doi: 10.15503/onis2017.102.110

Ochrona danych osobowych a prawo dostępu do dziennika elektronicznego – aspekt formalnoprawny

Berenika Czerwińska
Uniwersytet Wrocławski
pl. Uniwersytecki, 50-137 Wrocław
E-mail: berenikaczerwinska@uwr.edu.pl

Abstrakt

Cel artykułu. Celem artykułu jest omówienie problematyki związanej ochroną danych osobowych, w kontekście danych gromadzonych przez szkoły publiczne w formie dzienników elektronicznych. Istotne zagadnienie omawiane w artykule stanowi także pytanie czy opiekunowie prawni pełnoletnich dzieci powinni być uprawnieni do wglądu do danych osobowych zawartych w dzienniku elektronicznym. Obecnie, w praktyce, rodzice mają dostęp do informacji zawartych w dzienniku elektronicznym bez względu na wiek swojego dziecka.

Metoda. Analizie zostały poddane podstawy wyróżniania danych osobowych, sposób zabezpieczenia tak przechowywanych danych w ramach prowadzonych e-dzienników, a także wskazanie kręgu osób uprawnionych do wglądu do danych osobowych ucznia. Istotne zagadnienie, które zajmuje część rozważań, odnosi się do możliwości udostępniania danych osobowych uczniów zarówno pełnoletnich, jak i niepełnoletnich ich opiekunom prawnym. Całość rozważań została oparta na podstawach wynikających z przepisów prawa powszechnie obowiązującego poczynając od Konstytucji Rzeczpospolitej Polskiej.

Wyniki badań. Badanie wykazało, iż szkoły coraz częściej zmieniają formę prowadzenia dzienników w szkołach publicznych. Wynika to w dużej mierze z chęci dostosowania nauczania i szkolnictwa do informatyzacji wszelkich aspektów życia człowieka. Z całą pewnością wprowadzenie e-dzienników spowodowało przyspieszenie i ułatwienie kontaktu nauczyciela z rodzicem, który może na bieżąco kontrolować zarówno postępy dziecka, absencje, jak i jego uwagi.

Wnioski. Elektroniczna forma prowadzenia zbioru danych osobowych wymaga zastosowania odpowiednich, zwiększonych zabezpieczeń, tak aby nie mogły one zostać ujawnione osobom nieuprawnionym. Podstawy prawne funkcjonowania e--dzienników obowiązujące w Polsce nie dają żadnych podstaw do ograniczenia możliwości wglądu do nich przez opiekunów prawnych uczniów. Wydaje się jednak, że to zagadnienie powinno zostać uregulowane w szczególności w odniesieniu do uczniów pełnoletnich.

Słowa kluczowe: dane osobowe, ochrona, e- dziennik, informatyzacja, prawo dostępu

Protection of personal data and the right of access to an electronic diary - formal and legal aspects

Abstract

Aim of the study. The aim of the paper is to discuss issues related to the protection of personal data in the context of data collected by public schools in the form of electronic logs. Important question is: whether guardians should be entitled to access to personal data of their adult children contained in the electronic log.

Method. The analysis highlighted the basics of personal data protection as a way of storing data in the framework of e-journals, as well as indication of the persons entitled to access to student's personal data. The whole discussion was based on the grounds resulting from the provisions of current law beginning with the Polish Constitution.

Results. The study showed that schools are increasingly changing the form of carrying logs in public schools. This stems largely from a desire to adapt teaching and education to the informationalision of all aspects of human life. Certainly the introduction of e-journals has resulted in accelerating and facilitating contact between the teacher and parent who can keep control of the child's progress, absenteeism, and his remarks.

Conclusions. The electronic form of conducting collection of personal data requires the use of appropriate, enhanced security, so that it cannot be disclosed to unauthorized persons. The legal framework for e-journals in force in Poland does not give any reason to restrict the access to them by the legal guardians of students. It seems, however, that this issue should be regulated, in particular, in relation to adult students.

Key words: personal data, protection of privacy, e-register, informatization, the right to access

Uwagi wstępne

Prawo do prywatności jest dobrem chronionym przez Konstytucję Rzeczypospolitej Polskiej, i tak zgodnie z jej art. 47 (Konstytucja RP, 1997) każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (Nazaruk, 2016). Sama idea prawa do prywatności wywodzi się z doktryny amerykańskiej i można ją zdefiniować jako „prawo do bycia pozostawionym w spokoju" (ang. *right to be let alone*) (Sobolewski, 2013; Motyka, 2006; Krzysztofek, 2014). Pomimo, iż ustawodawca wśród dóbr osobistych z art. 23 k.c. (Kodeks Cywilny, 1964) nie wymienił wprost prawa do prywatności możemy znaleźć takie odniesienia w ustawodawstwie szczególnym (Ustawa, 1984; Ustawa, 2001). Znacząco przyczynił się do rozwoju koncepcji ochrony prywatności jako dobra osobistego Antoni Kopff (1972), który w swojej publikacji dokonał podziału sfery życia prywatnego na sferę intymnego życia osobistego i sferę prywatnego życia osobistego (Panowicz-Lipska, 2016). Zgodnie z zaprezentowanym podejściem sfera intymnego życia osobistego podlega ścisłej ochronie i nie jest możliwe wnikanie przez osoby trzecie w ten obszar, natomiast sfera prywatnego życia osobistego co do zasady podlega ochronie, ale mogą zaistnieć okoliczności usprawiedliwiające ingerowanie w nią (Kędzierska, i inni, 2015). Podobny pogląd jest wyrażany przez judykaturę. Pierwszym przełomowym orzeczeniem w tej materii był wyrok SN (1984), zgodnie z którym: „otwarty katalog dóbr osobistych (art.

23 i art. 24 KC) pozwala na włączenie do ich zakresu dóbr, które spełniają wszystkie wymagania odnoszące się do pojęcia dobra osobistego według obowiązującego prawa, a które są związane ze sferą życia prywatnego, rodzinnego, sferą intymności. Ochrona w tym zakresie może odnosić się do wypadków ujawniania faktów z życia osobistego i rodzinnego, nadużywania uzyskiwanych informacji, zbierania w drodze prywatnych wywiadów informacji i ocen ze sfery intymności, aby je opublikować lub w inny sposób rozgłaszać". Przyjmuje się także, iż prywatność nie ogranicza się do życia rodzinnego i osobistego, ale obejmuje także m.in. dane osobowe i prawo do dysponowania danymi osobowymi (Wyrok, 2014). Zgodnie ze stanowiskiem Trybunału Konstytucyjnego ochrona życia prywatnego, o której mowa w art. 47 Konstytucji RP obejmuje także autonomię informacyjną (art. 51 Konstytucji RP), która oznacza prawo do samodzielnego decydowania o ujawnieniu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeżeli znajdują się one w posiadaniu innych podmiotów (Wyrok, 2002). Można więc wskazać, iż prawo do dysponowania własnymi danymi osobowymi jest szczególną postacią prawa do prywatności (Pyziak-Szafnicka i Księżak, 2014).

Ograniczenie konstytucyjnie chronionej prywatności informacyjnej jednostki, zgodnie z art. 51 ust. 2 Konstytucji RP, przez umożliwienie organom władzy publicznej pozyskiwania, gromadzenia i udostępniania informacji o obywatelach, dopuszczalne jest wyłącznie w takim zakresie, w jakim jest to niezbędne w demokratycznym państwie prawnym (Barta i Fajgielski, 2015). W związku z powyższym w każdym przypadku wykorzystanie informacji stanowiących dane osobowe, musi nosić cechy niezbędności charakterystycznej dla demokratycznego państwa prawnego (Barta, Fajgielski, 2015).

Dane osobowe

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych określa zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych (Ustawa, 1997). Wskazana ustawa stanowi realizację norm konstytucyjnych odnoszących się do ochrony danych osobowych (Krasuski, 2012). Pierwszą definicją danych osobowych o charakterze definicji legalnej była definicja z art. 6 Ochr. Dan. Os., zgodnie z którą za dane osobowe należy uznać wszelkie informacje odnoszące się do oznaczonej lub możliwej do oznaczenia osoby fizycznej (Ustawa, 1997). Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Wskazana definicja danych osobowych nawiązuje do definicji tego pojęcia zawartej w art. 2 lit. a dyrektywy 95/46/WE (Dyrektywa, 1995)[1].

1 Dyrektywa w swoim słowniczku stanowi, iż pojęcie „dane osobowe" oznacza wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość.

Należy wspomnieć w tym miejscu o istnieniu legalnej definicji danych osobowych, gdzie ustawodawca wskazał zamknięty katalog informacji, które należy uznać za dane osobowe. Zgodnie z art. 2 pkt 33 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych (Ustawa o funduszach inwestycyjnych, 2004) danymi osobowymi są: imiona i nazwisko, data i miejsce urodzenia, adres zamieszkania, a w przypadku obywateli Rzeczypospolitej Polskiej także numer PESEL. Definicja ta jest zgodna z definicją z art. 6 Ochr. Dan. Os. (Ustawa, 1997) przed jego nowelizacją w 2004 r. (Ustawa, 2004). W pierwotnym brzmieniu wskazanego przepisu ustawa za dane osobowe uznawała „każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby", zarzucano jej jednak, że była niezgodna z dyrektywą 95/46/WE (Dyrektywa, 2005) ponieważ za dane osobowe uznawała wyłącznie tzw. dane identyfikacyjne (Sibiga, 2003; Wyrok NSA, 2000)[2]. Obecnie przepisy obowiązujące w polskim porządku prawnym należy interpretować w kontekście prawa unijnego, dlatego też ustalając definicję danych osobowych na gruncie ustawy o funduszach inwestycyjnych należy sięgnąć do wyżej wskazanej dyrektywy 95/46/WE (Kowalik-Bańczyk, 2000).

W kontekście tak szerokiej definicji danych osobowych wskazać należy po pierwsze, iż każda informacja, niezależnie od sposobu i formy jej wyrażenia może podlegać ocenie z punktu widzenia pojęcia danych osobowych i zostać uznana za informację o charakterze osobowym (Barta i Litwiński, 2016). Informacja taka nie musi być ani powszechnie zrozumiała (Sibiga, 2003), ani prawdziwa (Barta i Fajgiel, 2015), a status danych osobowych może zostać przyznany wszelkim informacjom odnoszącym się do osoby fizycznej, w tym danym o charakterze ekonomicznym, odnoszącym się m.in. do życia zawodowego (Dammann, Simitis, 1999). Po drugie, możliwość uznania informacji za należącą do katalogu danych osobowych stanowi możliwość powiązania tych informacji ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Ustawodawca wprost wskazuje kim jest osoba możliwa do zidentyfikowania, natomiast za osobę zidentyfikowaną należy uznać taką osobę, której tożsamość jest znana administratorowi danych, w związku z czym, administrator danych powinien mieć obiektywną możliwość powiązania konkretnej informacji z konkretną osobą, bez konieczności podejmowania jakichkolwiek innych działań, składających się na proces ustalania tożsamości (Barta, Litwiński, 2016). Co więcej, o tym, czy określona informacja ma charakter danych osobowych, czy też nie, decyduje jej przydatność do ustalenia tożsamości osoby, której ta informacja dotyczy nie można więc uznać, że zawsze konkretna informacja dotycząca konkretnej osoby jest informacją pozwalającą na ustalenie tożsamości tej osoby (Szewc, 1999; Barta, Litwiński, 2016).

Pewnego rodzaju wskazówkę interpretacyjną w tym zakresie stanowi ust. 3 art.6 Ochr. Dan. Os., który nakazuje, żeby informacje nie były uznawane za umożliwiające określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań (Ustawa, 1997). Jak wskazuje się w rekomendacji Komitetu Ministrów Rady Europy (Rekomendacja, 1997) w dobie rozwoju technik komputerowych, kryterium kosztów traci na znaczeniu jako kryterium pozwalające na ustalenie, czy osoba fizyczna jest możliwa do zidentyfikowania. Ustalenie, czy mamy do czynienia z nadmiernymi kosztami, czasem lub działaniami, powinno być każdorazowo dokonywane

2 W omawianym wyroku Naczelny Sąd Administracyjny uznał, że przedmiotem ochrony ustawy „nie są wszystkie dane o osobach fizycznych lecz jedynie tzw. dane identyfikujące, a więc imię, nazwisko, adres, PESEL, NIP, itp.".

z uwzględnieniem specyfiki konkretnego administratora danych osobowych – może się więc zdarzyć, że ta sama informacja, która dla jednego podmiotu może być wystarczająca do szybkiego ustalenia tożsamości osoby, której dotyczy, dla innego podmiotu wiąże się z działaniami nieproporcjonalnymi (Sibiga, 2003).

Ustawa wyróżnia podział na dwa rodzaje danych osobowych, który jest związany z przesłankami dopuszczalności przetwarzania danych osobowych. Są to dane osobowe zwykłe oraz dane szczególnie chronione, czyli tzw. dane wrażliwe.

Istnieje szereg informacji, które są szczególnie ważne dla ochrony prywatności każdego człowieka. Stąd też nazywa się je danymi wrażliwymi. Zgodnie z przepisem art. 27 ust. 1 Ochr. Dan. Os., danymi szczególnie chronionymi są informacje: o pochodzeniu rasowym lub etnicznym; o poglądach politycznych, przekonaniach religijnych lub filozoficznych; o przynależności wyznaniowej, partyjnej lub związkowej; o stanie zdrowia; o kodzie genetycznym; o nałogach; o życiu seksualnym oraz informacje dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (Ustawa, 1997). Wymienione przez ustawodawcę rodzaje informacji stanowiących dane wrażliwe należą do zamkniętego katalogu. W związku z tak wskazaną regulacją za tzw. dane osobowe zwykłe należy uznać wszystkie te dane, które nie zostały uznane za dane wrażliwe. W związku z tym, wskazany podział obejmuje wszystkie kategorie danych osobowych, a więc stanowi on podział zupełny. Rozróżnienie danych, wrażliwych a zwykłych jest zwykle bardzo trudne i zależne od kontekstu w jakim tych pojęć używamy. Podział ten ma również niebagatelne znaczenie w kontekście przetwarzania danych osobowych, gdyż inne zasady ustawodawca wprowadził dla danych osobowych zwykłych, a inne dla danych wrażliwych.

Zgodnie ze słowniczkiem pojęć z art. 7 Ochr. Dan. Os. przez przetwarzanie danych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych (Ustawa, 1997). Ustawodawca przewidział inne zasady w odniesieniu do przetwarzania danych zwykłych i wrażliwych.

Przetwarzanie danych osobowych zwykłych jest zgodnie z prawem jedynie wtedy, gdy wystąpi jedna z przesłanek z art. 23 Ochr. Dan. Os. tj. osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych; jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (Ustawa, 1997).

Natomiast przetwarzanie danych wrażliwych jest generalnie zakazane, ustawodawca dopuścił jednak sytuacje kiedy zakaz ten zostaje wyłączony. Podstawową przesłanką uchylającą zakaz przetwarzania danych sensytywnych jest wyrażenie pisemnej zgody przez osobę, której te dane dotyczą (Ustawa, 1997). Istnieją także

inne przesłanki, których wystąpienie uchyla zakaz przetwarzania danych sensytywnych. Określone zostały one w art. 27 ust. 2-10 Ochr. Dan. Os. i zaliczymy do nich sytuacje, kiedy: jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa; jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą; jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (Ustawa, 1997).

Zgodnie z art. 3 w zw. z art. 2 Ochr. Dan. Os. wszystkie dane osobowe przetwarzane przez szkołę w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych oraz w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych podlegają ochronie na zasadach określonych we wskazanej ustawie (Ustawa, 1997). W szkołach i placówkach oświatowych gromadzone są przede wszystkim dane osobowe nauczycieli i innych pracowników szkoły, uczniów a także rodziców bądź opiekunów prawnych.

Dziennik elektroniczny

Zakres informacji o uczniach, które mogą być gromadzone przez szkoły określa rozporządzenie Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Rozporządzenie, 2014) wydane na podstawie ustawy z dnia 7 września 1991 r. o systemie oświaty (Ustawa, 1991). Rozporządzenie to weszło w życie 3 września 2014 r. i uchyliło dotychczasowy akt prawny regulujący te kwestie wprowadzając zmiany m.in. w zakresie informacji gromadzonych w dokumentacji. Natomiast możliwość prowadzenia dzienników lekcyjnych w formie elektronicznej została przewidziana w § 22 niniejszego rozporządzenia, a zatem prowadzenie dziennika elektronicznego jest alternatywą dla dziennika prowadzonego w formie tradycyjnej, papierowej.

Zakres informacji jakie mogą być gromadzone w e-dzienniku określa §10 rozporządzenia (Rozporządzenie, 2014). I tak, obok takich danych jak imię, nazwisko ucznia, data i miejsce jego urodzenia, adres zamieszkania, imiona i nazwiska jego rodziców oraz ich adresy (jeżeli są różne od adresu zamieszkania ucznia), imiona i nazwiska poszczególnych nauczycieli, plan zajęć edukacyjnych, obecności, tematy zajęć, oceny oraz liczba godzin usprawiedliwionych i nieusprawiedliwionych, można także zamieścić numer telefonu oraz adres e-mail rodziców (opiekunów prawnych). Taka regulacja oznacza, że szkoła posiada podstawę prawną do przetwarzania tych, wskazanych w przepisie, danych osobowych i nie jest już konieczne pozyskiwanie zgody zainteresowanych w tym zakresie.

Zgodnie z art. 7 Ochr. Dan. Os. to administrator danych decyduje o celach i środkach przetwarzania danych osobowych, w przypadku szkoły jest to dyrektor (Ustawa, 1997). W związku z powyższym nie ma prawnych możliwości, aby inny podmiot stał się administratorem tych danych i szkoła nie może korzystać z usług dostawcy,

który oczekuje od szkoły przekazania danych osobowych zgromadzonych w dzienniku lub rezerwuje sobie prawo do ich przetwarzania w celach innych niż wynikające z prowadzenia dziennika elektronicznego.

Większość zbiorów danych osobowych musi być zgłoszona do zarejestrowania w ewidencji prowadzonej przez Generalnego Inspektora Ochrony Danych Osobowych. Natomiast w związku z regulacją art. 43 Ochr. Dan. Os., który określa listę zbiorów, których administratorzy są zwolnieni z obowiązku zgłoszenia zbioru do rejestracji, szkoła jest zwolniona z obowiązku rejestracji zbioru dziennika elektronicznego, a także wszystkich innych zbiorów dotyczących osób zatrudnionych i uczących się, bez względu na formę prowadzenia tego zbioru, elektroniczną lub papierową (Ustawa, 1997).

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, ponadto administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz użyte środki, o których mowa powyżej (Ustawa, 1997).

Szkoła może korzystać z usług podmiotów świadczących usługę dziennika elektronicznego i przechowujących dane na serwerach zlokalizowanych poza terenem szkoły na podstawie art. 31 Ochr. Dan. Os. (Ustawa, 1997), przy czym muszą zostać spełnione następujące warunki, po pierwsze, umowa świadczenia usługi dziennika elektronicznego pomiędzy szkołą, a dostawcą musi mieć formę pisemną. Po drugie, w umowie takiej należy dokładnie wskazać m.in. podmiot, któremu dane są powierzane (operatora systemu informatycznego, w którym prowadzony jest e-dziennik), zakres powierzanych danych, cel ich powierzenia. Zakres i cel przetwarzania danych musi być związany ze świadczeniem usługi dziennika elektronicznego i nie może być rozszerzany samodzielnie przez dostawcę. Podmiot przyjmujący dane w powierzenie powinien złożyć oświadczenie o przestrzeganiu obowiązujących przepisów z zakresu danych osobowych oraz że przetwarzanie danych będzie odbywało się wyłącznie we wskazanym zakresie i w celu.

W związku z powyższym faktycznie zabezpieczenia realizowane będą przez podmiot obsługujący system informatyczny e-dziennika, nie staje się on jednak administratorem danych osobowych. W takim przypadku to na dyrektorze szkoły, jako administratorze danych, spoczywa odpowiedzialność za właściwe prowadzenie i przechowywanie dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz za wydawanie przez szkołę dokumentów zgodnych z posiadaną dokumentacją. Nie wyłącza to jednak odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Prowadzenie dziennika elektronicznego jest obwarowane specjalnymi wymaganiami polegającymi m.in. na obowiązku: zachowania selektywności dostępu do danych stanowiących dziennik elektroniczny; zabezpieczenia danych stanowiących dziennik elektroniczny przed dostępem osób nieuprawnionych; zabezpieczenia danych stanowiących dziennik elektroniczny przed zniszczeniem, uszkodzeniem lub utratą; rejestrowania historii zmian i ich autorów; umożliwienia bezpłatnego wglądu

rodzicom do dziennika elektronicznego, w zakresie dotyczącym ich dzieci (Rozporządzenie, 2014). To dyrektor szkoły decyduje jaki zakres gromadzonych danych zostanie udostępniony rodzicom (opiekunom prawnym) uczniów, a decyzja ta powinna w równym stopniu obejmować wszystkich rodziców i określać jednakowe warunki korzystania z e-dziennika oraz uniemożliwiać użytkownikom przenoszenia danych osobowych znajdujących się w dzienniku elektronicznym na komputery osobiste. Co więcej, art. 32 Ochr. Dan. Os. przewiduje co prawda katalog sytuacji, kiedy osoba, której dane dotyczą może wnieść sprzeciw wobec przetwarzania danych osobowych, ale żadna z opisanych sytuacji nie ma zastosowania w przypadku prowadzenia dokumentacji przez szkoły, co jest jej ustawowym obowiązkiem (Ustawa, 1997).

Ustawodawca nałożył obowiązek na dyrektora szkoły do wprowadzania takich e-dzienników, które zapewnią dostęp do danych dziecka jedynie jego prawnym opiekunom (Rozporządzenie, 2014). Nie ma więc możliwości przeglądania konta danego ucznia przez osoby nieuprawnione. Ponadto e-dzienniki muszą zapewniać ochronę danych przed wykasowaniem, kradzieżą lub utratą w inny sposób, a dodatkowo każdy system musi umożliwiać rejestrację historii zdarzeń, tzn. każda zmiana danych musi być rejestrowana wraz z informacją, kto tej zmiany dokonał (Rozporządzenie, 2014).

Podsumowanie

Prowadzenie e-dziennika wymaga zachowania selektywności dostępu do danych w nim przetwarzanych. Dostęp do e-dziennika oprócz nauczycieli mogą mieć również rodzice (opiekunowie prawni), jak i sami uczniowie – w zakresie ustalonym przez dyrektora szkoły.

Czy opiekunowie prawni (rodzice) osób pełnoletnich powinni mieć dostęp do dziennika elektronicznego i danych w nim zawartych? Zasadniczo, zgodnie z brzmieniem cytowanego wcześniej rozporządzenia, dyrektor szkoły ma obowiązek umożliwienia bezpłatnego wglądu rodzicom do dziennika elektronicznego w zakresie dotyczącym ich dzieci (Rozporządzenie, 2014). Żaden przepis prawa, z kolei, nie reguluje zagadnienia czy uczniowie pełnoletni powinni być traktowani jak nieletni, tj. jak „dzieci", dlatego też mamy tu do czynienia z luką w prawie. Z pozoru wydaje się to problem błahy i nieistotny i faktycznie taki będzie w przypadku braku konfliktu między rodzicem (opiekunem prawnym), a uczniem. Poprzez konflikt mam tu na myśli całkowite, zupełne zerwanie więzi, jakie zazwyczaj kształtują się pomiędzy członkami bliskiej rodziny. Może dojść do sytuacji kiedy pełnoletni uczeń nie będzie chciał aby jego rodzic miał wgląd do e- dziennika ponieważ znajdują się tam informacje wrażliwe, takie jak choćby adres zamieszkania czy przebywanie na L4 (w szczególności w sytuacjach patologicznych). Zdaje się, że każdy będąc osobą dorosłą, posiadający pełną zdolność do czynności prawnych, powinien mieć prawo decydować o tym kto ma dostęp do powzięcia wiadomości na jego temat. W związku z powyższym wydaje się kwestią bardzo istotną uregulowanie prawne w tym zakresie tak, aby nie było żadnych wątpliwości, jakie założenia miał ustawodawca regulując możliwość bezpłatnego wglądu rodzicom do dziennika elektronicznego.

Wprowadzenie dzienników elektronicznych jest symbolem tworzenia nowoczesnej polskiej szkoły, aby ulepszyć, uprościć i przyspieszyć kontakt m.in. między nauczycielami, a rodzicami uczniów. Coraz więcej placówek oświatowo-wychowaw-

czych decyduje się na korzystanie z e-dzienników gdyż jest to rozwiązanie niezwykle wygodne, ale też nie wolne od niebezpieczeństw zwłaszcza w zakresie ochrony danych osobowych i bezpiecznym ich przetwarzaniem. Nie ulega bowiem wątpliwości, że w dziennikach elektronicznych gromadzone są dane osobowe zwykłe jak i wrażliwe, a więc należy zapewnić jak najlepszą ochronę przed ewentualnym dostępem do nich przez osoby trzecie.

Bibliografia

[1] Barta, J., Fajgielski, P., Markiewicz, R. (2015). *Ochrona danych osobowych.* Warszawa: Wolters Kluwer Polska SA.
[2] Barta, P., Litwiński, P. (2016). *Ustawa o ochronie danych osobowych. Komentarz.* Warszawa: C.H. Beck Wydawnictwo Polska.
[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. UE.L Nr 281, str. 31.
[4] Kędzierska, K., Gałach, A., Pietrzak, B., Szustakiewicz, P., Opaliński, B., Lipiński, A., Zołotar, A. (2015). *Dostęp do informacji publicznej a prawo do prywatności.* Warszawa: C.H. Beck Wydawnictwo Polska.
[5] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r., Nr 78, poz. 483 ze zm.
[6] Kopff, A. (1972). *Koncepcja praw do intymności i do prywatności życia osobistego, Studia Cywilistyczne.* Kraków.
[7] Kowalik-Bińczyk, K. (2000). Prowspólnotowa wykładnia prawa polskiego. *Europejski Przegląd Sądowy*, 3, str. 9.
[8] Krasuski, A. (2012). *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy.* Warszawa: Wolters Kluwer Polska SA.
[9] Krzysztofek, M. (2014). *Ochrona danych osobowych w Unii Europejskiej.* Warszawa: Wolters Kluwer Polska SA.
[10] Motyka, K. (2006). *Prawo do prywatności i dylematy współczesnej ochrony praw człowieka: na przykładzie Stanów Zjednoczonych.* Lublin: Oficyna Wydawnicza Verba.
[11] Nazaruk, P. (2013). W: J. Ciszewski, *Kodeks Cywilny. Komentarz.* Warszawa: LexisNexis.
[12] Panowicz-Lipska, J. (2016). W: M. Gutowski, *Kodeks Cywilny, tom I. Komentarz art. 1-449[11].* Warszawa: CH.BECK Wydawnictwo Polska.
[13] Pyziak-Szafnicka, M., Księżak, P. (2014). *Kodeks Cywilny. Część ogólna.* Warszawa: Wolters Kluwer Polska SA.
[14] Rekomendacja Nr R (97) 5 dotycząca ochrony danych medycznych przyjęta przez Komitet Ministrów 13 lutego 1997 r. w trakcie 584 spotkania Delegatów Ministrów, Pobrano z:http://www.giodo.gov.pl/230/id_art/1698/j/pl/.
[15] Rozporządzenie Ministra Edukacji Narodowej z dni 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumntacji, Dz. U. 2014 poz. 1170 ze zm.
[16] Sibiga, G. (2003). *Postępowanie w sprawie ochrony danych osobowych.* Warszawa: Wolters Kluwer Polska SA.
[17] Sobolewski, P. (2013). W: K. Osajda, *Kodeks Cywilny. Komentarz. Tom I. Przepisy wprowadzające, Część ogólna, Własność i inne prawa rzeczowe.* Warszawa: C.H.Beck Wydawnictwo Polska.
[18] Szewc, A. (1999, nr 5). Z problematyki Ochrony danych osobowych, cz.III. *Radca Prawny*, str. 24.
[19] Ulrich, D., Simitis, S. (1999). *EG-Datenschutzrichtlinie.* Kolonia.
[20] Ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe, Dz. U. 2004 nr 33 poz. 285.
[21] Ustawa z dnia 23 kwietnia 1964 r- Kodeks Cywilny, tekst jedn. Dz. U. z 2016 r. poz. 380 ze zm.
[22] Ustawa z dnia 26 stycznia 1984 r.- Prawo prasowe, Dz. U. z 2013 r. poz. 771 ze zm.
[23] Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych, tekst jedn. Dz. U. z 2016r. poz. 1896 ze zm.
[24] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, tekst jedn. Dz. U. z 2016 poz. 922 ze zm.
[25] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, tekst jedn. Dz. U. z 2016 r. poz. 1764 ze zm.
[26] Ustawa z dnia 7 września 1991 r. o systemie oświaty, tekst jedn. Dz. U. z 2016 r. poz. 1943 ze zm.
[27] Wyrok NSA z dnia 17 listopada 2000 r. sygn. akt II SA 1860/00, niepubl.
[28] Wyrok SN z dnia 18 stycznia 1984 r., sygn. akt I CR 400/83, OSNCP, Nr 11, poz. 195 .
[29] Wyrok SN z dnia 24 czerwca 2014 r. sygn. akt I CSK 532/13, OSNC 2015, Nr 5, poz. 61.
[30] Wyrok TK z dnia 20 listopada 2002 r. sygn. akt K 41/02, OTK-A 2002, Nr 6, poz. 83.