CyberPOLICY
NASK

Postawy Polaków wobec prywatności w internecie

– wywiad Moniki Stachoń
z dr. hab. Danielem Miderem
i mjr. rez. Pawłem Tomczykiem

Naruszenia prywatności danych użytkowników internetu stały się jednym z największych współczesnych wyzwań w zakresie cyberbezpieczeństwa. O postawie Polaków wobec prywatności w internecie rozmawiamy z autorem artykułu *Privacy on the Internet: An Empirical Study of Poles' Attitudes*, dr hab. Danielem Miderem, *a także* ekspertem w zakresie cyberbezpieczeństwa, mjr. rez. Pawłem Tomczykiem.

Dr hab. Daniel Mider – (d.mider@uw.edu.pl) wykładowca Uniwersytetu Warszawskiego, adiunkt na Wydziale Nauk Politycznych i Studiów Międzynarodowych, certyfikowany informatyk śledczy. Autor licznych publikacji z zakresu socjologii internetu, socjologii przemocy, białego wywiadu i cyberbezpieczeństwa.

Mjr rez. Paweł Tomczyk – (pawel@sekkura.com.pl) absolwent Wojskowej Akademii Technicznej i Akademii Sztabu Generalnego, wyższy oficer Wojska Polskiego (przeniesiony do rezerwy). Specjalista w zakresie ochrony informacji niejawnych, licencjonowany detektyw, wykładowca UO UW.

Monika Stachoń – specjalistka w obszarze cyberbezpieczeństwa w Zespole Analiz Strategicznych NASK-PIB. Szczególnie interesuje się szeroko pojmowanymi możliwościami wykorzystania cyberprzestrzeni w zakresie zapewnienia bezpieczeństwa państwa.

MS: Co możemy powiedzieć o poziomie świadomości Polaków na temat naruszeń ich prywatności w internecie?

DM: Świadomość Polaków na temat naruszeń prywatności w internecie ma charakter potoczny. Wiedza pochodzi zazwyczaj z przekazów medialnych oraz codziennych, incydentalnych kontaktów międzyludzkich. Jako taka nie jest ani pełna, ani systematyczna, ani – co najważniejsze – poprawna. Zaledwie jeden na dziesięciu Polaków odczuwszy taką potrzebę samodzielnie podjął szkolenie lub kurs z zakresu metod i technik ochrony swoich danych w internecie. Nieco lepiej sytuacja wygląda na gruncie szkolenia zinstytucjonalizowanego formalnego i nieformalnego. Odpowiednio, w szkole lub w pracy, jeden na pięciu badanych skorzystał z tej wiedzy. Mniej niż 15 proc. Polaków potrafi właściwie odpowiedzieć na pytanie, co takiego ujawnił Edward Snowden lub co było istotą skandalu Cambridge Analytica i jaką rolę miał w tym Facebook. Dodam, iż Polacy mają niewygórowane potrzeby uzupełniania tej wiedzy. W badaniu przeprowadzonym w październiku 2022 roku aż trzech na czterech Polaków zadeklarowało brak zainteresowania uczestnictwem w szkoleniu z szeroko pojętego cyberbezpieczeństwa (badanie przeprowadzono na reprezentatywnej próbie dorosłych Polaków; *niniejsza deklaracja odnosi się do pozostałych badań cytowanych przez mjra Tomczyka oraz przeze mnie w tym tekście).*

Świadomość zagrożeń prywatności Polaków oceniam jako słabą, a w środowisku akademickim niedocenianą jako obiekt badań. Trudno o to w promowanej przez media społecznościowe kulturze ekshibicjonizmu społecznego (pojęcie to – jakże trafnie charakteryzujące współczesność – wprowadziły dwie badaczki z Uniwersytetu Śląskiego, Katarzyna Borzucka-Sitkiewicz i Karina Leksy).

MS: W jaki sposób możemy dowiedzieć się, co dzieje się z informacjami o nas zamieszczonymi w internecie, a zwłaszcza z danymi, które wyciekły?

PT: Na to pytanie brak jednoznacznej odpowiedzi. Większość Polaków nie zdaje sobie sprawy z tego, jak wiele informacji na nasz temat można znaleźć w internecie i jak są one dokładne. Najłatwiej wskazać, jakie dane wpadły w ręce cyberprzestępców. Istnieje ogólnie dostępny darmowy i zaufany projekt australijskiego programisty, dyrektora Microsoftu, Troy'a Hunta. Na stronie tej agregowane są globalnie wycieki danych i w prosty sposób przez podanie swojego adresu e-mail, nazwiska, nickname'a lub numeru telefonu możemy sprawdzić, czy dane zostały skradzione, a także w jakim zakresie i kiedy. Strona znajduje się pod adresem https://haveibeenpwned.com/, ma charakter globalny i zawiera obecnie informacje o ponad 12 miliardach zhakowanych kont internautów do różnego rodzaju serwisów. Jednak wiedza stąd pochodząca będzie cząstkowa.

Nasze cyfrowe alter ego, a więc komplet informacji o danej osobie figurujący w rozmaitych zakątkach internetu jest możliwe do zrekonstruowania tylko przez specjalistę. Możemy w tej sprawie zwrócić się do infobrokerów, specjalistów białego wywiadu, detektywów, wywiadowców gospodarczych. Każdy z wymienionych podmiotów zapewnia odrębny co do zakresu i treści typ usługi informacyjnej.

MS: Dlaczego o wyciekach danych tak rzadko mówi się publicznie?

PT: Cyfrowe dane stały się ropą naftową XXI wieku. Często są przedmiotem gry wywiadów politycznych i gospodarczych, a także organizacji przestępczych całego świata. Zdarza się, że sam fakt wycieku danych pozostaje nieujawniony w ogóle lub ujawniony po upływie długiego czasu. Wycieki ujawnione, mogące stać się obiektem analizy wykwalifikowanego użytkownika internetu bardzo często przeszły długą drogę. W pierwszej kolejności skorzystały z nich organizacje wywiadowcze lub cyberprzestępcy, dopiero wtórnie informacje takie, dla stworzenia swoistego „szumu", zatarcia śladów, umieszczono w szarej strefie do użytku ogólnego.

MS: Jak ocenia Pan wiedzę Polaków na temat możliwości ochrony prywatności w internecie?

DM: Zainspirowany zachodnimi badaniami świadomości bezpieczeństwa informacji podjąłem to zagadnienie w czerwcu 2021 roku. Oceniam, że sytuacja nie zmieniła się istotnie od tego czasu. Na podstawie przeprowadzonych badań wyodrębniłem wówczas trzy grupy Polaków: Newbies – zdecydowanie niedoświadczonych w sferze ochrony informacji, Normcores – umiarkowanych w tym aspekcie, Geeks – stosunkowo biegłych w sztuce niwelacji omawianych zagrożeń. Pewna

frywolność związana z nazewnictwem miała charakter zamierzony, lecz żadnego z tych określeń nie uznaję za pejoratywne. Sytuację w zakresie świadomości cyberzagrożeń, a także wiedzy, kompetencji, umiejętności i podejmowanych działań zapobiegawczych w społeczeństwie polskim należy uznać za daleką od zadowalającej. Blisko jedną trzecią populacji (30,4%) dorosłych w Polsce stanowią osoby, które nie opanowały nawet rudymentów zachowania bezpieczeństwa podczas korzystania z komputera i internetu (Newbies). Z kolei Normcores (22,7%) charakteryzują się niską wiedzą, lecz stosunkowo wysoką dozą zdrowego rozsądku we wdrażaniu rozwiązań zapewniających ochronę informacji. Podejmują oni działania niewymagające kompetencji informatycznych. Są to jednak wciąż działania niewystarczające, mające możliwość zapobiegania co najwyżej typowym atakom. Blisko połowa dorosłych (46,9%) Polaków określonych jako Geeks wdraża środki bezpieczeństwa o charakterze zaawansowanym. Jednakże tak znaczny udział zaawansowanych użytkowników jest złudnym świadectwem wysokiego poziomu „higieny informatycznej" polskich użytkowników internetu. Grupa ta – niestety – jest heterogeniczna, w tym sensie, że środki zabezpieczające stosuje wybiórczo i niekonsekwentnie, a więc ich świadomość cyberzagrożeń jest nieciągła i fragmentaryczna, przez co niewystarczająca.

Odnośnie do poziomu wiedzy prawnej Polaków w tym zakresie niestety nie mogę się wypowiadać, bowiem przedmiotem moich badań są elementy afektywne (stosunek do prawa), nie zaś kognitywne (wiedza o nim). Uznaję, że warto ten aspekt w przyszłości zgłębić.

MS: Co możemy zrobić, żeby ta wiedza była większa?

PT: Przede wszystkim należy uświadamiać użytkowników internetu na temat zagrożeń, wskazywać metody ich neutralizacji, a następnie edukować w zakresie tych metod. Pierwsze dwa cele mogą być realizowane w toku rozmaitych kampanii reklamy społecznej. Edukacja natomiast powinna mieć charakter formalny na wszystkich szczeblach, jak i również nieformalny w postaci rozmaitych kursów. Rodzi się tu jednak pewien problem. Otóż zapoznawszy się z najnowszym raportem PARP[1] na temat branży telekomunikacyjnej i cyberbezpieczeństwa poweźmiemy przekonanie, że ze względu na dramatyczny niedobór specjalistów z zakresu cyberbezpieczeństwa w najbliższych latach... nie będzie komu szkolić Polaków.

MS: W podsumowaniu badania, którego wyniki opublikowane zostały w artykule *Privacy on the internet: An Empirical Study of Poles' Attitudes* stwierdzono, że Polacy stosują nieskuteczne środki ochrony swojej prywatności w internecie. Jakie są w takim razie skuteczne środki?

PT: Istnieje wiele takich środków, pracowicie tworzonych od czasów powstania ponad trzy dekady temu kalifornijskich Cypherpunks, z którymi współpracował też twórca WikiLeaks Julian Assange. W toku refleksji własnej, wdrażanej następnie w działaniach edukacyjnych, wyróżniliśmy trzy obszary ochrony prywatności: wetware, software i hardware. Nieprzypadkowo te trzy terminy wymieniłem w tej kolejności.

Wetware to obszar działań ludzkich (nieco żartobliwie, po Lemowsku sformułowane, by słowo to pasowało do dwóch pozostałych z triady). To właśnie niedostateczna lub błędna ocena sytuacji przez jednostkę prowadzi najczęściej do zagrożeń bezpieczeństwa informatycznego i informacyjnego. Warto w tym miejscu przywołać podtytuł książki, której współautorem jest jeden z najsłynniejszych hakerów ostatniego dziesięcioletnia XX wieku – Kevin Mitnick. Podtytuł ów brzmi: Łamałem ludzi, nie hasła. A zatem to człowiek stanowi najsłabsze ogniwo łańcucha cyberbezpieczeństwa. Jesteśmy przekonani, że człowiek może pozostawać bezpieczny w cyberprzestrzeni, nawet jeśli nie posiada ponadpodstawowych kompetencji informatycznych. Konsekwentne wdrożenie odpowiedniej polityki informacyjnej i procedur użytkowania sprzętu komputerowego w sposób istotny ogranicza powierzchnię potencjalnego ataku lub nawet go uniemożliwia.

Drugim obszarem ochrony prywatności (czy szerzej – bezpieczeństwa) jest software, czyli oprogramowanie. Jest to szeroka kategoria rozciągająca się od systemów operacyjnych szanujących lub nawet strzegących prywatności użytkownika (tu można polecić choćby takie jak: QubesOS, Whonix, Tails, czy odpowiednio skonfigurowane odmiany BSD

1 J. Wróblewski, K. Kuźma, D. Mider, A. Kargul, W. Terlikowski, Branżowy Bilans Kapitału Ludzkiego II – branża telekomunikacji i cyberbezpieczeństwa, PARP, Warszawa 2022.

lub zwykłe dystrybucje GNU/Linux, w szczególności „debianopochodne"), aż do oprogramowania zestawiającego bezpieczne połączenia komunikacyjne (od powszechnie znanego Signal do np. Briar). Warto także wspomnieć o sieciach zapewniających prywatność, a w efekcie bezpieczeństwo. Większość internautów słyszała o Tor (choć zapewne będzie to wiedza powierzchowna i zaburzona). Jednak większe bezpieczeństwo zapewnia choćby Invisible Internet Project lub Lokinet.

Ostatni ze składników – hardware – dotyczy bezpiecznego sprzętu komputerowego, od komputerów, których używamy do ruterów, które stanowią „bramę do internetu". Krótko tylko wskażę, że niezależnie od zabezpieczeń na poziomach wyższych, poniesiemy porażkę, jeśli skorzystamy z urządzeń posiadających tzw. „hardware backdoors".

Dodajmy, że problem stanowi negatywna zależność pomiędzy wygodą użytkowania a zachowaną prywatnością i bezpieczeństwem. Im wyższy poziom prywatności, tym używane oprogramowanie wymaga poświęcenia więcej czasu i uwagi oraz nabycia większej wiedzy. Nie jest rzeczą prostą odnalezienie równowagi, szczególnie, że żyjemy w społeczeństwie, gdzie odraczanie gratyfikacji nie stanowi wartości.

Wyniki badań wskazują na luki Polaków – nawet tych najbardziej zaawansowanych informatycznie – w zakresie „know why". Przeciętny użytkownik komputera uważa, że wystarczy firewall oraz program antywirusowy. Jak wspomniałem wcześniej, są to środki niewystarczające (Łamałem ludzi nie hasła). Takie postępowanie daje więc złudne poczucie bezpieczeństwa i prowadzi do zaniechania innych działań. Ponadto większość użytkowników dla wygody lub z powodu braku świadomości używa jedynego słusznego systemu operacyjnego, zamiast wspomnianych już przeze mnie systemów z rodziny GNU/Linux. I nie chodzi tu o to, że GNU/Linux jest super bezpiecznym, pozbawionym luk systemem, takich nie ma. Jednak, luki bezpieczeństwa w systemach Linux są „łatane" natychmiast po wykryciu, ponadto, jeśli na 100% – 95% ma rozpoznane luki i wady łatwiej i bardziej opłacalnie jest przygotowanie ataku na te właśnie 95%.

A zatem brakuje świadomości o charakterze strategicznym. Rekomendowałbym w tym zakresie, co już nadmieniałem, budzenie świadomości, a w konsekwencji edukację.

MS: W artykule zwraca Pan uwagę, że występuje silna polaryzacja postaw Polaków wobec obowiązku ujawniania tożsamości w internecie, a także zapewniania dostępu do wszelkich informacji o użytkownikach przez organy ścigania. Z czego ona wynika? Czy są jakieś dominujące czynniki, który wpływają na stosunek do ujawniania tożsamości w internecie?

DM: Pewne czynniki dają się wyodrębnić, jednak ze względu na ograniczenia finansowe i organizacyjne zbadano głównie kategorie socjodemograficzne. Wymienię te, które okazały się istotne statystycznie. Należy jednak zaznaczyć, że odnotowane współzmienności są umiarkowanie silne. Istotnym czynnikiem wydaje się wiek: średnie pokolenie skłonne jest w nieco większym stopniu ukrywać swoją tożsamość w internecie niż należący do pozostałych kategorii wiekowych. Pojęcie pokolenia definiuję w kategoriach klasycznych, durkheimowskich: młode pokolenie to 18-35 lat, średnie powyżej 35 do 65 roku życia i starsze – powyżej 65 roku życia. Wykształcenie (szczególnie techniczne) pozytywnie koreluje z chęcią anonimizacji. Ponadto zwolennikami ukrywania tożsamości w internecie są osoby wyrażające postawy radykalne wobec nadużyć władzy, twierdzące że należy na takowe odpowiadać działaniami z użyciem przemocy. To niewiele wskazówek, natomiast jest to wiedza pewna, ugruntowana empirycznie. W dalszych badaniach zweryfikujemy czynniki o charakterze psychograficznym, w tym tak zwanego stylu życia, tworząc wielowymiarowe profile postaw internautów.

MS: Czy sami chcemy chronić swoją prywatność w internecie, czy też oczekujemy ochrony w tym zakresie od podmiotów takich jak państwo czy korporacje?

DM: Polacy są w tym zakresie zróżnicowani. Badanie przeprowadzone przez Stowarzyszenie Absolwentów Nauk Politycznych w 2021 roku pozwoliło na dostrzeżenie największej z grup oczekującej ochrony, w której przeważają kobiety, osoby powyżej 55 roku życia, mieszkańcy wsi i małych miast, posiadający na ogół wykształcenie średnie. Grupa ta stanowi około 2/3 wszystkich badanych. Pozostałe dwie grupy, określone przeze mnie jako cyberlibertarianie pozostają stosunkowo sceptyczne wobec pierwszego sektora jako czynnika ochrony (w większym stopniu) oraz drugiego sektora (w nieco mniejszym stopniu).

MS: Czy uważa Pan, że obecnie obowiązujące prawo w wystarczający sposób chroni naszą prywatność w internecie?

DM: „Nienadążanie" prawa za nowymi zjawiskami, w szczególności technologicznymi ma charakter immanentny we wszystkich współczesnych systemach politycznych. Nieodmiennie, kolejnym etapem cyklu rozwojowego, gdy zagrożenie rozpoznano, jest „nadregulacja" (francuska socjologia ukuła na określenie tego zjawiska ciekawy termin: „krzyk zagubionych w przepisach", przy czym krzyczącymi – bezradnie na ogół – są obywatele). Owa „nadregulacja" dusi zarówno działania negatywne, jak i utrudnia, bądź uniemożliwia te pozytywne. Trzecim, nie zawsze następującym, lecz pożądanym etapem, jest normalizacja, a więc uzyskanie równowagi pomiędzy bezpieczeństwem i wolnością.

W chwili obecnej warto przygotowywać już przedpole ochrony prawnej w przestrzeni metawersów i podejmować refleksję nad konsekwencjami prawnymi działania sztucznych inteligencji oraz wdrażania projektów Web3.

MS: W 2011 roku do Kodeksu Karnego został dodany art. 190a § 2, który penalizuje kradzież tożsamości. Pod koniec ubiegłego roku na stronach Rządowego Procesu Legislacyjnego opublikowano projekt ustawy o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości. Jak odnosi się Pan do tej propozycji? Co może zmienić ustawa dla nas, jako użytkowników internetu?

DM: Częściowa ochrona tych wartości funkcjonowała już na podstawie artykułu 105 prawa bankowego, a także można było skorzystać na zasadach komercyjnych z pomocy biur informacji gospodarczej. Usługa miała jednak przede wszystkim walor informacyjny i działała *post factum*. Obecny projekt to nowa jakość, przewiduje bowiem zdjęcie odium odpowiedzialności ofiary za zaciągnięte w jej imieniu zobowiązania finansowe, prawne lub związane z obrotem nieruchomościami. Przewiduje ponadto szybkość i skuteczność działania kanałów realizacji procedur ochrony. Proponowane rozwiązania w takim kształcie i zakresie wydają się niezbędne w obecnej sytuacji. Regulacja ta wpisuje się w oczekiwania Polaków odnośnie do ochrony przed przestępczością. W prowadzonym przeze mnie empirycznym rankingu obaw Polaków przed przestępczością (Fear of Crime Index) kategoria „wyłudzenie danych, w tym kradzież tożsamości" znajduje się nieodmiennie na pierwszym miejscu od kilkunastu miesięcy. Ponad jedna trzecia Polaków obawia się kradzieży tożsamości bardzo, a kolejna jedna trzecia zgłasza umiarkowane obawy. Lęk przed tym przestępstwem istotnie wyprzedza pozostałe typy przestępstw, w tym oszustwa, kradzieże, włamania i naruszenia miru domowego, które również stanowią przedmiot obaw społecznych.

MS: Jakie znaczenie ma proponowana ustawa o zapobieganiu kradzieży tożsamości w kontekście możliwości podszycia się pod daną osobę?

PT: Nie ulega wątpliwości, że regulacja jest konieczna, zastępując akt nieprzystający do współczesnego krajobrazu prawnego. Przede wszystkim zapobiega ona *post factum* odpowiedzialności finansowej i majątkowej wszystkich, którzy zawierają umowy. Co do ochrony *ex ante* możliwości kradzieży tożsamości, to ustawa uniemożliwia takie działania poprzez wprowadzenie procedury zastrzeżenia numeru PESEL.

MS: Obecnie trwają prace nad przyjęciem ustawy Prawo Komunikacji Elektronicznej, która wzbudza sporo emocji. Szczególnie kontrowersyjny dla wielu ekspertów jest art. 43, w którym zobowiązuje się przedsiębiorców komunikacji elektronicznej do zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania przez służby „komunikatów elektronicznych przesyłanych w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej" oraz wielu danych abonentów związanych z tymi komunikatami, m.in. numeru i danych lokalizacyjnych. Jak ocenia Pan proponowane rozwiązania prawne?

DM: Po pierwsze, „Prawo komunikacji elektronicznej" zastępuje „Prawo telekomunikacyjne" – akt prawny liczący niemal dwie dekady i przez to nieprzystający do współczesności technologicznej. Po wtóre, nie jest to uregulowanie autonomiczne, lecz wdrożenie europejskiego kodeksu łączności elektronicznej. Po trzecie, regulacje tego typu mają charakter globalny, wpisując się w ogólny trend, który nazwać można suwerenizacją in-

ternetu, rozumianą jako przejmowanie przez podmioty państwowe kontroli nad „narodową" cyberprzestrzenią. Trend ów ilościowo wyraża się wskaźnikiem Wolności internetu Freedom House. Ilościowe reprezentacje obniżania tego wskaźnika obserwujemy od dekady. W takiej oto deterministycznej sytuacji moja opinia nie będzie niczym więcej, niż wyrażeniem emocji.

Co do potencjalnych skutków, to wskazane regulacje prawne obciążają przedsiębiorców pod względem finansowym i organizacyjnym. Nie zetknąłem się jeszcze z taką analizą, ale jako że sam jestem przedsiębiorcą, przyznaję, że może to rodzić negatywne skutki o charakterze gospodarczym, choć raczej dla pojedynczych podmiotów lub co najwyżej poszczególnych segmentów w branżach. W mojej ocenie problem jest inny: tworzenie przez podmioty drugiego sektora zbiorów danych, konieczność długotrwałego ich przechowywania i udostępniania na żądanie stwarza pokusy, a więc ryzyko ich kradzieży. Będzie to cel podmiotów takich jak obce służby specjalne oraz grupy przestępcze.

Zainteresowany internauta znajdzie powszechnie dostępną zbiorczą bazę wycieków liczącą ponad 23 miliardy (sic!) kont, haseł, telefonów osób fizycznych i prawnych z całego świata. Bazę dostępną, z przyjaznym interfejsem, z abonamentem za kilka dolarów. A zatem, jak poucza doświadczenie, nie powinno być przedmiotem rozważań i obaw „czy", lecz „kiedy" dane te wyciekną.

W ramach badania odpowiada Pan na pytanie dotyczące stosunku społeczeństwa do dostępu służb do dostępu do informacji o użytkownikach sieci, nawet w ważnych przypadkach. Zauważona została duża polaryzacja w tym względzie (47% respondentów udzieliło negatywnej odpowiedzi i tyle samo pozytywnej). Jaki wpływ mogą mieć nowe regulacje prawne zachowania Polaków w internecie i ich stosunek do władz?

DM: Biorąc pod uwagę przeszłe doświadczenia reakcji społecznych na kontrowersyjne regulacje, nie oczekuję gwałtownych wyrazów sprzeciwu. Na podstawie prowadzonych przeze mnie innych wieloletnich badań empirycznych, jak również wyżej przytoczonych pomiarów, stawiam hipotezę o możliwości pojawienia się w niektórych grupach społecznych postaw antysystemowych. Niewątpliwie zabrzmiało to niepokojąco, zatem spieszę wyjaśnić. Otóż postawy antysystemowe Polaków, jeśli wystąpią, to bardziej będą one lokować się w obszarze tzw. innowacyjności, niż innych groźniejszych formach bezprawnego sprzeciwu. Przez innowacyjność w teorii anomii rozumie się poszukiwanie przez zainteresowanych rozmaitych luk i możliwości ominięcia niekorzystnego i niechcianego prawa. W reprezentatywnych ogólnopolskich badaniach odsetek osób deklarujących gotowość podjęcia działań innowacyjnych oscyluje w ciągu ostatnich dwóch lat w granicach 8-15 procent dorosłej populacji. Ludzi tych w większym stopniu łączą cechy psychograficzne, niż socjograficzne, choć i te ostatnie mają pewne znaczenie.

Liczne możliwości komunikowania się bez ujawniania danych i tworzenia metadanych istnieją. Są one dynamicznie rozwijane od trzech dekad w działaniach ruchu społecznego technologii wspierających prywatność (Privacy Enhancing Technologies, PET). Narzędzia PET utrudniają lub uniemożliwiają identyfikację użytkownika procesu komunikacji, a także rejestrowanie, zbieranie i kontrolę przesyłanych danych. Wniosek odnośnie zagrożeń i szans wynikających z powstania w polskim społeczeństwie grup biegłych w technikach anonimizacji i ukrywaniu swojej tożsamości w internecie pozostawiam Czytelnikom.

Bardzo dziękuję za rozmowę.