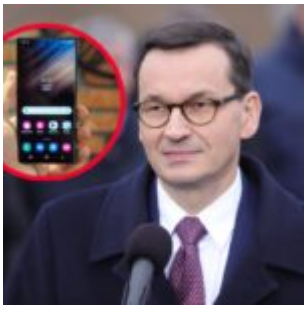
Rząd prześwietli smartfony Polaków. Klamka zapadła



Idą zmiany w prawie komunikacji elektronicznej. Dadzą one służbom specjalnym większe możliwości inwigilowania Polaków poprzez zbieranie najróżniejszych danych o nich.

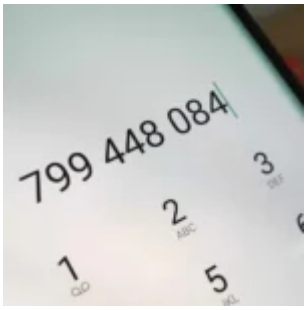
Rząd dał zielone światło zmianom w **prawie komunikacji elektronicznej**. Dzięki nim służby specjalne otrzymają nie tylko dostęp do danych lokalizacyjnych smartfonów czy billingów, ale również – jak informuje dziennik.pl – do **treści przesyłanych e-maili** czy **zapisów rozmów na komunikatorach**.

Innymi słowy, do przesyłania danych o nas do służb będą zobowiązane nie tylko **firmy telekomunikacyjne**, ale także **dostawcy poczty elektronicznej oraz innych usług internetowych**. Rząd za pomocą nowego prawa chce pozyskiwać dane, które pozwolą na **jednoznaczną identyfikację użytkownika w sieci**.

Jeśli zamierzasz zapytać, **czy nowe przepisy będą zgodne z prawem Unii Europejskiej**, to spieszymy z odpowiedzią. **Oczywiście, że nie będą**. Co więcej, jak podaje **Dziennik Gazeta Prawna**, rząd doskonale zdaje sobie z tego sprawę. Podsekretarz stanu w Kancelarii Prezesa Rady Ministrów (KPRM) napisał w opinii do projektu nowych regulacji, że ***pogłębia on zakres niezgodności przepisów z prawem UE***. To jednak prawdopodobnie niczego nie zmienia w ocenie autorów nowego prawa.

Źródło

799 448 084 – ten numer trzeba znać



Numer +48799448084 to jeden z wielu, które warto zapisać w telefonie. Szczególnie w okresie wzmożonych ataków SMS-wych może się przydać w zasadzie codziennie. Przypominamy, dlaczego jest tak istotny i w jaki sposób z niego korzystać.

Numer 799448084 został uruchomiony przez CERT Polska specjalnie na potrzeby zgłaszania incydentów bezpieczeństwa. Każdy, kto dostanie podejrzaną wiadomość SMS (na przykład taką z wezwaniem do uregulowania rachunku za energię elektryczną) może ją przesłać do analizy. **SMS wystarczy przekazać w niezmienionej formie właśnie na numer +48799448084**, a trafi do specjalistów.

W CERT Polska wiadomość zostanie sprawdzona pod kątem bezpieczeństwa, co docelowo może poskutkować wydaniem dodatkowych komunikatów. W praktyce **wysłanie podejrzanego SMS-a na numer 799448084 może więc przełożyć się na stworzenie ostrzeżenia dla innych użytkowników**, którzy w danej chwili nie są świadomi, że ma miejsce atak SMS-owy. W ostatnim czasie najpopularniejsze są głównie te związane z energetyką i podszywaniem się oszustów pod dostawców prądu.

799 448 084 – jak przekazać wiadomość?

Aby przesłać podejrzaną wiadomość SMS do analizy CERT Polska, wystarczy po jej otrzymaniu **przekazać ją na wspomniany numer 799448084**. Najłatwiej to zrobić, jeśli ten został wcześniej zapisany w kontaktach. Co ważne, **treść nie może zostać w żaden sposób zmieniona**. Należy po prostu użyć funkcji „przekaż dalej”, którą można znaleźć w opcjach wiadomości SMS w każdym telefonie.

Warto podkreślić, że co do zasady do analizy można przekazywać podejrzane SMS-y na przykład z nieznanymi linkami lub zachęcające do instalacji nieznanych aplikacji. Wiadomości SMS Premium nie zaliczają się do tych kategorii. **CERT Polska podaje, z jednego numeru można przesłać do analizy maksymalnie 3 SMS-y w ciągu 4 godzin.**

Oskar Ziomek

Upublicznianie w sieci materiałów o dziecku wiąże się z zagrożeniami. Eksperci radzą, jak im zapobiegać

Mimo informacji o kolejnych wyciekach danych oraz o inwigilacji relacjonowanie codziennego życia w mediach społecznościowych wciąż wydaje się nie tracić na popularności. Na stronie Centrum Informacji Konsumenckiej czytamy, że w Polsce ok. 40 proc. rodziców regularnie korzystających z internetu publikuje materiały dotyczące własnego dziecka. Z kolei według badań dr Anny Brosch z Wydziału Nauk Społecznych Uniwersytetu Śląskiego w Katowicach co czwarty rodzic permanentnie udostępnia w mediach społecznościowych informacje o swoich dzieciach, które traktowane jak „mikrocelebryci" dorastają w przeświadczeniu, że dzielenie się szczegółami z prywatnego życia jest naturalną praktyką.

„Życie na wirtualnym świeczniku"

Zjawisko to nazywa się sharentingiem (ang. share – dzielić się i parenting – rodzicielstwo) i odnosi się do częstego upubliczniania informacji intymnych o dziecku, które naruszają jego prywatność i które mają zasięg publiczny, a więc mogą trafić do anonimowego odbiorcy. Mogą to być np. zdjęcia przedstawiające codzienne życie, ale i zdjęcia prześmiewcze, np. gdy dziecko zaśnie z nosem w talerzu.

Jak informują eksperci, ok. 23 proc. dzieci zaczyna istnieć w sieci jeszcze przed fizycznym przyjściem na świat, ponieważ ich rodzice zamieszczają zdjęcia bądź nagrania z USG. Czasem nawet dzieci przebywające w łonie matki mają już profile w mediach społecznościowych.

Z poradnika „Sharenting i wizerunek dziecka w sieci" wydanego przez Akademię NASK dowiadujemy się, że spora część rodziców zamieszczających w sieci treści o swoim dziecku nie stosuje

ograniczeń dotyczących wyświetlania materiałów i udostępnia je większym grupom osób.

Według badań przeprowadzonych przez dr Annę Brosch w 2018 roku w grupie 1036 rodziców dzieci w wieku przedszkolnym, co czwarty z nich nagminnie udostępnia takie informacje. „Nie jest to więc aż tak popularny proceder, ale na pewno zauważalny, bo jeżeli ktoś upowszechnia dziesiątki albo nawet setki zdjęć swoich dzieci, to odbiorcom wydaje się, że media społecznościowe są nimi zalane" – powiedziała dr Brosch.

Badaczka z Wydziału Nauk Społecznych Uniwersytetu Śląskiego zwraca uwagę, że sharentingiem zajmują się przeważnie matki.

„Dawniej np. w latach 70. XX wieku młode matki siadały przed blokiem na ławce, dzieci bawiły się w piaskownicy, a one rozmawiały o dzieciach. Teraz matki przeniosły się do sieci" – podkreśliła.

W ocenie dr Brosch matki udostępniają zdjęcia swoich dzieci z kilku powodów. Po pierwsze, żeby pokazać innym, jak dobrymi są matkami, że sobie doskonale radzą. Po drugie, poszukują wsparcia i akceptacji społecznej dla tego, co robią.

„Trzeci motyw związany jest z charakterystyczną dla naszych czasów modą na popularność. Chodzi o uzyskanie aprobaty społecznej poprzez lajki, co prowadzi do popularności. Wiele osób w sieci naśladuje innych – znanych tylko z tego, że są znani. Następnie oni sami chcą stać się takimi celebrytami. A że nie mają szansy dzięki sobie, to starają się to uzyskać chociaż dzięki dziecku. Stąd np. te zdjęcia ośmieszające dzieci, które mają po prostu przykuwać uwagę" – tłumaczyła badaczka.

Brosch dodała, że ojcowie w dużo mniejszym stopniu ulegają sharentingowi, a jeżeli już, to najczęściej w sytuacji, gdy starają się o prawa do opieki nad dzieckiem.

Częściej kobiety ulegają sharentingowi niż mężczyźni. Robią to, by pokazać, że są dobrymi matkami, choć wiele z nich poszukuje również akceptacji i popularności. Zdjęcie ilustracyjne (MarieXMartin / Pixabay)

Stacey Steinberg, profesor z Levin College of Law na Uniwersytecie Florydy w Gainesville, podaje, że dla części rodziców sharenting jest rodzajem budowania więzi z rozproszoną rodziną, pomaga w dzieleniu się problemami i niweluje samotność. Badaczka podkreśla jednak, że należy pamiętać także o płynących z takiego działania zagrożeniach.

Jako obrończyni praw dzieci zaznaczyła, że dzieci powinny mieć prawo do decydowania, jakie informacje o nich chcą zamieścić w sieci ich rodzice.

Nawet jeśli w danym przypadku publikowane treści nie narażą dziecka na różnego rodzaju represje, kradzież tożsamości czy może nie trafią na strony z pornografią dziecięcą, to pediatrzy są coraz bardziej świadomi znaczenia ochrony obecności dzieci w cyfrowej rzeczywistości i zwracają uwagę, by nie zapominać o prawie dziecka do prywatności.

Prywatność i „długa pamięć internetu”

„Każdy człowiek powinien mieć możliwość tworzenia własnej tożsamości i wizerunku, także w świecie cyfrowym” – podkreślają Anna Borkowska i Marta Witkowska, autorki poradnika „Sharenting i wizerunek dziecka w sieci”. Wszystkim niezależnie od wieku należy się prawo decydowania, jakie szczegóły z własnej prywatności chce ujawnić. Rodzice nagminnie dokumentujący w mediach społecznościowych życie własnych dzieci pozbawiają je możliwości wyboru, co i czy w ogóle chciałyby opowiedzieć o sobie w wirtualnym świecie.

Ponadto autorki poradnika dla rodziców o upublicznianiu wizerunku dziecka w sieci wymieniają jeszcze inne zagrożenia związane z sharentingiem.

Przypominają, że „internet ma długą pamięć” i w cyberprzestrzeni nic nie ginie, zwłaszcza że treści zyskujące dużą popularność dość szybko są rozpowszechniane, a zatem trudno je całkowicie usunąć.

„Internet nigdy nie zapomina, więc trudno przewidzieć konsekwencje tego procederu dla dzieci w przyszłości. W sieci nic nie ginie, a jeżeli wrzuci się do sieci jakieś zdjęcie, to zaczyna ono żyć własnym życiem. Nie mówiąc o skrajnych, ale jednak [mających miejsce], przypadkach kradzieży tożsamości w internecie czy pedofilach w sieci” – mówi dr Brosch.

Utrata kontroli

Na przykład w 2015 roku w Australii wykazano, że około połowa z 45 mln zdjęć znajdujących się na stronie z pornografią dziecięcą pochodziła bezpośrednio z mediów społecznościowych i były to przeważnie niewinne zdjęcia z codziennej scenerii, które pojawiały się w kontekście niestosownych komentarzy.

Dlatego eksperci podkreślają, by pamiętać, że nad fotografiami

wrzuconymi do sieci, przestaje się mieć pełną kontrolę i nie można być pewnym, kto i w jaki sposób je wykorzysta. Mogą zostać bezprawnie użyte w celach majątkowych bądź przestępczych.

Specjaliści ostrzegają, że „media społecznościowe są bardzo często terenem poszukiwań dla pedofilów, którzy nagminnie pobierają z nich zdjęcia dzieci i handlują nimi na zamkniętych forach internetowych”.

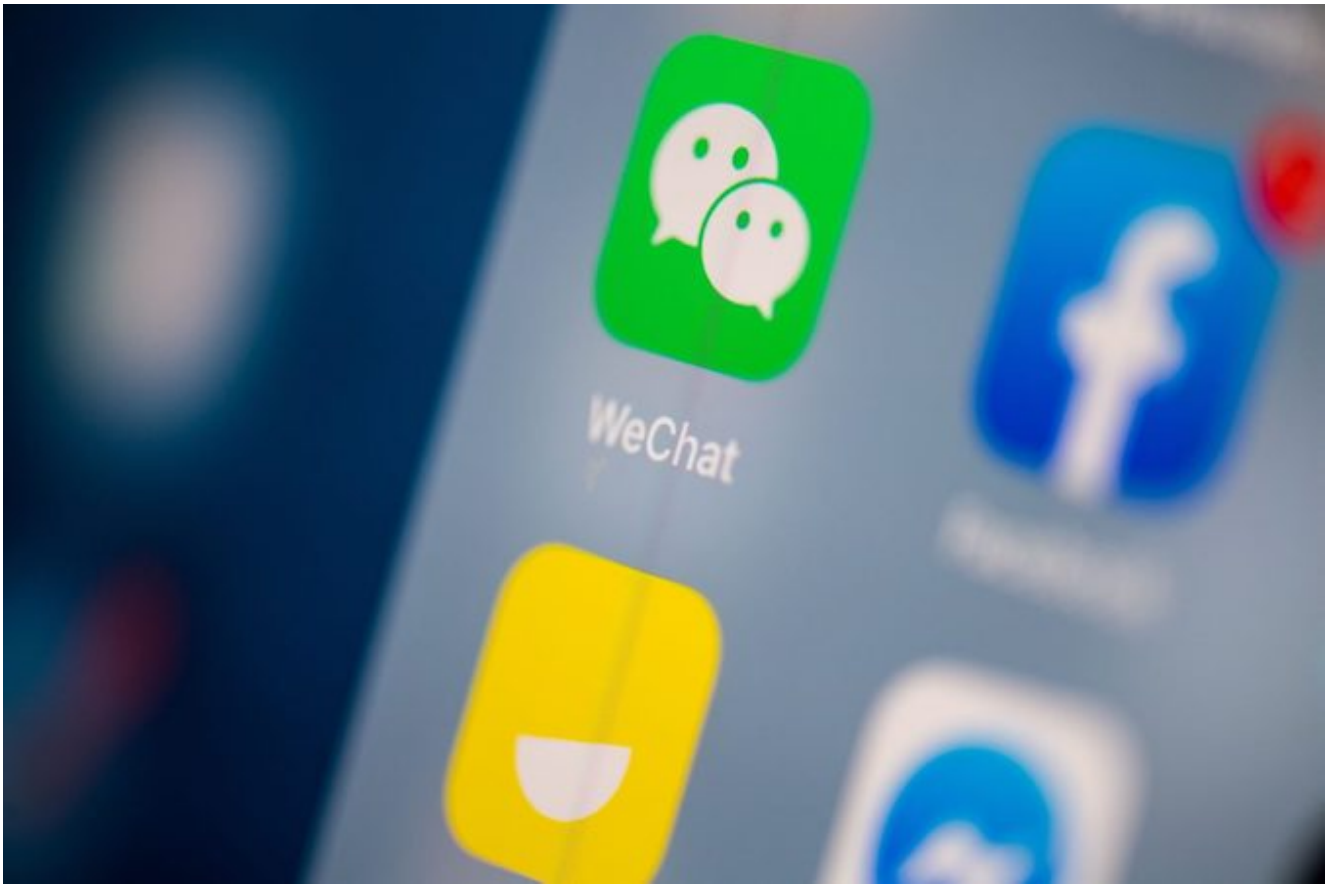
Przestępstwo posługiwania się skradzionym wizerunkiem dziecka w celu realizowania swoich fantazji nazywane jest cyfrowym kidnapingiem (ang. baby role play).

Nie powinniśmy też narażać dzieci na cyberprzemoc. Asumptem do tego może być publikowanie w naszej opinii zabawnych zdjęć dziecka, które jednak w szerszej perspektywie mogą zostać odebrane jako kompromitujące. To może spowodować falę hejtu i agresji ze strony zarówno nieznajomych internautów, jak i rówieśników dziecka oraz wpłynąć na jego samoocenę.

Wykorzystywanie danych osobowych

Pozostaje też kwestia udostępniania danych osobowych, które „wymieniamy” za możliwość korzystania z profilu w mediach społecznościowych. Stanowią one źródło informacji m.in. dla firm marketingowych.

Co więcej, eksperci ds. Chin, a także politycy od lat alarmują, by nie korzystać z chińskich technologii, m.in. TikToka czy WeChata, oraz innych pozornie niegroźnych narzędzi, które gromadzą dane na temat użytkowników, a także pozyskują w nielegalny sposób poufne informacje i wrażliwe dane z różnych instytucji. Gdy takie informacje znajdą się w rękach reżimu komunistycznego, mogą zagrażać bezpieczeństwu krajów oraz ich mieszkańców.



Ilustracja demonstrująca logo chińskiego komunikatora WeChat wyświetlonego na tablecie, 24.07.2019 r. (Martin Bureau/AFP/Getty Images)

Komunistycznej Partii Chin do zbierania danych służą np. platformy społecznościowe, komunikatory, programy do obróbki i „ulepszania" zdjęć lub aplikacje usprawniające pisanie maili.

Władze ChRL wykorzystują „systemy big data do inwigilacji – zwłaszcza w celu sprawdzenia, czy ktoś ma opinie sprzeczne z prezentowanymi przez chiński reżim. Jednym ze sposobów jest analizowanie zakupów w sklepach internetowych" – powiedział profesor nauk politycznych dr Titus C. Chen z Narodowego Uniwersytetu Sun Yat-sena na Tajwanie.

Niemal wszechobecny monitoring w Chinach oraz nadzorowanie aktywności w internecie używane są do tzw. systemu oceny (ang. social credit system). Według niego każdemu obywatelowi są przyznawane punkty „społecznej wiarygodności". Ludziom mogą zostać odjęte punkty z ich wyniku oceny społecznej, jeśli popełnią czyn uznawany przez KPCh za niepożądany, jak

np. przejście przez ulicę w miejscu niedozwolonym. Osoby z niskimi wynikami oceny społecznej są uważane za „niegodne zaufania”, a tym samym pozbawiane dostępu do usług i możliwości. Może chodzić np. o zakaz podróżowania samolotem lub uczęszczania do szkół.

System służy do prześladowania m.in. zwolenników duchowej praktyki Falun Gong, Ujgurów i innych grup, które KPCh próbuje zniszczyć.

Pojawiające się co jakiś czas informacje o wycieku danych pokazują, że KPCh infiltruje nie tylko obywateli ChRL, ale uważnie obserwuje osoby na Zachodzie.

Konsekwencje

Zdaniem dr Anny Brosch sharenting sprawia, że dzieci zaczynają być traktowane jak „mikrocelebryci”, którzy dorastają w przeświadczeniu, że dzielenie się szczegółami z prywatnego życia jest naturalną praktyką.

„Można więc przypuszczać, bo to wymaga jeszcze badań, że gdy w przyszłości sami zostaną rodzicami, będą jeszcze bardziej otwarci i skłonni do samoujawniania. Ale z drugiej strony, to już się dzieje, nastolatkowie proszą rodziców o usunięcie zdjęć i informacji o sobie; za granicą były nawet przypadki sądowych rozpraw” – mówiła dr Brosch.

Badania dr Brosch wykazują, że sharenting się zmienia.

„Coraz mniej już jest zasypywania całymi seriami przypadkowych zdjęć. Teraz są one przemyślane. Wzrasta jednak nastawienie rodziców na zachowania celebryckie i na zyski – im więcej lajków, tym większa popularność i być może możliwość zarabiania pieniędzy z umów na produkty lokowane. W takich przypadkach mogą to być nawet kompromitujące filmy, ale liczy się zasięg” – zauważyła.

Znawcy przedmiotu doradzają zastanowienie się, jakie treści

o naszych pociechach wrzucamy do sieci i jakie to może mieć konsekwencje w przyszłości. Jeśli decydujemy się na publikację, róbmy to odpowiedzialnie. Pamiętajmy, że nawet najlepsze zabezpieczenia nie dadzą nam pełnej ochrony przed niepożądaną kradzieżą wizerunku.

Dbajmy też o to, by nie narazić dzieci na ostracyzm i uczmy je świadomego podejścia do upubliczniania informacji w cyberprzestrzeni.

Źródła: PAP, Centrum Informacji Konsumenckiej, Akademia NASK, NPR.