

DOI: 10.31648/kpp.12319

Maciej Stanecki

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

ORCID: 0009-0004-1626-0330

stmaciej85@gmail.com

Prawo do bycia zapomnianym w europejskim porządku prawnym – od uprawnienia proceduralnego do prawa podstawowego

Wstęp

Rozwój technologii informacyjno-komunikacyjnych oraz postępująca digitalizacja życia społecznego zasadniczo zmieniły sposób gromadzenia, przechowywania i przetwarzania informacji dotyczących jednostki¹. Tradycyjne koncepcje prywatności, wywodzone z klasycznego ujęcia prawa do bycia pozostawionym w spokoju (ang. *right to be let alone*), sformułowanego przez Samuela Warrena i Louisa Brandeisa², koncentrowały się przede wszystkim na ochronie przestrzeni fizycznej i sfery życia osobistego przed niepożądanym wtargnięciem, inwigilacją oraz nieuprawnioną publikacją. Jak jednak wskazuje literatura przedmiotu, w warunkach powszechnej obecności Internetu prywatność nie może być już ujmowana wyłącznie w kategoriach negatywnych – jako brak ingerencji – lecz powinna obejmować również pozytywne uprawnienie do kontroli nad własnym wizerunkiem cyfrowym³.

Bartosz Wysocki trafnie zauważa, że Internet stał się narzędziem akumulującym ogromne ilości informacji, które – ze względu na swoją cyfrową naturę – nie znikają w sposób właściwy dla danych utrwalonych w środowisku analogowym, co nadaje problematyce ochrony danych osobowych szczególne znaczenie z perspektywy praw podstawowych⁴.

¹ P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025, s. 23–27.

² S.D. Warren, L.D. Brandeis, *The right to privacy*, „Harvard Law Review” 1890, vol. 4, nr 5, s. 193–220.

³ M. Jabłoński, J. Węgrzyn, *Prawo do bycia zapomnianym*, Wrocław 2021, s. 15–20.

⁴ B. Wysocki, *The right to be forgotten – a right in the digital world*, „Ars Educandi” 2016, t. 13, s. 117.

W warunkach powszechnie dostępnej pamięci cyfrowej oraz realiów „kapitalizmu nadzoru”⁵ klasyczne ujęcie prywatności okazuje się jednak niewystarczające⁶, a jednostka staje przed wyzwaniem ochrony swojej sytuacji prawnej i wizerunku cyfrowego w dynamicznie zmieniającym się środowisku sieciowym⁷. Informacja raz wprowadzona do sieci przestaje być w pełni kontrolowana przez podmiot, którego dotyczy, co wynika z technologicznej natury Internetu jako sieci autonomicznie połączonych węzłów⁸.

Środowisko cyfrowe prowadzi do zacierania granic między sferą prywatną a publiczną, co wymusza przekształcenie modelu ochrony prawnej jednostki – od biernej ochrony przed ingerencją ku aktywnemu uprawnieniu do kontroli nad dalszym przetwarzaniem raz ujawnionych danych osobowych. Nawet informacje początkowo marginalne mogą zostać utrwalone na nieokreślony czas, wywierając długofalowy wpływ na sytuację prawną i społeczną jednostki. Jak zauważa Viktor Mayer-Schönberger, współczesne społeczeństwo funkcjonuje w warunkach „wiecznej pamięci cyfrowej”, w której zapominanie przestało być procesem naturalnym i stało się wyjątkiem wymagającym aktywnej interwencji prawnej⁹.

Z perspektywy aksjologicznej brak możliwości „zatarcia” przeszłości cyfrowej prowadzi do ryzyka trwałej stygmatyzacji jednostki oraz ograniczenia jej zdolności do autonomicznego kształtowania własnej tożsamości. Problem ten szczególnie wyraźnie ujawnia się w działalności wyszukiwarek internetowych, które poprzez mechanizmy indeksowania i profilowania przekształcają rozproszone zasoby informacyjne w uporządkowany obraz cyfrowy jednostki. Dostęp do takich informacji jest dziś znacząco ułatwiony, a wyszukiwarka tworzy usystematyzowany profil osoby, co może prowadzić do sytuacji, w której błędy z odległej przeszłości oddziałują na jej aktualną sytuację zawodową i społeczną¹⁰. Skutkiem tego może być nieuzasadnione obciążenie wizerunku osoby, której dane dotyczą, nawet wówczas, gdy pierwotne źródło informacji utraciło aktualność lub znaczenie.

W odpowiedzi na zarysowane dylematy w europejskiej kulturze prawnej rozwinęła się koncepcja autonomii informacyjnej, rozumianej jako prawo jednostki do decydowania o ujawnianiu, wykorzystywaniu oraz dalszym losie informacji jej dotyczących¹¹. Koncepcja ta znajduje oparcie nie tylko w unijnym systemie ochrony danych osobowych, lecz także w standardach wynikających z art. 8 Europejskiej konwencji praw człowieka (dalej jako EKPC), gwarantującego prawo do poszanowania życia prywatnego

⁵S. Zuboff, *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, New York 2019, s. 52–62.

⁶Komunikat Komisji Europejskiej do Parlamentu Europejskiego i Rady, Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej, 4.11.2010, COM(2010) 609 final, s. 2–5.

⁷J. Smętek, Z. Warso, „Prawo do bycia zapomnianym” – wzmocnienie autonomii informacyjnej, czy wprowadzenie cenzury w Internecie?, „Europa Praw Człowieka” 2011, nr 2, s. 1–3.

⁸B. Wysocki, op. cit., s. 118.

⁹V. Mayer-Schönberger, *Delete: the virtue of forgetting in the digital age*, Princeton 2009, s. 50–55.

¹⁰K. Ciuckowska, *Prawo do bycia zapomnianym a dostępność w wyszukiwarkach internetowych informacji odnoszących się do życia zawodowego osoby fizycznej*, „Studia Prawnoustrojowe” 2021, nr 53, s. 61–62.

¹¹A. Rouvroy, Y. Poullet, *The right to informational self-determination and the value of self-development*, [w:] S. Gutwirth i in. (red.), *Reinventing data protection?*, Berlin 2009, s. 45–48.

i rodzinnego¹². Szczególnym instrumentem realizacji tej autonomii stało się prawo do bycia zapomnianym, które nabiera cech prawa o charakterze podstawowym¹³. Jego istota nie ogranicza się do technicznego usunięcia danych z systemu informatycznego, lecz obejmuje ochronę godności jednostki oraz możliwość rozpoczęcia „cyfrowego nowego początku”, wolnego od nieuzasadnionego obciążenia przeszłymi informacjami¹⁴. Realizacja tego prawa wymaga jednak każdorazowego wyważenia w relacji do wolności wypowiedzi i przekazywania informacji, chronionej na mocy art. 10 EKPC¹⁵. W tym kontekście prawo do bycia zapomnianym stanowi istotny punkt odniesienia dla rozwoju ochrony praw jednostki w erze nowych mediów¹⁶.

Celem niniejszego artykułu jest analiza ewolucji prawa do bycia zapomnianym w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (dalej jako TSUE) oraz Europejskiego Trybunału Praw Człowieka (dalej jako ETPC)¹⁷. Opracowanie koncentruje się na kształtowaniu tego prawa jako elementu europejskiego systemu ochrony praw podstawowych, jego granicach w relacji do wolności wypowiedzi i interesu publicznego¹⁸ oraz na identyfikacji kryteriów służących waznieniu kolidujących wartości¹⁹. W artykule przyjęto hipotezę, zgodnie z którą prawo do bycia zapomnianym, choć normatywnie ujęte jako uprawnienie proceduralne, w praktyce orzeczniczej nabiera cech prawa o charakterze podstawowym, wymagającego każdorazowego testu proporcjonalności.

Podstawę metodologiczną opracowania stanowi metoda dogmatyczno-prawna, obejmująca analizę normatywną art. 17 rozporządzenia (UE) 2016/679 w kontekście Karty praw podstawowych Unii Europejskiej (dalej jako KPP) oraz EKPC. Metodę tę uzupełnia analiza orzecznictwa TSUE i ETPC, prowadzona z perspektywy funkcjonalnej i ewolucyjnej, a także krytyczny przegląd stanowisk doktryny prawa europejskiego i krajowego.

Normatywne podstawy prawa do bycia zapomnianym w Unii Europejskiej

Geneza prawa do bycia zapomnianym sięga okresu poprzedzającego wejście w życie rozporządzenia (UE) 2016/678. Już art. 12 lit. b dyrektywy 95/46/WE oraz art. 32 ust. 1 pkt 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych przewidywały możliwość usunięcia danych w przypadku ich niekompletności lub niezgodnego

¹²M. Jabłoński, J. Węgrzyn, op. cit., s. 45–50.

¹³Wyrok TSUE z 13 maja 2014 r. w sprawie C-131/12, *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, ECLI:EU:C:2014:317.

¹⁴M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 522–523.

¹⁵K. Ciuckowska, op. cit., s. 65–66.

¹⁶B. Wysocki, op. cit., s. 127.

¹⁷Wyrok TSUE z 24 września 2019 r. w sprawie C-507/17, *Google LLC przeciwko Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772.

¹⁸Wyrok NSA z 9 lutego 2023 r., sygn. akt III OSK 6781/21.

¹⁹Wyrok ETPC (Wielka Izba) z 4 lipca 2023 r., *Hurbain przeciwko Belgii*, skarga nr 57292/16, pkt 165–167.

z prawem przetwarzania²⁰. Rozwiązania te miały jednak charakter fragmentaryczny i nie tworzyły autonomicznego prawa podmiotowego o jednolitym zakresie.

Istotnym impulsem rozwojowym był komunikat Komisji Europejskiej z 2010 r., w którym wskazano na potrzebę zapewnienia użytkownikom Internetu skutecznych instrumentów kontroli nad własnym cyfrowym śladem, w tym prawa do usunięcia danych w razie cofnięcia zgody lub braku innych podstaw prawnych przetwarzania²¹. Współczesnym punktem odniesienia dla analizy normatywnej pozostaje art. 17 RODO, interpretowany w świetle KPP oraz EKPC²². Choć przepis ten posługuje się terminem „prawo do usunięcia danych”, motyw 65 preambuły wyraźnie odwołuje się do konstrukcji „prawa do bycia zapomnianym”, nadając jej samodzielne znaczenie aksjologiczne²³.

W doktrynie wskazuje się na zróżnicowane sposoby rozumienia tej terminologii – jako określenia opisowego tożsamego z prawem do usunięcia danych, szczególnej postaci tego uprawnienia odnoszącej się do określonych sytuacji faktycznych bądź jako konstrukcji rozszerzonej, obejmującej również obowiązek poinformowania innych administratorów. W tym ostatnim ujęciu, jak podkreśla Michał Czerniawski, prawo do bycia zapomnianym obejmuje również tzw. prawo do bycia nieodszukiwalnym, realizowane co do zasady automatycznie w przypadku żądania usunięcia danych uprzednio upublicznionych²⁴.

Kluczowe znaczenie dla ukształtowania tej koncepcji miało orzecznictwo TSUE, w szczególności wyrok w sprawie *Google Spain*. Trybunał wywiódł prawo do deindeksacji wyników wyszukiwania bezpośrednio z przepisów KPP jeszcze przed wejściem w życie RODO, uznając operatora wyszukiwarki internetowej za administratora danych osobowych, zobowiązanego do usuwania odnośników naruszających prawa jednostki do prywatności i ochrony danych osobowych²⁵. Ewolucja tego standardu doprowadziła następnie do doprecyzowania terytorialnego zakresu dereferencji w sprawie *Google LLC przeciwko CNIL*, gdzie TSUE ograniczył obowiązek usuwania linków do domen europejskich, ważąc interes ochrony danych z interesem użytkowników spoza Unii w dostępie do informacji²⁶.

Ogólne rozporządzenie o ochronie danych nie zawiera legalnej definicji pojęcia „usunięcia danych”. W doktrynie i w orzecznictwie przyjmuje się jednak, że obejmuje ono zarówno fizyczne zniszczenie nośnika informacji, jak i takie przekształcenie

²⁰Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31) oraz ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r., poz. 922 z późn. zm.).

²¹Komunikat Komisji..., s. 2–5.

²²Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012, s. 391); Konwencja o ochronie praw człowieka i podstawowych wolności (Dz.U. z 1993 r., Nr 61, poz. 284 z późn. zm.).

²³Zob. motyw 65 preambuły rozporządzenia 2016/679 (RODO).

²⁴M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), op. cit., s. 524–526.

²⁵Wyrok TSUE z 13 maja 2014 r. w sprawie C-131/12, *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, ECLI:EU:C:2014:317.

²⁶Wyrok TSUE z 24 września 2019 r., w sprawie C-507/17, *Google LLC, sukcesor prawny Google Inc. przeciwko Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772, pkt 64–72.

danych, które w sposób trwały i nieodwracalny uniemożliwia identyfikację osoby fizycznej. W tym znaczeniu skuteczna anonimizacja może zostać uznana za jedną z form realizacji obowiązku przewidzianego w art. 17 RODO, o ile ryzyko ponownej identyfikacji jest praktycznie wyeliminowane²⁷.

Przesłanki realizacji prawa do usunięcia danych zostały określone w art. 17 ust. 1 RODO i mają charakter alternatywny. W praktyce szczególne znaczenie ma ocena, czy dane osobowe pozostają „niezbędne” do celów, dla których zostały zebrane. Ocena ta bywa źródłem sporów, gdyż subiektywne przekonanie osoby, której dane dotyczą, o zakończeniu celu przetwarzania może pozostawać w kolizji z oceną administratora, powołującego się na potrzebę dalszego przetwarzania danych, w szczególności dla zabezpieczenia własnych roszczeń²⁸.

Jednym z kluczowych instrumentów realizacji autonomii informacyjnej jednostki jest cofnięcie zgody w sytuacji, gdy stanowiła ona jedyną podstawę przetwarzania danych osobowych. Motyw 65 preambuły RODO akcentuje w tym zakresie szczególną ochronę osób, które wyraziły zgodę jako dzieci, nie będąc w pełni świadome długofalowych konsekwencji upubliczniania informacji w środowisku cyfrowym. Z tego względu prawo do usunięcia danych powinno umożliwiać jednostce odzyskanie kontroli nad własną tożsamością także po osiągnięciu pełnoletności, co znajduje normatywne odzwierciedlenie m.in. w art. 17 ust. 1 lit. f RODO²⁹.

Istotną rolę w procesie realizacji prawa do bycia zapomnianym odgrywa również instytucja sprzeciwu, uregulowana w art. 21 RODO. Skuteczność żądania usunięcia danych zależy od charakteru sprzeciwu: w przypadku przetwarzania danych na potrzeby marketingu bezpośredniego sprzeciw ma charakter bezwzględny, natomiast w pozostałych sytuacjach wymaga przeprowadzenia testu równowagi interesów. W wyrokach z 7 grudnia 2023 r. w sprawach połączonych *SCHUFA Holding* (C-26/22 i C-64/22) TSUE wzmocnił pozycję jednostki, wskazując, że zgodnie z zasadą rozliczalności to na administratorze spoczywa ciężar wykazania, iż jego prawnie uzasadnione interesy mają nadrzędny charakter wobec praw i wolności osoby wnoszącej o usunięcie danych³⁰.

Realizacja prawa do usunięcia danych w środowisku cyfrowym napotyka istotne ograniczenia techniczne, które wynikają ze sposobu projektowania i funkcjonowania współczesnych systemów informatycznych³¹. Szczególne znaczenie mają w tym kontekście mechanizmy tworzenia kopii zapasowych (ang. *backup*), których celem jest zapewnienie ciągłości działania systemów oraz odporności na awarie i incydenty bezpieczeństwa.

Powszechnie stosowane rozwiązania archiwizacyjne często uniemożliwiają selektywne usunięcie pojedynczego rekordu bez naruszenia integralności całego zbioru danych. Z tego względu obowiązek realizacji art. 17 RODO powinien być analizowany w ścisłym

²⁷ Wyrok NSA z 11 kwietnia 2017 r., sygn. akt I OSK 2170/15, Lex nr 2293432.

²⁸ P. Litwiński, P. Barta, M. Kawecki, [w:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2025, s. 285.

²⁹ Zob. motyw 65 preambuły rozporządzenia 2016/679; por. ibidem, s. 287.

³⁰ Wyrok TSUE z 7 grudnia 2023 r. w sprawach połączonych C-26/22 i C-64/22, *UF i AB przeciwko Land Hessen*, ECLI:EU:C:2023:958, pkt 60–66.

³¹ P. Fajgielski, op. cit., s. 303–305.

związku z art. 32 RODO, który nakłada na administratora obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania³². Skuteczna realizacja prawa do usunięcia danych wymaga zatem przeprowadzenia rzetelnej analizy ryzyka, uwzględniającej aktualny stan wiedzy technicznej, charakter przetwarzania oraz koszty wdrożenia adekwatnych środków ochrony³³.

W doktrynie trafnie podkreśla się, że obowiązek zabezpieczenia danych osobowych nie ma charakteru zobowiązania rezultatu, lecz zobowiązania starannego działania³⁴. Administrator nie jest zobowiązany do stosowania rozwiązań absolutnie eliminujących wszelkie potencjalne ryzyka, lecz do wdrożenia środków ocenianych *ex ante* jako adekwatne w świetle dostępnych możliwości technicznych oraz specyfiki danego procesu przetwarzania³⁵.

W odniesieniu do kopii zapasowych środki te mogą obejmować m.in. procedury cyklicznego nadpisywania danych, ograniczenie dostępu do backupów wyłącznie do celów odtworzeniowych, a także mechanizmy logicznego usuwania danych, które uniemożliwiają ich odczyt po ewentualnym przywróceniu systemu³⁶. Dopuszczalne jest czasowe przechowywanie danych osobowych w systemach kopii zapasowych, o ile administrator zapewnia ich izolację od bieżących procesów przetwarzania oraz automatyczne usunięcie zgodnie z przyjętą polityką retencji. Skuteczność tych rozwiązań powinna podlegać regularnemu testowaniu i dokumentowaniu, co stanowi praktyczną realizację zasady rozliczalności z art. 5 ust. 2 RODO³⁷. Jak podkreśla Arwid Mednis, relacja między prywatnością a interesem publicznym wymaga każdorazowo ważenia wartości, a nie mechanicznego uprzywilejowania jednej z nich³⁸.

Zgodnie z art. 17 ust. 2 RODO administrator, który upublicznił dane osobowe, jest zobowiązany do poinformowania innych administratorów przetwarzających te dane o zgłoszonym żądaniu usunięcia wszelkich łączy, kopii lub replikacji danych. Rozróżnienie między kopiami a replikacjami ma przede wszystkim charakter techniczny – kopia stanowi statyczne odwzorowanie określonego zbioru informacji, natomiast replikacja polega na dynamicznej synchronizacji danych pomiędzy systemami³⁹. Obowiązek notyfikacyjny obejmuje oba te sposoby utrwalenia danych, niezależnie od ich technicznej formy.

Zakres działań wymaganych od administratora został przez prawodawcę ograniczony kryteriami „dostępnej technologii” oraz „kosztu wdrożenia”, wskazanymi w motywie 66 preambuły RODO. Kryteria te wymagają dokonania wieloaspektowej oceny kontekstowej, obejmującej aktualny stan wiedzy technicznej, skalę i charakter operacji przetwarzania, a także realne możliwości organizacyjne i finansowe administratora⁴⁰.

³² P. Barta, M. Kawecki, P. Litwiński, [w:] P. Litwiński (red.), op. cit., s. 289.

³³ Ibidem, s. 290.

³⁴ G. Sibiga, *Prawne aspekty bezpieczeństwa danych osobowych*, Warszawa 2023, s. 88–92.

³⁵ P. Barta, M. Kawecki, P. Litwiński, [w:] P. Litwiński (red.), op. cit., s. 383.

³⁶ Szerzej: P. Fajgielski, op. cit., s. 308–310.

³⁷ Ibidem, s. 374.

³⁸ A. Mednis, *Prawo do prywatności a interes publiczny*, Warszawa 2006, s. 42–44.

³⁹ M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), op. cit., s. 525.

⁴⁰ Ibidem, s. 527.

W konsekwencji miernik należytej staranności podlega zróżnicowaniu: od globalnych platform cyfrowych oczekuje się wdrażania bardziej zaawansowanych rozwiązań technicznych i organizacyjnych niż od podmiotów o ograniczonych zasobach⁴¹.

Obowiązek wynikający z art. 17 ust. 2 RODO ma charakter zobowiązania starannego działania, a nie zobowiązania rezultatu. Administrator jest zobligowany do podjęcia rozsądnych i proporcjonalnych środków zmierzających do poinformowania innych administratorów, nie ponosi natomiast odpowiedzialności za okoliczności pozostające poza jego faktyczną kontrolą⁴². Należy przy tym podkreślić, że samo dokonanie notyfikacji nie skutkuje automatycznym związaniem powiadomionych administratorów żądaniem usunięcia danych. Każdy z nich zachowuje autonomię w zakresie oceny, czy w danym przypadku nie zachodzą przesłanki uzasadniające dalsze przetwarzanie danych, w szczególności te wskazane w art. 17 ust. 3 RODO⁴³. W tym sensie skuteczność prawa do bycia zapomnianym zależy nie tylko od samej normy prawnej, lecz także od jakości procedur, infrastruktury technicznej i przyjętego modelu odpowiedzialności administratora⁴⁴.

Prawo do bycia zapomnianym nie ma charakteru absolutnego. Art. 17 ust. 3 RODO ustanawia katalog przesłanek wyłączających obowiązek usunięcia danych osobowych w sytuacjach, w których realizacja tego prawa pozostawałaby w kolizji z interesem publicznym lub prawami i wolnościami innych osób. Szczególnie doniosłą płaszczyzną konfliktu jest relacja pomiędzy prawem do prywatności i ochrony danych osobowych a wolnością wypowiedzi i wolnością informacji. W orzecznictwie europejskim dostrzegana jest stopniowa ewolucja standardów, zmierzająca ku coraz bardziej zniuansowanemu modelowi wagi kolidujących wartości, opartemu na zasadzie proporcjonalności oraz ocenie roli danej informacji w debacie publicznej. Kluczowe znaczenie mają przy tym takie kryteria, jak upływ czasu, charakter informacji, status osoby, której dane dotyczą, oraz funkcja, jaką dana publikacja pełni w przestrzeni publicznej⁴⁵. Analiza tych przesłanek musi być dokonywana w ścisłym powiązaniu ze standardem wyznaczonym przez art. 10 EKPC. Jak podkreśla Marek A. Nowicki, gwarantowana konwencyjnie swoboda wypowiedzi, a więc termin o zakresie znacznie szerszym niż potoczna wolność opinii, stanowi jeden z fundamentalnych warunków funkcjonowania demokracji⁴⁶. Swoboda ta nie ma jednak charakteru absolutnego. Na mocy art. 10 ust. 2 EKPC korzystanie z tej wolności może podlegać ograniczeniom i sankcjom, które są niezbędne w społeczeństwie demokratycznym, między innymi ze względu na ochronę dobrego imienia i praw innych osób. To właśnie ta klauzula limitacyjna – w interpretacji strasburskiej – stanowi normatywny pomost do realizacji prawa do bycia zapomnianym. Wymusza ona bowiem na państwie nie tylko obowiązek powstrzymania się od ingerencji, ale również podejmowanie

⁴¹ P. Barta, M. Kawecki, P. Litwiński, [w:] P. Litwiński (red.), op. cit., s. 289–290.

⁴² Ibidem, s. 520.

⁴³ M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), op. cit., s. 290.

⁴⁴ M. Jabłoński, J. Węgrzyn, op. cit., s. 145–148.

⁴⁵ P. Barta, M. Kawecki, P. Litwiński, [w:] P. Litwiński (red.), op. cit., s. 291–292.

⁴⁶ M.A. Nowicki, *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, 2025, Lex, komentarz do art. 10.

aktywnych działań w celu ochrony prywatności jednostki przed nadmierną i trwałą stygmatyzacją w przestrzeni cyfrowej⁴⁷.

Ilustracją tego podejścia jest wyrok Wielkiej Izby ETPC w sprawie *Hurbain przeciwko Belgii*, w którym ETPC uznał, że nałożenie na wydawcę obowiązku anonimizacji danych osobowych sprawcy wypadku drogowego w cyfrowym archiwum prasowym, po upływie okresu zatarcia skazania, stanowiło proporcjonalną ingerencję w wolność wypowiedzi. ETPC podkreślił, że trwała i łatwa dostępność informacji w archiwach internetowych może prowadzić do powstania swoistej „wirtualnej kartoteki karnej”, co w określonych okolicznościach uzasadnia wzmocnioną ochronę interesów jednostki, zwłaszcza gdy osoba, której dane dotyczą, nie pełni funkcji publicznych⁴⁸.

Na gruncie prawa polskiego relacja między art. 17 RODO a działalnością prasową ujawnia istotne napięcia interpretacyjne. W wyroku z 9 lutego 2023 r. Naczelny Sąd Administracyjny przyjął restrykcyjną wykładnię pojęcia działalności prasowej, wskazując na to, że samo udostępnianie materiałów archiwalnych w Internecie nie zawsze wypełnia jej znamiona. Taka interpretacja prowadzi do zawężenia zakresu stosowania tzw. klauzuli prasowej, a w konsekwencji może ułatwiać realizację żądań usunięcia danych osobowych⁴⁹. Stanowisko to spotkało się jednak z istotną krytyką w doktrynie, w której podnosi się, że nadmiernie formalistyczne podejście do pojęcia działalności prasowej może zagrażać integralności cyfrowych archiwów prasowych oraz osłabiać konstytucyjną rolę prasy jako „publicznego stróża” w demokratycznym państwie prawnym⁵⁰. Spór ten unaocznia trudność w wyznaczeniu stabilnej granicy między ochroną autonomii informacyjnej jednostki a potrzebą zachowania dostępu do informacji o znaczeniu publicznym. Ostatecznie prawo do bycia zapomnianym przekształciło się z technicznego uprawnienia do korekty danych w samodzielne prawo podstawowe, będące istotnym gwarantem godności i wolności jednostki w zautomatyzowanym społeczeństwie informacyjnym⁵¹.

Podsumowując, prawo do bycia zapomnianym stanowi konstrukcję dynamiczną, której znaczenie ukształtowało się na styku ochrony danych osobowych, prywatności oraz wolności wypowiedzi. Analiza genezy i przesłanek jego realizacji prowadzi do wniosku, że art. 17 RODO nie jest jedynie martwym zapisem, lecz mechanizmem ochronnym o charakterze złożonym, którego skuteczność zależy od kontekstu normatywnego, technologicznego i aksjologicznego. Prawo to nie ma charakteru absolutnego; jego realizacja wymaga każdorazowego, precyzyjnego ważenia z wolnością wypowiedzi, zwłaszcza w świetle art. 10 EKPC i bogatego orzecznictwa ETPC. W konsekwencji europejski standard ochrony prawa do bycia zapomnianym należy postrzegać jako wyraz współczesnego modelu ochrony godności jednostki w środowisku cyfrowym, który w centrum zainteresowania stawia podmiotowość jednostki wobec „wiecznej pamięci” algorytmów.

⁴⁷ Zob. wyrok Wielkiej Izby ETPC z 4 lipca 2023 r., *Hurbain przeciwko Belgii*, skarga nr 57292/16, pkt 165–167.

⁴⁸ Ibidem, pkt 192–210.

⁴⁹ Wyrok NSA z 9 lutego 2023 r., sygn. akt III OSK 6781/21.

⁵⁰ M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), op. cit., s. 530–532.

⁵¹ M. Jabłoński, J. Węgrzyn, op. cit., s. 145–148.

Rola sądów europejskich w kształtowaniu standardu ochrony prawa do bycia zapomnianym

Wyrok TSUE z 13 maja 2014 r. w sprawie *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González* stanowi punkt zwrotny w rozwoju prawa do bycia zapomnianym w europejskim porządku prawnym⁵². Orzeczenie to zapadło na tle problemu trwałości informacji w Internecie, którego „doskonała pamięć” pozostaje w sprzeczności z naturalnym procesem zapominania właściwym dla relacji społecznych poza środowiskiem cyfrowym. TSUE uznał, że działalność operatora wyszukiwarki internetowej obejmująca indeksowanie oraz udostępnianie informacji opublikowanych przez osoby trzecie stanowi przetwarzanie danych osobowych, a sam operator jest administratorem tych danych. W konsekwencji TSUE przesądził, że wyszukiwarka nie pełni jedynie biernej funkcji technicznej, lecz uczestniczy w kształtowaniu dostępności informacji o jednostce, a więc bezpośrednio wpływa na zakres ochrony jej prywatności i danych osobowych.

W doktrynie zwraca się uwagę, że taka kwalifikacja jest przedmiotem kontrowersji, gdyż prowadzi do odejścia od postrzegania pośredników internetowych jako podmiotów pełniących pasywną funkcję techniczną⁵³. Przyjęcie, że wyszukiwarka jest administratorem, implikuje konieczność dokonywania przez nią ocen o charakterze quasi-prawnym, dotyczących kolizji prywatności z wolnością informacji⁵⁴. W tym sensie rozwój standardu TSUE można określić jako przejście od konstrukcji deindeksacji jako środka jednostkowego do bardziej złożonego modelu ochrony, w którym wążenie interesów jednostki i interesu publicznego odbywa się również z uwzględnieniem terytorialnego zasięgu oddziaływania prawa. TSUE przyjął, że prawa wynikające z art. 7 i 8 KPP co do zasady mają pierwszeństwo przed interesem gospodarczym operatora oraz interesem użytkowników w dostępie do informacji, chyba że dostęp ten znajduje uzasadnienie w nadrzędnym interesie publicznym⁵⁵. Prawo do bycia zapomnianym nie ma zatem charakteru absolutnego i nie prowadzi do usunięcia informacji z przestrzeni publicznej, lecz do ograniczenia możliwości ich odnalezienia i dalszego rozpowszechniania.

Istotną cezurę w procesie kształtowania się standardów ochrony danych stanowi wyrok TSUE z 24 września 2019 r. w sprawie *Google LLC przeciwko CNIL*, dotyczący terytorialnego zakresu obowiązku dereferencji⁵⁶. Sprawa ta ujawniła napięcie między potrzebą skutecznej ochrony danych a suwerennością państw i pluralizmem standardów wolności wypowiedzi w skali globalnej. Istotnym punktem odniesienia była opinia Rzecznika Generalnego TSUE Macieja Szpunara, który opowiedział się przeciwko koncepcji globalnej dereferencji, wskazując na ryzyko eksterytorialnego stosowania prawa

⁵² Wyrok TSUE z 13 maja 2014 r. w sprawie C-131/12, *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, ECLI:EU:C:2014:317.

⁵³ P. Fajgielski, op. cit., s. 303.

⁵⁴ M. Czerniawski, [w:] E. Bielak-Jomaa, D. Lubasz (red.), op. cit., s. 524.

⁵⁵ Wyrok TSUE z 13 maja 2014 r. w sprawie C-131/12, pkt 97–99.

⁵⁶ Wyrok TSUE z 24 września 2019 r. w sprawie C-507/17, *Google LLC przeciwko Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772.

UE⁵⁷. W opinii tej podkreślono również, że obowiązek usuwania wyników wyszukiwania w skali światowej mógłby prowadzić do nadmiernego uprzywilejowania standardu unijnego kosztem innych porządków prawnych i wolności informacji w państwach trzecich.

TSUE podzielił to stanowisko, uznając, że ani dyrektywa 95/46/WE, ani art. 17 RODO nie nakładają na operatora obowiązku dokonywania dereferencji w skali ogólnoświatowej⁵⁸. Jednocześnie TSUE podkreślił, że realizacja tego prawa nie może mieć charakteru iluzorycznego, zobowiązując operatora do usunięcia linków we wszystkich wersjach wyszukiwarki odpowiadających państwom członkowskim UE oraz do zastosowania środków takich jak geoblokowanie⁵⁹. Rozwiązanie to spotkało się z krytyką w doktrynie, gdyż ograniczenie dereferencji do obszaru UE może osłabiać realną skuteczność ochrony, czyniąc ją fragmentaryczną⁶⁰. Orzeczenie to potwierdziło, że standard ochrony wypracowany przez TSUE opiera się na równoważeniu prawa jednostki do prywatności z interesem społecznym w dostępie do informacji, również w kontekście terytorialnych granic stosowania prawa UE. W tym sensie rozwój standardu TSUE można określić jako przejście od konstrukcji deindeksacji jako środka jednostkowego do bardziej złożonego modelu ochrony, w którym ważenie interesów jednostki i interesu publicznego odbywa się również z uwzględnieniem terytorialnego zasięgu oddziaływania prawa.

Analiza standardu ochrony prawa do bycia zapomnianym wymaga wyjścia poza relację jednostka-pośrednik (w szczególności operator wyszukiwarki internetowej) oraz uwzględnienia obowiązków nakładanych bezpośrednio na wydawców prasowych. Kluczowym punktem odniesienia jest tutaj wyrok Wielkiej Izby ETPC z 4 lipca 2023 r. w sprawie *Hurbain przeciwko Belgii*, który redefiniuje granice ingerencji w cyfrowe archiwa mediów. Sprawa ta dotyczyła żądania anonimizacji materiału prasowego z lat 90., dokumentującego wypadek drogowy. Mimo upływu kilku dekad oraz zatarcia skazania sprawca zdarzenia pozostawał łatwo identyfikowalny dzięki cyfrowym zasobom dziennika „Le Soir”, co prowadziło do jego trwałej stygmatyzacji w przestrzeni publicznej. Trybunał potwierdził, że art. 8 EKPC może uzasadniać ingerencję w wolność prasy, wprowadzając koncepcję anonimizacji „u źródła”. ETPC – w przeciwieństwie do paradygmatu TSUE – wskazał na to, że w określonych warunkach to wydawca, jako podmiot kontrolujący treść, jest zobowiązany do modyfikacji materiału archiwalnego w sposób chroniący prywatność jednostki. Jednocześnie zaznaczył, że ingerencja ta nie ma na celu „pisanie historii na nowo”, lecz ograniczenie nieproporcjonalnej identyfikowalności osoby, której dane dotyczą.

Wielka Izba podkreśliła rolę prasy jako „publicznego strażnika” (ang. *public watchdog*), podkreślając jednocześnie, że trwała dostępność informacji o przeszłości karnej w formie cyfrowej prowadzi do powstania swoistej „wirtualnej kartoteki karnej”⁶¹.

⁵⁷ Opinia Rzecznika Generalnego Macieja Szpunara z 10 stycznia 2019 r. w sprawie C-507/17, *Google LLC przeciwko CNIL*, ECLI:EU:C:2019:15, pkt 47–60.

⁵⁸ Wyrok TSUE z 24 września 2019 r. w sprawie C-507/17, pkt 60–65.

⁵⁹ Ibidem, pkt 70–72.

⁶⁰ P. Barta, M. Kawecki, P. Litwiński, [w:] P. Litwiński (red.), op. cit., s. 283–284.

⁶¹ Wyrok Wielkiej Izby ETPC z 4 lipca 2023 r., *Hurbain przeciwko Belgii*, skarga nr 57292/16, pkt 167–168.

Jak trafnie podnosi w głosie do tego wyroku Dominika Bychawska-Siniarska, orzeczenie to sankcjonuje prawo do „nowego cyfrowego początku”, uznając, że upływ czasu oraz brak statusu osoby publicznej u skarżącego stanowią okoliczności przeważające nad interesem publicznym w dostępie do niezmienionego materiału⁶². ETPC nie odrzuca przy tym funkcji archiwalnej prasy, lecz wskazuje na to, że także archiwa cyfrowe muszą być oceniane z perspektywy art. 8 i art. 10 EKPC w świetle zasady proporcjonalności.

Trybunał zaznaczył, że anonimizacja online jest środkiem mniej dolegliwym niż całkowite usunięcie artykułu (co naruszałoby integralność archiwów), a jednocześnie skuteczniejszym niż dereferencja w wyszukiwarkach, gdyż trwale eliminuje bezpośrednią identyfikowalność w materiale źródłowym. Bychawska-Siniarska wskazuje jednak na ryzyka płynące z tego wyroku, podkreślając, że może on generować tzw. efekt mrozący (ang. *chilling effect*) wobec wydawców, zmuszając ich do merytorycznej rewizji zasobów archiwalnych pod presją roszczeń osób prywatnych⁶³. Aby tego uniknąć, ETPC nakazuje stosowanie technologii selektywnych, takich jak *tagi noindex* czy edycja nazwisk wyłącznie w wersji cyfrowej, co pozwala pogodzić autonomię informacyjną jednostki z historyczną funkcją mediów⁶⁴. Wyrok w sprawie *Hurbain* domyka tym samym europejski standard ochrony, wskazując na to, że w dobie „wiecznej pamięci cyfrowej” ochrona godności wymaga niekiedy aktywnej modyfikacji cyfrowego śladu bezpośrednio u źródła publikacji.

Warto też zauważyć, że standard ten nie powstał w próżni, lecz wpisuje się w szerszą linię orzecniczą ETPC, odnoszącą się do ważenia prywatności z wolnością wypowiedzi, rozwijaną wcześniej w sprawach *Axel Springer AG przeciwko Niemcom* oraz *Von Hannover przeciwko Niemcom* (nr 2), gdzie ETPC wypracował kryteria oceny dopuszczalności ingerencji w życie prywatne osób publicznych i prywatnych⁶⁵.

Analiza dorobku orzecniczego TSUE oraz ETPC wskazuje na to, że prawo do bycia zapomnianym wyewoluowało w elastyczny standard ochrony, oparty na paradygmacie ważenia konkurujących wartości. Kluczowe dla zrozumienia tego mechanizmu jest rozróżnienie jego trzech płaszczyzn: normatywnej (wyznaczonej przez art. 17 RODO), technicznej (obejmującej prawo do deindeksacji w rozumieniu wyroku *Google Spain*) oraz archiwalnej (opartej na standardzie anonimizacji u źródła wypracowanym w sprawie *Hurbain*). Europejskie trybunały konsekwentnie odrzucają absolutny charakter tego uprawnienia, podkreślając jego relacyjny i kontekstowy wymiar. Granice ochrony wyznacza każdorazowo test proporcjonalności, w którym decydującą rolę odgrywa status osoby (publiczny albo prywatny), charakter informacji oraz upływ czasu, który, pełniąc funkcję erozyjną, stopniowo wygasza interes publiczny w dostępie do danych kosztem ochrony

⁶²D. Bychawska-Siniarska, *Pamięć cyfrowa a prawo do prywatności. Glosa do wyroku Wielkiej Izby ETPC z dnia 4 lipca 2023 r. w sprawie Hurbain przeciwko Belgii*, „Europejski Przegląd Sądowy” 2024, nr 1, s. 36.

⁶³Ibidem, s. 39–41.

⁶⁴Wyrok Wielkiej Izby ETPC z 4 lipca 2023 r., *Hurbain przeciwko Belgii*, pkt 211–215. Por. też wyrok ETPC z 16 czerwca 2015 r., *Delfi AS przeciwko Estonii*, skarga nr 64569/09.

⁶⁵Wyroki ETPC z 7 lutego 2012 r.: *Axel Springer AG przeciwko Niemcom*, skarga nr 39954/08; *Von Hannover przeciwko Niemcom* (nr 2), skargi nr 40660/08 i 60641/08.

sfery prywatnej. W tym modelu prawo do bycia zapomnianym nie jest już wyłącznie technicznym środkiem korekty danych, lecz staje się jednym z instrumentów ochrony godności jednostki w warunkach trwałej cyfrowej identyfikowalności.

Ewolucja orzecznictwa zmierza wyraźnie w stronę pragmatycznego ujęcia terytorialnego i funkcjonalnego. Wyrok w sprawie *Google przeciwko CNIL* ustalił granice geograficzne ochrony, co pozwoliło pogodzić standardy unijne z pluralizmem informacyjnym państw trzecich. Z kolei judykatura ETPC oraz orzecznictwo krajowe odchodzą od binarnego rozumienia „usunięcia danych” na rzecz środków pośrednich. Rozwiązania, takie jak deindeksacja, depozycjonowanie lub selektywna anonimizacja, umożliwiają realizację postulatu „cyfrowego nowego początku” (ang. *clean slate*) bez naruszania integralności archiwów cyfrowych i niszczenia zasobów historycznych. Jednocześnie jednak praktyka ta ujawnia napięcie między skutecznością ochrony jednostki a ryzykiem fragmentaryzacji pamięci zbiorowej, które musi być każdorazowo rozstrzygane z uwzględnieniem zasady proporcjonalności.

Szczególne wyzwania interpretacyjne w tym obszarze generuje działalność wydawnicza i archiwalna. Na gruncie prawa polskiego kluczowe znaczenie ma ewolucja stanowiska Naczelnego Sądu Administracyjnego, zmierzająca w stronę wzmocnienia ochrony jednostki kosztem autonomii archiwów prasowych. W przełomowym wyroku z 9 lutego 2023 r., sygn. akt III OSK 6781/21 Naczelny Sąd Administracyjny przyjął restrykcyjną wykładnię tzw. klauzuli prasowej. Sąd uznał, że samo udostępnianie archiwalnych materiałów prasowych nie zawsze stanowi działalność prasową pozwalającą na skorzystanie z wyłączenia przewidzianego w art. 2 ust. 1 ustawy Prawo prasowe. Według Naczelnego Sądu Administracyjnego ochrona ta przysługuje tylko wtedy, gdy publikacja realizuje ustawowe zadania prasy związane z prawem obywateli do rzetelnej informacji i jawnością życia publicznego, co w przypadku wieloletnich zasobów cyfrowych nie zawsze jest spełnione. Takie stanowisko legitymizuje roszczenia o realizację prawa do bycia zapomnianym bezpośrednio wobec wydawców, nakładając na nich obowiązek anonimizacji dawnych publikacji, jeśli ustał cel ich przetwarzania (np. upłynął okres zatarcia skazania). W doktrynie wskazuje się jednak na to, że takie podejście może prowadzić do niebezpiecznego zjawiska „retuszowania historii” i naruszenia integralności narodowych zasobów informacyjnych. Dlatego też współczesny standard ochrony nie sprowadza się do prostego uprzywilejowania jednostki albo prasy, lecz do poszukiwania rozwiązań, które umożliwiają zachowanie archiwów przy jednoczesnym ograniczeniu nieproporcjonalnej identyfikowalności osoby.

Mimo tych postępów obecny model ujawnia istotną niespójność systemową. Przerzucenie ciężaru merytorycznej oceny wniosków na operatorów wyszukiwarek doprowadziło do prywatyzacji rozstrzygania kolizji dóbr podstawowych. Podmioty komercyjne, występując w roli quasi-sędziów (ang. *gatekeepers*), w obawie przed dotkliwymi sankcjami administracyjnymi mogą stosować nadmierne blokowanie treści (ang. *over-blocking*), co stanowi realne zagrożenie dla wolności słowa i prawa do informacji. Z tego względu zarówno TSUE, jak i ETPC coraz wyraźniej akcentują potrzebę procedur pozwalających

na kontrolę sądową lub quasi-sądową nad rozstrzygnięciami podejmowanymi przez administratorów i pośredników internetowych.

W dobie „cyfrowej nieśmiertelności” prawo do bycia zapomnianym staje się fundamentem ochrony godności jednostki. Jego ostateczna skuteczność zależy jednak nie od mechanicznego usuwania treści, lecz od wypracowania przejrzystych procedur nadzoru sądowego nad procesami automatycznej moderacji. To właśnie ewolucja w stronę ochrony przed stygmatyzacją, realizowana przez precyzyjne instrumenty techniczne, a nie tylko normatywne nakazy, stanowi o sile europejskiego modelu ochrony praw podstawowych. W konsekwencji prawo do bycia zapomnianym należy dziś postrzegać jako instrument ochrony prawa do prywatności i autonomii informacyjnej, którego zakres oraz granice są współkształtowane przez orzecznictwo TSUE, ETPC oraz praktykę krajową.

Podsumowanie

Przeprowadzona analiza prawa do bycia zapomnianym w europejskim ekosystemie cyfrowym prowadzi do wniosku, że instytucja ta przeszła ewolucję od wąskiego uprawnienia proceduralnego do jednego z elementów standardu ochrony praw podstawowych, nierozzerwalnie związanego z autonomią informacyjną i godnością jednostki. W warunkach trwałej cyfrowej pamięci prawo to pełni kluczową funkcję korekcyjną, ograniczając nieproporcjonalne skutki utrwalania informacji o przeszłości człowieka, które w świecie analogowym uległyby naturalnemu procesowi zatarcia.

Analiza dorobku orzeczniczego TSUE, zapoczątkowana wyrokiem w sprawie *Google Spain*, potwierdziła pierwszeństwo praw jednostki wynikających z art. 7 i 8 KPP nad interesem ekonomicznym operatorów wyszukiwarek. Jednocześnie ewolucja tego standardu, widoczna w sprawie *Google LLC przeciwko CNIL*, wskazuje na dążenie do pragmatycznego kompromisu między efektywnością ochrony danych w Unii Europejskiej a globalnym charakterem obiegu informacji. Standard ten został istotnie dopełniony przez orzecznictwo ETPC, w szczególności wyrok w sprawie *Hurbain przeciwko Belgii*, wprowadzający koncepcję anonimizacji u źródła. Podejście to pozwala rozumieć cyfrowe zapomnienie nie jako fizyczną eliminację treści, lecz jako ograniczenie identyfikowalności jednostki, przy jednoczesnym poszanowaniu integralności archiwów prasowych jako depozytariuszy pamięci zbiorowej.

Istotnym wnioskiem z badań jest dostrzeżenie systemowych napięć związanych z rolą operatorów wyszukiwarek jako podmiotów o charakterze quasi-orzeczniczym. Obciążenie podmiotów komercyjnych obowiązkiem merytorycznego ważenia kolidujących dóbr konstytucyjnych rodzi ryzyko „prywatyzacji cenzury”. Choć mechanizmy wprowadzone przez akt o usługach cyfrowych (ang. *Digital Services Act* – DSA) porządkują procesy moderacji, nie eliminują w pełni problemu algorytmicznego filtrowania dostępu do informacji.

Potwierdza się również teza o rygorystycznym podejściu organów krajowych. Polska linia orzecznicza (m.in. wyrok Naczelnego Sądu Administracyjnego z 9 lutego 2023 r.) jednoznacznie dowodzi, że bariery technologiczne nie mogą zwalniać administratorów z obowiązku realizacji art. 17 RODO. Wymusza to realne stosowanie zasady ochrony

prywatności (ang. *privacy by design*), co w praktyce oznacza konieczność wdrażania rozwiązań funkcjonalnie równoważnych, takich jak zaawansowana anonimizacja czy kryptograficzna izolacja danych.

Podsumowując, postawiona w artykule hipoteza badawcza została potwierdzona. Prawo do bycia zapomnianym ukształtowało się jako trwały instrument ochrony autonomii informacyjnej, jednak jego pełna efektywność pozostaje uzależniona od dalszego rozwoju standardów orzeczniczych, technologicznych oraz organizacyjnych. Przyszłość tego prawa będzie zależeć od wypracowania funkcjonalnej wykładni przepisów, która połączy paradygmat jurydyczny z rozwiązaniami technicznymi umożliwiającymi skuteczną ochronę danych w środowisku cyfrowym. Skuteczna ochrona praw podstawowych w XXI w. wymaga bowiem nie tylko precyzyjnych regulacji prawnych, lecz również rozwiązań technologicznych i organizacyjnych, które zapewnią rzeczywistą realizację zasady poszanowania godności oraz autonomii informacyjnej jednostki.

BIBLIOGRAFIA

Literatura

- Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.
- Bychawska-Siniarska D., *Pamięć cyfrowa a prawo do prywatności. Glosa do wyroku Wielkiej Izby ETPCz z dnia 4 lipca 2023 r. w sprawie Hurbain przeciwko Belgii*, „Europejski Przegląd Sądowy” 2024, nr 1.
- Ciuckowska K., *Prawo do bycia zapomnianym a dostępność w wyszukiwarkach internetowych informacji odnoszących się do życia zawodowego osoby fizycznej*, „Studia Prawnoustrojowe” 2021, nr 53.
- Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2025.
- Jabłoński M., Węgrzyn J., *Prawo do bycia zapomnianym*, Wrocław 2021.
- Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2025.
- Mayer-Schönberger V., *Delete: the virtue of forgetting in the digital age*, Princeton 2009.
- Mednis A., *Prawo do prywatności a interes publiczny*, Warszawa 2006.
- Nowicki M.A., *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, 2025, Lex.
- Rouvroy A., Pouillet Y., *The right to informational self-determination and the value of self-development*, [w:] S. Gutwirth i in. (red.), *Reinventing data protection?*, Berlin 2009.
- Sibiga G., *Prawne aspekty bezpieczeństwa danych osobowych*, Warszawa 2023.
- Smętek J., Warso Z., *„Prawo do bycia zapomnianym” – wzmocnienie autonomii informacyjnej, czy wprowadzenie cenzury w Internecie?*, „Europa Praw Człowieka” 2011, nr 2.

Warren S.D., Brandeis L.D., *The right to privacy*, „Harvard Law Review” 1890, vol. 4, nr 5.
Wysocki B., *Prawo do bycia zapomnianym – prawem cyfrowej rzeczywistości*, „Ars Educandi” 2016, nr 13.

Zuboff S., *The age of surveillance capitalism. The fight for a human future at the new frontier of power*, New York 2019.

Akty prawne i dokumenty

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31).

Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012, s. 391).

Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz.U. z 1993 r., Nr 61, poz. 284 ze zm.).

Komunikat Komisji Europejskiej do Parlamentu Europejskiego i Rady, Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej, 4.11.2010, COM(2010) 609 final.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, s. 1).

Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (t.j. Dz.U. z 2018 r., poz. 1914).

Orzecznictwo

Opinia Rzecznika Generalnego Macieja Szpunara z 10 stycznia 2019 r. w sprawie C-507/17, *Google LLC przeciwko CNIL*, ECLI:EU:C:2019:15.

Wyrok ETPC z 7 lutego 2012 r., *Axel Springer AG przeciwko Niemcom*, skarga nr 39954/08.

Wyrok ETPC z 7 lutego 2012 r., *Von Hannover przeciwko Niemcom (nr 2)*, skargi nr 40660/08 i 60641/08.

Wyrok ETPC z 16 czerwca 2015 r., *Delfi AS przeciwko Estonii*, skarga nr 64569/09.

Wyrok ETPC (Wielka Izba) z 4 lipca 2023 r., *Hurbain przeciwko Belgii*, skarga nr 57292/16.

Wyrok NSA z 11 kwietnia 2017 r., sygn. akt I OSK 2170/15.

Wyrok NSA z 9 lutego 2023 r., sygn. akt III OSK 6781/21, CBOSA.

Wyrok TSUE z 13 maja 2014 r. w sprawie C-131/12, *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Costeja González*, ECLI:EU:C:2014:317.

Wyrok TSUE z 24 września 2019 r. w sprawie C-507/17, *Google LLC przeciwko CNIL*, ECLI:EU:C:2019:772.

Wyrok TSUE z 7 grudnia 2023 r. w sprawach połączonych C-26/22 i C-64/22, *UF i AB przeciwko Land Hessen (SCHUFA)*, ECLI:EU:C:2023:958.

The right to be forgotten in the European legal order – from a procedural entitlement to a fundamental right

Summary

This article examines the right to be forgotten as an instrument for protecting individual rights within the European legal order, focusing specifically on its evolution in the case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). The study is centered on Article 17 of Regulation (EU) 2016/679 (GDPR), interpreted in light of the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. An analysis of landmark rulings, including *Google Spain* and *Google LLC v. CNIL*, illustrates the emergence of the dereferencing standard as a means of exercising the right to be forgotten and defines its boundaries, particularly regarding territorial scope. The EU perspective is further enriched by Strasbourg jurisprudence, notably *the Hurbain v. Belgium* judgment, which emphasizes the necessity of balancing the right to privacy with freedom of expression and the archival function of the press. In the final section, the article highlights the technological challenges associated with the implementation of the right to erasure in the digital environment and presents *de lege ferenda* proposals concerning a functional interpretation of Article 17 of the GDPR.

Keywords: right to be forgotten, Article 17 GDPR, dereferencing, CJEU case law, ECtHR case law, informational autonomy, fundamental rights