PŁATNOŚCI NATYCHMIASTOWE MAJĄ BYĆ POWSZECHNE I TANIE

PRZELEW TYLKO W 10 SEKUND

Parlament Europejski przyjął nowe przepisy dotyczące tzw. przelewów natychmiastowych w Unii Europejskiej. Dzięki temu klienci i firmy dostaną swoje pieniądze w ciągu 10 sekund od dokonania przelewu. Przepisy zostały przyjęte przeważającą większością głosów. Na razie dotyczą tylko płatności w euro.

Przelewy natychmiastowe (np. Express Eliksir, BlueCash) nie są w Polsce nowością. Wiele banków oferuje je także dzisiaj. Tego typu przelewy są jednak drogie, a każdy bank ustala swoją cenę. To idealne wyjście, gdy spóźniamy się z ratą kredytu albo w ostatniej chwili spłacamy kartę kredytową czy regulowali zaległy rachunek. Gdybyśmy jednak płacili np. 5 zł za każdy przelew, to szybko przestałoby się nam to opłacać. A jeśli w dodatku wysyłamy przelew w euro, do banku za granicą to pieniądze mogą iść nawet 3 dni. Zaś opłata za taki przelew bywa dość wysoka, bo oprócz opłaty pobierana jest także prowizja. W innych krajach europejskich działa to podobnie. Dlatego Komisja Europejska złożyła do Parlamentu Europejskiego wniosek, który został właśnie rozpatrzony.

Niezależnie od dnia i godziny

Parlament Europejski przyjął przepisy, na mocy których natychmiastowe polecenie przelewu ma być wykonywane niezależnie od dnia i godziny, a pieniądze muszą dotrzeć na konto odbiorcy w ciągu dziesięciu sekund. Płatnik musi też dostać informację (także w ciągu 10 sekund), że pieniądze dotarły na konto odbiorcy.

Przepisy dotyczą Strefy Euro, ale państwa członkowskie, których walutą nie jest euro (np. Polska), będą również musiały stosować zasady, w przypadku rachunków oferujących już regularne transakcje w euro. Otrzymają jednak dłuższy czas na przystosowanie systemów bankowych -przepisy mają wejść w życie w Strefie Euro do końca 2024 r., a w pozostałych państwach Unii Europejskiej kilka miesięcy później. Będzie też istniało specjalne odstępstwo od zasady dziesięciu sekund dla przelewów dokonywanych poza godzinami pracy banków. Chodzi o obawy o dostęp do płynności w euro.

Oczekiwana zmiana

To prawdziwa rewolucja w płatnościach! Do tej pory przelewy potrafiły iść dwa, a nawet trzy dni. Prywatne osoby i firmy długo czekały więc na swoje pieniądze, które były przetrzymywane w bankowych systemach. Komisja Europejska szacuje, że każdego dnia w europejskim systemie finansowym około 200 mld euro jest przetrzymywanych w drodze do odbiorców przelewu! Banki zarabiają, a dla firm, zwłaszcza tych najmniejszych, jest to ogromny problem, a niekiedy nawet katastrofa.

– Rozporządzenie w sprawie płatności natychmiastowych oznacza długo oczekiwaną modernizację płatności w ramach jednolitego rynku europejskiego. Pożegnajmy się z niedogodnościami związanymi z oczekiwaniem na dostęp do środków przez dwa lub trzy dni robocze. Dostarczamy coś, na czym naprawdę zależy ludziom i firmom: przelewanie pieniędzy w ciągu 10 sekund o każdej porze dnia – powiedział po głosowaniu poseł sprawozdawca Michiel Hoogeveen z frakcji Europejscy Konserwatyści i Reformatorzy.

Ceny muszą spaść!

Banki i firmy pośredniczące np. w przelewach międzynarodowych nie będą mogły pobierać opłat dodatkowych za przyspieszenie przelewu. Słowem: przelew natychmiastowy i zwykły Maja kosztować tyle samo! Dostawca usług płatniczych powinien niezwłocznie wymienić kwotę transakcji na euro, jeżeli płatność następuje z rachunku, który nie jest prowadzony w euro

Większe bezpieczeństwo

Aby zagwarantować bezpieczeństwo, dostawcy usług płatniczych muszą mieć solidne i aktualne mechanizmy wykrywania oszustw i zapobiegania im. Wszystko po to, by uniknąć sytuacji, w której przelew trafi na niewłaściwy rachunek z powodu oszustwa lub błędu. Muszą więc - niezwłocznie i bez żadnych dodatkowych opłat -świadczyć usługę weryfikacji tożsamości odbiorcy. Chodzi o sprawdzenie, czy tzw. numer IBAN i nazwa odbiorcy są prawidłowe. Czym jest numer IBAN? W Polsce składa się z 28 znaków – 2 liter z przodu (PL) i 26 cyfr (numeru rachunku).

Ten wymóg bezpieczeństwa będzie dotyczył także przelewów regularnych.

Bank musi też nam umożliwić, jako dodatkową ochronę przed oszustami, ustalenie maksymalnej kwoty przelewy. Tę kwotę będziemy mogli w każdej chwili zmodyfikować. Jeśli bank czy firma finansowa nie wywiąże się z tych obowiązków, a klient straci pieniądze, to będzie mógł zażądać od banku odszkodowania.

3 ciekawostki o płatnościach

RZADKA USŁUGA

Na początku 2022 r. zaledwie 11 proc. wszystkich przelewów bankowych w euro w Unii Europejskiej zostało zrealizowanych w ciągu kilku sekund. Tymczasem takie płatności istnieją od lat w wielu innych krajach np. w Indiach, Australii i Meksyku.

POLACY NIE LUBIĄ GOTÓWKI

Polska jest jednym z liderów płatności elektronicznych wśród 13 państw Unii Europejskiej - wynika z badania „Postawy wobec form płatności", przeprowadzonego przez firmę eService. Objęło ono 13 państw europejskich: Polskę, Czechy, Słowację, Węgry, Rumunię, Chorwację, Bułgarię, Słowenię, Niemcy, Irlandię, Wielką Brytanię, Hiszpanię i Portugalię. Partnerem badania w regionie Europy Środkowo-Wschodniej była Visa. Z badania wynika, że 55 proc. osób biorących udział w badaniu woli elektroniczne metody płatności (kartą, telefonem, zegarkiem lub innym urządzeniem) od dla płatności gotówką podczas tradycyjnych zakupów. 37 proc. kupujących jest jednak za starym systemem płacenia. Najbardziej płatności elektroniczne cenią sobie Brytyjczycy – 71 proc. mieszkańców Wysp woli płatności elektroniczne. W Irlandii to 63 proc. Polska zajmuje 3. miejsce na podium – 62 proc. Polaków nie chce płacić gotówką.

MAMY TAKŻE BLIK

W Polsce mamy także unikalną usługę płatności natychmiastowych BLIK. To jednorazowy, 6-cyfrowy kod, który otrzymujemy za pośrednictwem aplikacji banku. Kodu używamy do płatności – m.in. wypłacania pieniędzy z bankomatu, płacenia za zakupy, przesyłania pieniędzy na numer telefonu czy płacenia za zakupy w Internecie.

Parlament Europejski

Projekt współfinansowany przez Unię Europejską w ramach programu dotacji Parlamentu Europejskiego w dziedzinie komunikacji. Parlament Europejski nie uczestniczył w przygotowaniu materiałów; podane informacje nie są dla niego wiążące i nie ponosi on żadnej odpowiedzialności za informacje i stanowiska wyrażone w ramach projektu, za które zgodnie z mającymi zastosowanie przepisami odpowiedzialni są wyłącznie autorzy, osoby udzielające wywiadów, wydawcy lub nadawcy programu. Parlament Europejski nie może być również pociągany do odpowiedzialności za pośrednie lub bezpośrednie szkody mogące wynikać z realizacji projektu.

foto SHUTTERSTOCK

TWÓJ GŁOS SIĘ LICZY

Będziemy lepiej chronieni w internecie

BEZPIECZNI w świecie cyfrowym

Dzisiaj żyjemy w dwóch rzeczywistościach. Jedną jest ta prawdziwa, realna, drugą zaś rzeczywistość cyfrowa. Za pośrednictwem internetu kontaktujemy się ze sobą, spotykamy w mediach społecznościowych, pracujemy, oglądamy filmy czy robimy zakupy. Okazuje się jednak, że w świecie cyfrowym czyha na nas nie mniej złodziei i zwyczajnych bandytów niż w tym realnym. Dlatego Parlament Europejski tworzy przepisy, które mają nas przed cyberprzestępcami chronić.

Cyberprzestępcy są groźni dla każdego użytkownika internetu – dla osoby prywatnej, która korzysta tylko ze swojego smartfonu czy laptopa, ale także dla firm, wielkich koncernów czy instytucji, a nawet całych państw.

Komuś może się wydawać, że jeśli nie korzysta z internetu, nie ma smartfona czy bankowości elektronicznej, to nic mu nie grozi. Nic bardziej mylnego! A jeśli halerzy zaatakują ZUS i jego systemy? Miliony ludzi nie dostaną na czas emerytur i rent! Dlatego bezpieczeństwo cyfrowe jest tak bardzo ważne.

Liczba przestępstw w sieci rośnie

W 2022 r. na świecie było trzy razy więcej cyberataków niż rok wcześniej. Ataki za pomocą oprogramowania wymuszającego okup mają miejsce średnio co 11 sekund i powodują straty szacowane na 20 mld euro rocznie! W Polsce każdego miesiąca średnio 1000 firm pada ofiarą hakerów.

Przestępstwom nie zapobiegniemy, ale można przestępcom utrudnić życie. W domu montujemy dobre zamki i antywłamaniowe drzwi. W podobny sposób trzeba zabezpieczyć sprzęt elektroniczny np. laptopy, tablety, komputery czy smartfony oraz oprogramowanie do nich czy aplikacje. Tak, by było trudniej się do nas włamać, śledzić nas, podglądać, buszować i szkodzić w naszej domowej sieci wi-fi. Jednak dziś przed cyberatakami chronią nas głównie programy antywirusowe i standardowe zabezpieczenia np. dostęp po wprowadzeniu hasła. Parlament Europejski uznał, że to zdecydowanie za mało.

Prawo o odporności

Parlament Europejski i Rada Europejska (składa się z szefów rządów państw członkowskich) zawarły porozumienie w kwestii europejskiego aktu dotyczącego cyberodporności – Cyber Resilience Act. To pierwsze i przełomowe tego typu prawo na świecie. Ma ono poprawić poziom cyberbezpieczeństwa produktów cyfrowych z korzyścią dla konsumentów i przedsiębiorstw w całej Unii. Teraz zarówno Parlament jak i Rada muszą to porozumienie formalnie zatwierdzić, a potem wejdzie ono w życie.

Producenci będą mieli prawny obowiązek dbania o bezpieczeństwo użytkowników. Wymogi obejmą wszystkie typy sprzętu i oprogramowania, od elektronicznych niań, smartwatchów i gier komputerowych po bardzo skomplikowane zapory sieciowe i routery. Sprzęt komputerowy i oprogramowanie będą nosiły specjalne oznakowanie CE, wskazujące, że są zgodne z wymaganiami zawartymi w akcie o cyberodporności. Tylko wtedy będzie je można sprzedawać w Unii Europejskiej.

Akt nałoży na producentów oprogramowania obowiązek prawny dostarczania nam aktualizacji zabezpieczeń jeszcze przez kilka lat po zakupie. Producenci będą też musieli w przejrzysty sposób informować nas o bezpieczeństwie swoich produktów i ponosić za nie odpowiedzialność.

JAK SIĘ BRONIĆ

- **stosujmy programy antywirusowe i systematycznie je aktualizujmy,**
- **nigdy nie podawajmy swoich danych – każdy, kto zadzwoni do nas i domaga się podania danych, np. kodów BLIK lub loginu i hasła do logowania do konta, czy numeru karty kredytowej, to stuprocentowy oszust!**
- **nie instalujmy żadnego oprogramowania ani aplikacji – cyberprzestępca może próbować nakłonić nas do np. zainstalowania oprogramowania, które ma nas chronić przed oszustwami i włamaniami. W rzeczywistości umożliwia mu ono dostęp do naszego komputera czy telefonu. Będzie wykradać dane albo śledzić wszystko to, co wpisujemy na klawiaturze – w tym hasła dostępowe do naszego konta. Gdy już uzyska dane, wyczyści nam konto z oszczędności,**
- **uważajmy na linki i załączniki w mailach, wiadomościach w mediach społecznościowych sms-ach itp. – warto dokładnie sprawdzić, kto jest ich nadawcą. Przestępcy mogą podszywać się pod naszych znajomych, bank, ubezpieczyciela. Fałszywy link czy załącznik kieruje nas na podstawioną stronę albo ściąga na nasz sprzęt złośliwe oprogramowanie.**

RODZAJE CYBERATAKÓW

-= DDoS =- czyli blokowanie przez sztuczny tłok

Polega na przeprowadzeniu ataku jednocześnie z wielu miejsc (z wielu komputerów czy smartfonów). Atak taki przeprowadzany jest głównie z komputerów, nad którymi przejęta została kontrola przy użyciu wirusów komputerowych. Oznacza to, że właściciele tych komputerów mogą nawet nie wiedzieć, że ich komputer czy smartfon może być właśnie wykorzystywany do ataku! Tak ogromna liczba fałszywych prób skorzystania z usług danej firmy np. wejście na jej stronę internetową czy do sklepu internetowego całkowicie blokują system. Po co? Na przykład by wymusić okup.

-= PHISHING =- czyli podszywanie

Tu chodzi o kradzież danych. Przestępcy podszywają się pod instytucje, naszych bliskich, w firmie pod kolegów z innego działu, klientów itp. Stosują najbardziej wyrafinowane konstrukcje psychologiczne. Stąd nierzadko słyszymy o wycieku danych np. z przychodni czy ostatnio z firmy wykonującej badania diagnostyczne. My też dajemy się zwieść obietnicy okazji zakupowej na nieznanej stronie, otwieramy załączniki czy instalujemy oprogramowanie, do czego namawia nas przestępca podający się np. za pracownika banku. Po co? Przestępcy wykorzystują nasze dane, by nas okradać. Brać na nasze nazwisko kredyty, włamywać się na nasze konto bankowe, robić zakupy korzystając z numerów naszej karty bankomatowej.

-= Ransomware =- blokowanie za pośrednictwem złośliwego oprogramowania

Sami instalujemy je w swoim smartfonie czy na komputerze. Dzieje się tak, gdy otwieramy załączniki do wiadomości z niewiadomego źródła albo klikamy w linki, które mają nas np. doprowadzić do ciekawych zdjęć czy żartów. Przestępca wkrada się do naszego lub firmowego oprogramowania, blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w naszym prywatnym komputerze danych. Po co? Dla wymuszenia okupu.

Parlament Europejski

Projekt współfinansowany przez Unię Europejską w ramach programu dotacji Parlamentu Europejskiego w dziedzinie komunikacji. Parlament Europejski nie uczestniczył w przygotowaniu materiałów; podane informacje nie są dla niego wiążące i nie ponosi on żadnej odpowiedzialności za informacje i stanowiska wyrażone w ramach projektu, za które zgodnie z mającymi zastosowanie przepisami odpowiedzialni są wyłącznie autorzy, osoby udzielające wywiadów, wydawcy lub nadawcy programu. Parlament Europejski nie może być również pociągany do odpowiedzialności za pośrednie lub bezpośrednie szkody mogące wynikać z realizacji projektu.

foto SHUTTERSTOCK

Transformacja cyfrowa i bezpieczeństwo

Czas pandemii koronawirusa jeszcze bardziej przyspieszył rozwój technologii cyfrowych, by sprostać wymaganiom świata, w którym przyszło nam żyć. Obecnie rewolucja technologiczna goni rewolucję technologiczną i pojawia się pytanie, jak państwa i instytucje międzynarodowe powinny reagować na to błyskawiczne tempo postępu. Regulować czy dać wolną drogę do rozwoju? O roli Unii Europejskiej i państwa w tym procesie dyskutowali zaproszeni do organizowanej przez „Super Express" i Parlament Europejski debaty goście: dr Rafał Lange, kierownik działu badań nad cyberprzestrzenią i cyberbezpieczeństwem w Thinkstat w NASK, Piotr Borczyński, przewodniczący samorządu studentów SGH, oraz posłowie do Parlamentu Europejskiego: Róża Thun z frakcji Renew Europe i Marek Balt, Socjaliści i Demokraci.

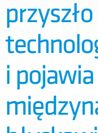
Róża Thun, posłanka do Parlamentu Europejskiego z frakcji Renew Europe

Marek Balt, poseł do Parlamentu Europejskiego, Socjaliści i Demokraci

Od lewej: Tomasz Walczak, redaktor „Super Expressu", Rafał Lange, kierownik działu badań nad cyberprzestrzenią i cyberbezpieczeństwem w Thinkstat w NASK, oraz Piotr Borczyński, przewodniczący samorządu studentów SGH

TOMASZ WALCZAK
redaktor „Super Expressu":

– Trwa w skali globalnej technologiczny wyścig zbrojeń. Jak powinna się zachowywać Unia Europejska, by go nie przegrać? Tak jak Chiny, nie wprowadzając regulacji dla firm technologicznych, czy jednak starym zwyczajem Europy próbować jakoś ten błyskawiczny postęp ucywilizować za pomocą prawa?



RÓŻA THUN
posłanka do Parlamentu Europejskiego:

– Unia Europejska jest wyjątkowym projektem w skali świata i nie musimy nikogo naśladować. Nie musimy puszczać wszystkiego na żywioł, biorąc Chiny za przykład i próbować iść ich drogą. Nie powinniśmy też iść drogą jakichś żelaznych regulacji w każdej dziedzinie. Bo my mamy swoją trzecią drogę unijną. Ona zakłada m.in., że na początku rozwoju jakiejś technologii prawo i regulacje nie wtrącają się za bardzo w ten proces. Z czasem przychodzi jednak moment, że trzeba wprowadzić pewne regulacje. I nie jest tak, że biznes nie chce żadnych regulacji. Chce po prostu jasnych, przejrzystych zasad i oczekuje, że będą z nim one konsultowane. Chodzi o to, żeby te regulacje nie hamowały postępu.

Tomasz Walczak:

– A jak na to patrzy Marek Balt?

MAREK BALT
poseł do Parlamentu Europejskiego:

– Cyfryzacja jest nam potrzebna, ponieważ jest to narzędzie. I jak każde narzędzie może służyć dobru ludzi albo być używane na szkodę ludzi. Cyfryzacja czy rozwój sztucznej inteligencji same w sobie nie są złem wcielonym. Czy się nim staną, zależy od tego, co z nimi zrobimy. I dlatego są potrzebne regulacje, by utrudnić użycie technologii tworzonych w złym celu. Dzisiaj dostęp do bardzo skomplikowanych cyfrowych technologii mają zwykli ludzie, a nawet dzieci. I to one przede wszystkim powinny być chronione przed przestępcami, którzy mogą używać narzędzi cyfrowych, by zrobić dzieciom krzywdę. Cyfryzacja jest po to, żebyśmy lżej i krócej pracowali, ale nie po to, żeby nam odebrać pracę. Musimy się chronić przed tą sztuczną inteligencją, bo dzisiaj słyszymy, że można ukraść komuś profil, twarz, głos i zmontować film, żeby reklamować jakieś produkty. Słyszymy, że w niektórych krajach są kradzione całe profile, sylwetki znanych influencerów w celu reklamowania rzeczy, których oni nigdy by sami nie polecali. Musimy więc chronić się przed skutkami złego używania narzędzi cyfrowych.

Tomasz Walczak:

– Róża Thun mówiła, że regulacje muszą być jasne, żeby rynek je rozumiał. Pojawia się jednak pytanie, czy regulacje są w ogóle w stanie nadążyć za postępem technologicznym?

dr RAFAŁ LANGE
kierownik działu badań nad cyberprzestrzenią i cyberbezpieczeństwem w Thinkstat w NASK:

– Przede wszystkim próba regulacji, która ma służyć końcowemu użytkownikowi, czyli nam, użytkownikom technologii, jest jak najbardziej wskazana. Te regulacje powinny być bardziej skierowane w stronę korporacji bigtechowych, które nie zawsze grają fair względem tego końcowego użytkownika. To jest jedna rzecz. A czy regulacje nadążają za postępem technologicznym? Niestety, nigdy tego nie robią. Technologia rozwija się szybciej niż społeczeństwo. Ono najpierw musi zdiagnozować problem, później się naradzić i zaproponować pewne rozwiązania. Zawsze to będzie gonienie peletonu, ale taka jest natura technologii. To jest problem strukturalny. Ja bym nad tym nie płakał. Problem z regulacjami polega na tym, że powinny być one trochę jak żona Cezara. Muszą być bardzo czyste i jasne, bez podejrzenia, że są skierowane przeciwko końcowemu użytkownikowi, że regulacja służy do tego, żeby go ograniczyć albo kontrolować.

Tomasz Walczak:

– Z badań przeprowadzonych na potrzeby naszej rozmowy wynika, że dla młodych najważniejszą troską, jeśli chodzi o postęp technologiczny, jest bezpieczeństwo danych w sieci. Badani wskazują też na zabezpieczenia przed przestępstwami finansowymi, manipulacjami, fake newsami czy na ochronę najmłodszych. To dowód na dużą świadomość wyzwań, przed którymi stają młodzi?

PIOTR BORCZYŃSKI
przewodniczący samorządu studentów SGH:

– Ważne jest to, żeby wspomnieć o tym, iż te regulacje muszą iść na każdym poziomie. Nie tylko na poziomie europejskim czy naszego państwa, lecz także we wszystkich miejscach. Ja reprezentuję samorząd studencki i na uczelni zmagamy się z problemami dotyczącymi tego, jak wykorzystywanie nowych technologii powinno się doregulować i czy pozwalamy na to, czy staramy się je bardzo mocno blokować. To są różne podejścia w zależności od miejsca i tego, jaka jest świadomość środowiska akademickiego na danej uczelni. Mnie osobiście się wydaje, że trzeba iść z tymi technikami do przodu, doregulowywać pewne kwestie. Być może zmieniać formę egzaminowania czy weryfikowania prac dyplomowych tak, by iść z tymi nowymi trendami i wykorzystywać nowe media.

Róża Thun:

– Chciałabym jeszcze szerzej opisać to, jak kwestie regulacji wyglądają w UE. Jak wspomniałam, najpierw przyglądamy się rozwojowi technologii, potem patrzymy, w jaki sposób ona funkcjonuje, a dopiero potem regulujemy. Robimy to bardzo powoli, co często jest ostro krytykowane, ale tempo regulacji wynika także z tego, że my wcale nie chcemy wprowadzać ich za szybko. Chcemy zostawić czas na samoregulację. Tak było m.in. w sprawie roamingu, nad którym pracowałam. Bardzo długo czekaliśmy, żeby operatorzy uregulowali to między sobą. Podobnie było z ujednoliceniem ładowarek do telefonów. W obu sprawach musieliśmy się tym zająć na poziomie unijnym. Samoregulacja to jest coś bardzo ważnego i dobrze by było, gdyby ta kultura samoregulacji wzrastała, by niekoniecznie prawo wtrącało się we wszystko. Co więcej, uważam, że często poziom unijny regulacji to za mało. Chciałabym, żebyśmy na pewne sprawy umawiali się globalnie. Szczególnie jeśli chodzi o zbieranie danych, algorytmy, szeroko pojętą prywatność.

Tomasz Walczak:

– Także pana zdaniem poziom unijny to czasami za mało?

Marek Balt:

– Jako człowiek, który cyfryzację obserwuje w Polsce od 32 lat, także jako jej uczestnik, jestem zwolennikiem jak najszerszego używania nowych technologii. Ale musimy się bronić przed wykorzystywaniem przez nieuczciwych ludzi narzędzi cyfrowych przeciwko innym ludziom. Ja na przykład nie jestem zwolennikiem używania platform cyfrowych, social mediów do pokazywania całego naszego życia, ponieważ to może zostać użyte przeciwko nam. Możemy być profilowani przez nieuczciwe firmy, albo nawet przez instytucje nieuczciwych czy złych państw do tego, żebyśmy dostawali np. wiadomości profilowane, żebyśmy dostawali fake newsy i żeby na tej podstawie tworzyć nasze spojrzenie na świat. Widzieliśmy to w trakcie kampanii Donalda Trumpa w Stanach Zjednoczonych. Widzieliśmy to, kiedy Rosjanie zaatakowali Wielką Brytanię w trakcie kampanii brexitowej, podczas której udostępniano fake newsy, czyli nieprawdziwe informacje. Dlatego musimy się przed takimi rzeczami bronić na każdym możliwym poziomie.

Tomasz Walczak:

– Czy szukanie porozumień globalnych to właściwy kierunek?

Marek Balt:

– Zdecydowanie tak. Globalne rozwiązania byłyby najlepsze. Natomiast nie sądzę, żeby Chiny były skłonne w tym cyfrowym wyścigu zbrojeń do kompromisów i do samoograniczeń. Ponieważ inne płaszczyzny rozwoju technologicznego pokazały, że Chiny swoje, a reszta świata swoje. Ale nie można niczego nie robić tylko dlatego, że Chiny się nie zgadzają. Dobrym rozwiązaniem, przynajmniej na poziomie Unii Europejskiej, jest wprowadzenie pewnych regulacji, które można egzekwować. Oczywiście sieć ma taką naturę, że nie wszystkie pomysły mogą zostać zrealizowane. Ale te na poziomach państw narodowych i Unii Europejskiej są jak najbardziej wskazane. Tym bardziej że użytkownikiem internetu są małe i większe dzieci, które w tej przestrzeni są bezbronne. Rodzice abdykowali często ze swojej roli opiekunów z bardzo prozaicznych powodów. Brak czasu, brak kompetencji, brak pieniędzy, umiejętności, żeby za tą technologią nadążać. Więc ktoś musi tych najmniejszych użytkowników bronić, siłą rzeczy najbardziej w rewolucję cyfrową zaangażowanych? I dlatego właśnie rolą państwa jest to, by przygotowywać młodzież do korzystania z komputerów, z technologii, z nowych systemów w sposób odpowiedzialny i bezpieczny.

Rozmawiał TOMASZ WALCZAK

W zderzeniu z technologią zwykły obywatel jest po prostu bezbronny. Nie ma odpowiedniej wiedzy, żeby dobrze ją zrozumieć, często nie ma odpowiednich kompetencji, żeby korzystać z niej bezpiecznie. To jest chyba jeden z tych głównych argumentów za regulacjami.

dr Rafał Lange:

– Zdecydowanie. Struktura budżetu, czasu rodziców, na których przerzuciliśmy obowiązek wychowania cyfrowego, na chwilę obecną nie pozwalają im na to, żeby w stu procentach realizowali swoją rolę rodzicielską. I te dzieci od niemal dekady są w świecie cyfrowym bezbronne, poddawane różnym wpływom. Mamy w NASK taką komórkę, która zajmuje się przyjmowaniem zgłoszeń o treściach seksualnych, w których są dzieci. Przerażające jest to, że zdecydowana większość materiałów pedofilskich jest wytwarzana przez same dzieci. To ktoś je do tego namówił, ktoś przekupił, ktoś zasugerował, że to jest sposób np. na zarobienie pieniędzy albo na przyciągnięcie atencji. Bo jak pytamy uczniów szkół podstawowych i średnich, czy rodzice z nimi rozmawiali o tych treściach, to mniej więcej dwie trzecie z nich odpowiadają, że rodzice nie rozmawiali.

Tomasz Walczak:

– Pokolenie rodziców nie ma czasu na wychowanie cyfrowe. A czy młodzi mają czas, by ten cyfrowy świat zrozumieć i samemu w nim nie zginąć?

Piotr Borczyński:

– Ja mam 22 lata i już powoli przestaję tak naprawdę nadążać za tym, co teraz się dzieje w wielu obszarach. Podobnie jest z wieloma moimi rówieśnikami. Kiedyś to było tak, że komputer był po prostu złożony głównie z Excela, Worda i kilku innych programów. Aktualnie jest tam niezliczona liczba programów. Pytanie, czy to nasze najmłodsze pokolenie jest w stanie z tego wszystkiego korzystać bezpośrednio i ma świadomość tego, jak to jest wykorzystywane. Czy też możemy już mówić o wykluczeniu cyfrowym nawet osób młodych, siłą rzeczy najbardziej w rewolucję cyfrową zaangażowanych? I dlatego właśnie rolą państwa jest to, by przygotowywać młodzież do korzystania z komputerów, z technologii, z nowych systemów w sposób odpowiedzialny i bezpieczny.

Tomasz Walczak:

– Myślę, że to, na co pan zwrócił uwagę, to dosyć istotny fakt.

Projekt współfinansowany przez Unię Europejską w ramach programu dotacji Parlamentu Europejskiego w dziedzinie komunikacji. Parlament Europejski nie uczestniczył w przygotowaniu materiałów; podane informacje nie są dla niego wiążące i nie ponosi on żadnej odpowiedzialności za informacje i stanowiska wyrażone w ramach projektu, za które zgodnie z mającymi zastosowanie przepisami odpowiedzialni są wyłącznie autorzy, osoby udzielające wywiadów, wydawcy lub nadawcy programu. Parlament Europejski nie może być również pociągany do odpowiedzialności za pośrednie lub bezpośrednie szkody mogące wynikać z realizacji projektu

Parlament Europejski

Wszelkie prawa, w tym Autora i Wydawcy, zastrzeżone. Jakiekolwiek dalsze rozpowszechnianie artykułów zabronione.

803888_WA