

26.10.2017

Warto przewidywać. Edukacja i kształtowanie odpowiednich postaw to ochrona przed cyfrowymi zagrożeniami

„Dzieci muszą po prostu rozumieć, co je czeka w sieci” – podkreśla Generalny Inspektor Ochrony Danych Osobowych dr Edyta Bielak-Jomaa.

Generalny Inspektor Ochrony Danych Osobowych, dr Edyta Bielak-Jomaa, zapowiedziała, że w ramach odbywającego się 26-27 października szkolenia dla uczestników VIII edycji programu „Twoje dane – Twoja sprawa” zostaną przedstawione różne propozycje i rozwiązania, zapobiegające zagrożeniom związanym z danymi osobowymi dzieci i młodzieży. Chodzi nie tylko o apele szkolne, przedstawienia teatralne, ale o zaangażowanie osób, znajdujących się w otoczeniu szkoły, czyli społeczności lokalnych, starszych osób, rodziców i dzieci.

Pytana, jak wygląda zabezpieczenie danych osobowych dzieci, poinformowała, że „odpowiada za to szkoła jako administrator danych i jej dyrektor - za te dane, które są przetwarzane w związku z procesem uczenia dzieci”.

Istotna w jej ocenie jest umiejętność przekazywania młodym ludziom wiedzy dotyczącej zagrożeń w związku z korzystaniem z usług cyfrowych, a także wiedza o tym, jakie mają prawa, jak powinni zabezpieczać się przy korzystaniu z tego rodzaju usług.

Ma to duże znaczenie, ponieważ dzieci z łatwością poruszają się w cyfrowym świecie, a przy tym mają niską świadomość tego, co się dzieje np. po ściągnięciu aplikacji. „Dzieciom się wydaje, że skoro aplikacja jest darmowa, to znaczy, że ściągamy ją sobie, możemy grać w grę albo utworzyć jakieś konto, nie mając świadomości (...), że sprzedajemy, oddajemy dane osobowe, oddajemy fragment swojej prywatności” – podkreśliła.

Jak mówiła, musimy dzieci wyposażyć w wiedzę, czym jest ta prywatność? Co to są dane osobowe? Że to jest część ich praw. Prawo do prywatności to podstawowe prawo każdego człowieka.

Po drugie w jej przekonaniu trzeba uzmysławiać im konsekwencje takich zachowań: pozwalania wkraczania w swoją sferę prywatności. A także nauczyć je wyznaczania granic (tam, gdzie jest to możliwe) tak, żeby w ich prywatność nikt nie ingerował. Przekazać wiedzę, że są określone zagrożenia wynikające z korzystania z takich usług.

Negatywne skutki to chociażby zagrożenia psychologiczne czy odpowiedzialność prawna w ramach korzystania z tych usług. „Dzieci muszą po prostu rozumieć, co je czeka w sieci” – przestrzegała.

Odnosząc się do kwestii stosowania kamer i monitoringu wizyjnego, Bielak-Jomaa oceniła, że szkoły mają świadomość odpowiedzialności za prawidłowe przetwarzanie danych osobowych, ale naturalnie wygląda to różnie. „Jeśli chodzi o monitoring, kamery, które są umieszczone w szkołach, to wiemy, że są one umieszczane w różnych miejscach” – mówiła.

„Kamera nie może być zamontowana w tych miejscach, które naruszają prywatność i godność dzieci. Czyli na pewno nie przebieralnie i nie toalety” – przestrzegała.

Dodała, że „kamera nie załatwi bezpieczeństwa w szkole, jeśli nauczyciele, pedagodzy, rodzice, bo to jest też niezwykle istotne, nie wezmą tej odpowiedzialności na siebie”. Nie bowiem nie zastąpi kształtowania właściwych postaw u młodych ludzi.

„Pamiętajmy o tym, że w szkołach kamery, jeszcze obecnie, na podstawie prawnej, zgodnie z ustawą o ochronie danych osobowych, mogą być umieszczane dla celów bezpieczeństwa dzieci i osób, które znajdują się na terenie szkoły” – podkreśliła.

„Trzeba pamiętać, że monitoring wizyjny to monitoring, który nagrywa obraz. Natomiast jeśli mówimy o nagrywaniu dźwięku, jest to już inwigilacja” - zaznaczyła. Kamery nie mogą służyć inwigilowaniu dzieci i nauczycieli. Nie można np. w ten sposób dokonywać kontroli czasu pracy nauczycieli, a taka informacja dotarła do GIODO.

Według dr Edyty Bielak-Jomaa należy zwrócić uwagę na jeszcze jeden istotny problem. „Mówimy o rozporządzeniu europejskim. Przewiduje ono możliwość wyrażenia samodzielnej, swobodnej, świadomej zgody przez dziecko, które skończyło 16 lat na korzystanie z usług społeczeństwa informacyjnego. Na przykład profili społecznościowych czy gier on-line” – zauważyła.

Wyjaśniła, że rozporządzenie przewiduje możliwość, aby w ustawodawstwie krajowym wskazać niższy wiek. „Polski projektodawca Ministerstwo Cyfryzacji określiło ten wiek na poziomie lat 13. To jest minimum, o którym mowa w rozporządzeniu” – poinformowała.

Według Bielak-Jomaa należałoby ten problem rozpatrywać ze względu na istniejącą świadomość dzieci związaną z konsekwencjami udzielenia takiej zgody. „Proszę zauważyć, że dzieci albo nie czytają regulaminów, albo czytają je bez zrozumienia. Bo one niekoniecznie rozumieją te zawiłości języka, które w regulaminie występują” – oceniła.

Poza tym dzieci mogą same na siebie ściągnąć różnego rodzaju zagrożenia. Poprzez ujawnianie zbyt wielu informacji o sobie czy przez prezentację zdjęć.

„Słyszeliśmy i pamiętamy o tym, że dzieci podejmowały, niestety, też skuteczne próby

samobójcze i coraz częściej się to zdarza" - alarmowała. „Bo hejt, bo nienawiść w szkole, bo wyśmiewanie, itd. To się zaczęło właśnie w internecie”.

jas/

Opublikowano: 2017-10-26 15:23

Uwaga! Artykuł pochodzi z portalu internetowego [Serwis Samorządowy PAP](#).