

Karol Kościński\*

# Nakazy blokujące przeciwko pośrednikom internetowym: między unijnym standardem a krajowymi odrębnościami

## Streszczenie

W artykule przedstawiono wspólne standardy dotyczące jednego z najskuteczniejszych narzędzi stosowanych w walce z piractwem internetowym – nakazów blokujących wydawanych przeciwko różnego rodzaju pośrednikom internetowym w przypadku naruszenia praw autorskich. Autor analizuje podstawowe zasady regulujące tego rodzaju środki, ukształtowane w prawie europejskim i orzecznictwie TSUE. Na tym tle w artykule przedstawiono różnice, jakie pojawiły się w niektórych państwach członkowskich UE w toku rozwoju procedury stosowania nakazów. Artykuł wskazuje również na specyfikę polskiej sytuacji w tym zakresie, opierając się na orzeczeniach polskich sądów, które bezpośrednio lub pośrednio dotyczą nakazów wydawanych przeciwko pośrednikom internetowym.

**Słowa kluczowe:** nakazy blokujące, pośrednik internetowy, prawo autorskie, naruszenie prawa autorskiego, piractwo internetowe

\* Karol Kościński, radca prawny, stały współpracownik Światowej Organizacji Własności Intelektualnej, m.in. jako współautor reform prawa autorskiego w Armenii, Czarnogórze i Bhutanie.

## Kontekst faktyczny i rynkowy rozwoju nakazów blokujących

Jedną z wielu sfer, dla której pojawienie się internetu stanowiło ogromne wyzwanie, było egzekwowanie praw wyłącznych, w szczególności prawa autorskiego. Wyzwanie to wynikało z wykształcenia się i upowszechnienia nowych sposobów dystrybucji i eksploatacji utworów, które skutkowały zaangażowaniem w ten proces całego łańcucha zupełnie nowych rodzajów pośredników, tj.: dostawców internetu, dostawców hostingu, operatorów prowadzących serwisy internetowe. Nowe modele udostępniania treści były nie tylko bardziej skomplikowane, lecz także odzwierciedlały sieciową naturę internetu. Jako technologia ogólnego zastosowania – bez względu na sferę, którą przekształcił – działa on ponadgranicznie. Jednocześnie eksploatacja cyfrowa jest wolna od posługiwania się materialnym nośnikiem treści, zapewnia dużą anonimowość usługodawcy i łatwą zmianę miejsca świadczenia usługi. Możliwości w tym zakresie wzrosły wraz z rozwojem szerokopasmowego internetu, który pozwala na streaming utworów, w tym utworów audiowizualnych w czasie rzeczywistym.

W nowym ekosystemie udostępniania treści chronionych prawem autorskim ujawniły się ograniczenia instrumentów prawnych, które dotychczas służyły ochronie praw wyłącznych. Oprócz wspomnianych okoliczności natury faktycznej sytuację prawną uprawnionych skomplikowało pojawienie się przepisów, które pozwalały łatwo wyłączyć odpowiedzialność pośredników internetowych<sup>1</sup>, gdy ich usługi są wykorzystywane lub wprost służą do udostępniania treści chronionych prawem autorskim.

Źródłem krajowych przepisów w tym względzie były obowiązujące do dziś normy prawa europejskiego<sup>2</sup>, które regulują zasady działania pośredników internetowych. Powstały ponad 20 lat temu i określały okoliczności, w których możliwe jest wyłączenie odpowiedzialności prawnej tzw. biernych pośredników internetowych, w tym wynikającej z naruszenia prawa autorskiego. Przepisy tego samego aktu<sup>3</sup> umożliwiały wprowadzenie w regulacjach sektorowych

1 Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. 2002, nr 144, poz. 1204, z późn. zm., art. 12–14.

2 Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego, Dz. Urz. UE 2000, L 178/1.

3 Ibidem, art. 18, ust. 1

szczególnych podstaw prawnych do wydawania przez krajowe organy sądowe lub administracyjne środków, które mają służyć usunięciu indywidualnych naruszeń prawa oraz zapobieganiu ich powstawaniu w przyszłości. Niemal w tym samym czasie przyjęto także podstawowe unijne rozwiązania dotyczącą prawa autorskiego, w tym jego stosowania w środowisku cyfrowym<sup>4</sup>. Właśnie jako regulacje o charakterze sektorowym, wprowadziły one podstawę prawną<sup>5</sup> do stosowania nakazów wobec pośredników internetowych, w tym nakazów blokujących.

Korzystając z nieprzewidzianej interferencji obu zespołów norm, niektórzy pośrednicy nadużywali możliwości uchylenia się od odpowiedzialności za naruszenie praw własności intelektualnej na podstawie wyłączeń, które zostały stworzone z myślą o biernych pośrednikach internetowych (w szczególności dotyczących dostawców usług hostingu), mimo że oferowane przez nich usługi nie miała takiego charakteru. W tym celu – w wielu postępowaniach sądowych – pośrednicy internetowi twierdzili, że prawa autorskiego nie naruszają, gdyż to indywidualni użytkownicy internetu udostępniają treści chronione prawem autorskim. Jednocześnie wskazywali, że rola pośrednika ogranicza się tylko do zapewnienia neutralnej wobec tych treści przestrzeni internetowej lub technicznych narzędzi, które umożliwiają udostępnianie wszystkich ich rodzajów. Podkreślali ponadto, że zakaz ogólnego uprzedniego filtrowania treści przez pośrednika uniemożliwia odróżnienie treści chronionych prawem autorskim i takiej ochrony pozbawionych przed ich udostępnieniem.

Dość szybko stało się także jasne, że z ekonomicznego, prawnego i politycznego punktu widzenia niecelowe jest ściganie indywidualnych użytkowników sieci, którzy bezprawnie udostępniali chronione treści. Koszty w tym wypadku zdecydowanie przewyższały możliwe do uzyskania odszkodowania. Często było niemożliwe także uzyskanie danych osobowych osób fizycznych, a społeczny odbiór powództw, które były wymierzone w indywidualnych użytkowników internetu, był dość jednoznacznie negatywny.

4 Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, Dz. Urz. UE 2001, L 167/10.

5 Ibidem, art. 8 ust. 3 – w przypadku prawa autorskiego; Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej, Dz. Urz. UE 2004, L 157/45, art. 11, który wprowadza obowiązek zapewnienia możliwości uzyskania nakazu wobec pośredników internetowych także w przypadku innych praw własności intelektualnej niż prawo autorskie.

Słabość dotychczasowych instrumentów ochrony prawa autorskiego wiązała się z ograniczeniami zasad odpowiedzialności deliktowej<sup>6</sup>, które uzależniają jej przypisanie od udowodnienia aktywności oraz winy naruszcyciela. Nakazują one także stosować te same kryteria w przypadku pomocnictwa do czynu niedozwolonego<sup>7</sup>, co w kontekście naruszenia praw wyłącznych teoretycznie mogłoby być formułą na tyle pojemną, żeby w wielu wypadkach objąć nią relacje między pośrednikiem internetowym a indywidualnym użytkownikiem jego usług.

W takich okolicznościach reakcja uprawnionych wobec naruszeń praw wyłącznych była zazwyczaj mocno spóźniona, czasem uzależniona od zaangażowania organów ścigania oraz stosowania norm prawa karnego czy też nieefektywnych procedur administracyjnych<sup>8</sup>, a czasem wręcz niemożliwa. Oznaczało to, że narażeni na szczególne straty są posiadacze praw do tych utworów, które mają największą wartość ekonomiczną zaraz po ich udostępnieniu publiczności, czyli początkowo zwłaszcza utworów audiowizualnych, audycji telewizyjnych, w mniejszym stopniu utworów muzycznych czy słownych. Nie jest przypadkiem, że właśnie przedstawiciele grup uprawnionych do tych rodzajów utworów zaczęli występować o wydanie nakazów wobec pośredników internetowych, których usługi są wykorzystywane przez osobę trzecią do naruszenia praw wyłącznych<sup>9</sup>. Nakazy takie, których szczególnym rodzajem są nakazy blokujące, pozwalały zmniejszyć skalę nielegalnej eksploatacji konkretnych treści w niedługim czasie od ich udostępnienia. Ograniczały w ten sposób straty finansowe posiadaczy praw w sytuacji, gdy pełna rekompensata mogłaby być niemożliwa, ograniczona lub jej uzyskanie przynajmniej mocno odroczone w czasie.

6 W polskich realiach – Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, t.j., Dz.U. 2021, poz. 1509, art. 415 i nast.

7 W polskich realiach – ibidem, art. 422.

8 Najlepszym przykładem było francuskie Hadopi.

9 M. Husovec, *Injunctions against intermediaries in the European Union. Accountable but not Liable?*, Cambridge 2017, s. 3 i nast.

## Istota nakazów blokujących wobec pośredników internetowych, ich rodzaje oraz podstawy wprowadzenia w prawie europejskim

Ewolucja tej na pierwszy rzut oka dość niepozornej instytucji, która w przeciwieństwie do państw Europy Zachodniej i kilkunastu najbardziej rozwiniętych państw pozaeuropejskich<sup>10</sup> nie jest powszechnie wykorzystywana w państwach naszego regionu, z pewnością zaskoczyłaby twórców europejskiej regulacji stanowiącej podstawę jej wprowadzania w całej UE. Źródłem wspomnianego zaskoczenia byłaby m.in. lakoniczność przepisów, które zobowiązywały państwa członkowskie UE jedynie do stworzenia uprawnionym możliwości występowania o wydanie nakazu. Przepisy te nie określały jego zakresu, treści, warunków uzyskania, kręgu adresatów czy też – co w 2001 roku wydawało się oczywiste – jakichkolwiek kwestii proceduralnych, w tym związanych z transgranicznym wykonywaniem nakazów. Ustawodawca unijny wychodził z pragmatycznego założenia, że pośrednicy internetowi po prostu mają w wielu wypadkach realne techniczne możliwości, żeby efektywnie i przy względnie najniższych kosztach zakończyć stan naruszenia praw wyłącznych. Stosowanych wobec nich środków nie nazwano nawet sankcjami, ale instrumentami współpracy<sup>11</sup>.

W 2001 roku, gdy ewolucja modeli biznesowych udostępniania treści w internecie dopiero się rozpoczynała, niewielu mogło przewidzieć, jakiego rodzaju rozwiązania szczegółowe powstaną na podstawie tak ogólnej normy. Po kilkunastu latach okazało się, że jednymi z najbardziej skutecznych i najczęściej wykorzystywanych także poza państwami EU są nakazy blokujące, czyli nakładające na pośrednika internetowego obowiązek wdrożenia takich środków technicznych, które mają uniemożliwić dostęp do określonych treści lub konkretnej strony internetowej<sup>12</sup>.

10 W tym wypadku należy wskazać: Stany Zjednoczone Ameryki, Australię, Argentynę, Indie, Indonezję, Singapur, Malezję, Meksyk, Koreę Południową i Turcję. Więcej na ten temat zob. *Filtering, blocking and take-down of illegal content on the Internet*, <https://www.rcme-diafreedom.eu/layout/set/print/Publications/Reports/Filtering-blocking-and-take-down-of-illegal-content-on-the-Internet> [dostęp: 14.01.2022].

11 Por. Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich..., recital 59 preambuły.

12 Brakuje definicji legalnej nakazów blokujących. Więcej o kwestiach definicyjnych zob. T. Riis et al., *Study on Legislative Measures Related to Online IPR Infringements*, Alicante 2018.

W toku tej ewolucji wykształciły się trzy typy nakazów stosowanych w różnych sytuacjach praktycznych<sup>13</sup>. Pierwszym są nakazy statyczne (*static blocking injunctions*) używane zazwyczaj wobec stron internetowych, które zostały stworzone specjalnie po to, żeby udostępniać treści chronione prawami wyłącznymi. Podmiot, który je uruchamia, albo w ogóle nie jest zainteresowany współpracą z uprawnionymi, albo wręcz nie został przez nich zidentyfikowany. Adresatem nakazu w takim wypadku jest nie operator serwisu pirackiego, ale dostawca internetu, a jego skutkiem zablokowanie dostępu do określonej strony.

Drugim typem są nakazy dynamiczne (*dynamic blocking injunctions*), które służą do łatwiejszego rozwiązania przypadków, w których treści zidentyfikowane jako udostępnione z naruszeniem praw wyłącznych na jednej ze stron internetowych pojawiają na nowych stronach. Skutkiem nakazu jest zablokowanie dostępu do takiej strony, która może mieć inny adres URL, ale służy do udostępniania tych samych treści, co jej poprzedniczka. Strona taka często jest także powiązana ze swoją poprzedniczką nazwą domeny, żeby zapewnić jej większą rozpoznawalność i dla wygody użytkowników treści, którym wówczas łatwiej znaleźć daną stronę w wyszukiwarce. Nakaz dynamiczny musi być sformułowany w sposób, który umożliwi dodanie nowego adresu IP lub URL bez konieczności wszczynania nowej procedury sądowej w celu uzyskania nowego nakazu. Alternatywnie, gdy dane nazwy domen i/lub adresy IP są nieznane sądowi w momencie wydania orzeczenia, sądy określają przedziały czasowe (okresowe lub do określonego terminu) dla uprawnionych do przekazywania usługodawcom list stron, które mają być zablokowane na podstawie danego nakazu. Pozwala to uchronić uprawnionego przed występowaniem o osobny nakaz za każdym razem, gdy chronione treści zaczynają się pojawiać na kolejnych stronach internetowych, czyli umożliwia ograniczenie kosztów i innych trudności związanych z prowadzeniem postępowania. W ten sposób system ochrony praw wyłącznych odzyskuje konieczną równowagę zaburzoną, gdy ochrona praw jest kosztowna i długotrwała, a samo naruszenie, sprządzające się do stworzenia nowej strony oraz udostępniania nielegalnie tych samych treści, jest łatwe i tanie.

<sup>13</sup> Study on dynamic blocking injunctions in the European Union. IPR enforcement case-law collection, red. G. Frosio, O. Bulayenko, Strasbourg 2021.

Trzecim typem są nakazy blokujące stosowane w czasie rzeczywistym wobec treści udostępnianych na żywo (*live blocking injunctions*)<sup>14</sup>. W takim przypadku stosowanie nakazu ma jedynie sens w trakcie transmisji, więc reakcja uprawnionych i organów ochrony prawnej musi być szybka i ściśle ograniczona w czasie. Zastosowanie środków technicznych wskazanych w tego typu nakazie ma miejsce wyłącznie za każdym razem, gdy dany serwer jest wykorzystywany do udostępniania transmisji na żywo. Oznacza to, że nakaz jest przyznany na ściśle określony czas, w którym uprawniony ma z wyprzedzeniem poinformować pośrednika internetowego<sup>15</sup>, aż do zakończenia określonego sezonu rozgrywek sportowych.

Nie wszystkie typy nakazów blokujących są stosowane nawet w tych państwach członkowskich, które wprowadziły w swoim prawie krajowym generalną podstawę do występowania o ich wydanie<sup>16</sup>. W niektórych jurysdykcjach możliwość posłużenia się nakazami dynamicznymi lub ich zastosowania wobec transmisji na żywo nie została jeszcze sprawdzona przed sądem<sup>17</sup>. Czasem została sprawdzona z wynikiem negatywnym – w ten sposób orzecznictwo sądowe wymusiło doprecyzowanie krajowej podstawy stosowania nakazów w sytuacji, gdy proste przeniesienie przepisu prawa unijnego okazywało się niewystarczające.

Bez względu na typ nakazu, o którego wydanie w danej sytuacji występuje uprawniony, od strony technicznej ich stosowanie polega na tzw. blokowaniu domeny lub konkretnej strony internetowej lub blokowaniu przepływu danych przez dostawcę internetu<sup>18</sup>. Komputer indywidualnego użytkownika nie

14 Po raz pierwszy tego rodzaju nakaz zastosowano w Wielkiej Brytanii w przypadku transmisji meczów piłkarskich – R. Alexander, K. Hepburn, *Football Association Premier League Ltd vs. British Telecommunications Plc & Others* [2017] EWHC, 480 (Ch), <https://www.wiggin.co.uk/insight/football-association-premier-league-ltd-v-british-telecommunications-plc-ors/> [dostęp: 13.01.2022].

15 Na przykład w formie elektronicznej informacji pochodzącej od uprawnionego lub osoby trzeciej umocowanej do działania w jego imieniu.

16 Stosowanie nakazów blokujących – bez względu na ich charakter – zostało potwierdzone w orzecznictwie sądowym w Austrii, Belgii, Danii, Francji, Finlandii, Grecji, Irlandii, Holandii, Portugalii, Hiszpanii, Szwecji, Wielkiej Brytanii, Islandii i Norwegii. W Niemczech i na Litwie odwołania od pozytywnych wyroków są przedmiotem odwołań.

17 Możliwość stosowania dynamicznych nakazów blokujących została potwierdzona w Belgii, Danii, Francji, Niemczech, Grecji, Irlandii, Włoszech, Holandii, Hiszpanii i Szwecji.

18 W takiej sytuacji odbiorcy zapytania o dostęp do danej domeny nie zwracają komputrowi użytkownika właściwego adresu IP, który pozwalałby się z nią połączyć. W zastępstwie komputer uzyskuje informację, że dana domena jest nieznana lub uzyskuje inny numer IP, który kieruje go na stronę informującą, że dostęp do danej domeny nie jest dozwolony (tzw. *DNS Spoofing*). Ta metoda może być wykorzystywana zarówno do blokowania pojedynczego

może wówczas zlokalizować konkretnej domeny lub strony internetowej (następuje blokada DNS, URL lub numeru IP), co w konsekwencji prowadzi do zablokowania transmisji, np. utworu chronionego prawem autorskim, czy wręcz odmowy dostępu do całej strony, za której pośrednictwem treści są udostępnione. Konsekwentnie, nie dochodzi do usunięcia danych treści u źródła, lecz są one niedostępne dla odbiorcy w miejscu, w którym chce on uzyskać do nich dostęp. W ten sposób jest rozwiązany problem braku instrumentów prawnych do eliminowania serwisów pirackich operujących z terytoriów, na których prawo autorskie w ogóle nie jest chronione lub ochrona jest iluzoryczna. Na terytoriach państw członkowskich, do których dany serwis kieruje swoją usługę, nakazy wykorzystywane są najczęściej wobec kilku największych dostawców internetu w danym państwie – wówczas skala udaremnionych naruszeń jest najbardziej widoczna.

Wspomniana już elastyczność przepisów prawa unijnego czasem może okazać się zaletą, nie wyklucza bowiem posłużenia się innymi środkami technologicznymi niż typowo stosowane w przypadku nakazów blokujących, umożliwiając uprawnionym i sądom dostosowanie się do zmieniających się metod naruszeń. Na tej podstawie np. francuski Sąd Najwyższy (Sąd Kasacyjny)<sup>19</sup> utrzymał w mocy nakazy zobowiązujące wyszukiwarki do deindeksowania i blokowania dostępu do witryn, które są strukturalnie zaprojektowane do naruszania praw wyłącznych.

## Standardy stosowania nakazów blokujących w orzecznictwie TSUE

Abstrahując od potencjalnych zalet, ogólne brzmienie art. 8 ust. 3 dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z 22 maja 2001 roku w sprawie harmonizacji niektórych aspektów praw autorskich spowodowało, że praktyka stosowania nakazów w państwach członkowskich w dużym stopniu kształtowała się na podstawie orzecznictwa sądów krajowych i jego weryfikacji przez

adresu IP, jak i zestawu wielu adresów IP, które są odfiltrowane z wszystkich dostępnych adresów na podstawie wcześniej określonych kryteriów.

<sup>19</sup> Cour de cassation, civile, Société française du radiotéléphone (SFR) vs. Google France, Google Inc., Microsoft Corporation et Microsoft France, Chambre civile 1, 6 juillet 2017, 16-17.217 16-18.298 16-18.348 16-18.595, ECLI:FR:CCASS:2017:C100909, <https://www.legifrance.gouv.fr/juri/id/JURITEXT000035152528> [dostęp: 11.01. 2022].



TSUE. W wielu przypadkach, chociaż nie wszystkich, ustawodawcy, którzy dokonywali implementacji norm prawa unijnego, zanim w praktyce sprawdzono, w jaki sposób można posłużyć się nakazami wobec pośredników, po prostu przepisywali ogólny przepis prawa unijnego do krajowych aktów prawnych.

Sądy kształtowały standardy stosowania nakazów na styku wykładni nie-dookreślonych klauzul prawa europejskiego ustanawiających kryteria, jakie muszą spełniać środki ochrony praw własności intelektualnej (np. skuteczność i słuszność<sup>20</sup>, odstraszący charakter, niepowodowanie nadmiernych kosztów i nieuzasadnionych opóźnień, obowiązek zabezpieczenia przed nadużyciem środków ochrony)<sup>21</sup> i praw podstawowych zawartych w normach traktatowych. W ostatnim wypadku chodziło o wyważenie interesów uprawnionych, pośredników i użytkowników w sytuacji immanentnego konfliktu między ochroną własności, w tym własności intelektualnej<sup>22</sup>, a prawem dostępu do informacji<sup>23</sup> i swobodą prowadzenia działalności gospodarczej<sup>24</sup>. Prawa użytkowników mogłyby zostać naruszone, gdyby np. wydawano nakazy blokujące o nadmiernym zakresie przedmiotowym czy też okresie obowiązywania, nakładano obowiązki niemożliwe do wykonania przez ich adresata, wreszcie nakazy dotyczące treści, do których dostęp nie powinien być w ogóle zablokowany (*over-blocking*). W konsekwencji w razie odnowienia lub przedłużenia nakazu niektóre sądy krajowe<sup>25</sup> wymagają uprzedniej oceny skuteczności nakazu i rozważenia, czy przedłużenie jest właściwe.

Efektem działalności TSUE jest katalog standardów, które umożliwiają ocenę indywidualnego przypadku zastosowania nakazu. Niektóre z nich znajdują zastosowanie do wszystkich tego typu środków, inne nabierają szczególnego znaczenia w przypadku nakazów blokujących, wszystkie zaś skierowane są przede wszystkim do organów sądowych, bo to właśnie one ustalają, czy i jakie działania będzie miał podjąć adresat nakazu.

20 Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej..., art. 3, ust. 1.

21 Ibidem, art. 3, ust. 2..

22 Karta Praw Podstawowych Unii Europejskiej z 7 czerwca 2016 r., Dz. Urz. UE 2016, C 202/391, art. 17(2).

23 Ibidem, art. 11.

24 Ibidem, art. 16.

25 *The Football Association Premier league Ltd v. Eircom Ltd (Trading as Eir) & Others (Approved)* [2020] IEHC 332 (15 June 2020), <http://www.bailii.org/ie/cases/IEHC/2020/2020IEHC332.html> [dostęp: 20.02.2022].

Orzecznictwo TSUE, którego wyniki zostały częściowo powtórzone w ostatnim komunikacie Komisji Europejskiej dotyczącym egzekwowania praw własności intelektualnej<sup>26</sup>, w ten sposób: 1) doprecyzowało pojęcia pośrednika – adresata nakazu; 2) wskazało, że wydanie nakazu jest niezależne od ewentualnie własnej odpowiedzialności pośrednika za naruszenie praw wyłącznych, w tym od jego winy<sup>27</sup>; 3) określiło cel nakazu; 4) sprecyzowało, jakie okoliczności należy wziąć pod uwagę przy ocenie, czy wydany nakaz jest proporcjonalny; 5) wyjaśniło jak sądy powinny wyważyć interesy uprawnionych, pośredników i użytkowników.

Pojęcie „pośrednik”, wobec którego można nałożyć nakaz, należy rozumieć szeroko. Może nim być każdy przedsiębiorca świadczący usługę, która może być wykorzystana przez co najmniej jedną osobę do naruszenia praw wyłącznych<sup>28</sup>. W ten sposób lista potencjalnych pośredników pozostaje otwarta, a nie jest przy tym istotne, czy naruszcziela i pośrednika łączy jakkolwiek relacja umowna<sup>29</sup>. Trybunał Sprawiedliwości UE potwierdził wprost, że pośrednikiem jest dostawca dostępu do internetu, który jest najbardziej typowym adresatem nakazów blokujących. Od strony dowodowej w konsekwencji poza zakresem dowodzenia znajduje się okoliczność, czy indywidualni użytkownicy usług adresata nakazu faktycznie uzyskali dostęp do chronionych treści. Wystarczy po prostu wykazanie, że są one dostępne.

Brak konieczności zaistnienia jakiejś formy udziału pośrednika w naruszeniu powoduje, że do uzyskania nakazu nie jest konieczne wykazanie winy pośrednika. W tej sytuacji wystarczy, żeby pośrednik świadczył usługi, które potencjalnie mogą służyć do dokonywania naruszeń, nawet jeżeli jeszcze do nich nie doszło<sup>30</sup>. Konsekwentnie oznacza to także, że pośrednik nie może powołać się na jedną z podstaw do wyłączenia odpowiedzialności, służą one bowiem

26 Komunikat Komisji Europejskiej dotyczącym egzekwowania praw własności intelektualnej. Wytoczne dotyczące niektórych aspektów dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady w sprawie egzekwowania praw własności intelektualnej, COM/2017/0708 final.

27 Wyrok TSUE w sprawie L'Oréal przeciwko eBay (C-324/09), pkt 131; C-70/10, podobnie wyrok TSUE w sprawie Scarlet przeciwko Netlog, pkt 29, <https://curia.europa.eu/juris/liste.jsf?language=pl&num=C-324/09> i <https://curia.europa.eu/juris/liste.jsf?num=C-360/10&language=PL> [dostęp: 4.04. 2022].

28 Wyrok TSUE w sprawie UPC Telekabel Wien (C-314/12), <https://curia.europa.eu/juris/liste.jsf?num=C-314/12&language=PL> [dostęp: 4.04. 2022].

29 Wyrok TSUE w sprawie Tommy Hilfiger Licensing LLC i inni przeciwko DELTA CENTER (C-494/15), pkt 23, <https://curia.europa.eu/juris/liste.jsf?num=C-494/15&language=PL> [dostęp: 4.04. 2022].

30 M. Husovec, op. cit., s. 132 i nast.

do wyłączenia winy, a ta przesłanka nie jest w ogóle badana przy wydawaniu nakazu. Właśnie takie rozwiązanie – mimo możliwych innych interpretacji<sup>31</sup> – przyczyniło się do tego, że nakazy blokujące stały się z procesowego punktu widzenia wygodnym środkiem ochrony praw. Kwestia zaangażowania lub braku zaangażowania adresata nakazu w naruszenie praw wyłącznych może natomiast mieć znaczenie dla oceny, czy obowiązki nałożone nakazem nie są dla niego zbyt obciążające lub kosztowne<sup>32</sup>. Im większe jest zaangażowanie pośrednika, tym trudniej mu twierdzić, że nakaz stanowi dla niego nadmierne obciążenie.

Koresponduje to z szeroko ujętym w orzecznictwie TSUE celem nakazu. Jest nim nie tylko usunięcie zaistniałych już naruszeń, lecz także przeciwdziałanie przyszłym aktom nielegalnej eksploatacji praw autorskich; w ten sposób nakaz blokujący pełni także funkcję prewencyjną<sup>33</sup>. Takie ukształtowanie celu nakazu otworzyło w praktyce furtkę do postępowania się dynamicznymi nakazami blokującymi. Dodatkowo pozwoliło ono w toku dalszej ewolucji orzecznictwa na przesądzenie, że możliwe jest blokowanie identycznych lub równoważnych stron internetowych o różnych adresach IP lub URL zamiast wyłącznie węższego obowiązku stosowania określonych środków technicznych w celu zablokowania konkretnego adresu IP lub adresu URL. Istotne w tym wypadku jest przyjęcie, że równoważną stroną będzie strona zawierająca w istocie treści niezmienione lub w bardzo niewielkim stopniu różniące się od treści, które doprowadziły do stwierdzenia pierwotnego naruszenia<sup>34</sup>.

Oceniając z kolei w praktyce, które nakazy blokujące są proporcjonalne, istotne jest przede wszystkim zbadanie, czy środki wynikające z konkretnego nakazu są dla danego pośrednika możliwe do zastosowania w praktyce. W tym wypadku pierwsza grupa okoliczności dotyczy możliwości organizacyjnych i finansowych adresata nakazu, w tym także związanych z potencjalnymi

31 Odmienne podejście, ściśle wiążące możliwości zastosowania nakazu wobec pośrednika internetowego z możliwością przypisania mu winy za naruszenie, wyraził rzecznik generalny TSUE Maciej Szpunar w opinii do sprawy *Stichting Brein (C-527/15)*.

32 M. Piech, *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019, s. 337.

33 Wyrok TSUE w sprawie *Tobias Mc Fadden przeciw Sony Music Entertainment Germany GmbH (C-484/14)*, <https://curia.europa.eu/juris/liste.jsf?num=C-484/14> [dostęp: 4.04.2022], podobnie przywołany wcześniej wyrok w sprawie *L'Oreal v. Ebay (C-324/09)*.

34 Wyrok TSUE w sprawie *Eva Glawischnig-Piesczek przeciwko Facebook Ireland Ltd (C-18/18)*, <https://curia.europa.eu/juris/liste.jsf?num=C-18/18&language=PL> [dostęp: 4.04.2022]. Dotyczy on ochrony dóbr osobistych, ale rodzi także skutki na gruncie prawa własności intelektualnej.

skargami konsumentów, które mogą zostać złożone, jeżeli zablokowanie określonych treści okaże się niezasadne. Kontestowane może być obciążenie kosztami wyłącznie pośrednika<sup>35</sup>, szczególnie jeżeli on sam nie narusza praw wyłącznych. Bardziej zasadne jest rozłożenie kosztów na obie strony lub wręcz obciążenie nimi uprawnionego, zwłaszcza że to on niewątpliwie odnosi korzyści ekonomiczne dzięki wykonaniu nakazu.

W niektórych przypadkach podział kosztów, które wynikają z tego tytułu, jest uregulowany w danym państwie członkowskim UE w przepisach dotyczących postępowania egzekucyjnego. Drugą płaszczyzną, z której może być oceniana<sup>36</sup> proporcjonalność nakazu, jest jego skuteczność. Utopijne było podejście, że dany nakaz ma być niezawodny lub wskazane w nim środki techniczne nie mogą w ogóle być obchodzone. Wystarczy, żeby nakaz był w stanie choć częściowo zapobiec naruszeniom lub je w znaczny sposób utrudnić. Tak ukształtowany standard oczekiwań wobec adresata nakazu łączy się z obowiązkiem podjęcia przez niego racjonalnych, uzasadnionych wysiłków w realiach danej sprawy, żeby przynajmniej zniechęcić do popełnienia naruszenia. Tym samym nie można wydać nakazu, który będzie w danych okolicznościach całkowicie nieskuteczny lub wymagał od adresata wysiłków niemożliwych do zaakceptowania.

Oczywiste jest, że kryteria brane pod uwagę, w kontekście nakazów blokujących, przy ocenie praw podstawowych mają naturę najbardziej otwartą<sup>37</sup>. W przypadku prawa do informacji istotną granicę wyznacza tutaj zakaz wydawania nakazów, które byłyby niepotrzebne z punktu widzenia ich celu, a jednocześnie w nieuzasadniony sposób pozbawiałyby użytkownika legalnego dostępu do danych treści. W praktyce uznano za dopuszczalne zablokowanie dostępu do danej strony internetowej, jeżeli tylko część dostępnych za jej pośrednictwem utworów została udostępniona nielegalnie, a pozostałe nie mają takiego charakteru. Przepisy w poszczególnych państwach członkowskich UE zazwyczaj udostępniają indywidualnym użytkownikom możliwość złożenia skargi na działanie pośrednika, który wykonując adresowany do siebie nakaz, naruszył – w ocenie użytkownika – prawo do informacji. Użytkownik

35 Wyrok TSUE w sprawach Scarlet przeciwko Sabam (C-70/10), <https://curia.europa.eu/juris/liste.jsf?language=pl&num=C-70/10> [dostęp: 4.04. 2022], i przywołanej powyżej Scarlet przeciwko Netlog (C-360/10).

36 Podobnie przywołany już wyrok TSUE w sprawie Telekabel Wien (C-314/12).

37 Jest to zresztą krytykowane przez niektórych przedstawicieli doktryny jako wyraz nadmiernego uznania pozostawionego w rękach sędziego orzekającego w danej sprawie. Por. M. Husovec, op. cit., s. 190 i nast.

może niekiedy zwrócić się do organu sądowego z wnioskiem o usunięcie lub zmianę blokady. W praktyce użytkownicy korzystają z tego rodzaju środków raczej sporadycznie. Jedną z przyczyn może być brak możliwości odpowiedniego uzasadnienia takiej skargi, gdy oczywiste jest, że zablokowana strona internetowa została zaprojektowana, żeby naruszać prawa wyłączne. Inną przyczyną są niewątpliwie koszty prowadzenia takiego postępowania, które indywidualnego użytkownika mogą po prostu zniechęcić. Pozostawiając na uboczu kwestię wykorzystania środków ochrony praw użytkowników w praktyce, niewątpliwie uwzględnienie ich interesów może być dokonane zarówno na etapie wydawania nakazu, jak i już po jego wydaniu. W wypadku ochrony swobody prowadzenia działalności gospodarczej co do zasady przyjęto, że nakazy blokujące nie naruszają jej istoty, gdy mają skonkretyzowany charakter<sup>38</sup>. Poza tym sam pośrednik może ograniczyć poniesione przez siebie koszty przez podjęcie racjonalnych środków, żeby sprostać swoim obowiązkom<sup>39</sup>.

## **Podstawowe podobieństwa i rozbieżności w stosowaniu nakazów blokujących w państwach członkowskich UE**

Standardy dotyczące nakazów blokujących, które wynikają z orzecznictwa TSUE, narzucają pewne obowiązki dowodowe podmiotowi dochodzącemu ochrony swoich praw za pomocą tego środka.

Obowiązki te co do zasady są zbliżone w każdej jurysdykcji, ale m.in. ze względu na różnice w przepisach proceduralnych mogą być wykonywane w odmienny sposób. Wynikają one w pewnym stopniu z istoty samego nakazu – środka o charakterze punktowym, dotyczącego ściśle określonego pośrednika internetowego, a także zindywidualizowanych, przynajmniej w pewnym stopniu, stron internetowych czy treści. Jego stosowanie musi być także ograniczone w czasie – to kolejny przejaw punktowego charakteru nakazu, który stanowi swoiste zabezpieczenie przed wydawaniem nakazów nieproporcjonalnych, ale jednocześnie narzuca dodatkowe obowiązki procesowe.

W toku postępowania o wydanie nakazu uprawniony powinien precyzyjnie wskazać usługę, która służy do naruszania praw wyłącznych, oraz adresata

38 M. Piech, op. cit., s. 356 i nast.

39 T. Shapiro, *Directive 2001/29/EC on copyright in information society* [w:] *Copyright in the information society: a guide to national implementation of the European Directive*, red. idem, B. Lindner, wyd. 2, Cheltenham; Northampton, MA 2019, s. 29 i nast.

nakazu, czyli podmiot taką usługę świadczący. Dodatkowo wnioskodawca musi przedstawić dowody wskazujące, że przysługują mu prawa własności intelektualnej, które chce chronić, oraz okoliczności potwierdzające samo naruszenie lub możliwość jego zaistnienia. W tym wypadku nie obowiązują żadne szczególne reguły dowodowe – zazwyczaj są wykorzystywane zrzuty ekranu, różnego rodzaju raporty techniczne czy też zeznania, ale także powiadomienia o powtarzających się naruszeniach, które przed złożeniem wniosku o wydanie nakazu były kierowane wcześniej do jego przyszłego adresata. Nie ma natomiast powodu, co sądy w państwach członkowskich wielokrotnie potwierdzały<sup>40</sup>, żeby przedmiotem dowodzenia był charakter pośrednika (*access provider* vs *content provider*) i stopień jego zaangażowania w proceder naruszania praw autorskich.

Nakazy blokujące wydane przez sądy krajowe mają zwykle zastosowanie do dostawców usług dostępu pod jurysdykcją właściwego państwa członkowskiego oraz nielegalne działania mające skutki na tym samym terytorium. Sądy mogą nakazać blokowanie nielegalnych treści niezależnie od miejsca naruszenia praw własności intelektualnej lub miejsca, w którym znajdują się użytkownicy uzyskujący dostęp do treści, o ile nielegalne działania są skierowane do użytkowników w danym państwie członkowskim. Nakazy są narzędziem mającym terytorialny zakres zastosowania, co zresztą koresponduje z terytorialnym charakterem ochrony praw autorskich, ale jednocześnie – jak wskazano – rozwiązują problem ich ochrony, omijając wynikające z tego ograniczenia. Samo postępowanie o wydanie nakazu jest prowadzone obecnie w każdym państwie członkowskim UE osobno, zgodnie z krajowymi przepisami proceduralnymi. Dodatkowym źródłem rozbieżności w tym wypadku może być także sposób przeniesienia przepisów prawa europejskiego do krajowych porządków prawnych; nie we wszystkich przypadkach dokonano tego przez wiernie przeniesienie przepisu prawa europejskiego do regulacji narodowych.

Skutki obciążają w tym wypadku uprawnionych. Nawet jeżeli każde z tych postępowań dotyczy tego samego pośrednika, tych samych chronionych treści i tego samego okresu ich eksploatacji, to konieczne jest jego osobne prowadzenie w każdej jurysdykcji. Z punktu widzenia uprawnionych wymusza to konieczność koordynowania swojej aktywności procesowej, jeżeli nakaz w tym

40 Court of Milan, Ordinance No. 42163/2019 R.G., *Sky Italia, Lega Serie A v. Cloudflare et al.* zob. *Recent European case law on the infringement and enforcement of intellectual property rights*, May 2021, s. 82, [https://euipo.europa.eu/reports/New\\_Case\\_Law\\_en](https://euipo.europa.eu/reports/New_Case_Law_en) [dostęp: 4.04.2022].

samym czasie (np. czasie danej premiery kinowej) ma wyrzucić realny skutek na większym terytorium niż wyznaczone przez granice pojedynczego państwa członkowskiego UE. Konsekwencją systemową jest brak ponadgranicznego wykonywania nakazów. Być może wprowadzenie nowych reguł w ramach tzw. Digital Service Act<sup>41</sup>, nad którym aktualnie pracują organy UE, zmieni ten stan rzeczy. Projekt m.in. określa minimalne warunki, jakie musi spełnić nakaz, żeby mógł być wykonany w innym państwie członkowskim niż państwa jego wydania<sup>42</sup>, oraz tworzy sieć narodowych koordynatorów usług cyfrowych, którzy mają ułatwić ponadgraniczne wykonywania środków ochrony prawnej w internecie, tj. także nakazów blokujących<sup>43</sup>.

Oprócz kwestii możliwości ponadgranicznego wykonywania nakazów różnice proceduralne dotyczą: 1) zakresu badania okoliczności sprawy; 2) udziału obu stron w postępowaniu zmierzającym do wydania nakazu; 3) możliwości występowania przez pośrednika internetowego o zawieszenie stosowania nakazu; 4) zakresu środków odwoławczych dostępnych dla użytkowników i pośredników internetowych.

W pierwszym wypadku, jeżeli nakaz ma mieć charakter trwały, to jest konieczne zbadanie wszystkich okoliczności naruszenia w celu oceny ustalonego stanu faktycznego pod kątem ogólnych zasad sformułowanych w orzecznictwie europejskiego Trybunału Sprawiedliwości. W przypadku nakazów mających charakter tymczasowy w sprawach pilnych skład orzekający ma większą swobodę orzeczniczą; w większym stopniu może opierać się na uprawdopodobnieniu niektórych okoliczności<sup>44</sup>.

W drugim wypadku w niektórych państwach (Grecja, Irlandia i Hiszpania) przepisy proceduralne przewidują zawsze obowiązkowy udział zaangażowanych podmiotów w postępowaniu zmierzającym do wydania nakazu. Jednakże w kilku państwach członkowskich postępowanie pod pewnymi warunkami może mieć charakter *ex parte*. Warunki te obejmują: pilne okoliczności wydania nakazu (Niemcy); naruszenie praw wyłącznych już miało miejsce (Niderlandy); pośrednik internetowy, którego dotyczy nakaz, był wcześniejszej

41 Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (ustawa o usługach cyfrowych), zmieniająca dyrektywę 2000/31/WE, COM/2020/82, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A-2020%3A825%3AFIN> [dostęp: 23.01.2022].

42 Ibidem, art. 8.

43 Ibidem, art. 38.

44 *Mapping report on the national remedies against online piracy of sports content*, s. 80. <https://www.obs.coe.int/en/web/observatoire/mapping-reports> [dostęp: 18.01.2022].

powiadomiony o naruszeniach/zamiarze skorzystania przez uprawnionych z nakazu (Wielka Brytania).

Z kolei zawieszenie stosowania nakazu, które nie jest europejskim standardem, ale zostało wypracowane przez doktrynę orzeczniczą w Irlandii i Wielkiej Brytanii, ma charakter czasowy. Podstawy do występowania o zawieszenie służą albo skorygowaniu lub zbadaniu możliwego nadmiernego blokowania materiałów albo wiążą się z koniecznością zapewnienia przez pośrednika niezakłóconego z technicznego punktu widzenia funkcjonowania jego usług (np. utrzymania integralności usługi, konserwacji, usunięcia bezpośredniego zagrożenia bezpieczeństwa sieci, usługi lub pośrednika).

W czwartym wypadku przepisy wszystkich państw członkowskich UE zapewniają środki odwoławcze, które umożliwiają kwestionowanie nakazów blokowania zgodnie z tradycyjnymi zasadami postępowania cywilnego. Środki odwoławcze są dostępne dla pośredników i domniemanych naruszcycieli, których dotyczy nakaz. Ponadto w przypadku kilku państw członkowskich prawo do odwołania służy poszczególnym użytkownikom internetu, których dany nakaz pośrednio dotyczy (np. w Finlandii, Niemczech, Grecji, Irlandii, Holandii i Wielkiej Brytanii). Według niemieckiego Sądu Najwyższego<sup>45</sup> poszczególni użytkownicy internetu mają prawo do środka odwoławczego poprzez wszczęcie postępowania przeciwko swojemu dostawcy dostępu na podstawie łączącego ich stosunku umownego. Ponadto w nielicznych wypadkach (Holandia) dostępne są pozwy zbiorowe składane przez internautów przeciwko zakazom blokowania albo ochrona praw użytkowników sieci jest realizowana za pośrednictwem przepisów służących ochronie konsumentów (Szwecja).

Oprócz kwestii procedury sądowej istotne różnice między państwami członkowskimi EU, które dotyczą nakazów blokujących, wiążą się z możliwością ich wydawania w niektórych przypadkach przez organy administracyjne<sup>46</sup> lub ułatwieniem ich wykonywania dzięki zastosowaniu rozwiązań o charakterze samoregulacyjnym<sup>47</sup>. Relacja postępowania prowadzonego przed organem

45 Por. G. Frosio, *Enforcement of European Rights on a Global Scale* [w:] *Routledge Handbook of European Copyright Law*, red. E. Rosati, London 2021.

46 Taka możliwość istnieje w Grecji, Włoszech, Hiszpanii i na Litwie. We Włoszech domeny internetowe zablokowane w trybie administracyjnym podlegają obowiązkowemu wpisowi na tzw. czarną listę. Więcej na ten temat zob. *Study on dynamic blocking injunctions in the European Union...*, s. 20–22.

47 Przypadek Belgii, w której powstały wspólne punkty kontaktowe założone przez uprawnionych i potencjalnych adresatów nakazów blokujących, żeby odbierać i rozpoznawać skargi m.in. przeciwko naruszeniom praw wyłącznych.



administracyjnym do postępowania sądowego może być ukształtowana odmiennie; zazwyczaj obie ścieżki się nie wykluczają, chociaż istnieją sytuacje, gdy wszczęcie postępowania administracyjnego wyklucza możliwość wniesienia sprawy cywilnej<sup>48</sup>. Z kolei rozwiązania samoregulacyjne mają ograniczony zasięg i zastosowanie, służą jedynie ułatwieniu ochrony, uzupełniają bardziej sformalizowane postępowania lub zapewniają stosowane rozwiązanie, zanim dochodzi do zainicjowania bardziej sformalizowanych procedur<sup>49</sup>.

## Brak podstawy do stosowania nakazów blokujących w prawie polskim

W Unii Europejskiej nakazy blokujące nie są stosowane w państwach członkowskich naszego regionu, z wyjątkiem Litwy. W prawie polskim – jak potwierdza jedno z nielicznych orzeczeń dotyczących tej kwestii<sup>50</sup> – nie istnieje szczególna podstawa prawna, która umożliwiłaby złożenie wniosku do sądu o wydanie takiego nakazu. W analizowanym orzeczeniu sąd przesądził, że nakładanie przez niego środków prewencyjnych może dotyczyć wyłącznie konkretnego naruszenia prawa autorskiego, a nie rozciągać się na wiele naruszeń nawet tego samego prawa, które to naruszenia występują w danym momencie lub mogą wystąpić w przyszłości. Dodatkowo sąd wskazał, że przez konkretne naruszenie rozumie naruszenie dokonane lub które może być dokonane przez skonkretyzowanego naruszcziela, a nie istnienie abstrakcyjnego zagrożenia związanego tylko z profilem działalności danego pośrednika internetowego. Sąd w ten sposób uznał, że niemożliwe jest także nałożenie ogólnego i abstrakcyjnego nakazu, który obejmowałby wszystkie utwory audiowizualne nawet danego uprawnionego.

Brak stosownego przepisu umożliwiającego nakładanie nakazów blokujących – podobnie jak w kilku innych państwach unijnych – jest przedmiotem skargi uprawnionych o niewdrożenie prawa europejskiego do Komisji

48 Rozwiązanie przyjęte w Grecji. Na Litwie z kolei sądy cywilne zajmują się egzekucją nakazów wydawanych przez organ administracyjny.

49 Rozwiązanie znane w Belgii.

50 Wyrok Sądu Apelacyjnego w Warszawie w sprawie Wolters Kluwer Polska S.A. przeciw FS File Solutions Limited w Nikozji (Cypr), VI ACz 164/17, <https://classaction.pl/orzecznictwa/postanowienie-sadu-apelacyjnego-warszawie-wydzial-vi-cywilny-27-marca-2017-roku> [dostęp: 4.04.2022].

Europejskiej, która jak na razie nie doprowadziła do wszczęcia formalnego postępowania w tym względzie.

W tej sytuacji jedynym przepisem, który pozwalałby na uzyskanie podobnego, choć ograniczonego efektu, w przypadku praw autorskich jest art. 79 ust. 1 pkt 2 ustawy z 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych<sup>51</sup>, który przewiduje możliwość wystąpienia z roszczeniem o usunięcie skutków naruszenia. Realizacja takiego roszczenia może polegać m.in. na usunięciu treści udostępnionych z naruszeniem praw wyłącznych. W tym kontekście warto wspomnieć o postanowieniu Sądu Apelacyjnego w Krakowie z 18 września 2017 roku<sup>52</sup>, w którym sąd zobowiązał dostawców usług internetowych do usunięcia konta użytkownika zawierającego link do treści naruszających prawo. Sąd w uzasadnieniu uznał, że pośrednik internetowy nie jest bierny, skoro pobiera opłaty za przesyłanie treści, w ten sposób przypisał mu winę za naruszenie praw wyłącznych. Skupił się na możliwości przypisania pośrednikowi udziału, a w konsekwencji odpowiedzialności za naruszenie, a nie możliwości nałożenia na niego określonego obowiązku służącego ochronie prawa niezależnie od takiego udziału lub winy pośrednika<sup>53</sup>. To stanowi istotę nakazów blokujących. To odosobnione orzeczenie nie potwierdza – co warto wyraźnie podkreślić – że istnieje w naszym kraju ogólna możliwość ich wydawania. Stanowi ono raczej orzeczniczą próbę zaproponowania substytutu o ograniczonym zakresie zastosowania w praktyce w oczekiwaniu na konieczną interwencję legislacyjną.

## Zakończenie

W polskim prawie brakuje podstawy prawnej do stosowania przez sądy nakazów wobec pośredników internetowych, którzy nie są zaangażowani bezpośrednio w dokonywanie naruszeń prawa autorskiego. Oznacza to, że nie jest

51 Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j., Dz.U. 2021, poz. 1062.

52 Postanowienie Sądu Apelacyjnego w Krakowie z 18 września 2017 r., I Ca 1494/15, [http://orzeczenia.krakow.sa.gov.pl/content/\\$N/152000000000503\\_I\\_ACa\\_001494\\_2015\\_Uz\\_2017-09-18\\_001](http://orzeczenia.krakow.sa.gov.pl/content/$N/152000000000503_I_ACa_001494_2015_Uz_2017-09-18_001) [dostęp: 04.04.2022].

53 Podobną wykładnię przyjęły sądy Okręgowy i Apelacyjny w Krakowie w sprawie Chomikuj, ale podstawy prawnej do odpowiedzialności pośrednika internetowego i nałożenia na niego obowiązku proaktywnego działania na rzecz ograniczenia negatywnych skutków naruszeń prawa autorskiego poszukiwały w treści art. 439 kodeksu cywilnego. Sprawa aktualnie trafiła do Sądu Najwyższego.

zapewniona pełna zgodność polskiego prawa autorskiego z regulacjami europejskimi<sup>54</sup>. Ze względu na planowane wejście w życie rozporządzenia o jednolitym rynku dla usług cyfrowych i wynikającą z niego konieczność wskazania polskiego organu, który powinien odpowiadać za realizację obowiązków związanych z ponadgranicznym wykonywaniem nakazów wobec pośredników internetowych, wdrożenie norm prawa europejskiego regulujących nakazy blokujące jest jeszcze bardziej uzasadnione. Trudno za racjonalną uznać sytuację, w której polski wymiar sprawiedliwości będzie zobowiązany do wykonywania nakazów chroniących prawa uprawnionych z innych państw członkowskich UE, a jednocześnie polscy uprawnieni będą pozbawieni możliwości skorzystania z takiej ochrony zarówno na terytorium Polski, jak i całej UE.

Niektóre sądy próbują zapętnić tę lukę, stosując przepisy, które pozwalają na wyłączenie odpowiedzialności pośrednika internetowego – zresztą zgodnie z ich pierwotnym zakresem – wyłącznie wobec biernych pośredników, co skutkuje nałożeniem na pośrednika określonych obowiązków. Jednakże rozwiązanie takie nie zapewnia uprawnionym efektywnego i szybkiego narzędzia do ograniczania skali piractwa internetowego oraz wymaga prowadzenia skomplikowanego postępowania dowodowego. Poza tym orzeczenia sądowe są w tym wypadku nieliczne i trudno w ogóle mówić o jakiejś praktyce orzeczniczej.

Wobec tego polski ustawodawca powinien, korzystając z doświadczeń bardziej zaawansowanych państw członkowskich UE, wprowadzić do ustawy o prawie autorskim podstawę prawną dającą sądom możliwość nakładania nakazów blokujących na pośredników internetowych. Przepisy powinny wziąć pod uwagę standardy ukształtowane przez orzecznictwo TSUE, częściowo potwierdzone w komunikacie Komisji Europejskiej dotyczącym egzekwowania praw własności intelektualnej. Najistotniejsze w tym wypadku jest: 1) określenie odpowiednio dużego kręgu adresatów nakazu; 2) oderwanie możliwości jego nałożenia od udziału/winy pośrednika w naruszeniu praw wyłącznych; 3) przesądzenie, że sądy są uprawnione do nakładania nakazów dynamicznych i adresowanych do stron przeznaczonych do transmisji prowadzonym na żywo.

Ze względu na rozwiązania zawarte w projekcie rozporządzenia o jednolitym rynku dla usług cyfrowych jest zasadne określenie minimalnych elementów nakazów w sposób zbieżny z rozporządzeniem, żeby zapewnić możliwość ponadgranicznego wykonywania nakazów nałożonych przez polskie sądy.

54 Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich..., art. 8, ust. 3.

Biorąc pod uwagę negatywne doświadczenia niektórych państwa członkowskich UE ze zbyt lakonicznymi przepisami służącymi nakładaniu nakazów na pośredników internetowych i potencjalną dyskusję publiczną dotyczącą przepisów służących do blokowania dostępu do treści w internecie, projektowana regulacja powinna zawierać przepisy jasno określające procedury odwoławcze. Powinna także być zapewniona możliwość występowania o wstrzymanie nakazu, jeżeli przestał on pełnić swoją funkcję, wymagają tego okoliczności techniczne lub ze względu na zmianę okoliczności faktycznych, które są związane z działalnością danego pośrednika, prowadzą do nadmiernego blokowania treści.

Przepisy powinny również określać zasady podziału kosztów wdrożenia nakazów blokujących, przynajmniej w sytuacji, gdy nakaz dotyczy pośrednika w ogóle niezaangażowanego w naruszanie praw autorskich (tj. *access provider*). Obciążenie go wyłącznymi kosztami wykonania nakazu nie znajduje uzasadnienia ani w regułach słuszności, ani nie przyczyni się do ukształtowania trwałych relacji gospodarczych między uprawnionymi i pośrednikami internetowymi.

### Bibliografia

- Alexander R., Hepburn K., *Football Association Premier League Ltd vs. British Telecommunications Plc & Others* [2017] EWHC, 480 (Ch), <https://www.wiggin.co.uk/insight/football-association-premier-league-ltd-v-british-telecommunications-plc-ors/> [dostęp: 13.01.2022].
- Copyright in the information society: a guide to national implementation of the European Directive*, red. T. Shapiro, B. Lindner, wyd. 2, Cheltenham; Northampton, MA 2019.
- Filtering, blocking and take-down of illegal content on the Internet*, <https://www.rcmediafreedom.eu/layout/set/print/Publications/Reports/Filtering-blocking-and-take-down-of-illegal-content-on-the-Internet> [dostęp: 14.01.2022].
- Frosio G., *Enforcement of European Rights on a Global Scale* [w:] *Routledge Handbook of European Copyright Law*, red. E. Rosati, London 2021.
- Husovec M., *Injunctions against intermediaries in the European Union. Accountable but not Liable?*, Cambridge 2017.
- Mapping report on the national remedies against online piracy of sports content*, <https://www.obs.coe.int/en/web/observatoire/mapping-reports> [dostęp: 18.01.2022].
- Piech M., *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019.
- Riis T. et al., *Study on Legislative Measures Related to Online IPR Infringements*, Alicante 2018.
- Study on dynamic blocking injunctions in the European Union. IPR enforcement case-law collection*, red. G. Frosio, O. Bulayenko, Strasbourg 2021.

---

## **Blocking injunctions against online intermediaries: between EU standard and national peculiarities**

### **Abstract**

This article presents the common standards regarding one of the most effective tools used to combat online piracy: blocking injunctions issued against various types of internet intermediaries in case of the infringement of copyright. The author analyzes the basic principles regulating such measures, which have been shaped in the European law and jurisprudence of the CJEU. Against this background, article presents differences emerged in some EU Member States during process of application of injunctions. The article also indicates the specificity of the Polish situation in this regard, relying on the judgments of Polish courts, which directly or indirectly concern orders issued against internet intermediaries.

**Key words:** blocking injunctions, online intermediaries, copyright law, infringement of copyright, online piracy