które pozwalają na wyciągnięcie takich samych wniosków, jak analiza rzeczywistych danych klienta, ale nie wymagają bezpośredniego dostępu do danych. W tym celu stosuje się najczęściej dwa podejścia: *zaburzenie danych* oraz *bezpieczne wieloagentowe przetwarzanie danych*.

¹R. Agrawal, R. Srikant, *Privacy-Preserving Data Mining*, Proceedings of the ACM SIGMOD Conference on Management of Data, 439-450, 2000.

²Wydobywanie wiedzy z danych z zachowaniem prywatności.

Zaburzenie danych polega na tym, że oryginalne dane klientów są transformowane w taki sposób, że przestają one mieć cechy i własności oryginalnych danych osobowych (np. nie jest możliwe odtworzenie oryginalnych danych osobowych na ich podstawie). Jednocześnie stosowane transformacje gwarantują, że własności statystyczne nowego zbioru danych są identyczne ze zbiorem oryginalnym. Dzięki temu wnioski wyciągane z analizy danych zaburzonych są bardzo zbliżone do wniosków, które można wyciągnąć z analizy danych oryginalnych.

Podjęcie wieloagentowe analizuje dane rozproszone pomiędzy kilka instytucji bez konieczności łączenia ich w jedną bazę za pomocą tzw. bezpiecznych protokołów wymiany danych. Protokoły te gwarantują, że wynik analizy jest jedyną wiedzą uzyskiwaną w efekcie współpracy tych instytucji.

* * *

Podsumowując rozważania na temat problemu biznesowej wartości danych osobowych, warto przedstawić trzy zasadnicze wnioski. Po pierwsze – dane te są i będą w coraz większym stopniu wykorzystywane do usprawniania funkcjonowania przedsiębiorstw, a zwłaszcza – w obszarze aktywności marketingowych. W tym zakresie ich wykorzystanie można postrzegać jako ingerencję w prywatność osoby udostępniającej dane, a więc takie wykorzystanie powinno podlegać kontroli prawnej. W polskim systemie prawnym właśnie taka ochrona jest gwarantowana. Ustawa o ochronie danych osobowych nakłada szereg ograniczeń i obowiązków na podmioty gromadzące i przetwarzające takie dane. Drugim zasadniczym wnioskiem jest zwrócenie uwagi na fakt, że zasadniczym zagrożeniem związanym z ochroną danych osobowych jest nie to, że są analizowane, ale fakt ich gromadzenia w jednej bazie danych. Osoby, których te dane dotyczą, tracą nad nimi kontrolę, a dane mogą być bez ich zgody sprzedane lub skradzione. To z kolei prowadzi do trzeciego ważnego wniosku: istnieje potrzeba tworzenia takich algorytmów analizy danych, które nie wymagają ich gromadzenia w formie jawnej w jednym repozytorium. Badania nad takimi algorytmami rozwijają się od początku XXI wieku.

HANDEL PRYWATNOŚCIĄ A EKONOMIA

Tomasz Szapiro

*Instytut Problemów Współczesnej Cywilizacji oraz Szkoła Główna Handlowa
e-mail: tszapiro@sg.h.waw.pl*

Stanisław Matwin

*Uniwersytet Ottawski, Kanada
e-mail: stan@site.uottawa.ca*

1. Problem prywatności

Problem prywatności i związane z nim problemy odrodziły się w erze upowszechnienia komputerów i ich wpływu na życie ekonomiczne i społeczne. W tym wypadku, inspiracją do podjęcia problematyki prywatności stały się dwa teksty oddzielone wiekiem. Pierwszy tekst, *Prawo do prywatności* Warrena i Brandaisa¹, to artykuł opublikowany w harwardzkim przeglądzie prawniczym w roku 1890. Autorzy, sięgając do tekstów jeszcze z połowy XVII wieku, dowodzą, że prawo do ochrony własności należy aktualizować, by nadać za

¹W oryginalnym brzmieniu: „...*That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, – the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession – intangible, as well as tangible...*” – cyt. wg *The Right to Privacy Harvard Law Review*, Vol. IV, December 15, 1890, No. 5.1.

zmianami w życiu społecznym i ekonomicznym. Konsekwencją niezbywalnego prawa do życia jest prawo do cieszenia się życiem, cieszenia się własnością, cieszenia się zdolnością do przeżyć intelektualnych i emocji, i także – prywatnością. Nie wolno zagrażać życiu i zdrowiu innych, grabić bliźnich ani obrażać ich inteligencji, nie wolno uniemożliwiać zaspokojenia potrzeb emocjonalnych, także – zaspokojenia potrzeb związanych z potrzebą prywatności. Jak każde inne, prawa te wymagają ochrony.

Tekst drugi – *Prywatność i rynki* napisał Kenneth C. Laudon², profesor w Szkole Biznesu Sterna na uniwersytecie nowojorskim, specjalista w dziedzinie systemów informacyjnych i ochrony prywatności³, autor ekspertyz dla Kongresu i Prezydenta USA. Z pewną dozą przesady można powiedzieć, że tekst ten, który powstał ponad dekadę przed dzisiejszym spotkaniem, przedstawia dramatyzm związany z niedostatkami ochrony prywatności w USA. Zasób aktów prawnych powiązanych z problematyką ochrony prywatności jest różny w różnych krajach i skromny. Laudon wskazuje, że do końca lat dziewięćdziesiątych ubiegłego stulecia, instytucje rządowe w USA zobowiązywały do respektowania prywatności obywateli (i to w ograniczonym zakresie) tylko stosunkowo nieliczne akty prawne⁴. Podobnie rzecz się miała w przypadku instytucji prywatnych⁵. Wydaje się to niewiarygodne, ale prawo w USA nie chroniło danych dotyczących informacji genetycznej, medycznej, ubezpieczeniowej, danych osobowych, danych dotyczących nieruchomości, transakcji za pomocą kart magnetycznych, większości danych urzędów publicznych, danych dotyczących odbywanych wyroków, zatrudnienia, rachunków telefonicznych itp. Laudon wykazuje też słabości i luki istniejących rozwiązań prawnych i administracyjnych i proponuje rozwiązanie wykorzystujące mechanizm ekonomiczny.

Rozwiązanie to polega na wprowadzeniu nowego rynku – narodowego rynku informacyjnego (ang. *National Information Market, NIM*) na wzór rynku

²*Markets and Privacy*, Communications of the ACM, September 1996, Vol. 39, No. 9.

³Laudon jest autorem książki *Dossier Society* poświęconej problemom ochrony prywatności w środowiskach wielkiej skali, jakimi są narodowe systemy informacyjne w sektorze publicznym i prywatnym.

⁴Freedom of Information Act (1968), Privacy Act (1974), Right to Financial Privacy Act (1978), Electronic Communications Privacy Act (1986), Computer Security Act (1987), Computer Matching and Privacy Protection Act of 1988, Federal Managers Financial Integrity Act (1982).

⁵Fair Credit Reporting Act (1970), Family Educational Rights and Privacy Act (1978), Privacy Protection Act (1980), Cable Communications Policy Act (1984), Video Privacy Protection Act of 1988.

kapitałowego. Elementami zaproponowanego przez Laudona systemu byłyby osoby (właściciele, a dokładniej: posiadacze prywatności), banki informacji tworzące produkty informacyjne, krajowa izba rozrachunkowa, rejestrująca transakcje, i informacyjna giełda oraz konsumenci prywatni.

Niestety, artykuł Laudona zamyka wywód przekonujący skutecznie o nie-realistyczności tego rozwiązania (NIM). Podstawowe problemy to doprowadzenie do zgody na odsprzedaż praw uznawanych za podstawowe, uzyskanie społecznej akceptacji dla rynku dostępnego tylko dla zamożnych, rewolucyjny zakres zmian w prawodawstwie, konieczność akceptacji dla rządowej kontroli tego rynku, konieczność ponoszenia bardzo wysokich kosztów transakcyjnych, administracyjnych i kosztów nadzoru.

Te dwie inspiracje – prawnicza i informatyczna – w powiązaniu ze sobą mają charakter symboliczny. Opisana przez Laudona sytuacja w sferze rozwiązań prawnych zmieniła się radykalnie na korzyść, zwłaszcza w Europie. Powstały jednak nowe problemy prawne związane z projektowaniem i wdrażaniem rozwiązań informatycznych, a raczej – z zagrożeniami finansowymi, jakie dla twórców algorytmów i systemów niosą te skutki naruszeń dóbr osobistych, które są wynikiem nieprzemyślanego stosowania rozwiązań informatycznych. Spowodowały one – wspomniane wcześniej – odnowienie zainteresowania problematyką prywatności.

Zainteresowanie to przerodziło się w prowadzone głównie w USA poważne badania naukowe, których wyniki prezentowane są na międzynarodowych konferencjach. Przed niespełną kwartalem odbyła się także w Europie pierwsza konferencja poświęcona tej tematyce⁶. Algorytmy i architektury systemów informatycznych, służących generacji wiedzy i zachowujących prywatność osób, których dotyczy przetwarzana informacja (ang. *Privacy-preserving Data Mining; PPDM*), zakładają, że tylko dane źródłowe nie są zewnętrzne w stosunku do systemu, natomiast nie gwarantują, że wytworzona wiedza jest chroniona. Wytworzona wiedza – reguły i wzorce wykryte na podstawie analizy danych mogą być wykorzystywane bez wiedzy tych, których dane dotyczą, a nawet wbrew ich interesom.

Przyjmijmy na użytek dzisiejszego spotkania szeroko akceptowaną definicję prywatności, jaką podał Alan Westin⁷: *prywatność, to zdolność osoby do samodzielnego zadecydowania, kiedy, w jaki sposób i jak dalece informacja*

⁶Organizatorami warsztatów *First Interdisciplinary Workshop on Mobility, Data Mining & Privacy*, które odbyły się w lutym 2008 we Włoszech w Rzymie, są uczeni z Uniwersytetu w Pizie.

⁷Westin A.F.W, *Privacy and Freedom*, New York: Atheneum, 1967.

ich dotycząca może być komunikowana innym. Przykładowo przywołany przed chwilą zwolennik ochrony prywatności Kenneth C. Laudon, który jest także zapalonym konstruktorem łodzi żaglowych i żeglarzem biorącym udział w regatach, traci możliwość kontroli losów tej ostatniej informacji po uwidocznieniu jej w Internecie, co oznacza, że jego prywatność zostaje z tą chwilą pomniejszona. To, czy mamy w tym wypadku do czynienia z naruszeniem prawa do ochrony prywatności, zależy oczywiście od tego, czy wyraził on na to zgodę. Bardzo wielu przykładów utraty kontroli nad informacją osobistą dostarcza handel elektroniczny. O ich skali i znaczeniu mogliśmy się dzisiaj dowiedzieć z referatu doktora Kamińskiego, poprzedzającego to wystąpienie.

W przekonaniu, że tylko powiązanie regulacji prawnych i administracyjnych z mechanizmami ekonomicznymi, zabezpieczonymi rozwiązaniami informatycznymi, może doprowadzić do rzeczywistej ochrony prywatności, w dalszej części tekstu przedstawimy problematykę w jednostronnym, ekonomicznym ujęciu. Pozwoli to wyartykułować istotne założenia zarówno dla twórców rozwiązań regulacyjnych, jak i informatycznych.

2. Prywatność jako dobro

Tak jak w każdej innej nauce, w ekonomii narzędziem analizy są modele. Rozpoczynamy zatem od przedstawienia bardzo uproszczonych modeli (ludzkiej motywacji do działania, później – charakterystyki działań na rynku, wreszcie – samego rynku) wraz z komentarzami odnoszącymi się do problemu prywatności. Modele te posłużą do uzasadnienia wniosków dotyczących dynamiki i zjawisk związanych z kontrolą prywatności.

Przyjmijmy za Maslowem⁸, że do działań ludzi motywują potrzeby (od zaspokojenia głodu po samorealizację). Zaspokojenie *potrzeb wyższego rzędu* (np. godność) następuje po zaspokojeniu potrzeb podstawowych (np. sytość). Współczesne społeczeństwa uznają podstawowe prawo człowieka do zaspokojenia potrzeb i domagają się przestrzegania tego prawa w aktach regulacyjnych najwyższej rangi⁹.

⁸Maslow A.H., *A Theory of Human Motivation*, Psychological Review, Vol. 50, pp. 370-396, 1943.

⁹Ogłoszona w 1776 roku Deklaracja Niepodległości Stanów Zjednoczonych stwierdza: „... *We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain, that among these are Life, Liberty and the pursuit of Happiness...*”. Pierwsze dziesięć poprawek wniesione do w 1791 roku do pierwszej konstytucji (Stanów Zjednoczonych) zwane Kartą Praw Stanów Zjednoczonych Ameryki (ang. *United States Bill of Rights*): „...*No State shall make or enforce*

Bezpośrednio potrzeby zaspokajają *konsumpcja*. Wszystko to, co służy zaspokojeniu potrzeb ludzi, nazywa się w ekonomii *dobrem*. Dobra trzeba produkować, aby je konsumować lub wymienić na takie, których konsumpcja zaspokoi potrzebę. Na takim poziomie ogólności powiemy, że podmioty występują na różnych rynkach w rolach konsumentów i producentów, podejmując działania będące skutkami decyzji o sposobie zaspokojenia potrzeb. Podmioty te jako producenci posiadają zasoby przetwarzane na dobra, jako konsumenci – płacą za możliwość korzystania z dóbr.

Istnieje wiele opisów mechanizmów podejmowania decyzji – typów racjonalności. Model wyjściowy, który można na wiele sposobów modyfikować, niekiedy bardzo radykalnie, ale który na potrzeby dzisiejszego spotkania jest wystarczający, zakłada, że podmioty potrafią określić zbiór działań prowadzący do zaspokojenia ich potrzeb, a następnie wybierają z tego zbioru to działanie, które doprowadzi do konsumpcji dającej najwyższe zadowolenie (satysfakcję). Ilościowy miernik tego zadowolenia nazywany jest użytecznością, a opisana racjonalność – racjonalnością *homo oeconomicus*. Zasadę racjonalności, zgodnie z którą racjonalny podmiot – *homo oeconomicus* – wybiera działanie o największej użyteczności, czyli najwyższym możliwym poziomie zaspokojenia potrzeb, nazywa się *zasadą maksymalizacji użyteczności*. Zakłada się zazwyczaj, że użyteczność jest funkcją niemalejącą i wklęsłą, co odpowiada założeniu chciwości decydenta i jego niechęci do ryzyka.

Ten wyjściowy model jest w ekonomii rozbudowywany. Odnotujemy, że prywatność jest dobrem, które konsumujemy, odsłaniając informację o sobie stronom zainteresowanym czy to z powodów finansowych, czy informacyjnych, np. w przypadku udzielenia rekomendacji lub porady. W dalszym ciągu spróbujemy rozbudować przedstawiony model, dołączając założenia wynikające z uwzględnienia specyfiki potrzeby, jaką jest potrzeba kontroli informacji o sobie, czyli prywatności. W tym celu rozważymy teraz nieco bardziej złożoną charakterystykę dóbr.

Dobra można dzielić m.in. ze względu na ich własne charakterystyki oraz ze względu na charakterystyki wynikające ze sposobu ich konsumpcji. Pierwszy podział dóbr rozróżnia dobra materialne (chleb) i niematerialne (prawa autorskie). Niewątpliwie prywatność jest dobrem niematerialnym. Podział

any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws...". Interesujące jest porównanie z drugą uchwaloną – Konstytucją 3 maja, przyznającą prawa wszystkim obywatelom, choć ich zrównanie wobec prawa nie ma tak uniwersalnego charakteru, jak w konstytucji amerykańskiej.

drugi analizuje zjawiska *wyłączalności z konsumpcji* oraz *konkurowania o dobro*. Analizować dobra można ze względu na każdą z tych cech oddzielnie lub łącznie.

Oto przykłady analizy ze względu na jedną cechę. Wysoka cena może unieemożliwić korzystanie z porsche, ale nie można wyłączyć kogoś z korzystania z dobrodziejstw fluorowanej wody wodociągowej. Spożycie kromki chleba unieemożliwia jej konsumpcje przez innych, ale korzystanie z oświetlenia ulicznego nie odbiera innym tej możliwości.

Charakteryzacja ze względu na obie cechy łącznie prowadzi do czterech możliwości. Są oto dobra takie, jak wspomniany chleb – konsument konkuruje w powyżej rozumianym sensie i można go z konsumpcji wyłączyć. W takim przypadku mówimy ogólnie o *dobrach prywatnych*. Gdy o dobro trzeba konkurować, ale z konsumpcji nie można wyłączyć, jak w przypadku konsumpcji grzybów zbieranych w lesie, to mówimy o *wspólnych zasobach*. O *dobrach klubowych* mówimy wtedy, gdy z konsumpcji można wykluczyć, ale nie trzeba konkurować – przykładu dostarcza korzystanie z biletu do teatru. Gdy wreszcie z konsumpcji dobra nie można wykluczyć i nie trzeba o nie konkurować, mówimy o *dobrach publicznych*. Podręcznikowe przykłady dóbr publicznych, to czyste powietrze i obrona narodowa.

Dane służą zaspokojeniu potrzeb ludzkich – są dobrem w rozumieniu ekonomicznym. Są dobrem niematerialnym. Rozważmy dwie grupy takich dóbr – *indywidualne dane osobiste*¹⁰ i *zagregowane dane osobiste*. Dane osobiste to np. lista osiągnięć uczonego. Pozwalają zaspokoić potrzebę samorealizacji. Dziekan czy też Komisja d.s. Oceny Kadry korzysta z danych osobistych i łącząc je z danymi osobistymi innych osób, ustala jego sprawność jako nauczyciela i naukowca, co skutkuje pozycją lidera lub outsidera na Wydziale. Tak powstają zagregowane dane osobiste – pozycja osoby nie zależy tylko od jej danych.

Konsekwencją rozróżnienia dóbr na indywidualne i zagregowane jest w przypadku tych ostatnich konieczność uwzględnienia w opisie wymiany dodatkowego, trzeciego aktora. Dane podmiotów-producentów po zagregowaniu są konsumowane przez trzecią stronę, którą nazwiemy *dysponentami baz danych*.

Także prywatność – zdolność do samodzielnego korzystania z indywidualnych i zagregowanych danych osobistych – można traktować jako dobro.

¹⁰Wprowadzamy tu celowo termin dane osobiste, a nie – osobowe, by w wywodzie natury ekonomicznej nie wprowadzić nieporozumień z precyzyjną terminologią prawną.

Pogwałcenie prywatności to naruszenie własności tego dobra. Tabela 1 prezentuje najistotniejsze cechy dóbr osobistych i prywatności.

Tabela 1. Charakterystyka dóbr osobistych i prywatności

	Dane indywidualne	Dane zagregowane
Dane osobiste	<ul style="list-style-type: none"> • Osadzone w kulturze i wartościach • Niematerialne • Wpływają na status ekonomiczny • Każdy może je posiadać • Osoba może je wytwarzać • Nie mogą być sprzedawane i dziedziczone • Osoby są świadome swoich dóbr danych osobistych • Są to dobra klubowe: z ich konsumpcji można wyłączyć, ale konsumpcja ich nie pomniejsza 	<ul style="list-style-type: none"> • Aktorzy: osoby, dysponenci baz danych, konsumenci na rynku danych • Osoba nie może ich wytwarzać • Osoba może je konsumować • Dysponenci baz nie mogą sami wytwarzać danych • Dysponenci baz mogą dane konsumować (są to wtedy zasoby wspólne: można z konsumpcji wyłączać, ale konsumpcja dóbr nie pomniejsza) • Konsumenci nie mogą tych danych produkować • Konsumenci mogą dane kupić – są to wtedy zasoby wspólne • Sprzedane prasie stają się dobrem publicznym • Własność rozmyta i częściowo zapoznana • Dla osób jest to dobro klubowe: można być wyłączonym z konsumpcji, konsumpcja go nie pomniejsza • Dla dysponentów baz i firm są to zasoby wspólne
Prywatność	<ul style="list-style-type: none"> • Osoba może wytwarzać prywatność, konsumować ją i sprzedawać • Osoby mają świadomość prywatności • Dobro prywatne: można z konsumpcji wyłączyć, konsumowanie pomniejsza zasób 	<ul style="list-style-type: none"> • Osoba nie może wytwarzać prywatności • Osoba może konsumować prywatność • Trudno jest kontrolować zagregowane dane • Dobro prywatne: można z konsumpcji wyłączyć, konsumowanie pomniejsza zasób

Odnotujemy ważny wniosek wynikający z analizy tej tabeli. W przypadku dóbr zagregowanych danych osobistych, wymiana prywatności jest skomplikowana – występują trzy strony, dla których dobra mogą mieć różny charakter. Wynika stąd, że analiza procesu wymiany na rynku prywatności może prowadzić do nieoczekiwanych wniosków.

3. Dobra i rynki – efektywność, sprawność

Rynek definiują normy regulujące wymianę (transakcje). Na przykład, gdy nie ma interwencji zewnętrznych i wszystko (np. cena) w transakcjach jest uregulowane w wyniku decyzji stron transakcji, to mówimy o *wolnym rynku*. W *ekonomii centralnie planowanej* zasadą jest scentralizowana zewnętrzna kontrola transakcji (np. cen). Ale tyle mamy typów rynku, ile sposobów ich regulacji. W przypadku rozważania nowego dobra w naturalny sposób rodzi się pytanie o szczególnie pożądaną typ rynku. Racjonalna odpowiedź musi odnieść się do kryteriów. Rozważmy zatem dwa takie kryteria – kryterium *skuteczności* (efektywności, ang. *effectiveness*) i kryterium *sprawności* (ang. *efficiency*) rynku.

Kryterium skuteczności w ocenie organizacji rynku oznacza odniesienie się do faktu realizacji celów wspólnoty. Bezdomność, ubóstwo, głód, choroby dowodzą braku zaspokojenia potrzeb wspólnot – nieskuteczności rzeczywistych rynków. Realne rynki nie są efektywne. Na przykład, rynki dóbr publicznych nie są w stanie zaspokoić potrzeb społecznych (np. poziom opieki zdrowotnej). Rynki dóbr prywatnych mogą wykluczać z konsumpcji.

Gdy cele wspólnoty nie są w pełni zrealizowane, to można mówić o mniej lub bardziej niezadowolającym poziomie realizacji tych celów – mniej lub bardziej sprawnie działającym rynku. W sytuacji nieskuteczności rzeczywistych rynków dąży się do podniesienia sprawności rynku. Rozważa się różne organizacje rynku i porównuje je ze względu na poziom realizacji celów wspólnoty, aby wybrać optymalny, tj. taki, którego nie można już w rzeczywistych warunkach dalej usprawniać. Skoro rynki nie mogą być efektywne, niech chociaż będą możliwie sprawne.

Aby porównywać skutki różnej organizacji rynku (powiadamy krótko: różne rynki) trzeba porównywać skutki transakcji na tych rynkach – *alokacje dóbr*. Interesują nas alokacje prowadzące do lepszego zaspokojenia łącznych potrzeb. Dokładniej, powiadamy, że alokacja dóbr A jest bardziej efektywna od alokacji B, jeśli łączna satysfakcja jest w pierwszym przypadku wyższa. Alokacja A jest *Pareto-optymalna* (krótko: *optymalna*), jeśli nie ma bardziej od niej efektywnej alokacji B. Poszukujemy optymalnych alokacji, a dokładniej organizacji rynku, na którym mechanizm rynkowy prowadzi do alokacji optymalnej. Taki rynek nazwiemy *sprawnym*.

Odnotujmy, że satysfakcja z konsumpcji nie poddaje się łatwym rachunkom. Przykładowo, na jednoosobowym rynku Jasia – konsumenta dwóch dóbr: jabłek i czekoladek, jeśli alokacja A oznacza, że Jaś zje jabłko i dwie czekoladki,

a alokacja B, że zje on dwa jabłka, a czekoladkę tylko jedną, to obie alokacje są optymalne. Wiedząc tylko, że użyteczność (satysfakcja) rośnie z konsumpcją, nie możemy wskazać w tym przypadku, która alokacja – A czy B – jest bardziej satysfakcjonująca. A co dopiero, gdy na rynku jest wielu konsumentów i dóbr. Na rzeczywistych rynkach istnieje wiele optymalnych alokacji. Zmiana organizacji rynku nie wydaje się jednak wtedy oczywista, gdyż zwiększając satysfakcję z konsumpcji jednym, zmniejszalibyśmy ją innym.

Okazuje się, że w rzeczywistości zdarzają się też alokacje nieoptymalne – rynki niesprawne. Rynki publiczne i prywatne nie są sprawne – dopuszczają nieoptymalne stany równowagi, czyli stany, w których można poprawiać satysfakcję jednym, bez pogarszania jej innym.

Źródła nieoptymalności można upatrywać już na najniższym poziomie analizy – zachowań osoby. Brak optymalności ma miejsce np. w sytuacji zakupu dobra po zawyżonej cenie na skutek braku informacji o dostępności tego dobra w cenie niższej. Brak informacji prowadzi do poniesienia dodatkowego kosztu bez dodatkowej satysfakcji. Sytuacja, gdy strony transakcji mają różną informację o warunkach tej transakcji, nosi nazwę *asymetrii informacji*; w podanej sytuacji zakupów mamy przykład asymetrii informacji cenowej.

Brak optymalności ma też miejsce w sytuacji występowania pokusy naruszenia normy regulacyjnej (ang. *moral hazard*). Pokusa taka pojawia się, gdy prawdopodobieństwo poniesienia kary wydaje się niewielkie. Pokusa ta prowadzi do nieuprawnionego konsumowania dóbr (ang. *free riding*) i przeniesienia kosztów tej konsumpcji na inne podmioty. Z sytuacją tą mamy do czynienia, gdy bezpłatny dla klientów parking supermarketu wykorzystywany jest bezkarnie przez kierowców zamieszkujących okoliczne domy. Ukryty w marży koszt tej usługi ponosi klient supermarketu. W efekcie koszt parkowania aut okolicznych mieszkańców transferowany jest do strony zewnętrznej z punktu widzenia transakcji klient-supermarket, która nie uczestniczy w transakcji. Taki transfer kosztu (lub zysku) nazywamy *efektem zewnętrznym*.

Konsekwencją przeniesienia kosztu może być uruchomienie mechanizmu tzw. selekcji przeciwniejszej (ang. *adverse selection*), prowadzącej do występowania stanów nieoptymalnych. W przypadku nieuprawnionego wykorzystywania parkingu, klientom jest coraz trudniej parkować i robią oni zakupy w innych miejscach. Utrata klientów prowadzi do obniżenia zysku sklepu. Próby wyrównania tej straty przez podniesienie cen będą skutkowały dalszą stratą klientów, co może skłaniać do dalszego podniesienia cen, skutkującego przyspieszeniem odpływu klientów. Ten mechanizm selekcji prowadzi do przypadkowej populacji klientów i nieefektywnej alokacji.

Występowanie asymetrii informacji i pokusy nadużycia możliwości wystąpienia efektów zewnętrznych oznaczają niesprawność rynku (istnienie stanu nieoptymalnego). Wpływ tych mechanizmów można łagodzić za pomocą interwencji regulacyjnych. Np. w przypadku rynku usług medycznych, Arrow¹¹ (1963) wskazuje, że gdy występują stany nieoptymalne, to pojawia się skłonność do stopniowego wprowadzania regulacji na rynku (interwencje).

Ponieważ przywołane obserwacje dotyczą każdej organizacji rynkowej, więc zasadne jest odniesienie ich także do rynku prywatności.

4. Regulacja rynku prywatności

Skoro prywatność – prawo do kontroli informacji o sobie – może być przedmiotem transakcji, to rodzą się pytania o rynek prywatności. Wiemy już, że dobro, jakim jest prywatność, charakteryzuje złożona natura. Tabela 1 pokazuje, że w różnych transakcjach i sytuacjach prywatność może być zasobem wspólnym, dobrem klubowym, prywatnym albo publicznym. Handel prywatnością jest dzisiaj faktem, omówione w dzisiejszych referatach zagrożenia nakazują rozważyć problem organizacji tego rynku.

Stopień regulacji funkcjonującego handlu prywatnością jest niski, ale niewątpliwie można powiedzieć, że transakcje na nim nie są wolne od pokusy nadużycia – np. odsprzedaży informacji, a asymetria informacji jest weń wbudowana na wiele sposobów. Przykładowo, ani dysponent bazy danych nie informuje właściciela przetwarzanych danych o efektach ich agregacji, ani konsumenci informacji zagregowanej nie informują w zorganizowany sposób o swoich możliwościach i potrzebach. Konsekwencją tej sytuacji, jak wynika z poprzednich rozważań, jest zagrożenie pojawienia się nieuzasadnionego transferu zysku i występowanie nieefektywności – nieoptymalnych alokacji na rynku. Powstaje pytanie o taką regulację tego rynku, w której mechanizm rynkowy zagwarantuje alokacje optymalne.

Wydaje się, że istnieją bardzo poważne argumenty nakazujące odrzucić dwie narzucające się organizacje rynku – wolny rynek i rynek kontrolowany przez państwo. Wolny rynek w opisanych wyżej sytuacjach (asymetrii informacji i możliwości ulegania pokusie transferu zysku) zagrożony jest nieefektywnością. Kontrola państwa jako panaceum na defekty rynkowe także wykazała swoją niesprawność i na gruncie teorii, i praktyki. Instytucje rządowe mogą być wykorzystywane i mogą ignorować potrzeby społeczne. Co więcej, regulacje państwowe wymagają oceny jakości efektu i nadzoru wydajności pracowni-

¹¹Arrow K.J., *Uncertainty and the Welfare Economics of Medical Care*, American Economic Review, Vol. 53, pp. 941-973, 1963.

ków. Stawia to pod znakiem zapytania wiarygodność informacji przetwarzanej w decyzjach dotyczących gospodarki. Państwo jako regulator rynku prywatności nie eliminuje pokusy przenoszenia kosztów ani korzystania z przywilejów – nie wyklucza więc nieoptymalnych alokacji.

Teoria dostarcza innych typów organizacji – opartych o *umowę społeczną* zmieniającą charakter dobra oraz opartych o *rozwiązanie technologiczne* zmieniające charakter dobra i warunki transakcji. W obu przypadkach dojście do alokacji efektywnych uzyskuje się przez nadanie dobrom publicznych charakterystyk dóbr prywatnych. Próby stworzenia koszyków usług i leków w służbie zdrowia stanowią właśnie próbę regulacji części rynku zdrowia w oparciu o umowę społeczną. Umowa dzieli ten rynek na obszar centralnie regulowany w części objętej koszykami i obszar poddany regulacji rynkowej, takiej samej jak dla innych dóbr.

W przypadku włączenia do organizacji rynku rozwiązań technologicznych, możliwe staje się wykluczenie nieuzasadnionego transferu kosztów lub zysku i zmniejszenie asymetrii informacji. Tego ostatniego doświadczamy korzystając z Internetu, który pozwala uzyskać konsumentom informację o cenach w tak krótkim czasie, że w warunkach handlu elektronicznego uniemożliwia uzyskiwanie producentom zysku wynikającego z cenowej asymetrii informacji. Odpłatne i chronione hasłem korzystanie na lotniskach i w hotelach z Internetu za pomocą łączności radiowej (WiFi) jest przykładem interwencji technologicznej, która wyklucza efekty zewnętrzne przez nadanie dobrom publicznych charakterystyk dóbr prywatnych.

Jak Państwo się domyślają, nie da się obronić żadnego ze skrajnych rozwiązań. Z braku czasu pominię argumentację teoretyczną uzasadniającą, że każda z tych organizacji rynku z osobna dopuszcza nieefektywność. Natomiast chciałbym rekomendować myślenie, które drogi do optymalizacji handlu prywatnością upatruje w łącznej, hybrydowej organizacji rynku prywatności. W tym celu posłużę się metodą specyficzną dla nauk o zarządzaniu. Proponuję, byśmy poddali analizie studium przypadku – uproszczonego modelu dobrze interpretowalnej sytuacji – które zostało skonstruowane tak, by odzwierciedlało ogólne mechanizmy funkcjonalne.

Rozważmy państwo, w którym na mocy prawa działa tylko telewizja publiczna z dwoma kanałami. Kanał pierwszy oferuje informację, a drugi – rozrywkę. Państwo dysponuje budżetem na zaspokojenie potrzeb społecznych w obu tych obszarach. Budżet tworzą podatki i wpłaty z abonamentu.

Oba kanały oferują dobra publiczne – oglądanie TV nie wyklucza z tego innych, a i programu przy tym nie ubywa. Można oczekiwać nieefektyw-

ności i rzeczywiście istnieje pokusa ignorowania abonamentu. Koszt ścigania sprawia, że ryzyko kary jest zanedbywalne. Spadek wpłat zmniejsza wpływy do budżetu i jakość telewizji. Spadek jakości TV nie skłania do płacenia za abonament. Spadek opłat (rozpoznajemy zjawisko przeciwskutecznej selekcji) zmusza państwo do nowych wydatków z budżetu na podtrzymanie odpowiednio wysokiego poziomu TV. Jest to alokacja niesprawna, bo podatki ludzi, którzy nie korzystają z telewizji, pokrywają teraz koszty, nie powiększając ich użyteczności.

Rozważmy rozwiązanie hybrydowe – łączące umowę społeczną i rozwiązanie technologiczne. Umowa polega na regulacji rynkowej dopuszczającej telewizje prywatne do oferowania rozrywki i reklam oraz pobierania opłat za te usługi proporcjonalnie do popularności okresu nadawania tych reklam. Ten mechanizm uniemożliwia transfer kosztu, o ile programy są zakodowane (rozwiązanie technologiczne). Powstaje pytanie, dlaczego mogą działać sprawnie telewizje prywatne, a państwowe nie. Misja państwowej telewizji gwarantuje realizację potrzeb i praw ludzi. Zauważmy, że wyłączenie z dostępu do informacji może tworzyć stan asymetrii informacyjnej i mieć poważne skutki polityczne (w przypadku skrajnym – totalitarne nadużycie władzy). Zatem – w przeciwieństwie do rozrywki – wyłączenie z usług informacyjnych nie jest możliwe.

Umowa społeczna w połączeniu z technologią (kodowanie programów) prowadzi do zmniejszenia efektu zewnętrznego do niezbędnego minimum.

Odnotujemy, że rozwiązanie przedstawione w tym przypadku wynika z analizy struktury dobra (potrzeby indywidualne i cele społeczne zaspokajane są przez dobro rynkowe, dualność *informacja-rozrywka*), organizacji transakcji (abonament, podatki) i sposobu dostarczania dobra (dwa kanały). W przypadku handlu prywatnością zaczynamy dopiero rozpoznawać takie elementy.

5. Uwagi końcowe

Spróbujmy przedstawiony wywód podsumować.

Początek analizy pojęcia prywatności to dobra osobiste¹². Są one chronione prawem, przysługują każdej osobie fizycznej (a także osobom prawnym). Dóbr tych nie definiuje się w sposób ogólny, bo definicja musi korzystać z od-

¹²W Polsce do dóbr osobistych zalicza się m.in. (art. 23 kc): zdrowie, wolność, cześć, swobodę sumienia, nazwisko lub pseudonim, wizerunek, tajemnicę korespondencji, nietykalność mieszkania, twórczość naukową, artystyczną, wynalazczą i racjonalizatorską.

niesień do uznanych przez społeczeństwo oraz system prawny wartości, które są różne w różnych krajach i ulegają zmianom. Niemniej kodeksy krajowe zawierają regulacje chroniące przed bezprawnym naruszeniem dóbr osobistych, nie wymagając, aby naruszenie było zawinione¹³. Środkiem ochrony dóbr jest możliwość do domagania się na drodze sądowej m.in. zaniechania działań naruszających dobra osobiste (np. zaniechanie kolportażu publikacji naruszającej prywatność)¹⁴. Naruszenie dobra osobistego skutkujące szkodą materialną wymaga odszkodowania. Jak widać, obszar dóbr osobistych jest przez prawo precyzyjnie regulowany. W obszarach, gdzie dobro osobiste może być przedmiotem wymiany, funkcjonują precyzyjne rozwiązania, np. prawo autorskie.

System prawny rozwija się, włączając regulacje dotyczące nowych zjawisk społecznych. Ponieważ dobra osobiste związane są z obiegiem informacji, więc w sytuacji przemian w technologii przetwarzania informacji i ich skutków nie dziwi, że prawo nie wystarcza do ochrony dóbr osobistych. Na świecie pojawił się nieuregulowany, dziki handel danymi osobistymi indywidualnymi i zagregowanymi. Posiadacz dóbr osobistych utracił w znacznym stopniu kontrolę nad informacją o sobie – nad swoją prywatnością. Prawo nie chroni już wystarczająco tego dobra. Następuje uwłaszczenie podmiotów innych niż posiadacz prywatności. W tych warunkach spontanicznie ukształtowany rynek nie jest efektywny. Potrzebne są nowe rozwiązania.

Istniejące rozwiązania administracyjne, prawno-ekonomiczne i technologiczne nie przenoszą się automatycznie na rynek prywatności. W dodatku, próby wprowadzenia ich niezależnie od siebie niosą poważne problemy. Interwencja administracyjna zagrożona jest nieskutecznością, propozycja laudonowskiej rekonstrukcji rynku, zmieniająca charakter dobra na prywatne, oznacza konieczność nierealistycznej korekty systemu demokratycznego. Także oderwana od rynku i technologii umowa społeczna budzi poważne wątpliwości.

Efektywność rynku prywatności wymaga transakcji rynkowych, których opłacalność reguluje kontrakt hybrydowy oparty o umowę społeczną chronioną rozwiązaniami technologicznymi i wspartą regulacjami prawnymi.

¹³W Polsce wyjątkami są sytuacje wyrażenia zgodę na naruszenie praw osobistych (np. u dentysty zgadzamy się na bolesne naruszenie nietykalności), sytuacji funkcjonowania w ramach przepisu prawa (list gończy) oraz działania sprzecznego z zasadami współżycia społecznego.

¹⁴Inne takie środki prawne to usunięcie skutków naruszenia (np. sprostowanie w prasie) lub zadośćuczynienie pieniężne lub zapłata na cel społeczny.

Wydaje się, że jesteśmy dopiero na początku drogi do tak sformułowanego celu. Podejmowane są próby technologiczne zwiększające kontrolę właściciela danych osobistych nad tymi danymi. Twórcy oprogramowania dążą do tego, by w sytuacjach, gdy dane są rejestrowane, ich właściciel mógł ograniczyć zakres ich przetwarzania (np. blokować łączenie z innymi danymi), wymagać przeprowadzenia dodatkowych operacji (np. losowego zaburzenia danych lub specjalnego ich kodowania – wspomniał już o tym dr Kamiński)¹⁵. Wadą zaburzenia jest obniżka jakości danych, wynikająca z modyfikacji wartości pól rekordów baz danych. Dane zakodowane nie ujawniają swych oryginalnych wartości, a mimo to możliwe jest wykonywanie pewnych operacji matematycznych na zakodowanych wartościach (np. Zhang *et al.*¹⁶). Mimo, że proponowane rozwiązania dalekie są od upowszechnienia w wielkiej skali, można już wskazać pierwsze przesłanki do tworzenia niezbędnej umowy społecznej i nowego prawa. Jak dowiodło tego studium przypadku, należy uwzględnić analizę struktury dobra, jakim jest prywatność, odrębnie rozważać sposoby organizacji transakcji i dostarczania dobra.

Przygotowywane rozwiązania prawne mają wstępny charakter. Np. Uwaga 39 (spośród 72): „...*Niektóre czynności w zakresie przetwarzania danych angażują dane, których administrator danych nie uzyskał bezpośrednio od osoby, której te dane dotyczą; ponadto dane mogą być legalnie ujawnione osobie trzeciej, nawet jeżeli ich ujawnienie nie było przewidywane w czasie, kiedy uzyskiwano dane od osoby, której dotyczą; we wszystkich tych przypadkach osoba, której dane dotyczą, powinna być informowana przy rejestracji danych lub też najpóźniej kiedy dane są po raz pierwszy ujawnione osobie trzeciej...*”¹⁷, która zawarta jest w dyrektywie unijnej prowadzi m.in. do art. 17. p. 2. „*Państwa Członkowskie zobowiązują administratora danych, w przypadku przetwarzania danych w jego imieniu, do wybrania systemu przetwarzającego, o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz zapewnienia stosowania tych środków i rozwiązań*”. Ten wymóg docenia rolę rozwiązań technologicznych, ale aspekty ekonomiczne pozostawia jeszcze poza obszarem

¹⁵Matwin S., *Privacy-Related Aspects and Techniques*, a manuscript.

¹⁶Zhang J., Matwin S., Chang L., *Privacy-Preserving Collaborative Association Rule Mining*, Procs. of the 19th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Storrs, CT, August 2005, pp. 153-165.

¹⁷Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, str. 31) zmieniona przez Rozporządzenie (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. DZ.U. L 284 str. 1 z 31.10.2003).

regulacji, poprzestając na rozważeniu ograniczeń dostępu do informacji w sytuacjach naruszenia prywatności.

Wydaje się, że regulacja rynku prywatności dopiero się rozpoczyna i jej ostateczny kształt będzie wynikiem dwóch uzupełniających procesów: odgórnego – administracyjnego, i oddolnego – zakorzenionego w samorządności różnej skali społeczności. Przykładu funkcjonowania tego pierwszego dostarcza przywołana dyrektywa unijna, a w skali krajowej – działalność Głównego Inspektoratu Ochrony Danych Osobowych wspomiana w prezentacji doktora Kamińskiego. Proces drugi wynika ze zmieniających się postaw środowisk, takich jak środowisko akademickie. Przykładowo, na uczelniach w Polsce obserwujemy wyraźną staranność nauczycieli akademickich w ochronie prywatności studentów, np. przy komunikowaniu wyników nauczania. Właśnie problemy prywatności w edukacji poświęcimy nasze następne seminarium.

DYSKUSJA

Profesor Jerzy Osiowski (Instytut Problemów Współczesnej Cywilizacji)

– Dziękuję bardzo, muszę powiedzieć, że z wielkim zainteresowaniem wysłuchałem referatu Pana Redaktora. Temat właściwie dotyczy każdego z nas, dlatego że wyrzucamy do śmieci mnóstwo rozmaitych rzeczy, papierów, na których jest wiele danych. Ktoś mi zwrócił uwagę – już teraz tego przestrzegam, żeby na każdej kopercie przed jej wyrzuceniem w sposób jednak dokładny zamazywać imię, nazwisko i adres, bo jak nie, to jeżeli na kopercie jest nagłówek, skąd pochodzi korespondencja i w dodatku jest nazwisko i adres osoby, do której jest skierowana, to ktoś niepowołany może to wykorzystać. Jak już wspomniałem, przestrzegam tego, a Pan Redaktor mnie utwierdził w przekonaniu, że jest to słuszna metoda. Dziękuję bardzo.

Doktor Inga Oleksiuk (Instytut Problemów Współczesnej Cywilizacji) –

Dziękuję za zaproszenie. Z dużym zainteresowaniem uczestniczę w tym seminarium. Nie tylko ze względu na tematykę. W szczególności z powodu tradycyjnej dla Instytutu interdyscyplinarnej formy dyskusji i konfrontacji argumentów prowadzonych z diametralnie odmiennych perspektyw.

Problematyka ochrony dóbr osobistych człowieka, w tym równoważenia wolności wypowiedzi z prawem do prywatności jest przedmiotem mojego zainteresowania naukowego. Pracę badawczą w tym zakresie prowadzę na styku nauk humanistycznych i nauk prawnych. Z tej perspektywy chciałabym się odnieść do wypowiedzi prelegentów. Otóż – w moim przekonaniu – nie można mówić o prywatyzacji (komercjalizacji) prawa do prywatności i tworzeniu rynków prywatności (porównywalnych do rynków papierów wartościowych). Komercjalizacja dóbr osobistych (jeśli dobrze zrozumiałam problem badawczy postawiony przez prof. Tomasza Szapiro) nie jest – w moim przekonaniu – możliwa. Nawet, jeśli urynkowienie prywatności człowieka miałyby usprawnić gospodarkę i zwiększyć profity różnych podmiotów gospodarczych, to takie rozwiązanie nie mieści

się w naszym systemie konstytucyjno-prawnym. „Prywatność” w rozumieniu prawnym należy do podstawowych praw człowieka. Doktryna i orzecznictwo (sądów polskich, Europejskiego Trybunału Sprawiedliwości) jest nie tylko wyjątkowo złożona, ale i bardzo bogata. Dotyczy to zarówno rozumienia omawianego dobra, jak i zasad jego ochrony. „Rynki prywatności”, na których obraca się dobrami osobistymi konkretnych osób niezależnie od ich wyraźnie wyrażonej woli, znajdują się poza prawem. W moim przekonaniu tam powinny pozostać. Jeśli dziś istnieją, są to „czarne rynki”¹.

Profesor Tomasz Szapiro – Chciałbym zabrać głos *ad vocem*, jak to się teraz często mówi – wywołany do tablicy. Otóż obawiam się, że jednak prawo nie reguluje tak znakomicie kwestii prywatności, jak w ostatniej części swej wypowiedzi stwierdziła doktor Oleksiuk. Jak Państwo być może odnotowali, opinię publiczną w Polsce dwa miesiące temu poruszył przypadek, kiedy pewna młoda osoba, nie wiedząc o tym, w trakcie intymnego pożycia z partnerem, była przez długi czas przezeń skrycie filmowana. Postanowiła ona zerwać ten związek – nie z powodu nagrań, bo powtórzmy – absolutnie nic o nich wiedziała. Być może z powodu niezgodności charakterów. Była to para nieformalna. I w zasadzie nic by się nie stało, gdyby nie to, że dramatycznie cierpiący z powodu rozstania młody człowiek upowszechnił owe filmy. Bohaterka tej historii dowiedziała się od swoich kolegów, że funkcjonuje w Internecie na filmiku, który każdy może ściągnąć i obejrzeć. Zawiedziony amant powiadomił pocztą elektroniczną ogromną grupę jej znajomych i nieznaną jej osób o swojej filmowej produkcji. W polskim, niezbyt zgodnym Sejmie zawiązała się grupa posłów – z wielu ugrupowań, która obecnie zmierza zgodnie do zmiany prawa. Okazało się bowiem, że stajemy tu wobec deficytu prawa. Obecny stan prawny nie stwarza żadnej możliwości, żeby ewidentne dla każdego, dramatyczne naruszenie prywatności osoby zostało – zgodnie z prawem czy poprzez prawo – ukarane czy, jeżeli jest to w ogóle możliwe, zadośćuczynione.

Pozostawmy jednak na boku spór o to, czy istnieje, czy nie istnieje deficyt prawa dotyczącego prywatności. Mówiłem o czymś zupełnie innym – widocznie niezbyt jasno. Chodziło mi mianowicie o deficyt wiedzy. W sprawach prywatności bardzo mało wiemy. Trudno jest o dobre regulacje, jeżeli niewiele wiemy o ich przedmiocie.

¹Chciałabym zastrzec, że powyższe uwagi dotyczą rozwiązań przyjętych w systemie prawa kontynentalnego, w tym – w prawie polskim.

Redaktor Marek Ostrowski – Tu się cisną na usta rozmaite uwagi, więc od razu muszę zastrzec, że tylko mogę skrótowo zaznaczyć dwa obszary, które mnie zaciekały w tej dyskusji. Pierwsza, z całym szacunkiem dla Pani Ingi Oleksiuk, naszej młodej koleżanki, która głos zabrała; wydaje mi się, że wypowiedź można skomentować tak: dobrze, że młoda osoba wierzy w siłę regulacji prawnych. Mimo to, podtrzymywałbym tezę, że mamy do czynienia ze sferą płynną, budzącą wątpliwości co do przestrzegania prawa i możliwości ochrony praw jednostki. W ogóle wydaje mi się, że w polskiej myśli prawniczej za bardzo się skupiamy na regulacjach *in abstracto*, że tak powiem, na normach, a za mało na badaniu, jak te normy rzeczywiście są przestrzegane w życiu społecznym. Oto, żeby sięgnąć po wielki i nie odnoszący się bezpośrednio do prywatności, najprostszy przykład. Jednym z elementarnych praw w obrębie w ogóle prawodawstwa jest prawo człowieka do sądu. Otóż trudności rozmaite: techniczne, finansowe, społeczne powodują, że faktycznie ten dostęp do sądu jest bardzo, bardzo utrudniony albo że prawo do sądu przychodzi w końcu z takim opóźnieniem, że czyni z tego prawa wydmuszkę i tu się otwiera całe pole dyskusji, co tu jest rzeczywiście normą, jeśli ją rozpatrywać jako konkretnie wykonywalne prawo ludzkie. Więc upierałbym się przy swojej ocenie, że ochrona prywatności to sfera bardzo płynna.

Drugi obszar, który mnie zaciekał – bardzo ciekawą, wręcz pasjonującą, moim zdaniem, uwagę zgłosił prof. Szapiro. Mianowicie, że należałoby w obrębie regulacji rynkowych nadać niektórym dobrom publicznym charakterystykę, właściwości dóbr prywatnych. Otóż rozumiem, że założeniem tego postulatu jest spostrzeżenie, że dobra prywatne cieszą się na rynku większym uznaniem niż dobra publiczne. Chodziłoby więc o to, by rangę dóbr publicznych wzmocnić. Zachęcałbym go – po pierwsze – do rozwinięcia tej uwagi, a po wtóre – do dalszych prac nad tym postulatem, gdyż dobra publiczne są zwykle za mało dowartościowane. Wydaje się, że w takiej pożądanej, nowej umowie społecznej można je awansować. Dziękuję bardzo.

Profesor Tomasz Szapiro – Dziękuję bardzo. Starając zmieścić się w przewidzianym czasie, pominąłem ważny element, który mogę teraz króciutko uzupełnić – telewizyjne studium przypadku. Otóż, rynek dóbr publicznych wymaga elementów regulacji centralnej. Jak tego dowiodły systemy autorytarne, regulacje takie mogą być okrutnie nadużywane, co kompromituje system centralno-nakazowy w roli panaceum na defekty rynku. Rodzi się pytanie, czy wobec tego rynek prywatny nie robiłby tego lepiej. Próba uczynienia dobra publicznego, jakim jest oglądanie telewizji,

dobrem prywatnym jest pokusą naturalną. Rynki prywatne nie działają doskonale, ale dużo lepiej niż rynki centralnie nakazowo sterowane. Okazuje się jednak, że również takim rynkom nie można wszystkiego oddać, ponieważ rynek prywatny ma swoje defekty. Prawdopodobnie nie ma jednej uniwersalnej koncepcji i musimy się przygotować do tego, że w różnych obszarach rynku, dla różnych dóbr będą funkcjonowały różne organizacje rynku.

Doktor Anna Jankowska (Instytut Problemów Współczesnej Cywilizacji)

– Chciałabym odnieść się do terminu *umowa społeczna*. Wydaje się, że nie powinniśmy przywiązywać nadmiernej wagi do regulacji formalnych.

Rodzaj relacji wzajemnych i swego rodzaju komfort życia w dużym stopniu zależą od tak zwanego obyczaju. Gdyby panowała powszechna zgoda co do tego, co jest dopuszczalne, a czego się po prostu nie robi, sądy nie byłyby zamulane „pyskówkami”, a prawo do rozstrzygnięcia sądowego poważnych sporów w rozsądnym czasie byłoby egzekwowalne.

Jeżeli chcemy zmieniać jakość wzajemnych relacji i klimatu życia społecznego, to trzeba zaczynać w przedszkolu, w szkole, od innej wizji wychowania. Obyczajem się nasiąka, to wymaga czasu i harmonii oddziaływania różnych bodźców. Tymczasem w szkolnictwie pojawiają się zjawiska wręcz uniemożliwiające budowanie tak brakującego w Polsce kapitału zaufania społecznego: nadmierna kontrola wskazująca, że nikt do nikogo nie ma zaufania, odchodzenie od wspólnej pracy uczniów (np. większych, wieloaspektowych projektów) i bardzo sformalizowane mierzenie tylko ich indywidualnych osiągnięć. Nie mówiąc już o ochronie, kamerach, nadzorze, który przez swoją wszechobecność zdaje się uwalniać młodego człowieka od poczucia rzeczywistej, bezwarunkowej odpowiedzialności.

Tym zagadnieniom chcielibyśmy poświęcić jedno z następnych seminariów.

Profesor Tomasz Szapiro – Dyskusja wygasła w naturalny sposób. Mam nadzieję, że kawa nie wystygła w naturalny sposób i jest jeszcze gorąca. Zapraszamy. Przypomnę tylko, że po wakacjach planujemy drugą część tego spotkania, na którym spróbowałibyśmy zrozumieć, czym jest prywatność w obszarze edukacji.

Spis treści

Słowo wstępne	
<i>Marek Dietrich</i>	3
Wprowadzenie	
<i>Tomasz Szapiro</i>	5
Sfera prywatności – ile o sobie powinniśmy wiedzieć	
<i>Marek Ostrowski</i>	7
Przetwarzanie poufnych danych klientów – korzyści i koszty	
<i>Bogumił Kamiński</i>	15
Handel prywatnością a ekonomia	
<i>Tomasz Szapiro, Stanisław Matwin</i>	23
Dyskusja	39

Zeszyty opublikowane przez Instytut

Rok 1997

- I – Ochrona własności intelektualnej
- II – Etyka zawodowa
- III – Jakość kształcenia w szkołach wyższych
- IV – Akademyka Komisja Akredytacyjna. System oceny jakości kształcenia i akredytacji w szkolnictwie wyższym

Rok 1998

- V – Instrumenty rozwoju systemu kształcenia w Polsce
- VI – Bezpieczeństwo człowieka we współczesnym świecie
- VII – Misja uczelni
- VIII – Polska a integracja europejska w edukacji. Aspekty informatyczne

Rok 1999

- IX – Bezpieczeństwo człowieka we współczesnym świecie
- X – Problemy etyczne techniki
- XI – Koszty kształcenia w szkołach wyższych w Polsce. Model kalkulacyjnych kosztów kształcenia
- XII – Władza i obywatel w społeczeństwie informacyjnym

Rok 2000

- XIII – Kształcenie międzyuczelniane. Studium warszawskie
- XIV – Produkcja, konsumpcja i technika a ocieplenie klimatu
- XV – Czy kryzys demograficzny w Polsce?
- XVI – Ekonomiczne i społeczne efekty edukacji

Rok 2001

- XVII – Ekonomiczne i społeczne efekty edukacji
- XVIII – Wolność a bezpieczeństwo
- XIX – Ekonomiczne efekty edukacji w Polsce

Rok 2002

- XX – Pamięć i działanie
- XXI – Bezpieczeństwo człowieka we współczesnym świecie
- XXII – Problemy etyczne w nauce
- XXIII – Autorytet uczelni
- XXIV – Jakość kształcenia i akredytacja w szkolnictwie wyższym w Polsce

Rok 2003

- XXV – Zarządzanie bezpieczeństwem w sytuacjach kryzysowych
- XXVI – Kierunki kształcenia i standardy nauczania w polskim szkolnictwie wyższym

Rok 2004

- XXVII – Internet i techniki multimedialne w edukacji
- XXVIII – Uczelnie a innowacyjność gospodarki
- XXIX – Decyzje edukacyjne

Rok 2005

- XXX – Emigracja – zagrożenie czy szansa?
- XXXI – Zagadnienia bezpieczeństwa energetycznego
- XXXII – Polskie uczelnie XXI wieku
- XXXIII – Zagadnienia bezpieczeństwa wodnego

Rok 2006

- XXXIV – Humanizm i technika
- XXXV – Rola symboli
- XXXVI – Wizja polskich uczelni w społeczeństwie globalnym

Rok 2007

- XXXVII – Uczyć myśleć
- XXXVIII – Obraz postępu i zagrożeń cywilizacyjnych w mediach
- XXXIX – Czasopisma naukowe – zmierzch czy transformacja?

Rok 2008

- XL – Warszawa Akademicka – Seminarium
- XLI – Warszawa Akademicka
- XLII – Polscy uczniowie w świetle badań PISA
- XLIII – Prywatność – prawo czy produkt?