

UJAWNIANE DANYCH STUDENTÓW NIELEGALNIE UDOSTĘPNIAJĄCYCH FILMY W SIECI

Problem anonimowości w Internecie oraz naruszania praw własności intelektualnej w sieci wciąż się nasila. Choć jeszcze 5 lat temu, możliwość uzyskania przez podmioty prywatne danych osobowych potencjalnych sprawców przestępstw w Internecie była dużo prostsza, to dziś wywołuje dużo więcej wątpliwości¹.

Należy bowiem zaznaczyć, iż po wejściu w życie ustawy z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw² uchylony został art. 29 i powiązany z nim art. 30 przedmiotowej ustawy, mówiący o możliwości udostępniania danych osobowych w celach innych niż wyłącznie do zbioru danych osobowych podmiotom, które w sposób wiarygodny uzasadniały potrzebę posiadania danych i pod warunkiem, że udostępnianie danych nie będzie naruszać praw i wolności osób, których dane dotyczą. W 2004 r. przepis ten objął swym działaniem także podmioty prywatne³, w konsekwencji stał się on prawną podstawą do udostępniania danych osobowych osobom, których prawa zostały naruszone i które dążyły do uzyskania ochrony na drodze sądowej. W związku z tym, iż coraz powszechniejszym zjawiskiem stała się anonimowość w Internecie, zaczęły pojawiać się problemy z ustaleniem personaliów sprawcy danego czynu i tym samym skierowaniem sprawy do sądu.

Jednak naprzeciw tym problemom wyszedł Generalny Inspektor Danych Osobowych (*dalej jako GODO*), który w tego typu sprawach wskazywał jednoznacznie, iż konieczność określenia w pozwie danych osoby pozwanej jest wystarczającą i wiarygodną potrzebą posiadania danych osobowych⁴. Ponadto taką interpretację potwierdzały sądy administracyjne, podkreślając, iż udostępnienie danych jest możliwe także w momencie, gdy dane te będą podlegać szerszej ochronie niż tej wynikającej z ustawy o ochronie danych osobowych. Naczelny Sąd Administracyjny w wyroku z dnia 5 lutego 2008 r., sygn. akt I OSK 37/07, przyznał nawet, iż z art. 161 ust. 1 zd. 2 ustawy – Prawo telekomunikacyjne wynika, że przetwarzanie danych objętych tajemnicą telekomunikacyjną może odbywać się

¹ Tak P. Litwiński, *Anonimowość w sieci. Zagadnienia udostępniania danych osobowych* [w:] Internet. Prawno-informatyczne problemy sieci, portali i e-usług, G. Szpor, W. Wiewiórowski (red.), Warszawa 2012.

² Dz. U. Nr 229, poz. 1497.

³ Pierwotnie art. 29 ustawy o ochronie danych osobowych stosowano wyłącznie wobec administratorów danych ze sfery prawa publicznego, a sam przepis miał za zadanie realizację prawa obywatela do informacji, por. R. Szałowski, *Ochrona danych osobowych. Komentarz do ustawy z dnia 29 sierpnia 1997 r., Zielona Góra 2000*, s. 112.

⁴ Tak GODO m.in. w decyzji z 9 lutego 2004 r., GI-DEC-DS.-28/04.

na podstawie przesłanek określonych w innych aktach prawnych rangi ustawowej, w tym również na podstawie ustawy o ochronie danych osobowych⁵.

Dzięki takiej wykładni i interpretacji przepisów ustawy o ochronie danych osobowych większość osób, których prawa zostały naruszone w Internecie mogła skutecznie ubiegać się o udostępnienie im danych osobowych podmiotów, które dopuściły się takich czynów. Nie znaczy to jednak, iż dziś jest to niemożliwe. Aktualnie po uchyleniu przedmiotowego art. 29, możliwości udostępniania danych osobowych należy upatrywać w art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych, który wskazuje, iż *„przetwarzania danych jest dopuszczalne (...), gdy 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”*. Istotne w tym zakresie jest także wskazanie na definicję legalną pojęcia przetwarzania danych osobowych, która obejmuje swym zakresem jakiegokolwiek operacje wykonywane na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zamienianie, usuwanie czy właśnie udostępnianie danych. Dzięki temu podmiot prywatny starając się o ujawnienie danych osobowych potencjalnego sprawcy naruszenia jego praw w Internecie, może posłużyć się konstrukcją z art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych.

W związku z powyższym przedmiotowy mechanizm udostępniania danych osobowych znajdzie zastosowanie po spełnieniu kilku przesłanek. W pierwszej kolejności należy wskazać, iż regulacja odnosi się do administratorów danych, w zakresie zarówno podmiotów prywatnych, jak i publicznych⁶. W odniesieniu więc do przedmiotowej sprawy, przepis znajdzie zastosowanie wobec uczelni wyższej, która przetwarza dane osobowe swoich studentów, w związku z udostępnieniem im lokalnej sieci wifi.

Następnie należy wskazać, iż po stronie administratora udostępniającego dane lub podmiotu, który występuje z wnioskiem o udzielenie danych musi istnieć „prawnie usprawiedliwionych cel” ich udostępnienia. Na początku należy zaznaczyć, iż użycia spójnika „lub”, powoduje, że wystarczające będzie istnienie przedmiotowego celu tylko po jednej ze stron, nieuzasadnione byłoby wymaganie istnienia celu w odniesieniu zarówno do administratora danych, jak i podmiotu występującego o udostępnienie danych⁷. W odniesieniu już do samego pojęcia „prawnie usprawiedliwionego celu” w literaturze prawniczej podkreśla

⁵ Stanowisko takie potwierdzał również S. Piątek, Prawo telekomunikacyjne. Komentarz, Warszawa 2005, s. 866.

⁶ Por. szerzej J. Barta, P. Fajgielski, R. Markiewicz, Komentarz do art. 23 ustawy o ochronie danych osobowych [w:] Ochrona danych osobowych. Komenatrz, Warszawa 2011, LEX OMEGA 2015.

⁷ Por. J. Barta, P. Fajgielski, R. Markiewicz, Komentarz do art. 23..., LEX OMEGA 2015.

się, iż przetwarzanie danych osobowych na podstawie art. 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych będzie dopuszczalne w ramach dochodzenia roszczeń w ogólności, nie tylko tych wynikających z prowadzonej działalności gospodarczej⁸. Należy również wskazać, iż pojęcie „prawnie usprawiedliwionego celu” stanowi, co wielokrotnie podkreślał GODO, „zwrot niedookreślony oraz klauzulę generalną w znaczeniu funkcjonalnym. Daje to w szczególności pewnego rodzaju luz decyzyjny, dzięki któremu organ stosujący prawo, może przy podejmowaniu decyzji kierować się ocenami indywidualnymi konkretnej sytuacji, a także pewnymi zasadami postępowania niesformułowanymi w przepisach prawa”⁹.

W niniejszej sprawie przedstawiciele amerykańskich producentów filmowych jako cel udostępnienia danych studentów wskazali wykorzystanie ich do wystąpienia z żądaniem zapłaty odszkodowania za nielegalne udostępnianie filmów, a w razie odmowy – skierowania sprawy na drogę postępowania sądowego (cywilnego). Zgodnie bowiem z przepisami ustawy o prawie autorskim, uprawniony którego autorskie prawa majątkowe zostały naruszone może żądać odszkodowania w wysokości dwukrotności, a czasem nawet i trzykrotności wynagrodzenia, które byłoby należne tytułem zgody na korzystanie z utworu¹⁰. Twórczość autorska objęta jest również ochroną z art. 23 Kodeksu cywilnego i stanowi niezależną podstawę do żądania ochrony w odniesieniu do naruszenia interesów twórców, gdyby okazało się, że ochrona z ustawy o prawie autorskim i prawach pokrewnych nie byłaby wystarczająca. Zgodnie z art. 24 § 2 KC, jeżeli skutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

W konsekwencji należy wskazać, iż niniejszy podmiot wnioskując o udostępnienie danych w celu egzekwowania i dochodzenia swoich praw, w tym na drodze sądowej spełnia warunek prawnie usprawiedliwionego celu. Wskazanie bowiem przesłanki chęci wystąpienia z powództwem, co podkreśla GODO nie może być uznane za naruszenie praw i wolności osób, których dane dotyczą¹¹. Taka interpretację wskazał także Wojewódzki Sąd Administracyjny (dalej WSA) w Warszawie w wyroku z dnia 18 lipca 2014 r.¹², w którym odniósł się do art. 18 ust. 6 ustawy z 2002 r. o świadczeniu usług drogą elektroniczną, który to z kolei wskazuje na obowiązek administratorów danych do udostępniania danych osobowych organom państwa na potrzeby prowadzonych przez nie postępowań. Sędziowie przyznali

⁸ Por. A. Drozd, Ustawa o ochronie danych osobowych. Komentarz. Warszawa 2009, s. 119-121.

⁹ Tak GODO w decyzji z 13 czerwca 2013 r. DOLiS/DEC – 620/13, za: P. Barta, P. Litiwiński, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2009, s. 228.

¹⁰ Art. 79 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90 poz. 631).

¹¹ GODO, Prawnie usprawiedliwiony cel, www.godo.gov.pl [data dostępu: 10.05.2015].

¹² Wyrok WSA w Warszawie z dnia 18 lipca 2014 r., sygn. akt II SA/Wa 569/14, LEX nr 1480902.

jednak, iż „z brzemienia art. 18 ust. 6 ustawy z 2002 r. o świadczeniu usług drogą elektroniczną wynika jedynie obowiązek udzielenia informacji o danych, organom państwa, na potrzeby prowadzonych przez nie postępowań. Nie wynika natomiast zakaz udostępniania tych danych osobom, których prawa zostały naruszone. Zarówno jednak organ nakazujący ujawnienie danych, jak i sąd administracyjny rozpoznający skargę na tego rodzaju decyzję, muszą każdorazowo przy uwzględnieniu indywidualnych okoliczności danej sprawy, dokonać wyważenia przeciwstawnych interesów”. Co więcej „zgodnie z art. 23 ustawy o ochronie danych osobowych, do uzyskania adresu IP nie jest konieczne wystąpienie z powództwem, wystarczy już sam zamiar”.

Jednak i na co zwraca uwagę NSA w wyroku z dnia 21 sierpnia 2012 r., sygn. akt I OSK 166/12: „obecnie obowiązujący stan prawny pozwala na wysnucie wniosku, iż w ramach obowiązującego prawa można domagać się ujawnienia danych, jakie zgromadził administrator serwisu internetowego poprzez stosowanie (...) art. 23 tej ustawy, ale pod pewnymi warunkami. Warunkami tymi są proporcjonalność środków i celów oraz równowaga pomiędzy ochroną różnych dóbr, wolności wypowiedzi i prawa do ochrony dóbr osobistych. Podmiot żądający udostępnienia danych musi swoje stanowisko uzasadnić. Wedle art. 23 ust. 1 pkt 5 muszą to być „prawnie usprawiedliwione cele”¹³.

Odnosząc powyższe twierdzenia na grunt analizowanej sprawy, należy przyznać, iż wyważeniu podlegają tutaj takie dobra jak prawo do ochrony danych osobowych, w tym prawa do prywatności oraz ochrony prawa własności intelektualnej i prawa autorskiego. Przedmiotowy problem był już rozważany na gruncie prawa unijnego. Trybunał Sprawiedliwości Unii Europejskiej w sprawie LSG przeciwko Tele2 (C-557/07) przyznał, iż dyrektywy nie wykluczają nałożenia na dostawców usług internetowych obowiązku ujawnienia danych osobowych użytkowników podejrzanych o naruszenie praw autorskich, tak by umożliwić im wnoszenie do sądów cywilnych powództw. Natomiast linia orzecznicza Trybunału wskazuje, iż państwa są zobligowane do zapewnienia równowagi pomiędzy prawem do prywatności z jednej strony, a ochroną własności intelektualnej z drugiej strony. Oba bowiem te prawa mają swoje źródło w Karcie Praw Podstawowych i oba są objęte ochroną¹⁴. Z drugiej jednak strony należy również wskazać, iż Europejski Trybunał Praw Człowieka w wyroku w sprawie K.U. przeciwko Finlandii zwrócił uwagę na fakt, iż gwarancje prywatności dla użytkowników Internetu nie mogą być absolutne i takich

¹³ www.orzeczenia.nsa.gov.pl [data dostępu: 10.05.2015].

¹⁴ Wyrok Trybunału Sprawiedliwości UE z dnia 19 lutego 2009 r., sygn. akt C-557/07, www.curia.europa.eu [data dostępu: 10.05.2015].

sytuacjach jak zapobieganie przestępczości, czy ochrona praw i wolności innych osób, gwarancje prywatności będą mogły podlegać danym ograniczeniom¹⁵. Właściwe więc wywarzenie ochrony prawa do prywatności z prawem do ochrony praw autorskich i zapobieganie przestępczości w Internecie nie jest łatwe. Natomiast w omawianym przypadku należy również zwrócić uwagę na postulat zapewnienia każdej jednostce prawa do sądu. Uniemożliwienie bowiem poznania danych internautów, skutecznie tamuje konstytucyjne prawo jednostki do dochodzenia swoich praw. Należy bowiem zgodzić się z WSA w Warszawie, który w wyroku z dnia 3 października 2012 r., sygn. akt II SA/Wa 365/12 przyznał, iż *„przyjęcie, że udostępnienie danych osób, wobec których wytoczono powództwo cywilne, miałoby godzić w ich prawo i wolności prowadziłoby do nieuzasadnionej ochrony takich osób, przed ewentualną odpowiedzialnością za swoje działania.”*

Podsumowując powyższe rozważania należy dojść do wniosku, iż podmioty, których prawa zostały naruszone w Internecie powinny mieć prawo do egzekwowania tych praw na drodze sądowej. Jak wskazuje bowiem były już GODO Wojciech Wiewiórowski *„prawo do prywatności nie ma charakteru absolutnego, a jego ochrona nie może odbywać się kosztem braku poszanowania praw innych osób”*¹⁶. Podobnie orzekł NSA w wyroku z dnia 21 lutego 2014 r., przyznając, że *„artykuł 23 ust. 1 pkt 5 ustawy o ochronie danych osobowych dopuszcza ich przetwarzanie, gdy jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów. Takim celem jest między innymi ściganie sprawców przestępstw, również z oskarżenia prywatnego”*¹⁷.

Oceniając z kolei rodzaje danych o jakich udostępnienie wnosili przedstawiciele amerykańskich producentów, należy jednoznacznie stwierdzić, iż ich zakres nie jest adekwatny do celu. Należy bowiem zaznaczyć, iż dla skutecznego wytoczenia powództwa niezbędne jest wniesienie pozwu, który musi czynić zadość warunkom określonym w art. 187 § 1 pkt 1 Kodeksu postępowania cywilnego (*dalej jako KPC*). Zgodnie z dyspozycją przedmiotowego przepisu pozew musi czynić zadość warunkom pisma procesowego. Zgodnie natomiast z art. 126 § 1 pkt 1 KPC, każde pismo procesowe musi zawierać oznaczenie sądu, do którego jest skierowane, a także imię i nazwisko lub nazwę stron oraz ich ustawowych przedstawicieli i pełnomocników. Z kolei zgodnie z art. 126 § 1 2 KPC, gdy pismo procesowe

¹⁵ Wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 grudnia 2008 r., nr skargi 2872/02, hudoc.echr.coe.int [data dostępu: 10.05.2015].

¹⁶ M. Kołtuniak, Ukrycie się pod pseudonimem i wykorzystywanie faktu anonimowości w sieci do naruszania dobrego imienia oraz praw innych osób nie może oznaczać bezkarności, Rzeczpospolita, www.giodo.gov.pl [data dostępu: 11.05.2015].

¹⁷ Wyrok NSA z 21 lutego 2014 r., sygn. akt I OSK 2324/12, Rzeczposp. PCD 2014/46/3.

jest pierwszym pismem w sprawie, powinno także zawierać oznaczenie miejsca zamieszkania lub siedziby stron, ich przedstawicieli ustawowych i pełnomocników oraz przedmiotu sporu zaś dalsze – sygnaturę akt. W konsekwencji należy przyjąć, iż niezbędnymi elementami pozwu, w tym także o naruszenie praw autorskich, jest oznaczenie przyszłych stron procesowych, czyli imion, nazwisk i miejsc zamieszkania¹⁸. Tym samym udostępnianie takich danych jak imię ojca, kierunek studiów, data urodzenia czy też informacja o pobieranym stypendium socjalnym jednoznacznie wykraczają poza zakres wskazanego przez wnioskodawców celu. Z kolei zgodnie zarówno z GODO¹⁹, jak i sądami administracyjnymi, należy przyznać, iż adres IP użytkownika w pewnych sytuacjach należy traktować jako dane osobowe²⁰.

Ustosunkowując się więc zarówno do powyższych rozważań, jak i przedmiotowej sprawy, na pytanie dotyczące czy uczelnia może udostępnić dane studentów dla wskazanego powyżej celu, należałoby odpowiedzieć, że może, jednakże nie musi. Udostępniając bowiem dane administrator naraża się na odpowiedzialność karną (art. 51 ustawy o ochronie danych osobowych). Ponadto ocenianie tego typu spraw jest dość płynną sprawą, na co wskazuje również niejednolita linia orzecznicza sądów, przyznając, że każdą sprawę należy badać indywidualnie. Natomiast w momencie, gdy sprawa trafi do urzędu GODO interesy obu stron zostaną ocenione i właściwie wyważone. W przedmiotowej sprawie GODO będzie mógł zobowiązać uczelnię do udostępnienia danych, korzystając ze swoich uprawnień określonych w art. 18 ust. 1 pkt 2 ustawy, które mówią, iż w przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności m.in. udostępnienie danych osobowych.

¹⁸ Por. decyzja GODO z 5 listopada 2014 r., DOLiS/DEC – 1045/14, www.godo.gov.pl [data dostępu: 11.05.2015].

¹⁹ www.godo.gov.pl [data dostępu: 11.05.2015].

²⁰ Opinia Grupy Roboczej ds. Ochrony Danych, powołanej przez Parlament Europejski i Radę Europejską (rozdz. III pkt 3 przykład 15) uznała adres IP za dane dotyczące osoby możliwej do zidentyfikowania, stwierdzając, że: "dostawcy usług internetowych oraz menedżerowie lokalnych sieci mogą, stosując rozsądne środki, zidentyfikować użytkowników internetu, którym przypisali adresy ip ponieważ systematycznie zapisują w plikach daty, czas trwania oraz dynamiczny adres IP (czyli ulegający zmianie po każdym zalogowaniu) przypisany danej osobie. To samo odnosi się do dostawców usług internetowych, którzy prowadzą rejestr (logbook) na serwerze HTTP Nie ma wątpliwości, że w takich przypadkach można mówić o danych osobowych, w rozumieniu art. 2 Dyrektywy".