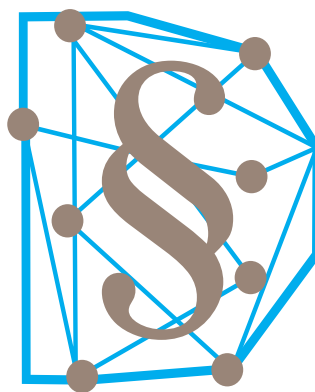


DEBATA  
Prywatność  
w nowych  
technologiach



Sprawozdanie



FUNDACJA  
bezpieczna  
cyberprzestrzeń



## Spis Treści

Sprawozdanie z debaty. Wstęp.....	3
Ochrona przed naruszeniami a prawo do prywatności.....	4
Ochrona prywatności a cookies.....	6
Prywatność w usługach świadczonych drogą elektroniczną.....	7
Prywatność w serwisach społecznościowych.....	9



# Prywatność w nowych technologiach

## Sprawozdanie z debaty

20 marca 2013r. odbyła się debata na temat prywatności w nowych technologiach, jako pierwsze wydarzenie spośród cyklu zaplanowanego przez Fundację Bezpieczna Cyberprzestrzeń, którego celem jest zaaktywizowanie dyskusji na wybrane tematy z zakresu bezpieczeństwa prawnego i technicznego w nowych technologiach. Fundacja może stać się platformą dla skonfrontowania różnych poglądów i środowisk z tego zakresu. Temat przewodni spotkania nie został wybrany przypadkowo, bowiem zostało ono zorganizowane na dwa dni przed wejściem w życie znowelizowanych przepisów prawa telekomunikacyjnego, dotyczących między innymi zagadnień prywatności użytkowników Internetu, które zrodziły wiele znaków zapytania. Ostatnie prace Komisji Europejskiej oraz wzmożona dyskusja na temat reformy ochrony danych osobowych stanowiły dodatkowe czynniki aktualizujące potrzebę głębszego omówienia zagadnienia prywatności w nowych technologiach.

Wydarzenie zostało zorganizowane wspólnie z Kołem Naukowym CyberLawUW działającym na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Patronat honorowy nad wydarzeniem objął Generalny Inspektor Ochrony Danych Osobowych – dr Wojciech Wiewiórowski, Dziekan Wydziału Prawa i Administracji Uniwersytetu Warszawskiego – prof. dr hab. Krzysztof Rączka, Polska Izba Informatyki i Telekomunikacji oraz Krajowa Izba Radców Prawnych.





Specjalne przesłanie do uczestników debaty wygłosił Minister Administracji i Cyfryzacji – Michał Boni, zapraszając do dalszych dyskusji również z udziałem Ministerstwa Administracji i Cyfryzacji. Przesłanie można odtworzyć:

<https://mac.gov.pl/dzialania/m-boni-potrzebne-nowe-spojrzenie-na-ochrone-danych-osobowych/>

Poniżej przedstawione zostały niektóre fragmenty debaty, wskazujące na wagę poruszanych problemów.

Merytorycznym otwarciem debaty był wykład Piotra Drobka z Biura Generalnego Inspektora Ochrony Danych Osobowych (Zastępca Dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej), który wskazał na problematyczną istotę ważenia rozwiązań prawnych i rozwoju technologii komunikacyjno informacyjnych. Podkreślił potrzebę tworzenia elastycznych ram prawnych, które pozwolą na zagwarantowanie podstawowych zasad i praw. Tym samym odwołał się do trudności w regulowaniu samego stosowania określonych rozwiązań technologicznych czy wykorzystywania informacji zbieranych o osobach. W kontekście Polski powołał się na art. 47 Konstytucji (gwarantujący prawo do prywatności) oraz art. 51 Konstytucji (gwarantujący autonomię informacyjną jednostki), które są podstawą przy inkorporowaniu przepisów jak i tworzeniu polskich regulacji.

## Ochrona przed naruszeniami a prawo do prywatności

Pierwszy panel dyskusyjny „Ochrona przed naruszeniami a prawo do prywatności” moderowany był przez Piotra Wąglowskiego, który postawił przed dyskutantami prowokacyjną tezę sprowadzającą się do pytania czy w 2015r. będziemy mogli ogłosić koniec prawa do prywatności, gdyż wszyscy będą wiedzieć wszystko o wszystkich. Doktor Arwid Mednis (Wierzbowski Eversheds), który jako pierwszy zabrał głos w dyskusji stwierdził, iż zasadniczy problem polega na działaniu wielu użytkowników Internetu – udostępnianiu przez nich szeregu informacji przy jednoczesnym braku świadomości o wiecznej pamięci Internetu oraz jego globalnym zasięgu. Tym samym wyraził on swoją obawę co do realnej ochrony w kontekście zachowań samych użytkowników. Katarzyna Szymielewicz (Fundacja Panoptikon) zgodziła się, że ryzyko w zakresie faktycznego końca prywatności obywateli (nie prawa do prywatności jako takiego) istnieje, ale w dużej mierze zależy ono właśnie od nich samych. Żadne regulacje nie będą bowiem skuteczne jeśli ludzie samowolnie będą rezygnować z własnej prywatności. Niemniej jednak państwo powinno zapewnić odpowiednie ramy regulacyjne tak by był zapewniony faktyczny wybór dla użytkowników/ obywateli w zakresie respektowania



ich prawa do prywatności przez państwo czy organizacje prywatne. W następnym pytaniu moderator odwołał się do przykładu osoby, która notorycznie posługiwała się przy wypełnianiu formularzy fałszywą tożsamością. Postawione pytanie brzmiało: Jak bardzo możemy zmusić obywateli do podawania prawdziwych danych na swój temat np. przy zawieraniu umowy i czy ta umowa zostanie skutecznie zawarta jeżeli dane będą fałszywe. Dr Arwid Mednis podkreślił, że to zależy od kształtu umowy i zarazem natury usługi. W zależności od serwisu, rodzaju i specyfiki usług podejmowane są różne środki w celu weryfikacji tożsamości. Katarzyna Szymielewicz odniosła się do problemu w odniesieniu do naruszania prywatności. Podkreśliła, że usługodawca w zależności od przyjętego modelu biznesowego może gromadzić tak wiele informacji na temat aktywności użytkownika (jego cyfrowych śladów), że bez najmniejszych problemów jest w stanie zweryfikować jego tożsamość bez stosowania wymogu podawania przez niego choćby imienia i nazwiska by skutecznie na niego oddziaływać (np. proponować mu określone oferty). Dr Mednis zgodził się, że można naruszać prywatność obywatela bez wiedzy na temat jego danych osobowych (wszak prywatność jest szerszym pojęciem aniżeli ochrona danych osobowych).



## Ochrona prywatności a cookies



Artur Piechocki będący moderatorem drugiego panelu wprowadził uczestników debaty do tematu prezentacją edukacyjną na temat cookies. Debata rozpoczęła się od zweryfikowania trafności lokalizacji przepisu dotyczącego cookies (niewielkie informacje tekstowe, wysyłane przez serwer WWW i zapisywane po stronie użytkownika Internetu) w przepisach ustawy prawo telekomunikacyjne. Igor Ostrowski (Salans) poprzedził swoją wypowiedź podkreśleniem, że bez cookies nie byłoby możliwe prosperowanie e-commerce czy wszelkiego rodzaju podmiotów świadczących usługi drogą elektroniczną stąd sposób regulacji jest nadzwyczaj ważny. Odpowiadając na pytanie uznał, że umiejscowienie przepisów w ustawie prawo telekomunikacyjne jest właściwe z uwagi na szeroki zakres podmiotów, do których owa ustawa się odwołuje. Xawery Konarski stwierdził z kolei, że ważne jest uzyskanie odpowiedzi nie tylko na to gdzie regulować, ale przede wszystkim co powinno zostać objęte przedmiotem regulacji. Jego zdaniem prawo unijne zajęło się reglamentowaniem zapisywania informacji w różnych celach w urządzeniach końcowych.. Mecenas Konarski odpowiadając na pytanie moderatora o trafność lokalizacji regulacji przytoczył przykłady państw członkowskich Unii Europejskiej, które implementowały przepisy dyrektywy i w tym kontekście wskazał, że polska regulacja mogła zostać umieszczona w innym miejscu. Xawery Konarski wskazał na cztery sposoby regulacji:



- 1) w ustawie prawo telekomunikacyjne (przepisy zostały wdrożone jeszcze w czterech państwach oprócz Polski);
- 2) w odpowiednikach polskiej ustawy o świadczeniu usług drogą elektroniczną;
- 3) za pomocą odrębnej regulacji (np. w Danii uchwalono ustawę o ochronie prywatności w usługach elektronicznych); 4) błędnie, a mianowicie za pomocą nowelizacji ustawy o ochronie danych osobowych (Włochy).

Problem i specyfika polskiej regulacji polega na tym, że ustawa o świadczeniu usług drogą elektroniczną reguluje już cookies (art. 6.2 ustawy). Problemem może być zatem aspekt interpretacji adresatów przepisów co zostało wielokrotnie poruszone w czasie późniejszej dyskusji. Mecenas Ostrowski w odniesieniu do wypowiedzi adwersarza wskazał, że miejsce regulacji przepisów o cookies w prawie telekomunikacyjnym jest swego rodzaju dopełnieniem ustawy o świadczeniu usług drogą elektroniczną.

Drugie pytanie Artura Piechockiego dotyczyło problematyki zakresu terytorialnego obowiązywania przepisów.

Xawery Konarski powołał się na ocenę prawa właściwego ze względu na siedzibę (Międzynarodowych Regulacji Telekomunikacyjnych), którym m.in. Polska zawetowała. Wskazał, że w dobie Internetu nie ma granic, a tym samym polskie regulacje powinny przyciągać przedsiębiorców do zakładania firm na terenie kraju i zgodził się z mec. Konarskim. W dalszej części debaty odniesiono się do problematyki zgody, a także możliwego wpływu przepisów na gospodarkę europejską, która w wyniku wprowadzania kolejnych wymogów, nakładanych na przedsiębiorców działających w Internecie może stać się mniej konkurencyjna.

## Prywatność w usługach świadczonych drogą elektroniczną

Trzeci panel debaty poprowadził Tomasz Kulisiewicz, zaczynając od unaocznienia jak bardzo rozbudowaną dziedziną jest świadczenie usług drogą elektroniczną, których z każdym rokiem przybywa coraz więcej i to w różnych odmianach. Posłużył się w tym celu wieloma przykładami



rozwoju takich usług, począwszy od prostych e-usług, a skończywszy na inteligentnych samochodach i licznikach energii. W kontekście swojej wypowiedzi Tomasz Kulisiewicz zasugerował, że ustawa o świadczeniu usług drogą elektroniczną zaczyna się „starzeć” i poprowadził krótkie rozważania na temat tego czy zostanie ona regulacją sektorową czy może pójdziemy w takim kierunku, że prawo telekomunikacyjne będzie dotyczyło części technicznej tymczasem ustawa o świadczeniu usług drogą elektroniczną będzie dotyczyła innych aspektów. Moderator jako pierwsze sformułował pytanie na ile i zarazem w jakim zakresie dostawcy, których reprezentują dyskutanci są zainteresowani prywatnością użytkowników. Agata Waclawik-Wejman (Google) zaczęła odpowiedź od wskazania, że gospodarka krajów rozwiniętych opiera się na przepływie informacji, w tym dotyczących danej osoby. Temat wymaga pewnego usystematyzowania, gdyż firm technologicznych jest coraz więcej, a istnieje wiele mitów na temat „czyhania tych firm” na prywatność użytkowników. Agata Waclawik-Wejman podkreśliła, że działalność takiej organizacji jak Google opiera się na zaufaniu użytkownika do usługodawcy. Użytkownik bowiem powierza swoje prywatne dane, a także informacje na swój temat. Dostawcy zależy na zapewnieniu jak najwyższych standardów bezpieczeństwa, aby użytkownik czuł się bezpiecznie. Agata Waclawik-Wejman wskazała, że Google przetwarza trzy rodzaje danych:

- 1) logi – dane logowania na temat wyszukiwania (zbierane na podstawie adresów IP, które identyfikują urządzenie);
- 2) dane, które przekazują zalogowani użytkownicy usługodawcy (dane te nie są ujawniane);
- 3) dane na temat funkcjonowania produktów (zbierane w celu poprawy usług).

Mariusz Grzesiuk (Grupa Onet) zgodził się co do zasady z panelistką. Swą wypowiedź zaczął od stwierdzenia, że wiedza jest dobra. Internet umożliwia zbieranie i przetwarzanie danych. Mitem jest twierdzenie, że informacje, które są przetwarzane powszechnie indywidualizuje się. Dane





są interesujące, ale nie takie, które indywidualizują każdego z osobna. Mec. Grzesiuk podkreślił także, że współcześnie każda organizacja przetwarza informacje natomiast problem dotyczy ich interpretacji. Mecenasek Grzesiuk podkreślił, że przedsiębiorcy, którzy mają miliardy użytkowników są zainteresowane grupami do których mają trafiać produkty. Mariusz Grzesiuk wskazał, że Internet to część infrastruktury technicznej takiej jak droga i o wiele większym problemem jest to w jaki sposób, przy obecnych regulacjach, zapobiegać monopolizacji rynku i dostępu do informacji, które znajdują się na tej drodze.

W tym kontekście wielkie

sieci reklamowe korzystając z danych cookies, które za pośrednictwem takich podmiotów jak np. Onet zbierają bardzo dużo informacji, które bezpośrednio nie dotyczą pojedynczych użytkowników, ale mogą „wypychać” z rynku mniejszych graczy. Zdaniem mecenasa Grzesiuka warto pochylić się nad prawem antymonopolowym. W toku dalszej dyskusji podkreślono, że sądownictwo polskie jest w trudnej sytuacji ze względu na niezrozumienie przez sędziów zagadnień występujących na styku prawa i technologii oraz sformułowane m.in. postulaty, że:

- a) Internet przenika do każdej dziedziny gospodarki a danymi osobowymi interesują się wszystkie branże.
- b) Powszechny system sądownictwa ma poważne trudności z dogonieniem tak szybko zmieniającej się dziedziny jednak tworzenie sądów specjalizacyjnych nie jest dobrą drogą;
- c) Reforma ochrony danych osobowych powinna odzwierciedlać gospodarkę ICT w każdym sektorze i nie być od niej oderwana;
- d) Największym wyzwaniem dla firm, prawników i regulatorów jest takie ułożenie ram by wyeksponować transparentne podmioty (dobrym rozwiązaniem jest samoregulacja);
- e) Świadomość użytkowników Internetu w zakresie bezpiecznego korzystania z sieci nie jest wysoka stąd trzeba ją podnosić.

## Prywatność w serwisach społecznościowych

Czwarty panel debaty został prowadzony przez Mirosława Maja. Moderator rozpoczął panel od przeprowadzenia bardzo ciekawego eksperymentu organizacji ENISA pod nazwą „kupuję bilet do kina”. Uczestnikom konferencji zostały przedstawione do wyboru dwa kina. Cena biletu do kina A była droższa o 2 zł niż w kinie B, ale klient kina A nie był obowiązany do podania nr telefonu. Pojawiło się wiele pytań i wątpliwości wśród uczestników debaty. Mirosław Maj porównał wyniki z sali z wynikami badania ENISA i wskazał, że świadomość użytkowników/obywateli w zakresie ochrony danych jest wysoka niemniej cena biletu do kina ma istotne znaczenie co do wyboru usługi. Prywatność ma zatem swoją cenę.



Grzegorz Wanio (Olesiński i Wspólnicy) nadmienił, że kiedy analizował jaki odsetek danych podawanych w serwisach internetowych jest prawdziwy w usługach poczty elektronicznej dane te były na poziomie 4-5%, w usługach płatnych odsetek podawania prawdziwych danych był jednak wysoki (dane te mają znaczenie dla funkcjonowania usługi). W dalszej części Mirosław Maj zadał pytanie czy dane klientów można sprzedawać. Mecenas Wanio podkreślił, że w serwisach społecznościowych wartość danych jest wysoka i dane te mają coraz większą jakość. Odwołując się do abstrakcyjnego przykładu panelista założył, że baza w praktyce może zostać opisana i sprzedana podmiotowi, który będzie od tej chwili administratorem tych danych. Maciej Kołodziej (nk.pl) potwierdził, że zbiory danych osobowych są w Polsce szeroko sprzedawane. Bazy społecznościowe są szczególnie atrakcyjne ze względów reklamy i marketingu. Sprzedanie danych osobowych w Polsce nie jest jednak legalnie możliwe w innym wypadku aniżeli takim, że użytkownik uprzednio wyrazi zgodę, że dane zostaną zbyte (udostępnianie) na rzecz podmiotu trzeciego (podmiot ten musi zostać wyraźnie określony). W innym wypadku zarówno podmiot sprzedający jak i kupujący naraża się na odpowiedzialność karną. Podkreślono, że problem sprzedaży bazy danych dotyczy w dużej mierze także startupów IT.

Jednym z tematów poruszanych w czasie tej części debaty był aspekt bezpieczeństwa dzieci oraz ich działalności w portalach społecznościowych. Maciej Kołodziej odpowiadając na pytanie Mirosława Maja czy dzieci mogą założyć konto na portalu społecznościowym zgodnie z zasadami polskiego prawa uznał, że tego typu umowa jest drobną bieżącą umową życia codziennego. Należałoby się jednak zastanowić nad pakietem uprawnień i usług dodatkowych w ramach danego serwisu. Aspektem, na który szczególnie zwrócił uwagę panelista było wadliwe wyrażenie zgody przez małoletniego na przetwarzanie jego danych w celach marketingowych w zamian za co otrzymuje on jakiś ekwiwalent. Mecenas Wanio odparł jednak, że świadomość dzieci jest bardzo wysoka, a przychody z mikropłatności,



które napędzają dzieci są znaczne i nie można tego ignorować. Dodał także, że dla samych dzieci serwisy społecznościowe jak i serwisy z grami dla nich dedykowanymi są rozrywką. Rozgorzała dyskusja na temat udzielania zgód przez przedstawicieli ustawowych bądź opiekunów prawnych co spowoduje efekt odwrotny od zamierzonego, gdyż dzieci będą zaznaczać odpowiednią granicę wiekową. Grzegorz Wanio podał także przykład portalu gdzie dzieci, nie nastolatki, odgrywały role dorosłych w Internecie i kreowały siebie na zupełnie inne postaci. Maciej Kołodziej podkreślił, że problem dotyczy przedsiębiorcy, a zgoda na przetwarzanie danych uzyskiwana od małoletnich będzie nieskuteczna stąd nie będzie przesłanki do wyświetlania np. reklam partnerów. Mecenas Wanio podkreślił jednak, że to rodzi problem tworzenia fałszywych tożsamości i weryfikowania danych. Stwierdzono, że zapłata za wyrażenie zgody na przetwarzanie danych w określonych celach jest dopuszczalna podobnie jak np. uniemożliwienie korzystania z danej usługi pod warunkiem, że nie jest to niezbędna usługa w ramach serwisu czy wręcz usług e- administracji.

Podsumowując debatę stwierdzono, że należy podnosić poziom edukacji użytkowników usług świadczonych drogą elektroniczną na temat ochrony danych osobowych, ochrony prywatności, bezpiecznego korzystania z Internetu, a także ilości udostępniania przez nich informacji w Internecie.

Osoby zainteresowane wsparciem i udziałem w kolejnych debatach, serdecznie zapraszamy do kontaktu z Fundacją Bezpiecznej Cyberprzestrzeń.



[www.cybsecurity.org](http://www.cybsecurity.org)

ul. Tytoniowa 20,  
04-228 Warszawa,  
tel.: +48 22 112 0 800,  
fax: +48 22 112 06 84