CYFROWY ŚLAD MAŁEGO DZIECKA

Seria: Internet – Edukacja – Bezpieczeństwo

NASK
dyżurnet.pl

NASK – Państwowy Instytut Badawczy

ul. Kolska 12, 01-045 Warszawa

Redakcja: Zuzanna Polak

Autorzy: Anna Kwaśnik, Zuzanna Polak, Piotr Sowiński

Konsultacje: Martyna Różycka, dr Agnieszka Wrońska

Korekta: Anna Hernik-Solarska

Opracowanie graficzne:

Julia Zdancewicz

Współfinansowane przez Unię Europejską
Instrument „Łącząc Europę”

SPIS TREŚCI

WSTĘP

Internet w życiu rodzica zajmuje bardzo ważne miejsce. Jest przestrzenią zdobywania wiedzy, kontaktów z innymi i budowania społeczności skupionej wokół dzieci, a także miejscem zakupów i poszukiwania najlepszych ofert. Regulaminy większości serwisów społecznościowych zabraniają tworzenia kont osobom poniżej 13. roku życia. Do tego czasu to rodzice są strażnikami prywatności dziecka[1]. Co jednak w sytuacji, gdy sami ją naruszają? W jaki sposób placówki świadczące opiekę nad najmłodszymi dziećmi powinny zarządzać kanałami komunikacji i jak publikować zdjęcia, na których występują podopieczni?

Niniejsza publikacja powstała w wyniku obserwacji ekspertów Dyżurnet.pl związanych z codziennym reagowaniem na treści nielegalne w sieci. Analitycy od wielu lat spotykają się z kolekcjami o charakterze pedofilskim, które oprócz treści łamiących prawo, przedstawiających seksualne wykorzystywanie dzieci, zawierają ogromne ilości neutralnych materiałów prezentujących dzieci. Te zdjęcia i filmy zostały najprawdopodobniej zebrane z legalnie działających serwisów społecznościowych. Większość tych materiałów została umieszczonych w sieci przez niefrasobliwych rodziców, którzy nie zdają sobie sprawy z tego, jak zdjęcia ich dzieci mogą być wykorzystane.

Przedstawiamy nową publikację, w której staramy się zaprezentować „w pigułce" zagrożenia, jakie płyną z nieostrożnego publikowania wizerunku dzieci, a także dobre praktyki, które pomogą rodzicom najmłodszych dzieci umiejętne zarządzać wizerunkiem swoich pociech. Zwracamy również uwagę na rolę placówek opiekuńczych dla najmłodszych, a także inne źródła danych o naszych dzieciach, które mogą pozyskiwać o`soby nieupoważnione.

Mamy nadzieję, że nasza publikacja dopełnia obrazu cyfrowego bezpieczeństwa najmłodszych prezentowanego przez NASK.

Zapraszamy do lektury,

Zespół Dyżurnet.pl

1 Brosch, A. (2018). Sharenting – why do parents violate their children's privacy? The New Educational Review, S. 75-85.

Niektóre dzieci zaczynają być obecne w sieci jeszcze przed urodzeniem. W mediach społecznościowych pojawiają się mamy prezentujące zdjęcia, nagrania już z okresu ciąży. Funkcjonuje moda na wirtualne ogłoszenie daty porodu i płci dziecka („gender reveal"), czasem w postaci profesjonalnej sesji zdjęciowej z elementami humorystycznymi. Fenomen przyjęć typu „gender reveal" jest coraz częściej krytykowany przez społeczność internetową, a blogerka Jenna Karvunidis, której przypisywane jest zapoczątkowanie trendu, sugeruje zaprzestanie tego rodzaju zabaw.[2] Według badań AVG (firmy zajmującej się cyberbezpieczeństwem), prowadzonych od 2010 r. w grupie rodziców z 10 krajów świata, tzw. ślad cyfrowy 23% dzieci sięga publikacji zdjęć USG płodu (w Europie ten odsetek wg badań jest niższy, ok. 15%; wg badań Anny Brosch[3] z 2015 r. – 10% polskich rodziców decyduje się taką publikację). AVG uznaje, że data cyfrowych urodzin dziecka wypada średnio w okolicach jego 6 miesiąca życia, chociaż w 1/3 przypadków pierwsze materiały o dziecku pojawiają się już w ciągu kilku pierwszych tygodni po urodzeniu. Potem rozwój dziecka jest na bieżąco dokumentowany zdjęciami w różnych serwisach społecznościowych, a kiedy maluch zaczyna swoją przygodę z placówką opiekuńczą, zaczynają się pojawiać zdjęcia z zajęć w żłobku i przedszkolu.

2 https://natemat.pl/319857,gender-reveal-party-na-czym-polegaja-w-usa-to-juz-szalenstwo#
https://www.theguardian.com/lifeandstyle/2020/jun/29/jenna-karvunidis-i-started-gender-reveal-party-trend-regret

3 Brosch, Anna. (2016). When the Child is Born into the Internet : Sharenting as a Growing Trend among Parents on Facebook. The New Educational Review. 43. 225-235.

ROLA RODZICA W OCHRONIE WIZERUNKU DZIECKA W SIECI A ZJAWISKO SHARENTINGU

Według badań organizacji Nominet[4] z 2018 r., brytyjski rodzic publikuje w serwisach społecznościowych średnio ok. 100 materiałów prezentujących swoje dziecko do 13 roku życia (71 zdjęć i 29 filmów wideo) przy czym 1/5 z nich ma profil całkowicie publiczny lub dostępny dla „znajomych znajomych". Opiekunowie nie zdają sobie sprawy, jak dużo informacji umieszczają publicznie w różnych miejscach internetu, jak łatwo je powiązać ze sobą, a także jakie to stanowi zagrożenia dla naszych bliskich. Przykładowo, jeżeli rodzic publikuje dane takie, jak data urodzenia dziecka i jego płeć, regularnie publikuje zdjęcia, „lubi" profil jego placówki opiekuńczej, a poza tym udziela się w lokalnej grupie sąsiedzkiej – łatwo namierzyć obszar, w którym można spotkać dziecko (np. często fotografowany plac zabaw).

Wśród przebadanych 168 polskich kont w serwisach społecznościowych w 2015 r., prawie 40% publikowało więcej niż 100 zdjęć temat swojego dziecka, a aż 90% podało imię dziecka i prawie 84% datę jego urodzenia. Im więcej informacji, tym pełniejszy wizerunek można zbudować, co ostatecznie może prowadzić nawet do kradzieży tożsamości. Badania przeprowadzone w 2019 r. pokazują, że 40%. Polaków regularnie publikuje zdjęcia swoich pociech na różnego rodzaju portalach społecznościowych. Co ciekawe, 81% rodziców ocenia udostępnianie zdjęć własnych dzieci pozytywnie lub neutralnie. Aż 57% badanych deklaruje, że o prywatności dziecka decydują rodzice i nie ma nic złego we wrzucaniu do internetu zdjęć lub filmów z jego udziałem. Niepokojące jest, że 60% dzieli się dokumentacją dzieciństwa własnych dzieci przynajmniej raz w miesiącu, a tylko około 25% zapytało własne dziecko o zgodę na udostępnianie jego zdjęć[5].

Sharenting (z ang. share- dzielić, parenting — rodzicielstwo), to regularne zamieszczanie przez rodziców w internecie (głównie na portalach społecznościowych, blogach, forach dyskusyjnych) szczegółowych informacji, zdjęć i filmów z życia dzieci. Jak pokazują liczne badania, zjawisko to jest bardzo popularne, a wielu rodziców nie zdaje sobie sprawy, że takie zachowania mogą nieść ze sobą różne zagrożenia i niebezpieczeństwa.

Brytyjski bank Barclays[6] szacuje, że do 2030 r. to właśnie sharenting będzie odpowiadał za 2/3 kradzieży tożsamości osób małoletnich, co może generować 670 mln funtów strat związanych z oszustwami finansowymi. Według specjalistów banku do skutecznej kradzieży tożsamości wystarczą trzy dane – imię i nazwisko, data urodzenia oraz adres – a wszystkie te informacje zdarza się rodzicom umieszczać w sieci, nie zawsze świadomie. Cyberprzestępca może wydedukować brakujące informacje ze zdjęć (np. adres zamieszkania ze zdjęcia budynku, datę urodzin ze zdjęć z przyjęcia). Co najbardziej niepokojące, ponad 67% rodziców udostępniło, co najmniej jedno zdjęcie, uznane przez badaczy za nieodpowiednie, najczęściej prezentujące nagość lub jej elementy, w szczególności chodziło tutaj o zdjęcia z kąpieli lub plaży, wykonane dzieciom poniżej 3 roku życia. Często publikowane są także tzw. „zabawne" zdjęcia – dziecka płaczącego, strojącego miny, śpiącego w dziwnej pozycji, czasem na nocniku. Takie zdjęcia mogą być groźne dla bezpieczeństwa dziecka na różnych płaszczyznach.

Przede wszystkim należy mieć na uwadze bezpieczeństwo fizyczne dziecka i jego ochronę przed internetowymi złoczyńcami o skłonnościach pedofilskich. Publikacja zdjęć prezentujących nagość w połączeniu z łatwymi do wyśledzenia danymi osobowymi dziecka (nawet tylko jego imieniem) może ułatwić nawiązanie relacji z dzieckiem, chociażby przez

4 https://www.nominet.uk/2-7m-parents-share-family-photos-complete-strangers-online/ [dostęp 18.06.2020]
5 Bierca M., Wysocka-Świtała A., (2019). „Sharenting po polsku, czyli ile dzieci wpadło do sieci?", Wydawnictwo: Clue PR
6 Child Commissioner Office (2018) Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data.

spersonalizowane zaczepienie go na placu zabaw. Poza tym, zdjęcia tego typu często stają się elementami kolekcji zdjęć osób wymieniających się materiałami nielegalnymi, prezentującymi seksualne wykorzystywanie dzieci (zwracają na to uwagę eksperci p. Dyżurnet.pl Raport 2014, 2015).

Z innej perspektywy, zdjęcia prezentujące dziecko w nieodpowiedniej sytuacji mogą być dla niego krępujące w przyszłości. Przypomina to sytuacje znane z czasów przedinternetowych, kiedy rodzice beztrosko dzielili się ze znajomymi opowieściami o intymnych sprawach dziecka, powodując u niego poczucie wstydu. W obecnej sytuacji, kiedy rzeczy raz umieszczone w internecie prawdopodobnie zostaną tam na zawsze, takie zdjęcia czy filmy odnalezione po latach, mogą stać się narzędziem cyberprzemocy w okresie młodzieńczym związanym z dużą wrażliwością na temat swojego wizerunku.

Innym, często niedocenianym aspektem nadużycia prawa do prywatności dziecka, może być również kradzież wizerunku, np. w celu uruchomienia fałszywej zbiórki internetowej lub w celach komercyjnych, np. poprzez wykorzystanie w reklamie czy blogu[7,8].

Nie należy także pomijać kwestii samej relacji rodzic — dziecko. W pewnym momencie swojego życia dziecko będzie już świadome, że rodzic umieszcza treści z jego udziałem w serwisach społecznościowych, może po prostu sobie tego nie życzyć oraz zażądać usunięcia materiałów z wcześniejszych lat.

Jednocześnie pojawia się kwestia kształtowania kompetencji cyfrowych u dziecka w zakresie bezpiecznego korzystania z internetu i ochrony swoich danych. Czy dziecko, którego prawo do prywatności jest nadużywane przez opiekuna, nabędzie umiejętności chronienia swojego wizerunku i poszanowania prywatności innych osób? Bardzo ważne jest podkreślanie wartości szacunku wobec wizerunku innych osób, oraz tego, że nikt nie ma prawa publikować w internecie bez zgody. Warto pamiętać, że cyberprzemoc, której zarówno sprawcami, jak i ofiarami są najczęściej nastolatkowie, jest ściśle związana z szacunkiem i respektowaniem praw innych osób.

Należy też wziąć pod uwagę, że decyzje w imieniu dziecka podejmują jego opiekunowie. Czas zaistnienia pierwszego śladu cyfrowego oraz budowania wizerunku przede wszystkim nie powinien naruszać dobra osoby nieletniej. Opiekunowie publikując materiały w internecie prezentujące dzieci, kształtują ich wizerunek, który prawdopodobnie będzie im towarzyszył przez całe życie.

7 Zjawisko kradzieży wizerunków dzieci digital kidnapping: https://wyborcza.pl/7,156282,25205865,czulam-sie-jakby-ktos-porwal-moje-dziecko-rodzice-masowo.html

8 Sprawa jednej z fałszywych zbiórek: https://niebezpiecznik.pl/post/kto-stoi-za-podejrzana-zbiorka-na-chorego-franka/

SEKSUALIZACJA

Przeglądając różne portale społecznościowe, nietrudno natknąć się na galerie zdjęć, w których pokazywane są małe dzieci, czasem już niemowlęta. Wiele z nich prezentuje dzieci w ubrankach wzorowanych na odzieży dla dorosłych, nago lub z akcesoriami, które zakrywają tylko miejsca intymne. Należy zdawać sobie sprawę, że takie zdjęcia mogą trafiać w różne miejsca i niepowołane ręce.

Warto również przytoczyć konkursy piękności dla małych miss, które cieszą się dużą popularnością w USA oraz Wielkiej Brytanii. Doniesienia medialne wskazują, że najmłodsza uczestniczka, która wzięła udział aż w 9 konkursach, miała zaledwie 3 lata[9]. Niepokojące jest to, że tak małe dziewczynki poddawane są różnym zabiegom (np. doczepianiu włosów, rzęs, opalaniu natryskowemu) i są traktowane bardzo przedmiotowo.

Eksperci z zespołu Dyżurnet.pl, którzy analizują treści przedstawiające seksualne wykorzystywanie dziecka i treści prezentujące najmłodszych w seksualnym kontekście, przestrzegają przed publikowaniem takich zdjęć swoich dzieci, ponieważ mogą one trafić np. do galerii pedofilskich) oraz być wykorzystywane sposób, który nie jest bezpieczny dla dziecka.

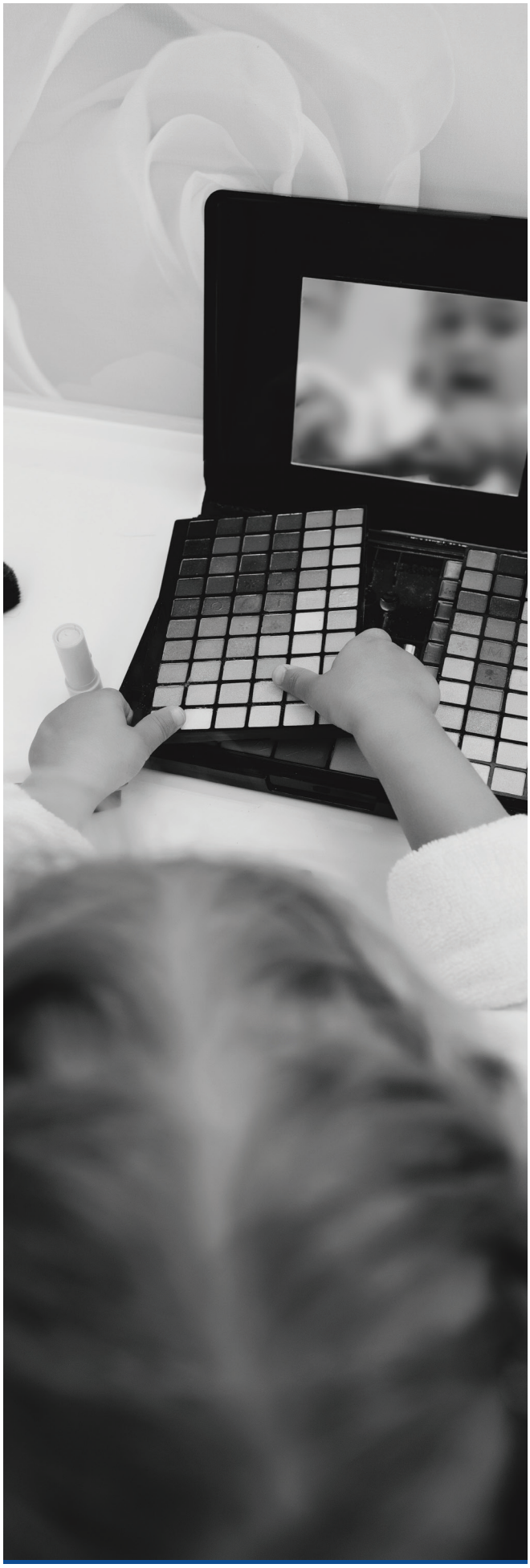
Zjawisko seksualizacji społeczeństwa jest obserwowane od wielu lat[10] i przenika różne aspekty współczesnego życia[11]. Niepokojący jest fakt, że dotyka ono coraz młodszych – również dzieci w okresie niemowlęcym czy przedszkolnym, a w związku z rozwojem mediów, internetu i innych nowoczesnych technologii, jego skala stale rośnie.

Istnieje wiele definicji seksualizacji, a do najczęściej stosowanych należy definicja Amerykańskiego Towarzystwa Psychologicznego, zgodnie z którą seksualizacja ma miejsce, gdy:

- wartość osoby wynika z jej atrakcyjności seksualnej lub zachowania – do tego stopnia, że wyklucza inne cechy;
- osoba jest dopasowywana do normy, według której atrakcyjność fizyczna (wąsko zdefiniowana) oznacza bycie seksownym;
- osoba jest uprzedmiotowiona pod względem seksualnym, czyli staje się dla innych raczej przedmiotem seksualnego wykorzystania niż osobą zdolną do podejmowania niezależnych działań i decyzji;
- seksualność jest narzucona osobie w niewłaściwy sposób".

Każda z czterech sytuacji jest przejawem seksualizacji, nie muszą one występować wspólnie[12].

9 https://www.dailymail.co.uk/femail/article-4987946/Michigan-s-three-year-old-beauty-queen.html
10 Zielona-Jenek, Monika. (2017). Seksualizacja — definicje, polemiki i próba rekonceptualizacji. Dziecko krzywdzone. 16. http://dzieckokrzywdzone.fdds.pl/index.php/DK/article/view/636/495
11 https://www.spidersweb.pl/rozrywka/2020/08/20/netflix-gwiazdeczki-plakat-opis-seksualizacja-dzieci/
12 APA Task Force on the Sexualization of Girls (2007). Report of the APA Task Force on the Sexualization of Girls, zob. https://www.apa.org/pi/women/programs/girls/ report-full.pdf



Trend można zaobserwować w produktach skierowanych dla dzieci – bajkach, zabawkach, akcesoriach i przede wszystkim modzie, szczególnie dla małych dziewczynek. Pojawiają się w sprzedaży zestawy do makijażu czy ozdabiania paznokci, które przeznaczone są dla najmłodszych.. Warto wiedzieć, że zbyt wczesne skupienie się na sprawach podkreślania płci czy „poprawiania" urody, ma znamiona seksualizacji, która może prowadzić do wielu zaburzeń nie tylko w okresie dzieciństwa, ale także w dorosłym życiu[13]. Mogą pojawić się problemy z rozwojem emocjonalnym, własną tożsamością płciową, a także trudności z odnajdywaniem się w grupie rówieśników, a nawet niewłaściwe przyjmowanie informacji ze świata zewnętrznego. Nadmierna stylizacja ciała i kult piękna może spowodować u dziecka przedmiotowe traktowanie swojego ciała oraz takie postrzeganie innych osób. Promocja tego rodzaju zachowań i mody w sieci jest niezwykle niebezpieczna dla wizerunku najmłodszyh. Przy jakiejkolwiek publikacji materiałów prezentujących dziecko, warto mieć na uwadze również tę kwestię.

Małe dzieci, zwłaszcza w okresie niemowlęcym czy wczesnoprzedszkolnym nie przywiązują wagi do mody oraz swojego wyglądu, dlatego należy mieć świadomość rodzicielskiej odpowiedzialności w tym zakresie. Wybierając ubrania i akcesoria dla dziecka warto pamiętać o poszanowaniu jego godności oraz o zapewnieniu wygody i bezpieczeństwa. Warto przytoczyć tu przykład jednej z firm, która kilka lat temu zaprojektowała buty na obcasie dla najmłodszych. Marka nie zyskała jednak zbyt dużego poparcia wśród internautów, wielu z nich negatywnie komentowało nowy trend, zdarzały się jednak osoby, które uważały produkt za uroczy[14].

13 Trojanowska, P. (2014). Seksualizacja dzieci i młodzieży – przyczyny, przejawy, konsekwencje i propozycje przeciwdziałania. Dziecko Krzywdzone. Teoria, badania, praktyka, 13(2), 55–78.
14 https://www.bbc.com/news/world-us-canada-39442090

DZIAŁALNOŚĆ RODZICÓW W INTERNECIE A PRYWATNOŚĆ DZIECKA

Przypadkiem szczególnym w kwestii ochrony prywatności dziecka jest sytuacja, kiedy rodzic prowadzi działalność w internecie w postaci bloga, wideobloga lub innego typu relacji w serwisach społecznościowych. Obserwując osoby prowadzące taką działalność profesjonalnie, znane publicznie, celebrytów, których konta mają bardzo dużą oglądalność, można zauważyć, że prywatność ich dzieci jest często chroniona bardzo ściśle[15]. Nawet przy okazji prezentacji artykułów dziecięcych, ubranek czy wystroju pokoju, sam wizerunek dziecka jest zazwyczaj ukryty. Do publicznego obiegu włączane są tylko pojedyncze, starannie dobrane zdjęcia dziecka (czasem w celach komercyjnych, związanych z promocją konkretnego produktu) i jest to robione stosunkowo rzadko.

Z drugiej strony funkcjonują również znani publicznie użytkownicy, którzy z większą łatwością dzielą się zdjęciami swoich dzieci, czasem nawet całymi wideorelacjami. Tacy celebryci i ich dzieci są najbardziej narażeni za omówione wyżej zagrożenia związane z publikacją wizerunku najmłodszych, ponieważ ich materiały mają dużą popularność w sieci i często budzą intensywne emocje – co może prowadzić do częstszych ataków na nich lub dzieci, a także prób kradzieży tożsamości. Odrębną kwestią jest też „własna" działalność internetowa dziecka (np. w e-sporcie), przynosząca czasem znaczące dochody[16]. Przy czym określenie „własna" zostało celowo wzięte w cudzysłów, ponieważ jest ona, w większości przypadków, zarządzana przez opiekunów.

Jeżeli rodzic prowadzi lub planuje prowadzić publicznie dostępnego bloga lub inną, podobną aktywność w internecie, w ramach której chce poruszać kwestie związane ze swoim rodzicielstwem, powinien zastanowić się, jak może to wpłynąć na bezpieczeństwo wizerunku dziecka. Należy wziąć pod uwagę możliwe zagrożenia i zdecydować, czy postrzegane korzyści są warte podjęcia ryzyka.

15 Znany bloger parentingowy o publikacji wizerunku własnych dzieci: „Nie publikuję zdjęć własnych dzieci, bo chcę, żeby moje dzieci stworzyły swoją własną historię, a nie nadpisywały tą wykreowaną przez rodziców." https://www.blogojciec.pl/dzieci/dlaczego-ukrywam-moje-dzieci-przed-swiatem/

16 https://dadhero.pl/285471,dzieciecy-youtuberzy-czyli-male-maszynki-do-zarabiania-pieniedzy

RODZICIELSKIE GRUPY SPOŁECZNOŚCIOWE

Miejscem, gdzie – w dobrej wierze – ale czasem z niedostatecznym poszanowaniem prywatności dziecka, komunikują się rodzice, są rodzicielskie grupy społecznościowe. W takich grupach omawiane są kwestie zdrowotne, wychowawcze czy rozwojowe, czasem bardzo poważne. Zdarza się, że szukając pomocy i rozwiązania problemów rodzice ujawnią zbyt wiele informacji na temat swojego dziecka – dokumentację medyczną, zdjęcia, na których oprócz objawów choroby widać również twarz dziecka, skomplikowane opisy trudnych relacji rodzinnych. A nawet jeżeli podstawowe informacje są ukryte, wiele można wywnioskować po innych, publicznie dostępnych danych z profilu rodzica. Umieszczając tego typu wpisy należy również pamiętać, że zostaną one poddane ocenie komentujących i można narazić siebie lub dziecko na nieprzyjemne sytuacje związane z nieprzemyślanymi komentarzami, a wręcz hejtem i cyberprzemocą, wiadomości prywatne od nieznanych osób oraz uwagi zupełnie niezwiązane z tematem zapytania. Przystępując do grupy należy zapoznać się z jej regulaminem, a przed umieszczeniem posta – poobserwować dynamikę grupy i sposób reakcji administratorów na niepożądane zachowania. Zawsze, kiedy umieszczamy zapytanie na grupie, należy zachować daleko idącą ostrożność. Warto korzystać z opcji udostępnienia treści anonimowo, za pośrednictwem administratorów grupy.

Podstawowe zasady ochrony prywatności w serwisach społecznościowych:

- **Ochrona wizerunku —** zdjęcia/filmy powinny w miarę możliwości nie ujawniać twarzy dziecka,
- **Ochrona intymności —** zdjęcia/filmy nie powinny w żadnym przypadku prezentować jego nagości ani być sfokusowane na intymne części ciała,
- **Usunięcie danych osobowych** ze skanów dokumentacji medycznej, łącznie z danymi lekarza/diagnosty,
- **Uzgodnienie z administratorem możliwości usunięcia postu po jakimś wczasie —** być może nie ma takiej możliwości, ponieważ posty traktowane są jako element stale budowanej bazy wiedzy dla innych rodziców,
- **Zapoznanie się z regulaminem grupy** pod kątem dozwolonych wpisów, polityki wobec zdjęć dzieci czy wsparcia przy publikacjach anonimowych.

Warto zapoznać się z różnymi zaleceniami i dobrymi praktykami w zakresie funkcjonowania grup parentingowych. Takie informacje można znaleźć w regulaminach największych grup oraz na blogach[17].

17 https://rodzicowo.pl/artykuly/7-bledow-popelnianych-na-grupach-parentingowych-na-facebooku/

PRYWATNOŚĆ DZIECKA A ZBIÓRKI NA CELE MEDYCZNE

Bardzo szczególnym przypadkiem wymagającym podzielenia się prywatnością dziecka i całej rodziny jest konieczność skorzystania ze zbiórki na cele medyczne. Takie działania organizuje się w celu zgromadzenia funduszy na leczenie niedostępne w kraju, rehabilitację, a także terapie doświadczalne. Czasem potrzebne są ogromne środki, sięgające kilku milionów złotych. Aby zbiórka miała szanse na osiągnięcie sukcesu, wymaga sporego rozgłosu, który osiąga się przez rozpowszechnianie informacji w portalach społecznościowych, wśród influencerów lub nawet za pośrednictwem mediów. Istota takiego rodzaju pozyskiwania funduszy opiera się na wzbudzeniu empatii i chęci pomocy ze strony nieznajomych. Aby to uzyskać, niezbędne jest podzielenie się informacjami na temat zdrowia dziecka, statusu finansowego całej rodziny oraz publikacji zdjęć czy filmików. Należy zwrócić uwagę, aby publikowane materiały nie zdradzały nadmiarowych informacji – czyli np. adresu zamieszkania, zbyt wielu danych dotyczących rodzeństwa, szczegółów procedur medycznych. Najlepiej korzystać z usług profesjonalnych fotografów – będą inni w stanie oddać poruszające emocje bez epatowania drastycznymi szczegółami.

Organizując zbiórkę należy być świadomym, że poddaje się internetowej ocenie, która może momentami przerodzić się w hejt. W przypadku starszych dzieci powinniśmy zwrócić szczególna uwagę na potencjalne oznaki cyberprzemocy skierowane wobec dziecka i jego trudne emocje związane z problemem medycznym, podsycane przez negatywne komentarze internautów.

Wpłacając pieniądze na zbiórkę, należy upewnić się, że serwis pośredniczący jest wiarygodny i czy dana zbiórka ma adnotację o weryfikacji przez serwis. Należy również reagować na przejawy hejtu w serwisach społecznościowych i zgłaszać komentarze o charakterze cyberprzemocy do administratorów serwisu.

TROLL PARENTING — CELOWA SZKODLIWA DZIAŁALNOŚĆ RODZICA?

Troll parenting, to zachowanie rodziców polegające na dzieleniu się w sieci treściami, które kompromitują dzieci, ośmieszają je lub pokazują trudne dla nich, wstydliwe czy wręcz upokarzające momenty. Bardzo często, te – w zamyśle zabawne – zdjęcia lub filmy przedstawiają bezradne, przestraszone, a nawet płaczące dzieci, bądź przebrane dla żartu w dziwaczne kostiumy i uposażone w różne akcesoria. Niemowlę włożone do miski, piekarnika lub kąpane w zlewie, chłopczyk z plamą na spodniach, która pokazuje, że nie zdążył do toalety, dziewczynka z brudną w czekoladzie buzią lub ze skrzywioną miną, bo właśnie zjadła cytrynę lub coś ostrego, to tylko nieliczne przykłady działań rodziców, którzy stroją sobie żarty ze swoich dzieci i umieszczają takie treści w sieci. Co więcej, producenci ubranek i różnych akcesoriów dla dzieci podkręcają ten trend i wytwarzają towary, które mogą ośmieszać wizerunek dziecka (np. smoczki z zębami dorosłego, wąsami).

Przeglądając internet często można napotkać na znane memy z udziałem dzieci. To często przypadkowe zdjęcia, czasem prezentujące dziecko w neutralnym lub niekorzystnym świetle, które dzięki pomysłowości internautów i dodatkowym komentarzom, zaistniały w cyberprzestrzeni. Warto się zastanowić, co może czuć dorastające dziecko, którego niefortunne zdjęcie krąży w sieci[18].

Będąc rodzicem należy pamiętać, że wrzucanie do sieci kompromitujących zdjęć dzieci może narazić je na internetowy hejt i agresję (cyberprzemoc), ale również może im uniemożliwić zbudowanie własnej historii w dorosłym życiu, a nawet odebrać godność i szacunek w oczach innych. Pomimo wielu praw jakie mają rodzice wobec dzieci zanim osiągną one wiek pełnoletności (np. sprawowanie pieczy, zajmowanie się majątkiem), mają oni również obowiązki, o których mówi kodeks rodzinny i opiekuńczy.

1. Władza rodzicielska obejmuje w szczególności obowiązek i prawo rodziców do wykonywania pieczy nad osobą i majątkiem dziecka oraz do wychowania dziecka, z poszanowaniem jego godności i praw.
2. Władza rodzicielska powinna być wykonywana tak, jak tego wymaga dobro dziecka i interes społeczny.
3. Rodzice przed powzięciem decyzji w ważniejszych sprawach dotyczących osoby lub majątku dziecka powinni je wysłuchać, jeżeli rozwój umysłowy, stan zdrowia i stopień dojrzałości dziecka na to pozwala, oraz uwzględnić w miarę możliwości jego rozsądne życzenia.

Co więcej, dziecku, podobnie jak każdej osobie dorosłej przysługuje prawo do ochrony wizerunku, które wynika bezpośrednio z kodeksu cywilnego (art. 23). W 2017 r. zapadł pierwszy prawomocny wyrok skazujący ojca, który wstawił do sieci ośmieszające zdjęcia dwuletniego synka[19].

18 https://gadzetomania.pl/547,dzieci-ktore-staly-sie-memami-fajna-sprawa-czy-trauma-na-cale-zycie
19 https://tvn24.pl/polska/ojciec-skazany-za-opublikowanie-zdjecia-ra731943-2464456

ROLA PLACÓWKI OPIEKUŃCZEJ A PRYWATNOŚĆ DZIECKA W SIECI

Placówki opiekuńcze często wykorzystują internet, a w szczególności media społecznościowe, z jednej strony do komunikacji z rodzicami, a z drugiej do prowadzenia działalności marketingowej (co ma miejsce szczególnie w przypadku placówek prywatnych), zachęcając rodziców do oddania pod opiekę swoich dzieci. W tym celu publikowane są zdjęcia z codziennych zajęć czy specjalnych wydarzeń (np. balów przebierańców, przeglądu prac plastycznych czy zabaw na dworze). Należy mieć na uwadze, że publikacja wizerunku dziecka, szczególnie w internecie, wymaga uzyskania zgody od rodzica lub opiekuna prawnego. Zaniedbanie tego obowiązku może skutkować konfliktem z rodzicem lub w skrajnych przypadkach skargą do odpowiedniego organu. Formularz zgody na publikację wizerunku powinien zawierać także klauzulę dotyczącą RODO, czyli informację m.in. o administratorze danych osobowych, danych kontaktowych do administratora danych osobowych, możliwości odwołania zgody itd. Dla pewności, że dokument został przygotowany prawidłowo, warto skorzystać z pomocy prawnika. Spełnienie tego wymogu formalnego, związanego z przestrzeganiem obowiązujących przepisów, to element niezbędny przy prowadzeniu aktywności w mediach społecznościowych, ale wiele aspektów publikacji wizerunku najmłodszych wymyka się regulacjom prawnym i pozostaje w sferze dobrych praktyk i zdrowego rozsądku osób zarządzających profilem. Należy mieć na uwadze, że utrzymywanie publicznego profilu, oznacza, że każdy użytkownik może zobaczyć treści na nim publikowane. Należy zatem zachować szczególną ostrożność przy publikacji wizerunku dzieci. Osoby o skłonnościach pedofilskich mogą poszukiwać materiałów publikowanych na publicznych profilach, aby zbierać materiały do prywatnych kolekcji lub w skrajnych przypadkach nawet wybierania konkretnych ofiar. Sprzyja temu publikacja zdjęć pojedynczych dzieci oraz używanie ich imion w tekście postów. Zaleca się, aby dobór zdjęć prezentowanych w publicznych profilach był bardzo staranny. Zdjęcia powinny:

- przedstawiać raczej dzieci w grupie, najlepiej z zachowaniem dystansu do fotografowania; zdjęcia portretowe nie powinny znajdować się w publicznym obiegu,
- nie prezentować dzieci niekompletnie ubranych (np. podczas zabaw sensorycznych, czy przygotowujących się do drzemki),
- nie prezentować czynności higienicznych, np. korzystania z nocników,
- nie odnosić się do imion dzieci (np. w formie podpisów pod trzymanymi pracami plastycznymi); nie należy również umieszczać imion dzieci w opisach,
- zdjęć nie powinno być dużo; W celach marketingowych wystarczą wyselekcjonowane, pojedyncze zdjęcia,
- prezentować sytuacji potencjalnie krępujących dla dzieci, np. ubrudzenia jedzeniem czy robiących miny.

Należy oddzielić funkcję komunikacji z rodzicami od prezentacji materiałów promocyjnych. Interakcja z rodzicami powinna odbywać się za pośrednictwem specjalnej grupy o restrykcyjnie przestrzeganych zasadach dołączania i usuwania uczestników lub też specjalnej aplikacji służącej do zarządzania placówką. Takie rozwiązania pozwalają na publikację większej liczby zdjęć, zachowanie prywatności korespondencji oraz poruszanie spraw, które nie powinny być omawiane w przestrzeni publicznej. Wykorzystywanie serwisu społecznościowego w publicznym dostępie, bez systemu grup czy prywatnej korespondencji, jest bardzo ryzykowne i naraża placówkę na konsekwencje naruszeń ochrony prywatności.

MONITORING WIZYJNY W PLACÓWKACH OPIEKUŃCZYCH

Kiedy media obiega informacja o poważnym incydencie związanym z aktem przemocy wychowawcy wobec dziecka przebywającego w żłobku, klubie dziecięcym czy placówce o innej formie zorganizowanej opieki, wielu rodziców przeżywa silne emocje. Pojawia się uzasadniony niepokój o bezpieczeństwo malucha i kusząca staje się możliwość podglądania na żywo tego, co dzieje się w miejscu, gdzie zostawiamy dziecko. Jest to również interesujące rozwiązanie dla dyrekcji placówki, która ma wtedy większe poczucie kontroli nad pracownikami, oraz organu dla prowadzącego, np. miasta czy gminy. Takie działania mogą odpowiadać też na niektóre potrzeby rodziców. Nagrania z monitoringu mogą dostarczać dowodów potencjalnych nadużyć i niebezpiecznych sytuacji, pomagają wyjaśnić sporne kwestie oraz w rozwiązywaniu konfliktów. Jednak gromadzenie tego typu danych to wyzwanie organizacyjne, prawne, logistyczne, a przez to kosztowne. Powinna zająć się tym wyspecjalizowana firma, która jest w stanie zapewnić profesjonalny sprzęt, bezpieczeństwo danych oraz usługę serwisową. Należy pamiętać, że dla placówki nie jest to inwestycja jednorazowa, będzie dodatkowo obowiązywał okresowy abonament oraz koszty niezbędnych napraw czy wymiany sprzętu i aktualizacji oprogramowania. Będzie również wymagana obsługa prawna, związana z ustanowieniem administratora bezpieczeństwa informacji, opracowaniem polityki bezpieczeństwa danych, zgodności z ustawą/rozporządzeniem o ochronie danych osobowych oraz dokumentacji zgód rodziców.

Dostęp online dla rodziców do monitoringu jest kwestią kontrowersyjną. Przede wszystkim wymaga większych nakładów finansowych związanych z utrzymywaniem systemu informatycznego z interfejsem użytkownika oraz zarządzania dostępem i bezpieczeństwem danych. Należy pamiętać, że nie istnieją całkowicie bezpieczne systemy informatyczne oferujące przekaz internetowy. Zawsze istnieje ryzyko dostępu przez osoby nieuprawnione i należy o nim powiadomić rodziców oraz opracować plan reakcji na tego typu incydent.

Pojawia się również pytanie na temat prywatności zarówno dzieci, jak i pracowników placówki. Kadra może czuć dyskomfort, co może potencjalnie odbić się na zaburzeniu relacji z dyrekcją, rodzicami oraz przede wszystkim z dziećmi, przynajmniej w początkowej fazie wdrożenia monitoringu. Zdarza się, że sytuacja wyrwana z kontekstu, bez transmisji głosowej może w poczuciu obserwatora być zachowaniem podejrzanym, być może nawet przemocowym ze strony opiekunów, ale po wyjaśnieniu nabiera zupełnie innego znaczenia. Przypadki związane ze skargami rodziców, którzy zobaczyli tylko pojedynczy moment, odebrany jako złe traktowanie dziecka, może być w istocie poprawnym działaniem wychowawczym. Przykładem takich trudnych w odbiorze wizyjnym sytuacji może być opanowanie napadu złości u dziecka przez opiekuna lub rozdzielenie bójki. Z drugiej strony zatrudnione w placówce osoby potencjalnie krzywdzące dzieci, prawdopodobnie znajdą inny sposób na nadużycia, poza zasięgiem kamer (np. podczas zabiegów higienicznych w pomieszczeniach nieobjętych monitoringiem) lub maskując swoje zachowanie (przemoc werbalna nieuchwytna dla kamery, szczypanie lub mocne chwytanie nie dające się zinterpretować z odległości).

Jeżeli chodzi o prywatność i ochronę wizerunku najmłodszych, rodzic każdego dziecka powinien wyrazić zgodę, aby transmisja z kamer była dostępna przez internet. Niedopuszczalna jest sytuacja, że część rodziców się nie zgadza na upowszechnienie wizerunku dziecka, ponieważ system nie ma możliwości ukrywania twarzy wybranych osób w czasie rzeczywistym. A jest zrozumiałe, że nie wszyscy życzą sobie, aby ich dziecko było pod taką obserwacją. Rodzice powinni się również zobowiązać do nieudostępniania przekazu ani danych dostępowych osobom postronnym, w tym członkom dalszej rodziny, ponieważ w ten sposób łatwo stracić kontrolę nad faktyczną liczbą potencjalnych odbiorców przekazu. Zwiększa to również prawdopodobieństwo nawet przypadkowego przejęcia danych przez osoby nieupoważnione, a co za tym idzie wycieku do cyberprzestrzeni, gdzie mogą stać się obiektem zainteresowania cyberprzestępców. Ze względów bezpieczeństwa zabronione powinno być również archiwizowanie transmisji na własnym sprzęcie komputerowym.

Jak widać na podstawie powyższych rozważań, decydując się na wprowadzenie monitoringu wizyjnego, szczególnie z dostępem online, dyrekcja placówki lub organ prowadzący powinni wziąć pod uwagę szereg czynników. Warto, aby rodzice również przemyśleli różne aspekty takiej usługi, a także odpowiedzieli sobie na pytanie czego od niej oczekują i czy tych potrzeb nie da się zaspokoić w inny sposób (aplikacja umożliwiająca komunikację z kadrą, zebrania, raporty dzienne). Wszelkie zmiany w zachowaniu dziecka świadczące o byciu ofiarą przemocy najprędzej zauważy rodzic, a nie oko kamery.

ZANIM UMIEŚCISZ ZDJĘCIE W SIECI

O czym warto pamiętać udostępniając zdjęcia dzieci w internecie?

1. Zdjęcia czy filmy umieszczane w serwisach społecznościowych nie mają żadnego zabezpieczenia przed **kopiowaniem**.
2. W ogólnodostępnych serwisach **nie istnieje sposób** na sprawdzenie, kto widział zdjęcie i czy je pobrał.
3. Nawet jeżeli po jakimś czasie zdecydujesz o usunięciu zdjęcia, nie oznacza to usunięcia wszystkich jego istniejących kopii.
4. Każdy materiał udostępniany w internecie prawdopodobnie zostanie w nim **na zawsze**.
5. Bardzo często wizerunek dziecka na zdjęciu łatwo powiązać z jego innymi danymi, np. **imieniem, adresem, placówką, do której uczęszcza, aktualnym miejscem przebywania** (np. ośrodkiem wakacyjnym).
6. Należy uważać, żeby nie publikować treści prezentujących krępujące dla dziecka sytuacje, czynności higieniczne, stany chorobowe lub elementy nagości.
7. W żadnym wypadku nie należy udostępniać w internecie **danych osobowych dziecka, kopii dokumentacji medycznej, w tym wyników badań, opinii poradni psychologicznych/pedagogicznych, dokumentacji sądowej**. Nawet jeżeli zasłonisz konkretne dane osobowe, można powiązać te dokumenty z danymi dostępnymi w innych miejscach sieci.
8. Warto zwrócić uwagę na opis zdjęcia i użyte hashtagi. Osoby o skłonnościach pedofilskich mogą poszukiwać konkretnych opisów np. **#nanocniku, #pierwszakąpiel, #nagolasa**[20].
9. Warto omówić zasady z członkami rodziny, tak aby wszyscy je stosowali dla dobra dziecka. To szczególnie ważna kwestia w przypadku konfliktów rodzicielskich, a także w przypadku internautów o niższym poziomie świadomości cyberbezpieczeństwa, którzy mniej uważnie korzystają z możliwości ochrony prywatności w sieci.

Z perspektywy rodzica

1. Czy zdjęcie lub film, które zamierzasz opublikować na pewno powinno znaleźć się w publicznym miejscu?
2. Czy nie przedstawia **krępującej sytuacji** dla Twojego dziecka? Czy gdyby to było Twoje zdjęcie, chciałbyś/ałabyś żeby inni mogli je zobaczyć?
3. Czy Twoje dziecko jest całkowicie ubrane lub chociaż ma zasłonięte części intymne?
4. Czy określałeś/aś ustawienia prywatności? **Kto będzie mógł zobaczyć materiał**? Wszyscy Twoi znajomi, znajomi znajomych czy może post będzie całkowicie publiczny? Czy wizerunek Twojego dziecka jest widoczny w twoim zdjęciu profilowym lub w tle?
5. Czy w Twoim profilu występują dane, które pozwolą na identyfikację dziecka? **Twoje nazwisko, imię dziecka, adres, aktualna geolokalizacja**?

20https://childrescuecoalition.org/educations/avoid-these-predator-attracting-hashtags-to-keep-your-kids-safe-online/

Z perspektywy placówki

1. Czy otrzymałeś/aś **zgody na publikację wizerunku** od rodziców wszystkich dzieci występujących w danym materiale?
2. Czy materiał może zostać uznany za krępujący?
3. Czy materiał nie zawiera elementów nagości lub widoku bielizny/pieluszki?
4. Czy na zdjęciach występują dane pozwalające na identyfikację poszczególnych dzieci? **Imiona** (także na pracach plastycznych), **podpisy pod materiałami, aktualna geolokalizacja**?
5. Czy jesteś przygotowany/a na ewentualne roszczenia rodziców, jeżeli nie wyrazili zgody na publikację wizerunku dziecka, a przypadkowo znalazło się ono na materiale lub w treściach, które zostaną przez nich uznane za nieodpowiednie?

PRYWATNOŚĆ – DANE – ASPEKTY KOMERCYJNE

Co jeszcze może się stać z danymi na temat naszych dzieci, które znajdą się w sieci? Algorytmy profilujące użytkowników dla celów komercyjnych to już codzienność. To właśnie dzięki tzw. mikrotargetowaniu możliwe jest kierowanie przekazu do grup o konkretnych kryteriach i dlatego wyświetlane są nam dobrane do upodobań reklamy konkretnych produktów czy partii politycznych[21]. Z biegiem lat i zwiększającym się obszarem zastosowań uczenia maszynowego takie profile będą coraz dokładniejsze, a ich zastosowanie można sobie na razie tylko wyobrażać – być może będą stosowane na szeroką skalę przy rekrutacji na wyższe uczelnie czy do pracy, być może w jakiejś formie systemu zaufania społecznego, jak w Chinach[22]. Abstrahując od tego, w którą stronę będzie się rozwijało społeczeństwo informacyjne, należy uświadomić sobie, że im więcej danych zostanie dostarczonych do systemu, tym więcej informacji będzie posiadał, co pomoże mu przewidywać wybory i wpływać na podejmowane decyzje – i dotyczy to wszystkich użytkowników, także dzieci. Wcześniej wspominany był przykład zbierania danych w celu namierzenia lokalizacji dziecka. Automatyczne algorytmy będą jeszcze bardziej precyzyjne. Będą rozpoznawać rozmiar ubrań, ulubione marki, style zakupowe oraz postawy – np. rodzicom udzielającym się na grupach zdrowotnych będą wyświetlać reklamy ubezpieczeń zdrowotnych czy leków i suplementów. Młodzi rodzice jeszcze przed urodzeniem dziecka zostawiają w sieci sporo danych — poszukują informacji na temat opieki nad dzieckiem, kwestii zdrowotnych, przeglądają niezliczone ilości ofert sprzedaży ubranek i akcesoriów niemowlęcych, często dopisują się do programów lojalnościowych w zamian za gratisowe produkty. W ten sposób pośrednio przekazują w celach marketingowych również dane swojego dziecka, takie jak dzień urodzin, płeć czy wymiary. Ustawodawcy na poziomie krajowym i ponadnarodowym zdają sobie sprawę z rosnącego problemu i proponują różne rozwiązania prawne w tym zakresie (np. w Polsce Rozporządzenie o Ochronie Danych Osobowych) nakładając dodatkowe regulacje dla danych dotyczących osób małoletnich. Jednak najlepszą ochroną pozostaje zdrowy rozsądek i świadomość, że każdy ruch w internecie zostawia ślad, który może być wykorzystany w celu wywarcia wpływu.

INTERNET ZABAWEK

Coraz większą popularność zdobywają wszelkiego typu gadżety codziennego użytku podłączone do internetu. Dbając o najmłodszych użytkowników, warto zwrócić uwagę na interaktywne zabawki podłączone do sieci (ang. smart connected), które łącząc wykorzystanie algorytmów sztucznej inteligencji i zasobów internetowych mają na celu interaktywną zabawę z dzieckiem. Takie zabawki „rozmawiają" z dziećmi, odpowiadają na pytania, proponują różne wspólne zabawy, które w zamierzeniu producentów wspierają rozwój poznawczy dziecka. Decydując się na zakup takiej zabawki, należy pamiętać o istotnych kwestiach związanych z bezpieczeństwem i prywatnością. Warto zapoznać się z poradami ekspertów (p. ramka)[23]:

21 Fundacja Panoptykon, Fundacja ePaństwo i SmartNet Research&Solutions (dostawcy Sotrender), przy wsparciu Civitates. (2020) https://panoptykon.org/ktocienamierzyl-raport
22 https://pl.wikipedia.org/wiki/System_zaufania_spo%C5%82ecznego
23 Rywczyńska A., Jaroszewski P. (2018), Internet zabawek – wsparcie dla rozwoju dziecka czy zagrożenie, Warszawa: NASK – Państwowy Instytut Badawczy,

„INTERNET ZABAWEK – WSPARCIE DLA ROZWOJU DZIECKA CZY ZAGROŻENIE” PORADNIK

Bądź świadom, że:

Zakres danych osobowych zbieranych i przetwarzanych (w tym przechwytywany dźwięk) przez producentów zabawek jest często niejasny, w konsekwencji czego producenci mogą przetwarzać co do zasady wszelkie dane pozyskane w trakcie interakcji z zabawką.

Istotnym zagrożeniem dla skutecznej ochrony danych osobowych przetwarzanych przez producentów zabawek jest możliwość przekazywania zbieranych przez nich danych do krajów, w których ochrona w tym zakresie jest na niskim poziomie lub w ogóle jej nie ma.

Możliwość udostępniania danych osobowych organom państwowym (w tym przypadku USA) – np. policji, prokuraturze, innym służbom – bez żadnej kontroli sądowej, stanowi istotną odmienność od zasad obowiązujących na terenie RP w tym zakresie i może wiązać się z bezpodstawną inwigilacją przeprowadzoną przez organy amerykańskiej administracji.

Zanim kupisz dziecku zabawkę podłączoną do internetu:

Zastanów się, czy biorąc pod uwagę wiek dziecka i jego potrzeby „inteligentna” zabawka jest niezbędna?

Przed zakupem zapoznaj się z informacjami producenta oraz opiniami w internecie, korzystaj z blogów rodzicielskich i filmów pokazowych, mając na uwadze, że spora część takich treści jest sponsorowana przez producentów (filmy posiadające płatną promocję powinny być wyraźnie oznaczone).

Poszukaj informacji na temat ewentualnych problemów z bezpieczeństwem zabawki – artykułów, technicznych opisów błędów.

Bądź szczególnie ostrożny w stosunku do zabawek, które dopiero pojawiły się na rynku, ponieważ ich bezpieczeństwo nie zostało jeszcze zbadane przez niezależnych ekspertów.

Nie kupuj zabawek z rynku wtórnego, ponieważ oprogramowanie zabawki mogło zostać zmodyfikowane – np. by wysyłać dane nie tylko do producenta.

Traktuj taką zabawkę jak każdy inny sprzęt podłączony do internetu:

- aktualizuj oprogramowanie,
- korzystaj z zaufanych sieci wifi,
- chroń dostęp silnym hasłem,
- dbaj o prywatność swoją i swoich najbliższych – podawaj tylko niezbędne informacje,
- jeśli jest taka możliwość usuń konto z serwisu, gdy zabawka przestanie być używana przez dziecko,
- obserwuj zachowanie dziecka podczas zabawy.

Więcej informacji w poradniku NASK: „Internet zabawek – wsparcie dla rozwoju dziecka czy zagrożenie”

INTERNET RZECZY

Inną, ale równie poważną kwestią są pozostałe inteligentne urządzenia (smart devices). Jak zwracają uwagę eksperci CERT Polska[24], producenci tego typu urządzeń często nie przykładają należytej uwagi do ich bezpieczeństwa.

Ostatnim głośnym przypadkiem takiej niefrasobliwości była sprawa pewnych smartwatchy (smart zegarków) przeznaczonych dla dzieci, które zgodnie z wizją producenta miały umożliwić opiekunom zdalną kontrolę miejsca pobytu ich dziecka. Jednak producent nie zabezpieczył danych użytkowników – zarówno danych osobowych, jak i nagranych za pomocą urządzenia wiadomości głosowych czy bieżącej lokalizacji GPS. Możliwe było uzyskanie danych ponad 5 000 użytkowników, z czego, jak przekazał serwis Sekurak, ponad 1 400 było zarejestrowanych na terenie Polski[25].

Mówiąc o urządzeniach dla dzieci, nie możemy zapominać o tym, że dorośli również korzystają z tego rodzaju urządzeń. W lipcu 2020 r. doszło do skutecznego ataku na serwery i linie produkcyjne jednego z większych producenta urządzeń do rejestrowania aktywności sportowej[26].

Należy pamiętać, że w obecnym świecie coraz więcej urządzań gromadzi o swoich użytkownikach informacje – laptopy, komputery osobiste, tablety, smartfony, TV, opaski sportowe, zegarki sportowe liczące aktywność, urządzenia domowe typu pralka, lodówka, robot sprzątający. Każde z tych urządzeń, jeżeli ma opcję łączenia się z siecią, ma możliwość zapisania danych i wysłania ich na serwer producenta. Należy się zastanowić nad gwarantowanym przez producenta bezpieczeństwem danych i czy zgadzając się bezrefleksyjnie na zapisy regulaminu nie pozwalamy na zbyt wiele.

Warto zwrócić również uwagę, że nasze dzieci, patrząc na zachowania dorosłych – przede wszystkim rodziców – w późniejszym czasie będą uznawać je za wzór i naśladować. Świat cyfrowy może być postrzegany przez najmłodszych za ten realny, a ciągła interakcja z urządzeniem jako niezbędna i to tylko od rodziców i opiekunów zależy, kiedy i w jakim stopniu dziecko dołączy do cyfryzacji. Należy pamiętać, że dzieci w odpowiednim dla siebie wieku powinny korzystać z urządzeń elektronicznych określony czas. Więcej na temat korzystania przez dzieci z urządzeń elektronicznych: https://www.domowezasadyekranowe.fdds.pl/

24 Raport CERT Polska 2019.
25 https://sekurak.pl/smartwatch-dla-dzieci-kazdy-mogl-je-lokalizowac-zmieniac-lokalizacje-sluchac-z-dowolnego-zakatka-na-swiecie/
26 https://niebezpiecznik.pl/post/garmin-zhackowany-stanela-linia-produkcyjna-i-synchronizacja-zegarkow/

Bibliografia

AVG Digital Diaries. https://www.avgdigitaldiaries.com/

Bierca M., Wysocka-Świtała A., (2019). „Sharenting po polsku, czyli ile dzieci wpadło do sieci?", Wydawnictwo: Clue PR

Brosch, A. (2018). Sharenting – why do parents violate their children's privacy? The New Educational Review, S. 75-85.

Brosch, A. (2016). When the Child is Born into the Internet : Sharenting as a Growing Trend among Parents on Facebook. The New Educational Review. 43. 225-235. https://depot.ceon.pl/bitstream/handle/123456789/9226/16.%20When%20the%20child%20is%20born%20into%20the%20Internet.pdf?sequence=1&isAllowed=y [dostęp 11.02.2021]

Child Commissioner Office (2018) Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data. https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/ [dostęp 11.02.2021]

Fundacja Panoptykon, Fundacja ePaństwo i SmartNet Research&Solutions (dostawcy Sotrender), przy wsparciu Civitates. (2020) https://panoptykon.org/ktocienamierzyl-raport [dostęp 11.02.2021]

Livingstone S., Blum-Ross A., Zhang D., (2018), What do parents think, and do, about their children's online privacy? Parenting for a Digital Future: Survey Report 3, London School of Economics [online: http://eprints.lse.ac.uk/87954/1/Livingstone_Parenting%20Digital%20Survey%20Report%203_Published.pdf [dostęp 31.07.2020]

Niebezpiecznik.pl, Garmin zhackowany. Stanęła linia produkcyjna i synchronizacja zegarków — https://niebezpiecznik.pl/post/garmin-zhackowany-stanela-linia-produkcyjna-i-synchronizacja-zegarkow/ [dostęp 11.02.2021]

Nominet (2018) https://www.nominet.uk/2-7m-parents-share-family-photos-complete-strangers-online/ [dostęp 11.02.2021]

https://childrescuecoalition.org/educations/avoid-these-predator-attracting-hashtags-to-keep-your-kids-safe-online/ [dostęp 11.02.2021]