

# Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE

Marcin Rojszczak<sup>1</sup>

Regulacje prawne związane z ochroną danych osobowych ewoluują w kierunku umożliwienia jednostkom skutecznej kontroli informacji ich dotyczących publikowanych w sieci Internet. Na świecie w awangardzie zmian w tym zakresie od lat znajduje się UE, w której prawa i wolności osobiste są trwale zagwarantowane w Karcie Praw Podstawowych. Bezkompromisowa ochrona praw jednostki jest wzmacniana zarówno przez prawodawcę unijnego, jak i przez orzeczenia sądów konstytucyjnych państw członkowskich oraz Trybunału Sprawiedliwości UE.

Celem niniejszego opracowania jest przedstawienie najważniejszych zasad prawa do bycia zapomnianym oraz analiza, czy obecny kształt tego prawa, będący następstwem orzeczeń TS, nie wpływa negatywnie na gwarancje związane z innymi prawami podstawowymi, takimi jak prawo do informacji czy swobody wypowiedzi.

## Uwagi wstępne<sup>2</sup>

Wraz z rozwojem usług informacyjnych duża część aktywności zawodowej i osobistej jest realizowana z wykorzystaniem Internetu. Każdego roku przybywa nowych e-usług, a istniejące podlegają transformacji i udoskonaleniu. Coraz więcej osób posiada po kilka profili na różnych portalach społecznościowych, za pomocą których prowadzi rozbudowaną korespondencję skierowaną do wszystkich użytkowników Internetu, wzbogaconą licznymi zdjęciami i treściami multimedialnymi z ich życia prywatnego. Zaawansowane algorytmy przetwarzania coraz częściej potrafią skutecznie korelować bardzo rozbudowane zbiory danych – w efekcie pozwalając np. na automatyczne rozpoznawanie produktów, miejsc czy twarzy na publikowanych zdjęciach. Dzięki analizowaniu aktywności użytkowników oraz korelowaniu rozproszonych zbiorów danych możliwe jest także prognozowanie zdarzeń przyszłych.

Niestety, nadal zrozumienie złożoności współczesnych usług informatycznych jest wśród ich użytkowników stosunkowo niewielkie. Udostępnianie dużej ilości danych osobistych nieokreślonej grupie osób, korzystanie z nowych – często dobrze niepoznanych – usług społecznościowych oraz bezrefleksyjne akceptowanie nowych polityk prywatności, wprowadzanych przez usługodawców, prowadzi do stopniowej utraty kontroli nad obiegiem informacji dotyczących sfery prywatności.

Osoby, które zdały sobie sprawę z tej sytuacji i chciałyby odzyskać kontrolę nad informacjami rozpowszechnianymi na ich temat, do niedawna trafiały w legislacyjną próżnię i były zdane na dobrą wolę poszczególnych usługodawców internetowych i regulacji wynikających z – często bardzo rozbudowanych i niejasnych – regulaminów świadczenia usług. Opisana luka wynika z faktu, że istniejące regulacje dotyczące danych osobowych – zarówno na poziomie krajowym (ustawa z 29.8.1997 r. o ochronie danych osobowych<sup>3</sup>), jak i eu-

ropejskim (dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych<sup>4</sup>) – zostały opracowane i przyjęte do stosowania w latach dziewięćdziesiątych XX w. – a więc w czasach, gdy znany nam obecnie Internet jeszcze nie istniał.

Przyjęta w 1997 r. Konstytucja RP nie definiuje wprost prawa do ochrony danych osobowych – jest ono wywodzone z ogólnych gwarancji dotyczących prawa do prywatności (art. 47) oraz ochrony informacji o sobie (art. 51). Zgodnie z art. 47 każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Natomiast poszczególne przepisy art. 51 wprowadzają dodatkowe gwarancje związane z gromadzeniem i przetwarzaniem danych osobowych, ale – jak wskazuje się w doktrynie – ich zakres podmiotowy i przedmiotowy jest węższy niż wynikający z art. 47. W takim przypadku prawa jednostek i obowiązki podmiotów przetwarzających powinny być wywodzone bezpośrednio z art. 47 Konstytucji RP<sup>5</sup>.

Prywatność obejmuje w szczególności ochronę informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności (zwanej autonomią informacyjną), w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym informacji o swoim życiu<sup>6</sup>. Autonomia informacyjna stanowi zatem istotny element składowy prawa do prywatności i może być zdefiniowana jako prawo do samodzielnego decydowania o ujawnianiu innym

<sup>1</sup> Autor jest absolwentem prawa i informatyki, doktorantem Instytutu Nauk Prawnych PAN.

<sup>2</sup> Stan prawny oraz odnośniki internetowe aktualne na 2.11.2017 r.

<sup>3</sup> T.j. Dz.U. z 2016 r. poz. 922; dalej jako: OchronaDanychU.

<sup>4</sup> Dz.Urz. UE L Nr 281, s. 31; dalej jako: dyrektywa 95/46.

<sup>5</sup> Zob. np. rozważania dot. podmiotów uprawnionych i zobowiązanych na tle art. 51 ust. 1 – M. Wild, Komentarz do art. 51, Nb 16, [w:] M. Saffan, L. Bosek (red.), Warszawa Konstytucja RP. Tom I. Komentarz do art. 1–86, Warszawa 2016.

<sup>6</sup> Zob. wyrok TK z 19.5.1998 r., U 5/97, OTK 1998, Nr 4, poz. 46.

informacji dotyczących swojej osoby oraz prawo do sprawowania kontroli nad tymi informacjami znajdującymi się w posiadaniu innych podmiotów<sup>7</sup>. W szczególności wyrazem korzystania z autonomii informacyjnej może być żądanie usunięcia określonych informacji z przestrzeni publicznej. W takim rozumieniu prawo do usunięcia danych dopełnia uprawnień jednostki dotyczących kontrolowania zakresu informacji dostępnych na jej temat w przestrzeni publicznej<sup>8</sup>.

Sąd Najwyższy zajmuje obecnie stanowisko, że przy wykładni krajowych przepisów związanych z ochroną danych osobowych nie można pominąć dyrektywy 95/46, w której już na wstępie podkreślono, że systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi, i muszą one szanować podstawowe prawa i wolności osób fizycznych, a szczególnie prawo do prywatności<sup>9</sup>.

Istniejące przepisy nie dość precyzyjnie definiowały prawa jednostki do żądania usunięcia danych przetwarzanych na jej temat, nawet jeżeli te informacje były prawdziwe i nie naruszały innych przepisów.

Sytuacja w ostatnich latach zaczęła się powoli zmieniać na skutek precedensowego wyroku TS w sprawie *Google Spain*<sup>10</sup> oraz uwzględnienia w przyjętym w 2016 r. rozporządzeniu 2016/679<sup>11</sup> przepisów wprowadzających tzw. prawo do bycia zapomnianym (a ściślej: prawo do usunięcia danych). Szczególnie interesujące wydają się prawne konsekwencje związane z wejściem w życie RODO, co nastąpi 25.5.2018 r.

## Okoliczności sprawy Google Spain

Aby zrozumieć formalną koncepcję prawa do bycia zapomnianym, należy przybliżyć najważniejsze okoliczności oraz tezy wyroku TS wydanego w sprawie *Google Spain*. Trybunał udzielił odpowiedzi na pytania prejudycjalne dotyczący sporu pomiędzy Google Spain SL i Google Inc. a hiszpańskim Urzędem Ochrony Danych Osobowych (Agencia Española de Protección de Datos, AEPD). Przedmiotem sporu była skarga obywatela Hiszpanii skierowana do AEPD w zakresie nakazania spółce Google zaprzestania przetwarzania informacji na jego temat, które – w jego ocenie – wpływały negatywnie na jego osobę, budując nieprawdziwy i mylny wizerunek wśród użytkowników Internetu. W szczególności po wpisaniu w okno wyszukiwania imienia i nazwiska skarżącego wyszukiwarka przedstawiała linki do artykułów dotyczących licytacji komorniczej majątku skarżącego, która miała miejsce wiele lat wcześniej. Już na tym etapie warto podkreślić kilka faktów, które będą istotne w dalszych rozważaniach nad zakresem i celowością wprowadzania do porządku prawnego prawa do bycia zapomnianym. Po pierwsze, zarówno skarżący, jak i w dalszym etapie postępowania AEPD nie kwestionowali prawdziwości opublikowanych informacji. Ponadto nie podniesiono także zarzutu, że udostępnione informacje były wprowadzone nielegalnie do domeny pu-

blicznej lub z naruszeniem praw majątkowych osób trzecich. Co więcej, adresatem żądania był nie tylko właściciel i operator wyszukiwarki internetowej (Google), lecz także wydawca dziennika La Vanguardia, w którym opublikowany został kwestionowany artykuł źródłowy. W odniesieniu do wydawcy La Vanguardia żądano usunięcia kwestionowanych treści, natomiast od Google – przyjęcia środków koniecznych do usunięcia danych osobowych dotyczących skarżącego z jej indeksu oraz uniemożliwienia dostępu do tych danych w przyszłości. Hiszpański organ nadzoru zdecydował się częściowo uwzględnić żądanie skarżącego. Mianowicie zobowiązał Google do usunięcia odniesień do kwestionowanych tekstów w dzienniku La Vanguardia, ale jednocześnie odrzucił żądania adresowane do wydawcy samego dziennika, wskazując, że usunięcie lub modyfikowanie źródłowych ogłoszeń opublikowanych na stronach internetowych nie jest potrzebne, ponieważ informacje te zostały opublikowane w ramach obowiązującego prawa (w rzeczywistości były to urzędowe ogłoszenia o licytacji komorniczej – znane, choć w innej formie, także w Polsce). AEPD uznał zatem, że chociaż sama informacja była opublikowana zgodnie z prawem, to jej dalsze rozpowszechnianie przez Google może naruszać interesy skarżącego. Na skutek odwołania przez Google oraz pytania prejudycjalnego zadanego przez hiszpański sąd sprawa zawisła przed TS.

Aby zrozumieć wywód prawny przedstawiony w uzasadnieniu wyroku Trybunału, a także jego implikacje w postaci prawa do bycia zapomnianym w kształcie wprowadzonym w RODO, omówienia wymaga prawna definicja administratora danych. Zgodnie z legalną definicją przedstawioną w art. 7 pkt 4 OchronaDanychU administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydujący o celach i środkach przetwarzania danych osobowych. Podobna definicja funkcjonuje na gruncie nadal obowiązującej dyrektywy 95/46. Zgodnie z art. 2 ust. d przez pojęcie administratora danych należy rozumieć osobę fizyczną lub prawną, organ publiczny, agencję lub inny organ, który samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych.

Jedną z osi sporu, którą musiał rozstrzygnąć Trybunał, było ustalenie, czy koncern Google (lub operator innej wyszukiwarki internetowej) może być uznany za administratora

<sup>7</sup> Zob. wyrok SN z 11.2.2015 r., I CSK 868/14, Legalis.

<sup>8</sup> Por. np. argumentację uzasadniającą potrzebę wprowadzenia prawa do bycia zapomnianym w: *M. Fazlioglu*, Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, *International Data Privacy Law* 2013, Nr 3, s. 149–150.

<sup>9</sup> Zob. wyrok SN z 15.2.2008 r., I CSK 358/07, OSNC 2009, Nr 4, poz. 63.

<sup>10</sup> Wyrok TS z 13.5.2014 r., *Google Spain SL v. AEPD*, C-131/12, ECLI:EU:C:2014:317.

<sup>11</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz.Urz. UE L Nr 119, s. 1); dalej jako: RODO.

danych. Innymi słowy – czy indeksowanie informacji dostępnych w sieci Internet, które niewątpliwie pod kątem *stricto* technicznym jest przetwarzaniem danych, jest także przetwarzaniem na gruncie przepisów o ochronie danych osobowych. W konsekwencji – czy na przedsiębiorcę przetwarzającego w ten sposób dane można nałożyć obowiązki analogiczne do innych administratorów danych. Trybunał Sprawiedliwości w pkt 43 wyroku stwierdził, że prowadzoną przez operatorów wyszukiwarek internetowych działalność, która polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie udostępnianiu ich internautom w sposób uporządkowany zgodnie z określonymi preferencjami, w sytuacji gdy informacje takie zawierają dane osobowe, należy uznać za „przetwarzanie danych osobowych”, a w konsekwencji operatora tej wyszukiwarki należy uznać za „administratora” odpowiedzialnego za przetwarzanie danych w rozumieniu przepisów prawa. Oczywiście i bezpośrednią konsekwencją takiej decyzji jest możliwość skorzystania przez każdą osobę, której dane są przetwarzane, z prawa do cofnięcia zgody na przetwarzanie danych – a w efekcie doprowadzenia do konieczności korygowania indeksu wyszukiwarki w sposób odzwierciedlający takie żądanie.

Trybunał w swoim wyroku stwierdził ponadto w sposób niebudzący wątpliwości, że żądanie dotyczące usunięcia danych z wyszukiwarki internetowej jest uprawnieniem niezależnym i niezwiązanym z żądaniem usunięcia takich danych z serwisu internetowego, który informacje te oryginalnie opublikował. W efekcie żądanie powinno być zrealizowane także w przypadku, gdy kwestionowane informacje nie zostały uprzednio czy jednocześnie usunięte ze źródłowych stron internetowych, a nawet wtedy gdy ich publikacja na tych stronach jest zgodna z prawem. Jednakże TS w tym zakresie słusznie zauważył, że „biorąc pod uwagę łatwość, z jaką informacje opublikowane na stronie internetowej mogą zostać skopiowane, oraz okoliczność, że podmioty odpowiedzialne za ich publikację nie zawsze podlegają przepisom prawa Unii, cel polegający na skutecznej i pełnej ochronie osób, których dotyczą dane, nie mógłby być zrealizowany bez uprzedniego czy też jednoczesnego uzyskania usunięcia dotyczących ich informacji przez wydawców stron internetowych”<sup>12</sup>.

W tym miejscu pojawia się pierwszy oczywisty problem techniczny, który wymyka się normom prawnym. W przypadku tradycyjnych baz danych żądanie usunięcia danych osobowych realizowane jest w sposób bezpośredni – poprzez trwałe skasowanie rekordu bazy danych i powiązanych z nim relacji, które dotyczą osoby występującej z żądaniem. Specyfika wyszukiwarek internetowych jest jednak inna. Baza danych jest tworzona dynamicznie, odzwierciedlając zmiany wprowadzane w indeksowanych stronach. Jakakolwiek ręczna manipulacja w bazie danych związana z usunięciem

rekordów jest z definicji tylko tymczasowa, ponieważ po ponownym zindeksowaniu źródłowej strony internetowej zawartość bazy zostanie odtworzona. Prowadzi to do potrzeby nie tyle usunięcia danych z rejestru wyszukiwarki, ile dodania nowego mechanizmu, odpowiedzialnego za „cenzurowanie” informacji wyświetlanych użytkownikom wyszukiwarki. W przypadku wyszukiwarek nie należy więc mówić o faktycznym usunięciu informacji z bazy danych (byłoby to bowiem działanie bezcelowe), a o filtrowaniu wyników wyszukiwania i usuwaniu z nich odniesień do stron zawierających informacje o osobach, które wystąpiły z żądaniem usunięcia danych. To z kolei prowadzi do wielu problemów praktycznych. Na przykład w jaki sposób zrealizować żądanie, jeżeli wnioskującym jest osoba o popularnym (lub chociaż powtarzalnym) imieniu i nazwisku. Czy w takim przypadku operator wyszukiwarki internetowej powinien skasować wpisy dotyczące wszystkich stron, odnoszące się wszystkich osób posiadających to imię i nazwisko? Co w przypadku, gdy wnioskodawca posiada imię i nazwisko identyczne z inną osobą pełniącą funkcje publiczne? Co jeżeli tą osobą jest czynny polityk, kandydujący w zbliżających się wyborach?

Na inny aspekt słusznie wskazują *E. Michałkiewicz* i *E. Milczarek*, zwracając uwagę na możliwość nadużycia prawa do usunięcia danych w kontekście osób skazywanych wcześniej za przestępstwa, zwłaszcza związane z wolnościami seksualnymi i obyczajnością<sup>13</sup>. W efekcie wzmocnienia praw jednostki dojść może do sytuacji, w której rodzice zostaną pozbawieni dostępu do informacji, że w miejscowości, do której chcą się przeprowadzić, mieszka osoba wielokrotnie karana za czyny o charakterze pedofilskim.

W związku z powyższym oczywiste jest, że wniosek związany z usunięciem danych musi być ręcznie analizowany przez operatora wyszukiwarki. Treść serwisów internetowych często nie pozwala na jednoznaczne określenie, czy publikowane materiały dotyczą osoby, która wystąpiła z wnioskiem, a to z kolei może prowadzić do wielu błędów i nadużyć.

Przykładem obszaru wymagającego dalszego doprecyzowania jest możliwość objęcia prawem do bycia zapomnianym danych zgromadzonych w udostępnionych w Internecie rejestrach państwowych, ze szczególnym uwzględnieniem danych historycznych. Problem ten stał się podstawą sprawy, która zawiła przed TS na skutek wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonym przez włoski trybunał kasacyjny. Jak wskazał rzecznik generalny *Y. Bot* w wydanej 8.9.2016 r. opinii, kwestią problematyczną w niniejszej sprawie było, czy organy krajowe prowadzące rejestry spółek po upływie określonego czasu od zakończenia działalności podmiotu i na wniosek zainteresowanej osoby powinny de-

<sup>12</sup> Wyrok *Google Spain SL v. AEPD*, s. 84.

<sup>13</sup> *E. Michałkiewicz, E. Milczarek*, Prawo do prywatności w dobie Internetu, PME 2015, Nr 2, s. 59.



cydować o wykreśleniu lub poddaniu anonimizacji jej danych osobowych zawartych w rejestrze albo o ograniczeniu ich jawności poprzez zawężenie kręgu uprawnionych odbiorców informacji<sup>14</sup>.

W opinii rzecznika rejestry publiczne, takie jak rejestr spółek, mogą realizować swój podstawowy cel, jakim jest wzmocnienie bezpieczeństwa obrotu gospodarczego, tylko w sytuacji, gdy dostęp do nich jest zagwarantowany dla każdego bez ograniczeń czasowych. Dlatego w takim przypadku możliwość z korzystania z prawa do bycia zapomnianym powinna być ograniczona. W wyroku z 9.3.2017 r. Trybunał co do zasady podzielił stanowisko rzecznika, wskazując na szczególną rolę jawności informacji na temat tożsamości i funkcji osób, upoważnionych do nadzorowania i kontrolowania spółek, bądź ich reprezentowania wobec osób trzecich<sup>15</sup>. Jednocześnie uznał jednak, że w szczególnych sytuacjach nie można wykluczyć, że prawa podmiotu danych do ochrony prywatności powinny przeważać nad prawami osób trzecich w dostępie do informacji zgromadzonych w jawnym rejestrze publicznym<sup>16</sup>. Przykładem może być upływ wystarczająco długiego okresu od daty likwidacji podmiotu, w którym pełniła funkcję dana osoba. Decyzja związana z możliwością wprowadzenia takich ograniczeń należy do kompetencji państw członkowskich. W ten sposób Trybunał wskazał, że prawodawcy krajowi, uwzględniając specyfikę bezpieczeństwa obrotu gospodarczego, mogą wprowadzić rozwiązania pozwalające na realizację prawa do usunięcia danych także w odniesieniu do informacji zgromadzonych w rejestrach publicznych.

## Zasięg terytorialny prawa do bycia zapomnianym

Trybunał Sprawiedliwości w sprawie *Google Spain* rozstrzygnął, w jaki sposób prawo do bycia zapomnianym powinno być stosowane przez operatorów internetowych posiadających siedzibę poza obszarem UE. Wszystkie główne wyszukiwarki internetowe są serwisami o zasięgu globalnym. Chociaż wyniki wyszukiwania są personalizowane dla konkretnego użytkownika, z uwzględnieniem państwa, w którym przebywa, czy języka, jakim się posługuje, to jednak w tle funkcjonuje ten sam mechanizm indeksujący – a więc ta sama, choć bardzo rozbudowana i rozproszona, baza danych. Powstają zatem dwa kolejne problemy. Po pierwsze, jaki powinien być zakres terytorialny stosowania prawa do bycia zapomnianym, a po drugie – czy prawo to powinno dotyczyć także przedsiębiorców posiadających siedzibę poza terytorium UE.

Analiza powyższych zagadnień musi uwzględniać, że zarówno użytkownik przeglądarki (lub innego publicznego serwisu internetowego), jak i osoba, która chce ograniczyć

dostęp do informacji na swój temat, mogą być obywatelami różnych państw, niekoniecznie należących do UE. Ponadto niezależnie od swojej narodowości mogą przebywać w państwach trzecich, które mogą mieć odmienne przepisy dotyczące ochrony danych osobowych. Zgodnie z wyrokiem TS operatorzy przeglądarek powinni zapewnić respektowanie prawa do bycia zapomnianym na terenie UE. Oznacza to, że filtrowanie wyników powinno być stosowane w odniesieniu do użytkowników przebywających na terenie Unii, co prowadzi do wniosku, że w zależności od miejsca pobytu, wpisując tę samą frazę w wyszukiwarce internetowej, możliwe jest uzyskanie różnych wyników.

Problem ten został dostrzeżony przez francuski krajowy organ nadzoru (Commission nationale de l'informatique et des libertés – CNIL), który po przeprowadzeniu postępowania wyjaśniającego 21.5.2015 r. wydał decyzję zobowiązującą Google do wprowadzenia mechanizmów globalnego filtrowania wyników wyświetlanych przez wyszukiwarkę. Ponieważ Google nie dostosował się do tej decyzji, 10.3.2016 r. na przedsiębiorcę nałożona została grzywna w wysokości 100 000 euro<sup>17</sup>. CNIL uznał, że jakkolwiek przeglądarka internetowa Google jest rozbudowanym systemem informatycznym, to za generowanie wyników prezentowanych w różnych państwach odpowiada ten sam algorytm. Skuteczne wdrożenie wyroku *Google Spain* wymaga zatem, aby kwestionowane przez jednostki treści nie były udostępniane na wszystkich rynkach, na jakich działa operator, a nie tylko w państwie, w którym wnioskodawca ma miejsce pobytu. CNIL wskazał ponadto, że globalne filtrowanie wyników wyszukiwania nie wpłynie na ograniczenie prawa do informacji, bowiem kwestionowane treści będą dostępne w indeksie wyszukiwarki po wprowadzeniu innych haseł niż imię i nazwisko osoby, która pragnie skorzystać z prawa do bycia zapomnianym. Warto w tym miejscu zaznaczyć, że podtrzymanie decyzji CNIL na drodze sądowej i utrwalenie tego poglądu w orzecznictwie europejskim doprowadziłoby do sytuacji, w której sądy państw członkowskich UE mogłyby kształtować treści prezentowane przez wyszukiwarki internetowe w państwach trzecich<sup>18</sup>.

Drugi z zaznaczanych wcześniej problemów – a więc określenie przedsiębiorców internetowych, wobec których można egzekwować prawo do bycia zapomnianym – ma oczywiste znaczenie praktyczne. Według danych z września 2017 r., sześć z 10 największych portali społecznościowych

<sup>14</sup> Opinia Rzecznika Generalnego Y. Bota z 8.9.2016 r., C-398/15, ECLI:EU:C:2016:652, s. 32.

<sup>15</sup> Wyrok TS z 9.3.2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. S. Manni*, C-398/15, ECLI:EU:C:2017:197, s. 32.

<sup>16</sup> *Ibidem*, s. 60.

<sup>17</sup> Decyzja CNIL z 10.3.2016 r., 2016-054, <https://goo.gl/sycKpf>.

<sup>18</sup> Reuters, Google appeals French order for global 'right to be forgotten', <http://www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8>.

według liczby aktywnych użytkowników jest zarządzanych przez przedsiębiorców mających siedzibę w Stanach Zjednoczonych, natomiast pozostałe cztery przez podmioty zarejestrowane w Chinach<sup>19</sup>. W efekcie – niejako z definicji – analizowane prawo będzie adresowane do usługodawców nieprowadzących podstawowej działalności w UE. Wskazać należy, że zgodnie z dyrektywą 95/46 o jej stosowaniu można mówić, m.in. gdy przetwarzanie danych odbywa się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium państwa członkowskiego (art. 4 ust. 1 pkt a) lub gdy administrator danych nie prowadzi działalności gospodarczej na terytorium Unii, ale do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane, jak i inne, znajdujące się na terytorium państwa członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium UE (art. 4 ust. 1 pkt b). Trybunał musiał zatem rozstrzygnąć, czy przedsiębiorca internetowy posiadający siedzibę oraz centra przetwarzania danych poza obszarem UE powinien – a jeżeli tak, to w jakim zakresie – realizować prawo do bycia zapomnianym. Trybunał przeanalizował ten problem i wskazał, że do uznania, że przedsiębiorca prowadzi na terenie państwa członkowskiego UE działalność podlegającą unijnym regulacjom związanym z danymi osobowymi wystarczy, aby ustanowił w danym państwie oddział lub spółkę zależną, których celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem głównej usługi internetowej, a działalność tego oddziału lub tej spółki była skierowana do osób zamieszkujących to państwo<sup>20</sup>.

Z kolei w sprawie *Weltimmo*<sup>21</sup> TS wprowadził elastyczne warunki uznania, że czynności przetwarzania danych odbywają się w kontekście działalności gospodarczej prowadzonej w UE. W ocenie Trybunału przesłanką taką może być np. zredagowanie strony internetowej usługodawcy w języku powszechnie wykorzystywanym w tym państwie członkowskim lub przyjmowanie płatności w walucie danego państwa członkowskiego<sup>22</sup>. Wyrok ten doprowadził do dalszego powiększenia kręgu zagranicznych usługodawców, zobowiązanych do stosowania europejskich przepisów o ochronie danych. Nadal jednak, na gruncie dyrektywy 95/46, czynności przetwarzania realizowane poza UE i przez przedsiębiorcę zagranicznego, które nie były ukierunkowane na obywateli Unii, nie musiały być realizowane zgodnie z unijnymi przepisami.

Naturalną konsekwencją przedstawionej przez Trybunał wykładni przepisów przepisów może być utrudnienie prowadzenia działalności gospodarczej przedsiębiorcom unijnym i zachęcenie, aby rozbudowane usługi internetowe były świadczone spoza obszaru UE. Operator wyszukiwarki internetowej, który zarejestrował podmiot zależny w dowolnym kraju UE, musi podporządkować się europejskim przepisom o ochronie danych. Operator wyszukiwarki internetowej, który prowadzi identyczną działalność w taki sam sposób,

ale nie posiada oddziału lub spółki zależnej na terytorium dowolnego państwa UE i nie kieruje wprost swoich usług na rynek państw członkowskich – tych samych przepisów stosować nie musi. Przy czym obaj przedsiębiorcy konkurują ze sobą i kierują swoje usługi do tego samego grona odbiorców, w dużej części obywateli UE.

Sytuacja ta zmieni się wraz z wejściem w życie RODO, w którym w art. 3 doprecyzowano zakres podmiotów zobowiązanych, uwzględniając także przedsiębiorców nieposiadających jednostek organizacyjnych w Unii, jednak przetwarzających dane obywateli UE, oferujących im towary lub usługi, a także monitorujących ich zachowania.

## Problemy interpretacyjne

Jakkolwiek wyrok Trybunału dotyczy konkretnej sprawy i okoliczności w niej przedstawionych, jest oczywiste, że z uwagi na swoją doniosłość tezy w nim zawarte stały się podstawą do dyskusji na temat praktycznych implikacji stosowania prawa do bycia zapomnianym. W pierwszej kolejności należy wskazać, że Trybunał swoim orzeczeniem znacząco wzmocnił prawne mechanizmy ochrony prywatności wynikające z art. 7 (poszanowanie życia prywatnego i rodzinnego) oraz art. 8 (ochrona danych osobowych) Karty Praw Podstawowych<sup>23</sup>. Jednocześnie wzbudził jednak liczne obawy dotyczące ograniczenia wolności wypowiedzi i informacji, także zagwarantowanych w Karcie. Internet i informacje przesyłane za jego pośrednictwem stały się jednym z filarów rozwoju społeczeństwa informacyjnego. Serwisy społecznościowe służą nie tylko komunikacji pomiędzy rodziną czy gronem znajomych, ale również mają istotne znaczenie w budowaniu świadomości obywatelskiej – czego przykłady można było zaobserwować w trakcie tzw. arabskiej wiosny czy nieudanego puczu wojskowego w Turcji<sup>24</sup>. W obu przypadkach wiadomości przekazywane za pośrednictwem popularnych sieci społecznościowych były źródłem informacji dla milionów obywateli na temat sytuacji wewnętrznej w ich państwach, w efekcie przyczyniając się do rozwoju protestów społecznych i wpływając na przemiany polityczne. Z kolei popularność przeglądarek internetowych stała się motorem rozwoju dziennikarstwa niezależnego i wpłynęła na powstanie wielu nieznanych wcześniej jego form, takich jak blogi czy kanały *podcast*.

<sup>19</sup> The Statistics Portal, <https://goo.gl/WCimA8>.

<sup>20</sup> Wyrok *Google Spain SL v. AEPD*, s. 60.

<sup>21</sup> Wyrok TS z 1.10.2015 r., *Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14.

<sup>22</sup> *Ibidem*, s. 29.

<sup>23</sup> Karta Praw Podstawowych Unii Europejskiej z 30.3.2010 r. (Dz.Urz. UE C Nr 83, s. 389); dalej jako: KPP.

<sup>24</sup> The Guardian, Social media may have been blocked during Turkey coup attempt, z 15.7.2016 r., <https://goo.gl/ikhqeg>.

Należy zauważyć, że mechanizmy, które w wykonaniu wyroku TS zaczęły być implementowane przez wiodących dostawców usług internetowych – służące do kontroli i filtrowania udostępnianych treści – nie różnią się w swoim przeznaczeniu od rozwiązań wykorzystywanych w Chinach. Oczywiście model chiński jest dużo bardziej skuteczny w kontrolowaniu udostępnianych treści, ponieważ państwo jest w stanie skutecznie nadzorować całą sieć transmisji danych<sup>25</sup>. W przypadku UE odpowiedzialność za tę kontrolę została przesunięta na prywatnych przedsiębiorców działających w warunkach wolnorynkowych – jest więc *de facto* formą autocenzury. Celem działania operatorów wyszukiwarek jest ułatwienie, a nie utrudnianie, dostępu do informacji. Jeżeli z powodu ochrony praw podstawowych wprowadzony ma zostać model kontroli treści internetowych – wydaje się rozsądne, aby koszty jego utrzymania były ponoszone przez państwa, a nie prywatnych przedsiębiorców. Jak wskazano w komunikacie opublikowanym przez Google, krajowe instytucje zajmujące się ochroną danych osobowych mogą być lepiej przygotowane do przeprowadzenia oceny, czy dane informacje powinny być usunięte z indeksu wyszukiwarki<sup>26</sup>.

Dodatkowo należy wskazać, że kryteria podane przez Trybunał – pozwalające na skuteczne zastosowanie prawa do bycia zapomnianym – są wyjątkowo szerokie. W analizowanym wyroku wskazano możliwość stosowania wyjątków pozwalających na odmowę usunięcia wyników wyszukiwania, jednak ich katalog nie został precyzyjnie zdefiniowany.

W tym miejscu należy przytoczyć pogląd ETPC, wyrażony w wyroku wydanym w sprawie *Węgrzynowski i Smolczewski v. Polska*, że nie jest rolą władzy sądowiczej angażowanie się w przepisywanie historii poprzez nakazywanie usunięcia ze sfery publicznej wszelkich śladów publikacji<sup>27</sup>. Na gruncie krajowym tezę tę podzielił SO w Warszawie, rozpatrując sprawę, której podstawą było określenie odpowiedzialności usługodawcy internetowego za szkodę wyrządzoną prezentowaniem odnośników do treści, których nie był twórcą: „Z momentem, gdy użytkownik wprowadzi do okna dialogowego silnika wyszukiwarki zapytanie, wyszukiwarka zidentyfikuje i wyświetli wyniki wyszukiwania na określonych pozycjach zgodnie z własnymi algorytmami, które zostały opracowane w celu identyfikacji trafnych i użytecznych wyników wyszukiwania. Kształtowanie zaś treści linków i opisów (snippetów) z wyników wyszukiwania leży przede wszystkim po stronie podmiotów administrujących stronami internetowymi wyświetlanymi na listach wyników wyszukiwania. Wyniki wyszukiwania oraz snippety nie zawierają zatem jakichkolwiek twierdzeń pochodzących od operatora wyszukiwarki. Treść linków i snippetów powinna być kształtowania przede wszystkim przez administratorów stron, do których odsyłają linki wyświetlane w wynikach wyszukiwania, w przeciwnym wypadku pozwany musiałby być traktowany co najmniej jako cenzor Internetu<sup>28</sup>”.

Na uwagę zasługuje przy tym fakt, że sąd w swoim uzasadnieniu uwzględnił treść orzeczenia w sprawie *Google Spain*.

Do innych wniosków – bliższych koncepcji wynikającej z przywołanego orzeczenia TS, doszedł jednak NSA w wyroku z 9.4.2015 r.<sup>29</sup> Wskazał mianowicie, iż za przetwarzanie danych osobowych może być uznane także ich pośrednie udostępnianie (np. poprzez przekierowanie do innej domeny internetowej), nawet jeżeli dany podmiot danymi tymi fizycznie nie dysponuje. Sąd podkreślił, iż nie może podlegać ochronie prawnej działanie podmiotów, które w sposób bezrefleksyjny dokonują świadomego odesłania do stron internetowych, które mogą naruszać chronione prawem polskim dane osobowe. Niewątpliwie, jeżeli przekierowanie takie nie łączy się z fizycznym posiadaniem danych udostępnionych na innej stronie internetowej, należy to uwzględnić w procesie oceny danego podmiotu jako przetwarzającego dane osobowe i nimi administrującego, jednakże brak posiadania danych nie wyłącza *per se* możliwości uznania danego podmiotu za ich administratora. Oczywiście nie jest tak, iż każde przekierowanie czy stworzenie innych warunków do wyszukania danych przez jedną witrynę internetową w zasobach innej będzie od razu mieścić się w ramach instytucji uregulowanych w ustawie o ochronie danych osobowych. Jak jednak wskazał NSA, nie może być zgody na to, by każde przekierowanie, które nie wiąże się z posiadaniem danych chronionych prawem, z założenia traktować jako nienaruszające przepisów ustawy.

Rozważając prawne konsekwencje funkcjonowania prawa do bycia zapomnianym, należy ocenić, w jaki sposób regulacja taka powinna dotyczyć internetowych repozytoriów wiedzy. Internet to nie tylko portale społecznościowe, ale także portale tematyczne czy encyklopedie elektroniczne. Czy prawo do bycia zapomnianym może prowadzić do wstecznej modyfikacji treści opublikowanych w Wikipedii? Jeżeli tak, to nie trudno wyobrazić sobie sytuację, w której to samo hasło będzie zaprezentowane odmiennie w papierowym i elektronicznym wydaniu tej samej encyklopedii<sup>30</sup>. Warto w tym miejscu przypomnieć tezę z przywołanego wcześniej wyroku ETPC: „nie jest rolą władzy sądowiczej angażowanie się w przepisywanie historii poprzez nakazywanie usunięcia ze sfery publicznej wszelkich śladów publikacji”.

<sup>25</sup> Problematyka stosowanej w Chinach cenzury treści internetowych znalazła szerokie omówienie w piśmiennictwie – zarówno w zakresie stosowanych procedur i prawodawstwa, jak i ich wpływu na kształtowanie norm społecznych. Zob. np.: *J. Lee, C. Liu, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China*, *Minnesota Journal of Law, Science, and Technology* 2012, Nr 1, s. 125–151.

<sup>26</sup> Google. Prywatność i warunki. Najczęstsze pytania, <https://www.google.pl/policies/faq/>.

<sup>27</sup> Zob. wyrok ETPC z 16.07.2013, *Węgrzynowski i Smolczewski v. Polska*, 33846/07, <http://hudoc.echr.coe.int/>.

<sup>28</sup> Wyrok SO w Warszawie z 12.10.2015 r., I C 1164/13, <http://orzeczenia.warszawa.so.gov.pl/>.

<sup>29</sup> Wyrok NSA z 9.4.2015, I OSK 2926/13, <http://orzeczenia.nsa.gov.pl/>.

<sup>30</sup> The Guardian, Wikipedia swears to fight 'censorship' of 'right to be forgotten' ruling, <https://goo.gl/1Adu22>.



Wydawca Wikipedii udostępnia statystyki na temat haseł encyklopedycznych, które zostały usunięte z wyszukiwarki Google na skutek realizacji prawa do bycia zapomnianym. W przypadku polskiego wydania Wikipedii jest to m.in. hasło poświęcone Parafii św. Wawrzyńca w Kurnie oraz AZS Legion Katowice<sup>31</sup>. To kolejny przykład, w którym zbyt daleko idące zastosowanie prawa do prywatności może prowadzić do nieadekwatnego ograniczenia prawa do informacji i swobody wypowiedzi.

Analiza wyroku *Google Spain* to także dowód, w jaki sposób nowoczesne technologie często wymykają się normom prawnym nie tylko na gruncie legislacji, ale przede wszystkim na etapie sądowym. Punktem wyjścia do dyskusji o przydatności wprowadzenia możliwości filtrowania (cenzorowania) wyników wyszukiwarki (a tym jest realizacja prawa do bycia zapomnianym) powinna być refleksja na temat celowości i skuteczności takiego działania. W zamierzeniu omawiane prawo powinno umożliwić osobom fizycznym usunięcie informacji na ich temat, które zostały opublikowane w Internecie – niezależnie od prawdziwości tych informacji, a także ich aktualności. Sposobem realizacji tego prawa – zgodnie z treścią wyroku – powinno być zgłoszenie żądania do operatorów wyszukiwarek ze wskazaniem listy kwestionowanych odnośników pojawiających po wpisaniu do okna wyszukiwarki frazy odpowiadającej imieniu i nazwisku danej osoby. Jeżeli jednak w oknie wyszukiwania zostanie wpisana inna fraza (niebędąca imieniem i nazwiskiem), wyniki wyszukiwania mogą zostać przedstawione w sposób odpowiadający rzeczywistości, a więc w sposób niefiltrowany, i umożliwić dostęp do stron, do których dostęp był zablokowany przy próbie wyszukiwania imieniem i nazwiskiem<sup>32</sup>.

Przeglądarka internetowa nie jest statycznym mechanizmem, w którym pozycja, na której wyświetlana jest dana strona w rankingu, zależy wyłącznie od analizy jej treści. Równie ważne jest zachowanie użytkowników przeglądarki, a w szczególności fakt, jak często wybierają dany odnośnik i jak oceniają treść prezentowaną na stronie docelowej (tzw. indeks odrzuceń)<sup>33</sup>. Innymi słowy – wyszukiwarka wyświetla na górze rankingu te strony, które są chętniej odwiedzane przez użytkowników w odpowiedzi na wyszukiwaną frazę. W efekcie to użytkownicy poprzez swoje zachowania i decyzje kształtują indeks wyszukiwarki i wpływają na to, w jaki sposób wyszukiwarka prezentuje treści. Wprowadzenie sztucznej – manualnej – kontroli do tego procesu jest o tyle nieskuteczne, że użytkownicy, którzy chcą dotrzeć do interesującej ich informacji, zaczną wybierać odnośniki do innych stron, zawierających tę samą informację, i w ten sposób w krótkim czasie przyczynią się do podniesienia rankingu danej strony w indeksie, przywracając w efekcie stan pierwotny, w którym odnośnik kierujący do niepożądanego informacji będzie prezentowany na szczycie listy wyników.

Ponadto warto wskazać, że mechanizmy wyszukiwania już dawno zostały rozwinięte poza granicę treści tekstowych. Wiodące wyszukiwarki od lat indeksują także zdjęcia i potrafią wskazać nie tylko treść związaną z daną frazą, ale także zestaw powiązanych fotografii. Wiele serwisów internetowych oferuje funkcjonalność tworzenia repozytorium zdjęć z opcjonalną możliwością rozpoznawania twarzy. W efekcie użytkownik, będąc zarejestrowanym w takich portalach, jak Flickr czy Picassa, może otrzymywać powiadomienia, gdy inne osoby (w domyśle – znajomi) opublikują zdjęcie, na którym się znajduje. Ten sam mechanizm jest wykorzystywany przez Google w usłudze Gogle – w tym jednak przypadku pozwala na fotografowanie dowolnego przedmiotu i wyszukiwanie w Internecie innych powiązanych zdjęć i informacji. Mechanizmy rozpoznawania twarzy i przeszukiwania zdjęć z pewnością w niedalekiej przyszłości zostaną udostępnione publicznie i pozwolą na przeszukiwanie fotografii w sposób analogiczny do wyszukiwania tekstu.

Interesująca w tym względzie wydaje się analiza spraw sądowych prowadzonych z powództwa *M. Mosleya* przeciwko Google oraz innym wydawcom internetowym. Sprawy dotyczyły zakazu publikacji materiałów wideo i fotograficznych dotyczących aktywności seksualnej *M. Mosleya* – pełniącego wówczas funkcję prezydenta Międzynarodowej Federacji Samochodowej (Fédération Internationale de l'Automobile, FIA) – które oryginalnie zostały opublikowane 30.3.2008 r. przez brytyjski tabloid *News of the World*. *Mosley* w kolejnych latach wygrał proces o ochronę dóbr osobistych wytoczony wydawcy tygodnika, jak również innym serwisom powielającym materiały przedstawione w oryginalnej publikacji. Ponadto *Mosley* zainicjował także sprawy przeciwko Google we Francji, Niemczech oraz Wielkiej Brytanii. *Mosley* zamierzał doprowadzić do stanu, w którym zdjęcia, których legalność została zakwestionowana przez sąd, nie będą indeksowane przez Google i wyświetlane w wynikach wyszukiwania – niezależnie, czy dany odnośnik został przez niego indywidualnie zgłoszony operatorowi przeglądarki. Oczekiwał, że Google wprowadzi mechanizmy autocenzury powodujące trwałe usunięcie kwestionowanych zdjęć z wyników wyszukiwania także tych stron, które zostaną dopiero zindeksowane w przyszłości. Zarówno francuski sąd okręgowy w Paryżu (Tribunal de Grande Instance de Paris)<sup>34</sup>, jak i niemiecki regionalny sąd w Hamburgu (Landgericht Hamburg)<sup>35</sup> orzekły o słuszności żądań powoda,

<sup>31</sup> Notices received from search engines, <https://goo.gl/HYaa2Z>.

<sup>32</sup> *W. Gregory Voss*, The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation, *Journal of Internet Law* 2014, Nr 1.

<sup>33</sup> Google Analytics – strona produktu, Współczynnik odrzuceń, <https://support.google.com/analytics/answer/1009409?hl=pl>.

<sup>34</sup> Wyrok Tribunal de Grande Instance de Paris z 6.11.2013 r., RG 11/07970, <https://goo.gl/mPspFP>.

<sup>35</sup> Wyrok Landgericht Hamburg z 24.1.2014 r., 324 O 264/11, <https://goo.gl/SSStx2>.

zobowiązując Google do trwałego usunięcia zdjęć z wyszukiwarki. Na szczególnie interesujący zapowiadał się proces wytoczony w Wielkiej Brytanii. Po pierwsze, sąd krajowy miał w tym wypadku wyrokować już po wydaniu orzeczenia *Google Spain*. Po drugie, prawo brytyjskie regulujące obszar ochrony danych osobowych<sup>36</sup> przewiduje nieznaną w polskim systemie prawnym uprawnienie jednostki do zgłoszenia żądania zaprzestania przetwarzania danych, jeżeli zostało uprawdopodobnione, że przetwarzanie to doprowadzi do powstania szkody. W analizowanej sprawie *Max Mosley* wystąpił z takim żądaniem, jednak Google odmówiło jego realizacji. Sprawa została skierowana na drogę sądową i w postanowieniu z 15.1.2015 r. sąd oddalił wniosek Google o umorzenie sprawy i skierował ją do dalszego rozpoznania. W sentencji postanowienia sąd uznał żądania powoda jako uprawdopodobnione<sup>37</sup>. Z uwagi jednak na fakt, że strony zawarły ugodę, sprawa nie była przedmiotem dalszego badania przez sąd. Niewątpliwie jednak w niedalekiej przyszłości sądy krajowe państw UE będą musiały rozstrzygnąć zakres stosowania prawa do bycia zapomnianym w kontekście prewencyjnego filtrowania zdjęć publikowanych w Internecie.

W dyskusji na temat prawa do bycia zapomnianym niepokoi także stałe utożsamianie koncernu Google z informacjami publikowanymi w Internecie. Internet jest siecią informacyjną, wielowarstwową i rozproszoną (zdecentralizowaną). Sieć Internet jest medium transmisyjnym dla bardzo wielu protokołów, a tylko kilka z nich jest wykorzystywanych przez aplikacje webowe (takie jak usługi Google). Stawianie znaku równości pomiędzy Google a Internetem i projektowanie rozwiązań prawnych przeznaczonych dla ochrony prywatności w Internecie – mając na horyzoncie wyłącznie usługi świadczone przez Google – stanowi znaczącą wadę, immamentnie związaną z koncepcją prawa do bycia zapomnianym. Zanim jeszcze powstała spółka Google i przed udostępnieniem jej wiodącej usługi – wyszukiwarki Google Search – istniały zdecentralizowane protokoły komunikacyjne, służące do dystrybucji treści pomiędzy setkami tysięcy użytkowników na całym świecie. Przykładem może być sieć Usenet stanowiąca podstawę dla znanych także w Polsce grup dyskusyjnych. Sieć Usenet jest zdecentralizowana, podobna w swojej architekturze do sieci *Peer-2-Peer*, a więc jakkolwiek wsteczna moderacja (filtrowanie czy usuwanie wcześniej opublikowanych informacji) jest technicznie niemożliwa. Sieć Usenet jest odrębną usługą internetową, działającą z wykorzystaniem protokołu NNTP, a więc niezależnie i w sposób niezwiązany z treściami WWW, z którymi większość użytkowników utożsamia Internet. Do kogo więc osoba, która stała się przedmiotem dyskusji/publikacji w sieci Usenet i która chciałaby skorzystać z prawa do bycia zapomnianym, powinna kierować swoje żądanie? Jest oczywiste, że nie do operatora serwisu Google (nawet jeżeli treści Usenet są także indeksowane przez wyszukiwarkę), ponieważ Usenet jest odrębną, autonomiczną usługą. Żądania nie można skierować także do administra-

torów serwerów Usenet, ponieważ – jak wskazano powyżej – jest to sieć zdecentralizowana, w której każdy węzeł zawiera tylko kopię danych. Internet to setki różnych protokołów wymiany informacji – WWW, z której korzysta większość usług udostępnianych przez Google, to tylko jeden z nich.

Innym z zastosowań Internetu, w ostatnich latach coraz bardziej rozpowszechnionym w związku z rosnącymi obawami o prywatność, są wirtualne sieci prywatne (VPN). Nie wchodząc w analizę techniczną, VPN pozwala na zestawianie bezpiecznych (szyfrowanych) połączeń pomiędzy dwoma dowolnymi segmentami sieci Internet (konkretnymi komputerami lub całymi sieciami). W praktyce VPN pozwala na realizację usługi tzw. bezpiecznego proxy, a więc połączenia, w którym cały ruch od użytkownika przesyłany jest do zdalnego serwera i dopiero za jego pośrednictwem przesyłany dalej do sieci Internet. Proxy pozwala na ukrycie tożsamości użytkownika, jak również na podłączenie się przez użytkownika do Internetu w dowolnej części sieci. Możliwe jest więc zestawienie takiego połączenia, w którym komputer stojący w Poznaniu będzie widoczny w Internecie, jakby był podłączony do sieci w Niemczech, Stanach Zjednoczonych czy w Australii. Usługi takie są szeroko oferowane komercyjnie, są w pełni legalne i mają wiele zastosowań praktycznych<sup>38</sup>. Zapewniając anonimowość użytkownikom, pozwalają na przeglądanie treści Internetu w częściach świata, gdzie funkcjonująca cenzura normalnie uniemożliwiłaby dotarcie do poszukiwanych treści. Ta sama technologia pozwala – w oczywisty sposób – ominąć mechanizmy cenzury państw niedemokratycznych, jak też reguły filtrowania stosowane na rynku UE w związku z realizacją prawa do bycia zapomnianym. Nie ma żadnego technicznego problemu, aby dowolny użytkownik (czy cała sieć) został przełączony – bez zmiany fizycznej lokalizacji – za pomocą VPN do innego segmentu Internetu i w ten sposób pomijając ograniczenia funkcjonujące w UE. Dlatego realizacja prawa do bycia zapomnianym poprzez odpowiednie filtrowanie wyników wyszukiwania na podstawie lokalizacji komputera użytkownika jest rozwiązaniem o znacznie ograniczonej skuteczności<sup>39</sup>.

## Ogólne rozporządzenie o ochronie danych osobowych

Trybunał swoim orzeczeniem wzmocnił gwarancje związane z ochroną danych osobowych w UE. Co jednak oczywi-

<sup>36</sup> Por. art. 10 brytyjskiej ustawy z 16.7.1998 o ochronie danych (Data Protection Act 1998), <http://www.legislation.gov.uk/ukpga/1998/29/contents>.

<sup>37</sup> Postanowienie High Court of Justice of England and Wales z 15.1.2015 r., HQ 14 X 02964, <https://goo.gl/1Xk4tu>.

<sup>38</sup> Strona internetowa dostawcy jednej z wiodących usług VPN dostępnej globalnie: <https://nordvpn.com>.

<sup>39</sup> K. Finley, In Europe, You'll Need a VPN to See Real Google Search Results, *Wired*, 3.8.2016, <https://goo.gl/FGQRze>.



ste, rolę Trybunału nie jest definiowanie prawa materialnego, a jedynie wyrokowanie w zakresie norm już obowiązujących. W przypadku sprawy *Google Spain* wzorcem kontroli była dyrektywa 95/46 – niemal 20-letnia norma prawna, przyjęta w czasach, w którym sieć Internet dopiero powstawała, a pojęcia, takie jak społeczeństwo informacyjne czy serwisy społecznościowe, nie miały dzisiejszego znaczenia. Jeszcze przed wydaniem orzeczenia w sprawie *Google Spain*, KE zainicjowała prace związane z opracowaniem nowej regulacji w obszarze ochrony danych osobowych<sup>40</sup>, która po zakończeniu procedury legislacyjnej została przyjęta jako rozporządzenie 2016/679. Chociaż rozporządzenie weszło w życie 4.5.2016 r. (art. 99 ust. 1), to przepisy będą miały zastosowanie od 25.5.2018 r. (art. 99 ust. 2). Do tego czasu będą obowiązywały przepisy obecne, a więc w przypadku prawa do bycia zapomnianym – w kształcie wynikającym z wyroku *Google Spain*.

Podstawową różnicą rozporządzenia w porównaniu z wcześniej obowiązującą dyrektywą jest rodzaj samego aktu prawnego. Zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej<sup>41</sup> rozporządzenie ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowalne. Natomiast dyrektywa wiąże w zakresie osiągnięcia określonych celów, pozostawiając jednak państwom członkowskim swobodę w zakresie wybranej formy i środków stosowania. Rozporządzenie jest więc źródłem praw i obowiązków dla jednostek, a dzięki bezpośredniej stosowalności może być podstawą do dochodzenia praw przed krajowymi organami sądowymi. Przyjęcie formy rozporządzenia w zakresie ochrony danych osobowych oznacza zatem standaryzację mechanizmów ochrony danych osobowych na terenie całej UE i ujednoczenie trybu postępowania we wszystkich państwach członkowskich<sup>42</sup>. Występująca w przypadku dyrektywy 95/46 implementacja prawa UE do porządku krajowego nie będzie już wymagana, a przepisy rozporządzenia będą stosowane wprost. Fakt ten ma kluczowe znaczenie zwłaszcza dla organizacji międzynarodowych, działających w wielu państwach członkowskich Unii. Standaryzacja mechanizmów ochrony danych osobowych to nie tylko wprowadzenie tych samych definicji administratora danych czy przetwarzania danych osobowych, ale również ustandaryzowanie praw i obowiązków osób, których dane są przetwarzane, oraz podmiotów przetwarzających. W obszarze prawa materialnego RODO jest odpowiedzią na potrzebę wprowadzenia regulacji prawnych zmierzających do zagwarantowania wysokiego poziomu ochrony prywatności w dynamicznie rozwijających się technologiach kształtujących nowoczesne społeczeństwo informacyjne, takich jak analityka Big Data, chmura obliczeniowa (ang. *cloud computing*) czy technologia rozszerzonej rzeczywistości (ang. *augmented reality*).

Rozporządzenie wprowadza także do unijnego porządku prawnego prawo do bycia zapomnianym. Chociaż, jak wska-

zано wcześniej, było ono częścią dorobku prawnego już od orzeczenia TS w sprawie *Google Spain*, dopiero w RODO prawo do bycia zapomnianym (określane jako prawo do usunięcia danych) zostało zdefiniowane w całości, jako oddzielna norma prawna, a nie przez pryzmat pojedynczego kazusu procesowego. Zgodnie z art. 17 ust. 1 RODO w określonych okolicznościach osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki te dane usunąć. Aby uniknąć niejasności i sporów w obszarze terytorialnego zakresu stosowania, w art. 3 ust. 1 doprecyzowano, że rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy samo przetwarzanie odbywa się w Unii. Natomiast zgodnie z art. 3 ust. 2 rozporządzenie stosuje się także do przetwarzania danych osobowych osób przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom lub monitorowaniem ich zachowania.

W efekcie rozporządzenie powinno być stosowane, jeżeli przetwarzane są dane osobowe obywateli Unii – niezależnie od tego, czy administrator danych prowadzi działalność na terenie UE, czy też samo przetwarzanie odbywa się w Unii. Rozporządzenie doprowadzi zatem do usunięcia nierówności w traktowaniu podmiotów mających siedzibę lub oddział w UE względem podmiotów prowadzących działalność spoza Unii, ale kierujących swoje produkty lub usługi do obywateli UE. Jak wcześniej wskazano, w obecnym stanie prawnym – będącym konsekwencją wyroku *Google Spain* – nie wszyscy przedsiębiorcy świadczący e-usługi i przetwarzający dane osobowe mieszkańców UE muszą stosować się do unijnych przepisów o ochronie danych. Wprowadzona w ogólnym rozporządzeniu zmiana prowadzi zatem do ujednoczenia obowiązków usługodawców, jest więc korzystna z punktu widzenia praw konsumentów z obszaru UE. Nałożenie jednakowych obowiązków, niezależnie od miejsca prowadzenia działalności czy wykorzystywanych środków technicznych związanych z przetwarzaniem informacji (przetwarzanie rozproszone, *cloud computing* itp.), prowadzi także do zwiększenia konkurencyjności przedsiębiorców europejskich.

<sup>40</sup> W tym miejscu warto zauważyć, że już pierwszy wniosek KE dotyczący projektu ogólnego rozporządzenia – opublikowany 25.1.2002 r. – uwzględnił w art. 17 wprowadzenie „prawa do bycia zapomnianym”, rozumianego jako rozszerzenie znanego na gruncie dyrektywy 95/46 prawa do usunięcia danych.

<sup>41</sup> T.j. Dz.Urz. UE z 2016 r. C Nr 202, s. 47.

<sup>42</sup> Parlament Europejski, Reforming the Data Protection Package, wrzesień 2012, <https://goo.gl/oaabmx>.

Istotą wyroku *Google Spain* było wskazanie, że podmiot danych ma prawo żądania zaprzestania prezentowania określonych informacji dotyczących jego prywatności. Należy podkreślić, że TS nie wskazał wprost konieczności „usunięcia” zakwestionowanych danych. Powstaje zatem zasadnicze pytanie, czy prawo do bycia zapomnianym (w kształcie wynikającym z orzeczenia *Google Spain*) i prawo do usunięcia danych (art. 17 ogólnego rozporządzenia) w rzeczywistości definiują to samo prawo podmiotu danych. Aspekt ten jest pomijany w trwającej dyskusji na temat przygotowania administratorów do nowych obowiązków prawnych. Uzasadniony wydaje się pogląd, że prawodawca unijny, definiując zakres prawa do usunięcia danych, może nałożyć na administratora *de facto* nowe obowiązki, odmienne od wynikających z orzeczenia *Google Spain*. Dlatego, chociaż zgodnie z terminologią przyjętą w ogólnym rozporządzeniu, w niniejszym artykule terminy prawo do bycia zapomnianym i prawo do usunięcia danych stosowane są zamiennie, to należy wskazać, że w rzeczywistości oba pojęcia *de facto* opisują inne prawo, bowiem wiążą się z odmiennymi obowiązkami po stronie administratorów danych<sup>43</sup>.

Prawo do usunięcia danych w kształcie wynikającym z ogólnego rozporządzenia nie powinno być analizowane w oderwaniu od formalnej podstawy przetwarzania. W przyjętej redakcji art. 17 ust. 1 określono enumeratywne przypadki, uzasadniające realizację żądania usunięcia danych. Podmiot danych może wystąpić z żądaniem, w przypadku gdy ustał cel przetwarzania. W efekcie można uznać, że prawo do usunięcia danych może być stosowane wyłącznie w sytuacji, gdy nie istnieje żadna formalna podstawa przetwarzania. W ten sposób prawo to stanowi dopełnienie zasady minimalizacji danych – a więc służy dostarczeniu legalnych środków, które mogą posłużyć do zobowiązania administratora do usunięcia danych, które nie powinny być dalej przez niego przetwarzane.

Jako trafną należy ocenić także regulację wprowadzoną art. 17 ust. 2, zgodnie z którą, jeżeli administrator upublicznił dane osobowe, co do których wpłynęło żądanie ich usunięcia (realizacja prawa do bycia zapomnianym), to – biorąc pod uwagę dostępną technologię i koszt realizacji – jest on zobowiązany podjąć rozsądne działania, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

Analizowany przepis wprowadza dwa korzystne rozwiązania z punktu widzenia praktycznej realizacji prawa do bycia zapomnianym. Po pierwsze, wprowadza mechanizm współdziałania pomiędzy wydawcami a innymi serwisami internetowymi – w szczególności operatorami wyszukiwarek – w zakresie komunikowania żądania usunięcia określonych danych. Poza zmniejszeniem pracochłonności dla usługow-

dawców, z punktu widzenia podmiotów danych mechanizm ten pozwoli na szybkie i automatyczne usuwanie z indeksu wielu wyszukiwarek treści, co do których wpłynęło żądanie ich usunięcia. Na praktyczne uzasadnienie takiego podejścia wskazywali także operatorzy wyszukiwarek internetowych, np. koncern Microsoft (operator wyszukiwarki Bing), twierdząc, że: „w przypadku utworzenia lub umieszczenia treści na stronach mediów społecznościowych, która ma być zablokowania, usunięta lub pomniejszona w wynikach wyszukiwania – w wyszukiwarce Bing i innych wyszukiwarkach – należy spróbować użyć narzędzi i procesów usuwania treści dostępnych na tych stronach mediów społecznościowych. Te narzędzia i procesy mogą być najskuteczniejszym sposobem usunięcia treści mediów społecznościowych z wyników wyszukiwania”<sup>44</sup>.

Warto zauważyć, że podobne rozwiązania techniczne są znane od lat. Polegają na stosowaniu odpowiednich znaczników w kodzie strony internetowej lub pliku *robots.txt* umieszczonym w indeksowanym folderze. Niezależnie od wybranej techniki wydawca treści internetowych ma możliwość wskazania oczekiwanego zachowania algorytmu indeksującego strony internetowe, w szczególności określenia, że dana strona nie ma być indeksowana (znacznik: *noindex*) lub odnośniki na niej zawarte nie mają być dalej przeszukiwane (znacznik: *nofollow*). Problem stosowania plików *robots.txt* był już analizowany przez TSw sprawie *Google Spain*. Przedstawiciele koncernu Google podnosili, że operator wyszukiwarki nie powinien być odpowiedzialny za ręczną modyfikację indeksu, skoro wydawcy stron dysponują narzędziem pozwalającym na wskazanie treści, które mają być indeksowane. Trybunał uznał jednak, że brak wskazania przez wydawców ograniczenia indeksowania danej strony nie zwalnia operatora wyszukiwarki internetowej ze spoczywających na nim obowiązków wynikających z faktu, że także jest podmiotem zobowiązanym do realizowania praw podmiotów danych. W tym zakresie również w RODO podtrzymano ten pogląd, dlatego norma art. 17 ust. 2 nie zwalnia z odpowiedzialności za przestrzeganie treści rozporządzenia usługodawców, którzy nie zostali poinformowani przez wydawcę treści o żądaniu usunięcia danej strony z rejestru.

Finalna redakcja art. 17 ust. 2, nakładając obowiązki na wydawcę treści, uwzględnia przy tym istniejące ograniczenia techniczne oraz koszty ich realizacji. W ten sposób prawodawca unijny próbuje zachować równowagę pomiędzy intere-

<sup>43</sup> Na różne możliwe skutki „zapomnienia” zbioru danych wskazywano już w analizie ENISA opublikowanej w 2012 r., odnoszącej się do treści prawa przedstawionej w pierwszym projekcie ogólnego rozporządzenia. W raporcie Agencji przedstawiono trzy możliwe płaszczyzny interpretacyjne, z czego tylko jedna prowadziła do konieczności fizycznego usunięcia wszystkich kopii danych. Więcej: P. Druschel, M. Backes, R. Tirtea, *The right to be forgotten – between expectations and practice*, European Network and Information Security Agency 2012, <https://goo.gl/Q4KNSL>, s. 7.

<sup>44</sup> Zob. <http://help.bing.microsoft.com/#apex/18/PL/10013/-1/PL>.

sem osób żądających usunięcia swoich danych a oczekiwaniami wydawców treści – związanymi z racjonalizacją kosztów realizacji tych żądań. Warto przypomnieć, że Trybunał w wyroku *Google Spain* podkreślił, że ochrona praw wynikających z KPP jest nadrzędna względem interesu gospodarczego przedsiębiorcy internetowego – co w odniesieniu do badanej sprawy oznaczało konieczność spełnienia żądania usunięcia danych niezależnie od kosztów, które operator musi ponieść w tym celu. W tym kontekście treść przepisu zaproponowana w RODO wydaje się bardziej racjonalna i uwzględniająca oczywisty fakt funkcjonowania przedsiębiorców w określonej przestrzeni biznesowej, w której rachunek ekonomiczny oraz możliwości techniczne są istotnymi elementami uzasadniającymi podejmowane decyzje.

Większe trudności interpretacyjne dotyczące sposobu stosowania prawa do usunięcia danych mogą dotyczyć przedsiębiorców zagranicznych, stosujących przepisy rozporządzenia na podstawie art. 3 ust. 2. W takim przypadku może bowiem dojść do oczywistej kolizji norm unijnych z prawem właściwym dla miejsca przetwarzania danych. W takim przypadku może się okazać, że realizacja prawa do bycia zapomnianym doprowadziłaby do naruszenia norm publicznoprawnych, do stosowania których zobowiązany jest administrator danych. Problem ten może mieć szczególnie wymiar w przypadku przedsiębiorców podlegających prawu Stanów Zjednoczonych. Obowiązujące w tamtejszym systemie prawnym normy konstytucyjne, w szczególności Pierwsza Poprawka, stoją na przeszkodzie wprowadzaniu regulacji ustawowych ograniczających „wolność słowa lub prasy”<sup>45</sup>. Prawo do bycia zapomnianym bez wątplenia należy do tego typu środków<sup>46</sup>.

Tak określone prawo do bycia zapomnianym budzi także zastrzeżenia natury technicznej. W szczególności wskazuje się na trudności związane z obowiązkiem usunięcia danych w sytuacji gdy znajdują się one także na kopiach zapasowych administratora. Nie jest jasne, czy w takim wypadku administrator powinien także usunąć dane z kopii zapasowych. Odpowiedź twierdząca prowadziłaby do kolejnych trudności, związanych ze spójnością przetwarzanych informacji. Cyfrowe kopie danych można podzielić na dwa rodzaje: kopie zapasowe oraz kopie archiwalne. Kopie zapasowe służą przywróceniu działania środowiska IT w przypadku awarii, a więc odtworzeniu utraconych informacji. Problem może wystąpić w przypadku, gdy po uwzględnieniu żądania usunięcia danych nastąpi awaria systemu informatycznego i odtworzona zostanie kopia zapasowa wykonana przed uwzględnieniem tego żądania. W takiej sytuacji istnieje możliwość, że usunięte wcześniej dane zostaną przywrócone, co doprowadzi do naruszenia obowiązków prawnych przez administratora danych. Chociaż obecnie problemowi temu poświęca się dużo uwagi, jego praktyczne znaczenie jest stosunkowo niewielkie. Należy pamiętać, że możliwość skorzystania z prawa

do usunięcia danych jest warunkowana spełnieniem jednej z wymienionych w art. 17 ust. 1 przesłanek. Należy zatem przyjąć, że realizacja żądania przez administratora nie jest związana wyłącznie z technicznym wykonaniem czynności skasowania określonego zestawu w bazie danych, ale jest poprzedzona analizą i weryfikacją wniosku. Proces ten powinien być udokumentowany, a zatem w przypadku awarii administrator nie powinien mieć trudności w identyfikacji zakresu danych objętych żądaniami zgłoszonymi po dacie wykonania odtwarzanej kopii.

Podsumowując rozważania dotyczące treści prawa do bycia zapomnianym w ujęciu wprowadzonym w ogólnym rozporządzeniu, należy zwrócić uwagę na treść art. 85 RODO. We wskazanym przepisie przewidziano możliwość wprowadzenia przez państwa członkowskie uzasadnionych ograniczeń w stosowaniu przepisów rozdziału III rozporządzenia, do których należy w szczególności art. 17, z uwagi na potrzebę wyważenia ochrony danych osobowych z innymi prawami podstawowymi, takimi jak wolność wypowiedzi i prawo do informacji. Cel wprowadzenia omawianego przepisu – a więc uniknięcie nadużycia prawa do bycia zapomnianym w sposób ograniczający prawo do informacji – jest oczywiście czytelny i słuszny. W praktyce jednak jego stosowanie może budzić liczne kontrowersje implementacyjne. Pozostawienie możliwości decydowania o sposobie wyważania praw do decyzji państwom członkowskim może skutkować przyjęciem odmiennych, potencjalnie niezgodnych, norm krajowych.

## Podsumowanie

Koncepcja prawa do bycia zapomnianym (prawa do usunięcia danych) jest stosunkowo nową instytucją prawną, będącą efektem adaptacji prawnych mechanizmów ochrony prywatności w zglobalizowanym świecie informacji elektronicznej. Jej obecny kształt, wynikający z orzeczenia TS w sprawie *Google Spain*, w wielu miejscach pomija złożoność technologii, którą stara się regulować. Zamiast tego wprowadzono regulacje w odniesieniu do jednej kategorii podmiotów działających na rynku e-usług, jakim są operatorzy wyszukiwarek internetowych. W efekcie obywatele UE otrzymali ułomny mechanizm ochrony swoich praw, który w wielu miejscach jest niespójny i nieskuteczny. Dlatego – nie kwestionując doniosłego znaczenia praktycznego analizowanego orzeczenia – nie można w pełni podzielić poglądu, że orzeczenie Trybunału stanowi „skuteczne narzędzie do walki o ochronę i obronę prywatności w zakresie przetwarzania danych osobowych, nawet względem potężnych operatorów

<sup>45</sup> Polskie tłumaczenie Pierwszej Poprawki do Konstytucji USA: <http://libr.sejm.gov.pl/tek01/txt/konst/usa.html>.

<sup>46</sup> Problem szerzej analizuje: M. Rustad, S. Kulevska, Reconceptualizing the Right To Be Forgotten to Enable Transatlantic Data Flow, *Harvard Journal of Law & Technology* 2015, Nr 2, s. 372–373.



[internetowych]<sup>47</sup>. Jednocześnie przedsiębiorcy internetowi uzyskali kolejny argument, aby prowadzić i rozwijać swoją działalność gospodarczą i – często innowacyjne – usługi poza obszarem UE. Problemy te zostały zauważone przez prawodawcę unijnego, w wyniku czego prawo do bycia zapomnianym zostało uwzględnione w zmodyfikowanym kształcie w ogólnym rozporządzeniu. Niewątpliwie treść normy wskazana w rozporządzeniu pozwala na uniknięcie niektórych z zauważonych wcześniej problemów. Niestety nie rozwiązuje ona problemu zasadniczego, jakim jest wprowadzenie mechanizmu prawnego, który z całą pewnością nie może skutecznie i całościowo rozwiązać problemu braku kontroli osób fizycznych nad publikowanymi na ich temat treściami elektronicznymi, natomiast może zostać wykorzystany do

wprowadzenia środków skutecznej cenzury czy nawet autocenzury na obszarze UE. Warto zaznaczyć, że do chwili obecnej sam tylko koncern Google otrzymał ponad 580 tys. wniosków o usunięcie łącznie ponad 1 750 000 odnośników internetowych<sup>48</sup>. Praktyczna ocena użyteczności prawa do bycia zapomnianych w kształcie wprowadzonym w RODO nastąpi oczywiście dopiero po 25.5.2018 r. Do tego czasu przedsiębiorcy internetowi przetwarzający dane osobowe mają czas na dostosowanie się do nowych regulacji.

<sup>48</sup> M. Wróbel, Prawo do „bycia zapomnianym” – glosa – C-131/12, MoP 2017, Nr 2, s. 112.

<sup>49</sup> Google, Europejskie żądania dotyczące prywatności: usunięcie wyników wyszukiwania, <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=pl>.

**Słowa kluczowe:** prywatność, prawo do bycia zapomnianym, prawo do usunięcia danych, cenzura, RODO.

## Analysis and practical comments on construction and implementation of right to be forgotten in the EU

*Legal regulations connected with the protection of personal data are evolving in the direction of granting the individuals an effective control of information concerning them, published on the Internet. In the world of forefront of developments in this field for many years is the European Union, in which individual rights and freedoms are permanently enshrined in the Charter of Fundamental Rights. Uncompromising protection of individual rights is encouraged by both the EU legislature, as well as the judgments of the constitutional courts of the Member States and the European Court of Justice.*

*The purpose of this article is to present the most important principles of the right to be forgotten and to analyze whether the current form of this law, which is a consequence of the ECJ rulings, does not contribute to the weakening of other fundamental rights such as the right to information and freedom of expression.*

**Keywords:** privacy, the right to be forgotten, the right to erasure, censorship, GDPR.



### Reforma ochrony danych osobowych 2018

[www.ksiegarnia.beck.pl](http://www.ksiegarnia.beck.pl)

