



**Wojciech Rafał Wiewiórowski**

*Uniwersytet Gdański*

## OCHRONA PRYWATNOŚCI JAKO OGRANICZENIE PRAWA DO PONOWNEGO PRZETWARZANIA INFORMACJI PUBLICZNEJ

Ponad dziesięcioletnie doświadczenie sądów powszechnych i administracyjnych w zakresie interpretacji ograniczenia dostępu do informacji publicznej ze względu na ochronę prywatności sprawia, że tematyka leżąca na zbiegu art. 61 i 47 Konstytucji RP obrosła znaczącą liczbą opinii doktryny. Jednocześnie nowelizacja ustawy o dostępie do informacji publicznej z dnia 16 września 2011 r.<sup>1</sup>, mająca na celu poprawną implementację do prawa polskiego dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, nie wywołała jak dotąd ponownej dyskusji doktrynalnej. Większość środowiska naukowego, sędziowie oraz – najbardziej zainteresowani sprawą – użytkownicy informacji publicznej, przyjęła milcząco, że wszelkie ograniczenia prawne przy ponownym wykorzystaniu informacji publicznej pojawiają się na etapie dostępu do niej. Prawdą jest to, że same przepisy nowelizowanej ustawy nie przewidują żadnych nowych rozwiązań. Wedle zasad przewidzianych w dyrektywie 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego<sup>2</sup>, jeżeli Państwo decyduje się na ujawnienie informacji z zasobów publicznych, to informacja taka podlega swobodnemu wykorzystaniu w dowolnej formie przez podmioty komercyjne lub niekomercyjne<sup>3</sup>. Takie swobodne przetwarzanie można co prawda w pewnym zakresie ograniczyć prawnie, ale można uczynić to tylko w ustawie i tylko z akceptowalnych – z punktu widzenia dyrektywy – powodów. Należy jednak pamiętać, że kwestia ograniczeń – prawnych i faktycznych – ponownego przetwarzania informacji publicznej ze względu na ochronę prywatności była dyskutowana przez ustawodawcę podczas prac nad nowelizacją. Przyjęto wówczas,

<sup>1</sup> Dz.U. Nr 204, poz. 1195.

<sup>2</sup> Dz.U. L 345 z dnia 31 grudnia 2003 r., s. 90.

<sup>3</sup> M.Groń, *Unia informacji*, „IT w Administracji” 2011, nr 11.

że uzupełnianie rządowego projektu ustawy o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw o jakiegokolwiek postanowienia dotyczące ochrony prywatności przy ponownym wykorzystaniu informacji publicznej nie jest konieczne, jako że zasady te wynikają wprost z innego obowiązującego aktu prawnego – ustawy o ochronie danych osobowych – którego stosowania w żaden sposób nie ograniczają nowe przepisy.

Podczas prac sejmowych nad zmianą ustawy o dostępie do informacji publicznej podkreślano, że informacja publiczna w rozumieniu ustawy zawarta jest nie tylko w klasycznych dokumentach urzędowych lub dokumentach informacyjnych przekazywanych przez podmioty zobowiązane do udzielenia informacji publicznej, ale również w prowadzonych przez nie rejestrach publicznych<sup>4</sup>. Za słuszny należy uznać pogląd, że dane z rejestrów publicznych stanowią informację publiczną. Są bowiem informacją sektora publicznego w rozumieniu dyrektywy, a polska ustawa nie zróżnicowała pojęć „informacja sektora publicznego” oraz „informacja publiczna”. Jeśli zaś dane rejestrowe są informacją publiczną, to mogą być ponownie wykorzystane, o ile jawność formalna rejestru nie została ograniczona. Pamiętając, że definicje rejestru publicznego i dokumentu elektronicznego zawarte w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne<sup>5</sup> są bardzo szerokie, należy mieć świadomość, że dane osobowe z rejestrów publicznych będą łączone przykładowo, obejmując także:

- dane z ksiąg wieczystych ujawniane w systemach teleinformatycznych<sup>6</sup>;
- dane z Krajowego Rejestru Sądowego ujawniane w systemach teleinformatycznych<sup>7</sup>;
- dane z dowolnych rejestrów publicznych, w których ujawniono obiekty przestrzenne (w rozumieniu ustawy z dnia 4 marca 2010 r. o infrastrukturze informacji przestrzennej)<sup>8</sup>;
- dane dotyczące sprawy zagospodarowania przestrzennego prezentowane dla celów tworzenia miejscowych planów zagospodarowania przestrzennego;
- dane z Centralnej Ewidencji i Informacji o Działalności Gospodarczej;

<sup>4</sup> O zakresie danych przetwarzanych przez administrację publiczną i stanowiących informację publiczną najszerszej pisali w ostatnich latach P. Fajgielski, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Presscom, Wrocław 2007, s. 33–62 oraz 74–112 oraz A. Pawłowska, *Zasoby informacyjne w administracji publicznej w Polsce. Problemy zarządzania*, Wyd. UMCS, Lublin 2002.

<sup>5</sup> Dz. U. Nr 64, poz. 565 ze zm.

<sup>6</sup> A. Gryszczyńska, *Nowa Księga Wieczysta. Informatyzacja rejestru publicznego*, LexisNexis, Warszawa 2012, s. 226–282; A. Stefańska, *Elektroniczna księga wieczysta*, LexisNexis, Warszawa 2011, s. 115–141 oraz A. Gryszczyńska, *Elektroniczny dostęp do Nowej Księgi Wieczystej i Krajowego Rejestru Sądowego*, [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, C.H. Beck, Warszawa 2012, s. 289–304.

<sup>7</sup> A. Gryszczyńska, *Elektroniczny dostęp...*, s. 296–300.

<sup>8</sup> A. Gryszczyńska, *Nowa Księga Wieczysta...*, s. 115–171.

- dane z krajowych rejestrów urzędowych w rozumieniu przepisów o statystyce publicznej (REGON, TERYT);
- publicznie dostępne dane z ofert przygotowanych na podstawie przepisów o handlu wierzytelnościami<sup>9</sup>;
- rejestry zawodowe<sup>10</sup>;
- oświadczenia majątkowe składane przez urzędników publicznych i członków władz publicznych oraz
- pozostające w gestii danego podmiotu dane przetwarzane z zachowaniem odpowiednich podstaw prawnych a dotyczące jego klientów lub potencjalnych klientów.

Nie ma wątpliwości, że informacja publiczna będzie tym samym wykorzystywana – z użyciem nowej podstawy prawnej formułowanej w prawie do ponownego wykorzystania informacji publicznej – do tworzenia profilu osobowego osoby fizycznej<sup>11</sup>, czyli „automatycznej techniki przetwarzania danych polegającej na przypisaniu danej osobie «profilu» w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji zachowań i postaw”<sup>12</sup>. Co więcej, takie profile będą miały także charakter tzw. „profilu predykcyjnych” (tworzonych w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności poprzez uzupełnianie informacji publicznej o monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które klika), jak i tzw. „profilu jawnych” (tworzonych na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą)<sup>13</sup>.

W tej sytuacji niezbędne jest wykorzystanie mechanizmów prawnych wynikających z ustawy o ochronie danych osobowych<sup>14</sup>. Wśród nich szczególną rolę odgrywać powinien obowiązek informacyjny. Należy bowiem przyjąć, że tworzenie profilu osobowego na podstawie danych pobieranych z różnych rejestrów

<sup>9</sup> B. Bińkowska-Artowicz, *Obrót informacją o zobowiązaniach finansowych dłużnika jako element gospodarki opartej na wiedzy*, „Czas Informacji” 2011, nr 4, s. 15–23.

<sup>10</sup> Zob. np. B. Michalak, *Zakres i jawność rejestrów lekarskich*, [w:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, red. G. Szpor, W. Wiewiórowski, C.H.Beck, Warszawa 2012, s. 341.

<sup>11</sup> W.R. Wiewiórowski, *Personal Profiling Based on Generally Accessible Data*, „International Journal on Information Technology and Security” 2012, nr 3, s. 31–46 oraz tenże, *Profilowanie osób na podstawie ogólnodostępnych danych*, [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, Warszawa 2013.

<sup>12</sup> Opinia Grupy art. 29 nr 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta dnia 22 czerwca 2010 r., pkt 2.3., s. 8.

<sup>13</sup> Tamże.

<sup>14</sup> Bardzo ciekawe opracowanie problematyki zbieżnego i komplementarnego rozwoju prawa ochrony prywatności i prawa dostępu do informacji publicznej przygotował I. Szekely, *Freedom of Information Versus Privacy. Friends Or Foes*, [w:] *Reinventing Data Protection?*, S. Gutwirth, Y.Poullet, P. De Hert, C. de Terwangne, S.Nouwet [eds.], Springer 2009, s. 293–316. Zob. również: F. Schoch, *Zagadnienie równowagi pomiędzy wolnością informacyjną a ochroną danych osobowych w niemieckim profesorskim projekcie kodeksu Informacyjnego*, [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. Szpor, C.Beck, Warszawa 2011, s. 16–36.

publicznych powinno być rozumiane jako przetwarzanie nowej informacji lub przetwarzanie w nowym celu<sup>15</sup>. Na szczególną rolę wypełnienia obowiązku informacyjnego w działaniach podmiotów (komercyjnych i niekomercyjnych) polegających na tworzeniu profili przy wykorzystaniu ponownie przetwarzanej informacji publicznej, zwrócono uwagę w Rekomendacji CM/Rec (2010) 13 Komitetu Ministrów państw członkowskich Rady Europy w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych podczas tworzenia profili<sup>16</sup>.

Rada Europy podkreśliła, że technologie informacyjne i komunikacyjne pozwalają na zbieranie na wielką skalę danych, w tym danych osobowych, zarówno w sektorze publicznym jak i prywatnym. Są one wykorzystywane dla wielu celów, w tym do świadczenia usług powszechnie akceptowanych i cenionych przez społeczeństwo, konsumentów i gospodarkę. Jednocześnie szczególną uwagę organy ochrony praw człowieka powinny zwrócić na uzupełnianie informacji publicznej zawierającej dane osobowe o zbierane w różnych sytuacjach i dla różnych celów dane dotyczące ruchu, zapytania internautów, nawyki konsumenckie, dane o aktywności, stylu życia i zachowaniu użytkowników urządzeń telekomunikacyjnych, w tym dane geolokalizacyjne oraz dane pochodzące w szczególności z portali społecznościowych, systemów wideonadzoru, systemów biometrycznych oraz systemów identyfikacji za pomocą fal radiowych (RFID), „*smart meteringu*” i „Internetu przedmiotów”. Tworzenie profili może być bowiem prowadzone w uprawnionym interesie zarówno podmiotu wykorzystującego ponownie informację publiczną jak i osoby, której są przypisywane, np. jeśli stosuje się je dla poprawy segmentacji rynku, analizy ryzyka, wykrywania oszustw czy dostosowywania oferty świadczonych usług do popytu, oraz że z tego względu może ono przynieść korzyści użytkownikom, gospodarce i całemu społeczeństwu. Jednocześnie takie działanie może narazić osobę fizyczną na szczególnie wysokie ryzyko dyskryminacji i ataków na ich prawa osobiste i godność a tworzenie profili dzieci może mieć dla nich poważne konsekwencje przez całe ich życie, a nie są one zdolne samodzielnie udzielić dobrowolnej, świadomej i wyraźnej zgody na zebranie ich danych osobowych dla celów profilowania<sup>17</sup>.

Pożądane jest tym samym monitorowanie stosowania zasad ponownego wykorzystania informacji publicznej w takim zakresie, w jakim obejmuje ona dane osobowe (bądź dane, które po powiązaniu z danymi posiadanymi przez ponow-

<sup>15</sup> O paradoksie „nietransparentności” przetwarzania dla potrzeb „transparentności” pisze M. Hildebrandt, *Who is Profiling Who? Invisible Visibility*, [w:] *Reinventing Data...*, S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, S. Nouwt (eds.), s. 239–252.

<sup>16</sup> Rekomendacja przyjęta przez Komitet Ministrów Rady Europy w dniu 23 listopada 2010 r. podczas 1099 posiedzenia wiceministrów, <https://wcd.coe.int/wcd/ViewDoc.jsp?id=1710949&Site=CM>.

<sup>17</sup> O uzupełniającej się roli przepisów o ochroni danych osobowych i przepisów antydyskryminacyjnych piszą W. Schreurs, M. Hildebrandt, E. Kindt, M. Vanfleteren, *Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector*, [w:] *Profiling the European Citizen. Cross-Disciplinary Perspectives*, M. Hildebrandt, S. Gutwirth (eds.), Springer 2008, s. 241–270.

nie wykorzystującego stają się danymi osobowymi) w odniesieniu do ochrony danych osobowych, które pozwoli na ochronę podstawowych praw i wolności obywateli, w szczególności prawa do prywatności oraz do zapobiegania dyskryminacji ze względu na płeć, pochodzenie etniczne i rasowe, wyznanie i przekonania, niepełnosprawność, wiek czy orientację seksualną.

Z punktu widzenia ochrony danych osobowych oznacza to m.in., że:

- każda osoba powinna być informowana, że jej dane osobowe uzyskane przy korzystaniu z prawa do informacji publicznej są ponownie wykorzystywane na zasadach określonych w omawianej ustawie;
- każdej osobie winno przysługiwać prawo dostępu do jej danych;
- każda osoba powinna znać zasady kierujące danym sposobem ponownego wykorzystania informacji publicznej.

Należy jednak pamiętać, że ochrona godności ludzkiej i innych podstawowych praw i wolności w odniesieniu do profilowania może być skuteczna tylko i wyłącznie wtedy, gdy wszystkie zainteresowane strony współpracują podczas tworzenia profili osób w sposób rzetelny i zgodny z prawem. Należy promować mechanizmy samoregulacji, takie jak kodeksy postępowania zapewniające poszanowanie danych osobowych i prywatności oraz do wdrażania technologii opisanych w wyżej wymienionej rekomendacji<sup>18</sup>.

Osoby, których dane dotyczą, winny mieć możliwość, w zależności od potrzeb, bezpiecznego poprawiania, usuwania lub blokowania własnych danych osobowych, w przypadku gdy profilowanie związane z przetwarzaniem danych osobowych wykonywane jest niezgodnie z przepisami prawa<sup>19</sup>.

Już przed uchwaleniem ustawy o informatyzacji doktryna prawa wskazywała, że rejestrem jest zbiór informacji o osobach, rzeczach lub prawach, utworzony na podstawie przepisów prawa (tj. przepisy przynajmniej przewidują jego utworzenie), prowadzony przez organ rejestrowy o charakterze publicznym, gdzie przyjęcie, utrwalenie, a następnie ujawnienie określonych w nim informacji co do zasady następuje w drodze decyzji, a prowadzenie rejestru i ujawnianie zawartych w nim danych rodzi skutki prawne zarówno dla osoby, której wpis dotyczy, jak i dla organu. Doktryna prawa uznaje również, że rejestr publiczny

<sup>18</sup> Należy jednak pamiętać, że samoregulacja nigdy nie obejmie wszystkich podmiotów przetwarzających ponownie informację publiczną. Charakterystyczną cechą prawa do informacji publicznej – a tym samym jej ponownego przetwarzania jest – powszechność, co oznacza, że krąg „ponownie przetwarzających” jest praktycznie niezamknięty. Zob.: D. Fleszer, *Zasada powszechności prawa do informacji publicznej*, „Czas Informacji” 2011, nr 1, s. 30–39.

<sup>19</sup> O sposobach ustalania równowagi pomiędzy prawem do informacji a prawem do prywatności pisze na podstawie wiodących orzeczeń Trybunału Konstytucyjnego i NSA K. Tarnacka, *Prawo do informacji w polskim prawie konstytucyjnym*, Wyd. Sejmowe, Warszawa 2009, s. 276–284. Nieco inne stanowisko w tej sprawie wyrażał J. Kochanowski, *Dostęp do informacji publicznej jako gwarancja ochrony praw człowieka i obywatela*, [w:] *Dostęp do informacji publicznej – rozwój czy stagnacja. Materiały z konferencji zorganizowanej 6 czerwca 2006 r. w Warszawie przez INP PAN, NSA i RPO, NSA*, Warszawa 2008, s. 17.

powinien być z zasady jawny, chyba że przepisy prawa wyraźnie taką jawność wykluczają lub ograniczają<sup>20</sup>.

Podmioty publiczne w wykonaniu przepisów ustawowych prowadzą obecnie ok. 270 zbiorów ewidencyjnych, które są rejestrami publicznymi w rozumieniu art. 3 pkt 5 ustawy o informatyzacji. Ich podstawę prawną stanowi ponad 150 ustaw i ponad 150 rozporządzeń<sup>21</sup>.

Należy pamiętać, że zasady dostępu do informacji publicznej i jej ponownego wykorzystywania odnoszą się do uzyskania informacji publicznej z jawnych rejestrów publicznych – w szczególności z rejestrów zawierających dane referencyjne dla infrastruktury informacyjnej państwa. Szczególne znaczenie dla polskiego organu ochrony danych ma ponowne wykorzystanie informacji publicznej zawierającej dane osobowe. Przy poprawnie zbudowanej infrastrukturze informacyjnej państwa dane referencyjne zgromadzone są tylko w rejestrze (np. w księgach wieczystych czy w zintegrowanym systemie informacji o nieruchomości, łączącym informacje z ksiąg wieczystych i z ewidencji gruntów i budynków), który można nazwać referencyjnym i dane takie nie są powielane w innych rejestrach, a co najwyżej uzupełniane o dane specyficzne dla owego rejestru pochodnego. To powoduje, że stworzenie zintegrowanego systemu informacji o nieruchomościach (nad czym pracuje minister właściwy ds. administracji wspólnie z ministrem właściwym ds. sprawiedliwości) wprowadziłoby zupełnie nową jakość co do zakresu informacji poddanej ponownemu wykorzystaniu.

Dyskutując nad informacją publiczną, którą stanowi dana lub dane przechowywane w zasobach infrastruktury informacyjnej państwa, trzeba podkreślić, że wyjątkowo często pojawiającym się błędem jest zamienne stosowanie pojęć „danych” i „informacji” w odniesieniu do baz danych. O ile w wielu dziedzinach wiedzy można utożsamiać posiadanie danych z posiadaniem informacji, o tyle w informatyce pojęcia te – choć bliskoznaczne – nigdy nie stanowią synonimów. Dane są wartościami przechowywanymi w bazie, rozumianymi wręcz jako wartości danego pola. Informacjami są zaś takie dane, które zostały przetworzone w sposób uwidaczniający ich znaczenie i tym samym czyniący je użytecznymi. By odwołać się do pojęć z teorii informacji, dane będą odpowiednikiem pojęcia informacji w znaczeniu komunikatu na poziomie formalnym, zaś informacja będzie odpowiednikiem pojęcia komunikatu w znaczeniu semantycznym. Informacją jest każdy czynnik zmniejszający entropię.

<sup>20</sup> T. Stawecki, *Rejestry publiczne. Funkcje instytucji*, LexisNexis, Warszawa 2005, s. 124–136.

<sup>21</sup> Najnowsze całościowe opracowanie tego problemu można znaleźć w pracy: *Systemy informacyjne administracji publicznej. Źródła danych dla badań statystyki publicznej*. Część 1, Główny Urząd Statystyczny 2011 (427 systemów). Warto również odesłać do – obejmującego 268 aktów prawnych – opracowania D. Chromicka, *Aneks. Dane identyfikujące w rejestrach publicznych w Polsce (stan prawny na dzień 1 maja 2008 r.)* [w:] G. Szpor et al., *Diagnoza barier technologiczno-prawnych w zakresie informatyzacji lokalnej i regionalnej administracji samorządowej i ich wpływ na zdolność wykonywania zadań publicznych oraz rekomendacje rozwiązań prawnych i technologicznych*, Fundacja Rozwoju Demokracji Lokalnej 2008, s. 137–162. Dokument elektroniczny: [http://www.frld.org.pl/downloads/Diagnoza\\_20\\_barier\\_w\\_JST.pdf](http://www.frld.org.pl/downloads/Diagnoza_20_barier_w_JST.pdf).



Dane z rejestrów publicznych – stanowiących podstawowe zasoby infrastruktury informacyjnej państwa – pobierane są w postaci dokumentu elektronicznego, czyli stanowiącego odrębną całość znaczeniową zbioru danych uporządkowanych w określonej strukturze wewnętrznej.

Tak rozumiany dokument elektroniczny jest zupełnie innym pojęciem niż „dokument” bądź „dokument urzędowy” definiowany dla różnych gałęzi prawa. Przy rozważaniu dalszych kwestii należy pamiętać, że ze względu na to, że pozyskiwanie informacji do ponownego wykorzystania następować będzie z zasady w postaci elektronicznej, przy regulowaniu tych czynności należy posługiwać się pojęciem „dokumentu elektronicznego”.

Jednym z oczywistych powodów transpozycji do prawa polskiego dyrektywy Parlamentu Europejskiego i Rady w sprawie ponownego wykorzystywania informacji sektora publicznego jest zwiększenie transparentności życia publicznego w Polsce. Temu samemu celowi powinno służyć realizowanie idei „otwartej władzy publicznej”. Trzeba jednak z przykrością stwierdzić, że działania te nie zostały poprzedzone żadnymi rozważaniami dotyczącymi rzeczywistego znaczenia pojęcia „otwartości”. Przy braku takiej refleksji pojawia się tendencja do utożsamiania „otwartości” i „przeszukiwalności” informacji pojęciem jawności formalnej utrwalonym w doktrynie prawa i orzecznictwie w Polsce. Tymczasem bez zmiany znaczenia pojęcia jawności formalnej lub bez odróżnienia tego pojęcia od „otwartego dostępu do informacji” (dostępności) będziemy mieli do czynienia z poważnym naruszaniem zasad ochrony prywatności przez przyjmowanie, że każdy zasób jawny formalnie powinien być dostępny do dowolnego ponownego wykorzystania<sup>22</sup>.

W tym miejscu rozważań warto zwrócić uwagę na pewną zmianę terminologiczną, którą świadomie zastosowano w niniejszym stanowisku. Rozważania, jakie dotychczas toczyły się w doktrynie prawa na temat jawności danych z rejestrów publicznych, określano zawsze jako badania nad „jawnością rejestrów”. Nie kwestionując tego przyjętego w teorii prawa pojęcia, z zasady należałoby dziś mówić o „jawności danych rejestrowych” lub „jawności danych z rejestru”. W większości przypadków mamy bowiem do czynienia nie tyle z jawnością samego rejestru, lecz z jawnością jego odbicia, jakim jest zestaw danych – a co za tym idzie informacji – przetwarzanych w systemie teleinformatycznym, który z założenia nie jest rejestrem samym w sobie. Jednocześnie dane przetwarzane w systemie teleinformatycznym są ze swej natury bardziej zatomizowane niż dokumenty przechowywane w rejestrze papierowym. Są po prostu wartościami pewnych pól stworzonych przez twórcę bazy i obsługiwanych wedle poleceń sformułowanych przez twórcę oprogramowania obsługującego daną bazę<sup>23</sup>.

<sup>22</sup> Niemiecką dyskusję na ten temat podsumowuje M. Eifert, *Państwowe struktury informacyjne i ponowne wykorzystanie informacji w niemieckiej administracji przez podmioty prywatne*, [w:] *Internet. Ochrona wolności, własności i bezpieczeństwa*, red. G. Szpor, Wyd. C.Beck, Warszawa 2011, s. 204–208.

<sup>23</sup> O zmianach, jakie niesie dostęp do rejestrów drogą elektroniczną pisze G. Sibiga, *Udostępnianie*

To zaś oznacza, że niezależnie od regulacji prawnej mogą być one – z technicznego punktu widzenia – selekcjonowane w dowolny dopuszczony przez obu twórców rozwiązania informatycznego sposób. Mogą być więc wydobywane z bazy w oderwaniu od innych danych, z którymi w dokumencie papierowym są logicznie powiązane oraz mogą być automatycznie wiązane logicznie z innymi danymi, z którymi w dokumencie papierowym nie są powiązane logicznie. Truizmem jest stwierdzenie, że w rejestrze prowadzonym w postaci relacyjnej bazy danych kwestia uzyskanego zestawu danych z różnych rekordów w jednej tabeli jest tylko kwestią sposobu skonstruowania zapytania do bazy. Równie wielkim truizmem jest stwierdzenie, że przetwarzanie danych z różnych dokumentów elektronicznych wywoływanych za pomocą różnych zapytań z tej samej lub z różnych baz danych jest tylko funkcją pomysłowości „*data minera*” i wydajności stosowanych przez niego narzędzi informatycznych<sup>24</sup>.

Taka sytuacja nakazuje nam przy wszystkich rozważaniach o rejestrach prowadzonych w postaci elektronicznej brać pod uwagę fakt, że przetwarzaniu podlega dana, a nie dokument rejestrowy. Każe nam również pamiętać o zagrożeniach, jakie niesie kojarzenie ze sobą danych występujących z pozoru w różnych miejscach danego rejestru lub nawet w różnych rejestrach. Każda próba myślenia o rejestrze prowadzonym za pomocą systemu teleinformatycznego wyłącznie w kategoriach „rejestru” i „dokumentu” jest z góry skazana na niepowodzenie.

W przypadku rejestrów niejawnych i poddanych bardzo ścisłemu reżimowi w zakresie przetwarzania danych oraz bardzo restrykcyjnej kontroli działań osób korzystających z rejestru (popularnie nazywanych „śladowalnością działań”) możemy twierdzić, że zapanowanie nad sposobem korzystania z narzędzi bazodanowych jest możliwe. Jednak w przypadku rejestrów jawnych i udostępnionych do ponownego wykorzystania próba takiego panowania nie jest ani możliwa ani wskazana. Trzeba tym samym przyjąć jako pewnik, że dane z rejestrów publicznych będą przetwarzane w taki sposób, jaki wymyśli użytkownik.

Czym jest jawność formalna danych rejestrowych, będąca dziś podstawą do uznania zasobu rejestrowego lub innego zasobu wchodzącego w zakres informacji publicznej za możliwy do ponownego wykorzystania? Stanowisko doktryny prawa w Polsce oraz przegląd poglądów wyrażonych w orzecznictwie można prześledzić na podstawie pomnikowej pracy Tomasza Staweckiego (Uniwersytet Warszawski) *Rejestry publiczne. Funkcje instytucji* z 2005 r.<sup>25</sup>

---

*danych z rejestrów publicznych a zastosowanie technologii informacyjno-telekomunikacyjnej*, [w:] *Internet...*, red. G. Szpor, s. 225–235.

<sup>24</sup> Porównaj choćby: *User-centred models of information retrieval oraz Intelligent information retrieval*, [w:] G.G.Chowdhury, *Introduction to Modern Information Retrieval*, Facet Publ., London 2008, s. 214–226 oraz 352–371.

<sup>25</sup> T. Stawecki, *Rejestry publiczne...*, s. 101 i n.



Podawany przez T. Staweckiego zestaw elementów składających się na jawność formalną – przyjęty i stosowany w doktrynie prawa – pochodzi z opracowania przygotowanego w 1935 r.<sup>26</sup> Obejmuje on:

- uprawnienie do wglądu do zbioru i bezpośredniego zapoznania się z treścią dokonanych wpisów oraz złożonych dokumentów (tj. prawo do poznania danych);
- uprawnienie do samodzielnego sporządzania odpisów i notatek (tj. prawo do prywatnego utrwalenia danych);
- uprawnienie do żądania wydania odpisów, wyciągów i zaświadczeń potwierdzających urzędowo treść wpisu w danym zbiorze (rejestrze) bądź treść dokumentów złożonych do zbioru lub towarzyszących mu akt (tj. prawo do otrzymania urzędowego dokumentu potwierdzającego dane zawarte w zbiorze), oraz
- obowiązek ogłaszania niektórych danych w gazetach lub przeznaczonych do tego celu publikacjach (obowiązek zapewnienia publicznej wiedzy o faktach opisanych w zbiorze).

Oczywiście ten ostatni aspekt dotyczył zdaniem zarówno Z. Fenichela jak T. Staweckiego tylko „papierowych” gazet i publikacji.

Katalog ten powinien być dziś uzupełniony o nowe elementy, jakimi są obowiązek ogłaszania niektórych danych rejestrowych w publicznie dostępnych systemach teleinformatycznych oraz o przekazywanie informacji publicznej do ponownego wykorzystania. Co więcej, jakkolwiek decyzja o uzupełnieniu powinna być poprzedzona analizą ryzyka przetwarzania konkretnych rodzajów danych (pól w relacyjnej bazie danych). Takie działanie musi prowadzić do odróżnienia jawności formalnej od dostępności i prawa do ponownego wykorzystania informacji publicznej.

W kolejnej – mało znanej – publikacji T. Stawecki<sup>27</sup> zachęca również do takiego działania, stwierdzając, że – jeszcze przed pojawieniem się omawianego projektu ustawy o zmianie ustawy o dostępie do informacji publicznej – trzeba było brać pod uwagę dwa podstawowe punkty widzenia:

- możliwe sposoby udostępniania osobom z zewnątrz informacji zawartych w bazach danych oraz
- zakres informacji, jakie są udostępniane, a przy tym uzasadnienie zapewnienia bądź wyłączenia jawności informacji zrodzonych w bazie danych.

<sup>26</sup> Por. Z. Fenichel, *Księgi gruntowe a rejestr handlowy. Próba zestawienia porównawczego*, „Przegląd Notarialny” 1935, nr 10, s. 11 [227].

<sup>27</sup> T. Stawecki, *Jawność publicznych baz danych [w:] Prawne uwarunkowania wymiany informacji w gospodarce*, red. K. Markowski, BIK, Warszawa 2007, s. 29–44 oraz tego samego autora: *Dostępność publicznych baz danych – stan dzisiejszy i kierunki zmian. Konspekt wypowiedzi przygotowanej na konferencję w dniu 7 grudnia 2006 r. pt. „Prawne uwarunkowania wymiany informacji w gospodarce”*, s. 25–26 <http://www.bik.pl/NR/rdonlyres/6E3BCFB2-4C4D-4E54-B7DC-D79828903612/230/Broszurastreszczeniarefart%C3%B3w1.pdf>.

Nowe technologie podpowiadają nam zarówno nowe możliwe sposoby zapewnienia dostępu do baz danych, jak i nowe związane z tym cele, zadania i tzw. „wyzwania”, a także zagrożenia. W szczególności:

- zapewnienie elektronicznego dostępu (on-line) do informacji, które wcześniej były i niekiedy nadal są udostępniane w tradycyjny sposób (np. do treści wpisów dokonanych w publicznych rejestrach czego przykładem są tzw. e-dostęp do danych zgromadzonych w Krajowym Rejestrze Sądowym albo program elektronicznej księgi wieczystej);
- zapewnianie dostępności określonego zakresu informacji, które są niekiedy gromadzone i przetwarzane w różnych bazach danych, a czasem są *ad hoc* organizowane i ujawniane publicznie;
- zapewnianie dostępu do baz danych (zwykle prowadzonych przez podmioty publiczne inne niż organy rejestrowe) z jednoczesnym założeniem, że dostęp polega na możliwości samodzielnego wyszukiwania, a następnie pobierania (jak to się mówi potocznie „ściągnięcia”) i dalszego przetwarzania plików tekstowych, grafiki, plików muzycznych itp.

W tym samym opracowaniu autor wskazuje na szczególny przypadek zastosowania idei jawności (*publicity*) do stosunków prawnych, jakim są obowiązki ujawniania określonych informacji w niektórych rejestrach publicznych. W tym kontekście zasadę jawności uważa się za jedną z zasad ustrojowych rejestrów i nazywa się ją „kamieniem węgielnym” rejestrów publicznych<sup>28</sup>. Podkreśla się ponadto jej nierozzerwalny związek z fundamentalnymi wartościami ustrojowymi: demokracją, wolnością, praworządnością oraz bezpieczeństwem prawnym. I w końcu T. Stawecki – powołując się na doktrynę zagraniczną – twierdzi, że w zakresie odnoszącym się do rejestrów publicznych idea jawności jest interpretowana wężej i nieco inaczej niż w innych dziedzinach prawa. Idea jawności formalnej prowadzi do prawnego zagwarantowania każdemu, bądź określonym osobom, dostępu do rejestru w celu poznania zawartych w nim informacji. W tym znaczeniu formułujemy po prostu zasadę „dostępności rejestru” (*Öffentlichkeit*) odróżnianą od prawa do ponownego wykorzystania informacji z rejestru<sup>29</sup>.

Podsumowując, mimo że dzisiejsze przepisy dotyczące przetwarzania danych pochodzących z rejestrów publicznych, w tym z ksiąg wieczystych, nie kreują formalnych ograniczeń w ponownym przetwarzaniu informacji rejestrowej, to za słuszne uznać należy ściśle trzymanie się wymagań ustawy o ochronie danych osobowych w zakresie obowiązków informacyjnych. Można również przewidy-

<sup>28</sup> Oczywiście owo „ustrojowe” znaczenie „zasady” musi być oceniane w świetle generalnej dyskusji o zasadach konstytucyjnych. Zob. A. Pułło, *O ustrojowej identyfikacji zasad konstytucyjnych*. Zob. *Księga pamiątkowa Profesora Marcina Kudeja*, red. A. Łabno, E. Zwierchowski, Oficyna Wydawnicza Waclaw Walasek, Katowice 2009, s. 16–17 oraz A. Pułło, *Idee ogólne a zasady prawa konstytucyjnego*, „Państwo i Prawo” 1995, nr 8 oraz A. Pułło, *Z problematyki zasad prawa: idee ogólne w prawie konstytucyjnym*, „Przeгляд Sejmowy” 1996, nr 1, s. 9–20.

<sup>29</sup> Porównaj też: M. Eifert, *Państwowe struktury...*, s. 193–210.

wać, że w najbliższej przyszłości zostaną wyraźnie rozdzielone pojęcia jawności formalnej danych rejestrowych i otwartego (wolnego) przetwarzania tych informacji w tych sytuacjach, gdy prowadzić to będzie to profilowania osoby fizycznej. Należy również uznać, że każdy podmiot publiczny ujawniający dane osobowe w systemach teleinformatycznych takich jak systemy elektronicznych ksiąg wieczystych, powinien już dziś przystąpić do sporządzania oceny wpływu takiego przedsięwzięcia na ochronę prywatności osób fizycznych.

**Wojciech Rafał Wiewiórowski**

### **PRIVACY PROTECTION AS THE RESTRICTION OF THE RIGHT TO REPROCESSING PUBLIC INFORMATION**

The amendment of the Act on the Access to Public Information of 2011, which aims at the appropriate implementation of the directive on the re-use of public sector information into Polish law, has led to a situation in which any information intended to be revealed in the mode of the access to public information goes as a rule to „public domain” and can be used for any purpose, even if it was originally collected or produced for the implementation of a specific public task. This situation causes the collision of constitutional principles of the freedom of economic activities and the freedom of information processing with - also included in the Constitution – the protection of privacy and the limitations of processing information concerning natural persons to the situation, when it is „necessary in a democratic state ruled by law”. The freedom of processing public information to some extent can be limited law, but only in the form of statute, and only because of the reasons acceptable from the point of view of the directive.

During the discussion on the amendment it was assumed that supplementing the government’s draft law amending the Act on the Access to Public Information with provisions concerning the protection of privacy in the re-use of public information is not necessary, as these rules directly result from other law – the Act on the Protection of Personal Data, which application is not limited by the new regulations.