PME
1/2019

PRAWO Mediów Elektronicznych

www.ksiegarnia.beck.pl
ISSN 2082-100X
01
9 772082 100190
Cena 65 zł (w tym 5% VAT)

C·H·BECK

PME

1/2019

Adres redakcji:

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl

C·H·BECK

Wydawca:

Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
fax: 22 33 77 602
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Contents

C·H·BECK

Szanowni Państwo,

zapraszam do lektury artykułów z pierwszego numeru czasopisma Prawo Mediów Elektronicznych w 2019 r. W tym wydaniu zamieszczamy opracowania dotyczące prawa autorskiego, zwłaszcza utworów audiowizualnych, dowodu z dokumentu elektronicznego w postępowaniu cywilnym, a ponadto tekst dotyczący obowiązków dostawców usług cyfrowych na gruncie ustawy o krajowym systemie. Z obszaru ochrony danych osobowych znajdziecie Państwo artykuł o stosowaniu monitoringu w miejscu pracy po reformie ochrony danych osobowych w UE. Numer zamyka artykuł anglojęzyczny o zasadzie „mozaiki" według art. 7 rozporządzenia I bis o jurysdykcji w sprawach deliktowych.

Życząc miłej lektury, zachęcam do publikacji w naszym czasopiśmie.

Z poważaniem
prof. dr hab. *Jacek Gołaczyński*

Dowód z elektronicznego dokumentu prywatnego w postępowaniu cywilnym

Mirosława Jesion[1]

Przedmiotem niniejszego opracowania są zagadnienia związane ze zdefiniowaniem pojęcia „elektroniczny dokument prywatny". Jednocześnie zostanie poruszona problematyka dopuszczenia i przeprowadzenia dowodu z elektronicznego dokumentu prywatnego w kontekście konieczności informatyzacji postępowania cywilnego.

Uwagi wstępne

Stałym elementem postępu cywilizacyjnego jest informatyzacja. Wraz z nią powszechny stał się dostęp do usług elektronicznych i informatycznych, a zatem i do sprzętu elektronicznego. Taki stan rzeczy jest związany z rozwojem nauki i postępem technologicznym w różnych dziedzinach życia. W tym kontekście należy dostrzegać kształtowanie się społeczeństwa informacyjnego oraz zwrócić uwagę na nowe oblicze prawa spowodowane procesem informatyzacji. W kontekście tematu niniejszego opracowania należy odnieść się pozytywnie do kolejnych nowelizacji Kodeksu postępowania cywilnego zachodzących na przestrzeni ostatnich lat w zakresie poszerzania katalogu środków dowodowych dopuszczalnych na gruncie cywilnego prawa procesowego, w szczególności dokumentu i jego formy elektronicznej.

W aktualnie obowiązującym Kodeksie postępowania cywilnego mianem dowodów określa się: a) dokumenty, w tym dokumenty elektroniczne; b) oględziny; c) opinie biegłych; d) zeznania świadków; e) przesłuchanie stron; f) inne środki dowodowe, do których zalicza się m.in. dowód z DNA, dowody związane z przesyłaniem wiadomości na odległość, eksperyment procesowy. Katalog środków dowodowych uregulowanych w ustawie procesowej ulega ciągłym przemianom i nie ma charakteru zamkniętego. Kolejność umiejscowienia środków dowodowych w Kodeksie postępowania cywilnego nie przesądza w sposób kategoryczny o ich wartości, gdyż zależy od konkretnych okoliczności i charakteru sprawy[2]. Ponadto systematyka Kodeksu postępowania cywilnego nie rozstrzyga o formalnej hierarchii środków dowodowych z punktu widzenia ich mocy i wiarygodności[3].

Definicja pojęcia – dokument elektroniczny

Przepisy Kodeksu postępowania cywilnego nie zawierają definicji legalnej pojęcia „dokument". Próby opracowania definicji objaśniającej analizowane pojęcie były podejmowane zarówno przez przedstawicieli doktryny prawa materialnego, jak i prawa cywilnego procesowego oraz przez judykaturę już w okresie międzywojennym. Najszerzej pojmowaną definicję pojęcia „dokument" przedstawił *M. Allerhand*. Autor ten uznawał za dokument każdy przedmiot wyrażający pewną myśl, bez względu na to, z czego jest ten przedmiot wykonany oraz jakimi środkami myśl ta została wyrażona[4]. Natomiast *E. Waśkowski* utożsamiał dokument z dowodem pisemnym. Jednak dopuszczał także możliwość rozszerzenia zakresu tego pojęcia na wszelkiego rodzaju przedmioty, zawierające utrwalone za pomocą znaków pisemnych wiadomości co do okoliczności faktycznych sprawy[5]. Samej istoty dokumentu autor ten upatrywał w wyartykułowaniu myśli, twierdzeń lub oświadczeń. Z kolei inny przedstawiciel doktryny prawa cywilnego procesowego okresu międzywojennego *L. Peiper* pojęcie dokumentu w ujęciu szerokim objaśniał jako każdy przedmiot, który ujawniał na zewnątrz jakieś zdarzenie w przyszłości. W ujęciu węższym określał dokument jako pismo bez względu na materiał, na którym je sporządzono, a także bez względu na osobę, od której pochodzi[6].

Z biegiem czasu, zarówno w okresie powojennym, jak i po uchwaleniu Kodeksu postępowania cywilnego z 1964 r., przedstawiciele doktryny, analizując pojęcie dokumentu, zawężali jego zakres wyłącznie do formy pisemnej. W opinii *W. Berutowicza* za dokument należało uznawać przedmiot pokryty pismem (napisem), bez znaczenia był zaś materiał, z jakiego przedmiot został wykonany[7]. Ponadto zdaniem powołanego tego autora dokument powinien utrwalać za pomocą znaków pisarskich treść o znaczeniu prawnym[8]. Podobną koncepcję przedstawił *W. Siedlecki*, według którego

[1] Autorka jest absolwentką kierunku Prawo Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego.

[2] *Z. Reich*, Istota procesu cywilnego, Warszawa 1985, s. 161 i n.

[3] *J. Studzińska*, [w:] *P. Cioch*, *J. Studzińska* (red.), Postępowanie cywilne, Warszawa 2012, s. 256.

[4] *M. Allerhand*, Kodeks postępowania cywilnego. Komentarz, Lwów, s. 283 i n.

[5] *E. Waśkowski*, Podręcznik procesu cywilnego, Wilno 1932, s. 196.

[6] *L. Peiper*, Komentarz do kodeksu postępowania cywilnego (część pierwsza) i przepisów wprowadzających Kodeks postępowania cywilnego wraz z ustawami i rozporządzeniami dodatkowemi, tudzież z umowami międzynarodowemi. Tom I art. 1–293, Kraków 1934, s. 589–590.

[7] *W. Berutowicz*, Postępowanie cywilne w zarysie, Warszawa 1983, s. 122.

[8] *Ibidem*, s. 146.

analizowane pojęcie znaczy tyle samo co dokument pisemny, rozumiany jako uzewnętrznienie jakiejś myśli lub widomości za pomocą pisma[9]. *Z. Resich* nie ograniczył swoich poglądów wyłącznie do formy pisemnej dokumentu. Podnosił, że za dokument powinien być uznany przedmiot, na którym treść utrwalona była za pomocą pisma, ale również za dokument *sensu largo* należało uznawać także plany, rysunki, fotokopie[10]. Zgodnie z obowiązującym Kodeksem postępowania cywilnego wskazywane przez *Z. Resicha* środki dowodowe (plany, rysunki, fotokopie i in.) zaliczane są do tzw. innych środków dowodowych. W konsekwencji na podstawie art. 308 KPC dowody z innych dokumentów, w szczególności zapis obrazu, dźwięku albo obrazu i dźwięku sąd przeprowadza, stosując odpowiednio przepisy o dowodzie z oględzin oraz o dowodzie z dokumentu.

Głęboką analizę przedmiotowego pojęcia przeprowadził *K. Knoppek*, według którego pojęcie dokumentu na gruncie prawa cywilnego materialnego i procesowego są rozłączne[11]. Dokumentami na gruncie materialnoprawnym są wyłącznie te obejmujące oświadczenia woli, a dokumentami w rozumieniu ustawy procesowej są uznawane również te obejmujące oświadczenia wiedzy (w tym zawierające informacje techniczne, jakościowe, ilościowe), a nawet oświadczenia uczuć. Przyznanie dokumentowi statusu procesowego zależy od jego pisemnej formy ze względu na jego istotę, która polega na wyrażeniu treści dokumentu pismem. Zdaniem tego autora konsekwencją faktu, że dokument wyraża jakąś myśl ludzką, jest jego treść. *K. Knoppek* sformułował własną definicję dokumentu, objaśniając dokument jako wyrażoną na piśmie w jakimkolwiek języku myśl ludzką, która opatrzona jest podpisem wystawcy, uzewnętrzniona w sposób trwały, nadający się do uwielokrotnienia oraz – przynajmniej formalnie do zastosowania w postępowaniu cywilnym[12]. Wskazana definicja odnosi się do podpisu jako elementu konstytuującego dokument na gruncie prawa cywilnego procesowego. Zagadnienia związane z podpisem zostaną podjęte w dalszej części opracowania.

Do czasu kolejnej nowelizacji Kodeksu cywilnego i Kodeksu postępowania cywilnego[13] ustawodawca nie wprowadził definicji legalnej terminu „dokument", a analizowane pojęcie przyjmowane było w znaczeniu węższym i rozumiane jako pisemne uzewnętrznienie jakiejś myśli lub informacji, a także woli człowieka, nadających się do wielokrotnego wykorzystania[14]. Jednocześnie wraz ze zmianami technologicznymi zachodzącymi w obrocie gospodarczym podjęto dyskusję nad koniecznością wykorzystania dokumentu w postaci elektronicznej. Zauważono, że w związku z rozwojem nowych dziedzin nauki zmiany technologiczne są koniecznością oraz że powinny one modyfikować, uzupełniać, a także gdy jest to możliwe, upraszczać dobrą praktykę prawną, nie niwelując dotychczasowego systemu prawa i dorobku doktryny[15].

W opinii *W. Kocota* pojęcie „dokument" ma znaczenie szersze niż konstrukcja formy pisemnej zwykłej i powinna być odnoszona do każdej metody trwałego uzewnętrznienia znaków językowych w widzialnej postaci, a w dobie rozwoju elektronicznych nośników informatycznych zakres znaczenia pojęcia „dokument" nie powinien być zawężany wyłącznie do postaci papierowej[16]. Mniej liberalnie dokument elektroniczny ujmowała *K. Górska*. Według niej wyróżnienie dokumentu elektronicznego jest konsekwencją uznawania kwalifikowanej formy elektronicznej za odrębną od formy pisemnej, gdyż ta pierwsza wiąże się zasadniczo z odmiennym sposobem utrwalenia oświadczenia woli, niż następuje to w przypadku dokumentu tradycyjnego[17]. Najbardziej pogłębioną analizę pojęcia dokumentu elektronicznego przedstawił *J. Jankowski*, inspirując się definicją dokumentu z okresu międzywojennego prezentowaną przez *M. Allerhanda*. Zdaniem *J. Jankowskiego* każdy dokument w sensie technicznym stanowi trwały zapis informacji, a w sensie prawnym jest również zapisem spełniającym określone przesłanki formalne[18]. Dokument elektroniczny nie różni się od dokumentu papierowego w swej funkcji (istocie), a tylko w swej strukturze (budowie), w tym charakterem nośnika sposobem zapisu, sposobem odczytu, trwałością w czasie, możliwością udostępnienia, sposobem kopiowania, techniką zabezpieczenia i podatnością na manipulacje[19]. W opinii *J. Jankowskiego* wskazywane różnice implikują niekiedy konieczność innego traktowania dokumentu w zwykłej formie papierowej i dokumentu elektronicznego, gdyż z drugim ze wskazanych dokumentów nie można zapoznać się bezpośrednio, lecz jedynie za pomocą urządzeń informatycznych umożliwiających ich odczytywanie z nośnika[20].

Nowelizacja Kodeksu cywilnego i Kodeksu postępowania cywilnego z 10.7.2015 r. była efektem dyskusji prowa-

[9] *W. Siedlecki*, Zarys postępowania cywilnego, Warszawa 1968, s. 256.

[10] *Z. Resich*, Uproszczenie postępowania dowodowego w świetle prawa cywilnego procesowego Polski i innych krajów socjalistycznych, NP 1987, Nr 7–8, s. 12.

[11] *K. Knoppek*, Dokument w procesie cywilnym, Poznań 1993, s. 18.

[12] *Ibidem*, s. 35.

[13] Ustawa z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych inny ustaw (Dz.U. poz. 1311).

[14] *M. Manowska*, Dokument jako środek dowodowy w postępowaniu nakazowym, Pr. Sp. 1999, Nr 4, s. 16 i n.

[15] *D. Szostek*, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, Warszawa 2012, s. 238.

[16] *W. Kocot*, Wpływ Internetu na prawo umów, Warszawa 2004, s. 335.

[17] *A. Górska*, Zachowanie zwykłej formy pisemnej czynności prawnych, Warszawa 2007, s. 234 i n.

[18] *J. Jankowski*, Elektroniczny obrót prawny, Warszawa 2008, s. 158 i n.

[19] *Ibidem*, s. 161.

[20] *Ibidem*, s. 161.

dzonej przez doktrynę[21] w zakresie definicji dokumentu, jego formy elektronicznej, zakresu zastosowania oraz mocy dowodowej. Główny cel nowelizacji był związany z kolejnym etapem informatyzacji postępowania cywilnego i polegał na wprowadzeniu zmian w zakresie formy czynności prawnych, a także nieznanej dotychczas formy dokumentu jako środka dowodowego. W konsekwencji wprowadzanych zmian dodano art. 77^3 KC, zgodnie z którym dokumentem jest nośnik informacji umożliwiający zapoznanie się z jego treścią. Jednocześnie ustawodawca postanowił, iż do zachowania dokumentowej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie (art. 77^2 KC). W wyniku wprowadzenia nowych regulacji do zachowania formy dokumentowej czynności prawnej wystarczające jest złożenie oświadczenia woli w postaci dokumentu w sposób umożliwiający zidentyfikowanie osoby, która złożyła oświadczenie. W ten sposób niejako zastosowano wyżej analizowaną, rozumianą szeroko koncepcję pojęcia „dokument", jednocześnie uwzględniając współczesny rozwój nowoczesnych technologii, z którym wiąże się kształtowanie nowego oblicza prawa spowodowane procesem informatyzacji.

W kontekście tematu niniejszego opracowania należy zwrócić uwagę na jeszcze jeden aspekt wprowadzonej 10.7.2015 r. nowelizacji dotyczącej postępowania dowodowego. W konsekwencji zmian wprowadzonych w przepisach odróżnić należy dowód z dokumentu zawierającego tekst od dowodu z dokumentów w innej postaci (np. zapisu dźwięku, zapisu obrazu i dźwięku). Taki stan rzeczy ma związek z rozwojem współczesnej techniki, w wyniku którego możliwe jest sporządzenie dokumentu w innej formie niż tradycyjna, rozumiana jako tekst składający się z ciągu liter alfabetu, co zostało dostrzeżone przez ustawodawcę. Za potrzebą przyjęcia z tym związanych zmian przemawiała praktyka stosowana coraz powszechniej zarówno przez uczestników postępowań, jak i przez sądy[22]. Efektem nowych regulacji jest konieczność odróżnienia dokumentów zawierających tekst, oraz dokumentów, których treść wyrażona jest w innej formie. Wskazane różnice na gruncie prawa cywilnego procesowego sprowadzają się do odpowiedniego stosowania art. 244 KPC do dokumentów zawierających tekst. Wystawca dokumentu sporządza tekst, korzystając ze znaków alfabetu zgodnie z regułami językowymi, którymi się posługuje. Natomiast wobec dokumentów, których treść wyrażona jest w innej formie, w szczególności dokumentów, na które składa się zapis obrazu, dźwięku lub obrazu i dźwięku, zastosowanie znajduje art. 308 KPC, zgodnie z którym dowody z innych dokumentów niż wymienione w art. 243^1 KPC sąd przeprowadza, stosując odpowiednio przepisy o dowodzie z oględzin oraz o dowodzie z dokumentów. Artykuł 243^1 KPC znajduje zastosowanie do tych dokumentów, które łącznie spełniają dwa warunki: 1) zawierają tekst oraz 2) można ustalić tożsamość ich wystawców[23]. Należy uznać, że przy kumulatywnym spełnieniu wskazanych przesłanek analizowany przepis znajdzie zastosowanie zarówno do dokumentów w formie pisemnej i elektronicznej, jak i w formie dokumentowej.

Podsumowując, należy zaakcentować, że pojęcie dokumentu na gruncie prawnym oderwało się od tradycyjnego myślenia o dokumencie jako podpisanej kartce papieru. Zasadniczą funkcją dokumentu jest utrwalenie określonych spostrzeżeń lub wszelkiego rodzaju oświadczeń w celu przedstawienia ich w tej formie w przyszłości[24]. W ujęciu szerokim za dokument powinien być uznany każdy przedmiot, jako zawierający określoną treść myśli człowieka, a to z kolei różni go od innych tzw. rzeczowych środków dowodowych. Nie ma znaczenia zastosowanie określonego rodzaju nośnika. Może nim być tradycyjny papier, jak również np. twardy dysk komputera, pamięć telefonu komórkowego lub inny sprzęt elektroniczny zawierający nośnik pamięci. Na gruncie postępowania cywilnego nie ma znaczenia kontekst, w jakim ujmowany jest dokument w prawie cywilnym materialnym. Natomiast dla postępowania dowodowego istotne jest, czy w rozumieniu art. 244 i 245 KPC dokument spełni kryterium jako środek dowodowy.

Rodzaje dokumentów

Kodeks postępowania cywilnego z 1932 r.[25] wprowadził podział dokumentów na publiczne i prywatne. Dokumenty publiczne musiały być sporządzone przez władze, urzędy i osoby zaufania publicznego w zakresie ich działania i nie obowiązywał wymóg sporządzania ich w przepisanej formie[26]. Natomiast dokumenty prywatne stanowiły dowód tego, że zawarte w nim oświadczenie pochodzi od osoby, która je podpisała. Wskazane rozróżnienie dokumentów zosta-

[21] Szerzej zob.: *B. Kaczmarek-Templin*, Dowód z dokumentu elektronicznego w procesie cywilnym, Warszawa 2012; *D. Szostek*, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, Warszawa, 2012; *D. Szostek*, *M. Świerczyński*, Moc dowodowa dokumentu elektronicznego w postępowaniu cywilnym, MoP 2007, Nr 17, s. 935–940; *B. Kaczmarek*, Moc dowodowa dokumentu elektronicznego w postępowaniu cywilnym – polemika, MoP 2008, Nr 5, s. 248–252; *D. Szostek*, *M. Świerczyński*, Moc dowodowa dokumentu elektronicznego w postępowaniu cywilnym – odpowiedź na polemikę, MoP 2009, Nr 6, s. 327–329.

[22] Uzasadnienie do projektu ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, druk sejmowy Nr 2678, Sejm VII kadencji, s. 7, http://legislacja, gov.pl/docs/2/177283/177320/177321/dokument 119983.pdf (dostęp z 3.1.2019 r.).

[23] *K. Flaga-Gieruszyńska*, [w:] *A. Zieliński* (red.), Kodeks postępowania cywilnego. Komentarz, Warszawa 2017, s. 494.

[24] *Ibidem*, s. 494–495.

[25] Rozporządzenie Prezydenta Rzeczypospolitej – Kodeks postępowania cywilnego z 29.11.1930 r. (t.j. Dz.U. z 1932 r. Nr 112, poz. 934).

[26] *K. Knoppek*, Dokument…, s. 77.

ło zmienione dopiero w Kodeksie postępowania cywilnego z 1964 r., w którym ustawodawca odstąpił od pojęcia dokumentu publicznego, zastępując je pojęciem dokumentu urzędowego.

W aktualnie obowiązującym Kodeksie postępowania cywilnego w art. 244 i 245 KPC ustawodawca klasyfikuje dokumenty na urzędowe i prywatne. Jednocześnie nie wskazuje *expressis verbis* kryteriów formalnych, jakie powinny spełniać, m.in. odnoszących się do nośnika, na którym mają być sporządzane. W zakresie wykładni wskazanych przepisów zastosowanie znajduje stanowisko doktryny, które generalnie jest jednolite, a według niego podział dokumentów opiera się na dwóch kryteriach – wystawcy i zakresu mocy dowodowej[27].

Mając na względzie pierwsze ze wskazanych kryteriów, zgodnie z art. 244 § 1 KPC, przez dokumenty urzędowe powinno uznawać się te sporządzone w przepisanej formie przez powołane do tego organy władzy publicznej i inne organy państwowe w zakresie ich działania. Stanowią one dowód tego, co zostało w nich urzędowo zaświadczone. Od czasu nowelizacji ustawy procesowej, która weszła w życie 8.9.2016 r., uogólnieniu uległ katalog podmiotów uprawnionych do wystawiania dokumentów urzędowych. Istnieje zasadnicza różnica pomiędzy sporządzeniem dokumentów urzędowych przez organy administracyjne, gdyż obligatoryjnie muszą one być sporządzone w zakresie ich działania (art. 244 § 1 KPC), a sporządzeniem dokumentów urzędowych przez podmioty określone w art. 244 § 2 KPC, te powinny być sporządzone wyłącznie w zakresie zleconych im przez ustawę zadań z dziedziny administracji publicznej. Można zatem stwierdzić, iż za dokumenty urzędowe powinny być uznawane zarówno te pochodzące od organów administracji rządowej, jak i administracji samorządowej, tj. organów gminy, powiatu i województwa, a także sporządzone przez organizacje zawodowe (np. samorząd adwokacki, radcowski, lekarski, aptekarski), związki zawodowe, organizacje pracodawców, związki spółdzielcze, cechy rzemiosł, izby gospodarcze, organizacje pozarządowe w zakresie zleconych im przez ustawę zadań z dziedziny administracji publicznej. Jeżeli organ wystawi dokument o treści wykraczającej poza jego kompetencje, to taki dokument nie ma waloru dokumentu urzędowego[28].

Dokumentami prywatnymi są wszystkie te, które nie spełniają przesłanek dokumentów urzędowych, a sporządzone w formie pisemnej albo elektronicznej stanowią dowód tego, że osoba, która je podpisała, złożyła oświadczenie woli zawarte w dokumencie. Na podstawie definicji ustawowej wskazać można szerszy katalog podmiotów, względem dokumentów urzędowych, osób, które mogą być wystawcami dokumentów prywatnych. Zgodnie z art. 245 KPC dla kwalifikacji dokumentu jako prywatnego nie ma znaczenia status wystawcy, gdyż może nim być każda osoba fizyczna, prawna, jednostka organizacyjna. Ponadto przedmiot dokumentu prywatnego nie musi być związany z działalnością tej osoby, przedmiot ten bowiem nie podlega żadnym ograniczeniom[29]. Jako przykład dokumentu prywatnego można wskazać: dziennik budowy, świadectwo pracy wystawione przez pracodawcę, ekspertyzę pozasądową z intencją uznania jej przez sąd za dowód w sprawie (prywatna opinia rzeczoznawcy), wyciąg z ksiąg rachunkowych, faktura VAT, karty choroby, historie choroby, listy przewozowe i inne.

Mając na względzie kryterium mocy dowodowej dokumentów, należy odnieść się do jej zakresu. W polskim procesie cywilnym każdy dokument zarówno urzędowy, jak i prywatny, korzysta z domniemań prawnych[30]. Istota domniemania prawnego polega na tym, że przepis prawa materialnego nakazuje przyjąć fakt sporny (wniosek domniemania) za prawdziwy na tej podstawie, że udowodniony został inny fakt mający związek z tym pierwszym (podstawa domniemania)[31]. Dokumenty urzędowe i prywatne korzystają z domniemania prawdziwości (autentyczności). Domniemanie prawdziwości polega na przyjęciu, że organ, który figuruje w dokumencie jako wystawca, jest tym, który go sporządził[32]. Zaprzeczenie prawdziwości dokumentu wynika z zarzutu sfałszowania lub podrobienia dokumentu. Dokument podrobiony to dokument sporządzony przez inną osobę niż ta, od której ma pochodzić, a dokument przerobiony to taki, który został zmieniony przez osobę nieuprawnioną[33]. W szczególności może to polegać na sfałszowaniu: osnowy dokumentu, druku firmowego, daty, podpisu lub innych części składowych dokumentu. Za dokument nieautentyczny należy uznać również taki, który został wystawiony przez osobę nieuprawnioną do jego wystawienia. Zarzut sfałszowania dokumentu elektronicznego może polegać np. na podważeniu jego autorstwa lub integralności danych[34]. W odróżnieniu od dokumentów prywatnych dokumenty urzędowe korzystają również z domniemania zgodności zawartych w nich oświadczeń z prawdą (art. 244 § 1 i art. 252 KPC). Polega ono na uznaniu zgodności z prawdą tego, co zostało w dokumencie urzędowo stwierdzone.

[27] *A. Klich*, Dowód z opinii biegłego w postępowaniu cywilnym, Biegły lekarz, Warszawa 2016, s. 50.

[28] *K. Flaga-Gieruszyńska*, [w:] *A. Zieliński* (red.), Kodeks postępowania cywilnego..., s. 495.

[29] *A. Klich*, Dowód z opinii biegłego…, s. 251.

[30] *K. Knoppek*, Dokument…, s. 66.

[31] *H. Dolecki*, Postępowanie cywilne. Zarys wykładu, Warszawa 2013, s. 190.

[32] *K. Flaga-Gieruszyńska*, [w:] *A. Zieliński* (red.), Kodeks postępowania cywilnego…, s. 495.

[33] *L. Peiper*, Komentarz do Kodeksu postępowania…, s. 918.

[34] *B. Kaczmarek-Templin*, Dowód z dokumentu elektronicznego w procesie cywilnym, Warszawa 2012, s. 104.

Wszystkie domniemania prawne określające moc dowodową dokumentów są wzruszalne za pomocą wszelkich środków dowodowych. Strona zaprzeczająca prawdziwość dokumentu urzędowego albo twierdząca, że zawarte w nim oświadczenia organu, od którego dokument ten pochodzi, są niezgodne z prawdą powinna okoliczności te udowodnić zgodnie z art. 252 KPC. W zakresie wskazanego przepisu strona może korzystać z wszelkich środków dowodowych. Jeżeli strona zaprzecza prawdziwości dokumentu prywatnego albo twierdzi, że zawarte w nim oświadczenie osoby, która je podpisała, od niej nie pochodzi, obowiązana jest okoliczności te udowodnić. Jeżeli jednak spór dotyczy dokumentu prywatnego pochodzącego od innej osoby niż strona zaprzeczająca, prawdziwość dokumentu powinna udowodnić strona, która chce z niego skorzystać (art. 253 KPC). Z tego przepisu wynika, iż zaprzeczenie prawdziwości dokumentu prywatnego złożonego przez jedną ze stron postępowania przenosi na stronę zaprzeczającą ciężar wykazania, że dokument jest nieprawdziwy. Strona, która w złej wierze lub lekkomyślnie zgłosiła zarzuty przewidziane w art. 252 i 253, podlega karze grzywny. Zakres przedmiotowy wskazanego przepisu obejmuje poza stroną postępowania również jej pełnomocnika, interwenienta ubocznego oraz inne podmioty postępowania.

Oparcie wyroku na dokumencie podrobionym lub przerobionym może stanowić podstawę wznowienia postępowania (art. 403 § 1 KPC). Problematyka sfałszowanych dokumentów jest przedmiotem szczegółowych rozważań prawa karnego materialnego i procesowego, do których odniesienie się wychodzi poza zakres tematu niniejszego opracowania.

Rozwój nowoczesnych technologii skutkował koniecznością zmiany tradycyjnie ujmowanego dokumentu. Istotne znaczenie dla analizowanego zagadnienia ma definicja dokumentu elektronicznego zawarta w rozporządzeniu Parlamentu Europejskiego i Rady UE Nr 910/2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na ryku wewnętrznym[35], która w art. 2 pkt 35 objaśnia dokument elektroniczny jako każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne. Zakres powołanej definicji obejmuje elektroniczny dokument prywatny uregulowany w art. 245 KPC. Ponadto korespondują z nią art. 244 i 308 KPC.

Procesowe znaczenie podpisu

Problematyka podpisu jako elementu konstytutywnego dokumentu była przedmiotem zainteresowania przedstawicieli doktryny i judykatury już w okresie międzywojennym[36]. Zagadnienie to analizowano również po uchwaleniu Kodeksu postępowania cywilnego z 1964 r.[37]. W obowiązującym stanie prawnym ustawodawca nie rozstrzygnął kwestii charakteru podpisu jako konstytutywnego elementu dokumentu. Ograniczone ramy niniejszego opracowania wyłączają możliwość wyczerpującego ujęcia problematyki podpisu i jego treści. Stąd jedynie możliwe jest odniesienie się do podpisu jako elementu elektronicznego dokumentu prywatnego i zasygnalizowania zagadnień z nim związanych.

Z treści art. 245 KPC jednoznacznie wynika, że koniecznym elementem dokumentu prywatnego (zarówno elektronicznego, jak i w formie pisemnej) jest podpis osoby, którym w nim złożyła oświadczenie zawarte w dokumencie. Zastanawiając się nad funkcją podpisu w obrocie prawnym, *K. Knoppek* wymienia cztery: a) identyfikacyjną; b) polegającą na zamiarze wywołania określonych skutków; c) polegającą na wskazaniu, iż dokument opatrzony podpisem zawiera wersję ostateczną danego oświadczenia, aprobowaną przez jego autora; d) zakończenia dokumentu[38]. Prowadzi to do wniosku, iż podpis jest łącznikiem oświadczenia z osobą, która je składa. Wynika z tego uznanie podpisu jako niezbędnego elementu dokumentu.

W zależności od rodzaju nośnika, na którym zapisywany jest dokument, oraz zastosowanej techniki utrwalania danych wyróżnić można: podpis własnoręczny i elektroniczny[39]. Definicję legalną podpisu elektronicznego wprowadziła dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[40]. Zgodnie z tym aktem normatywnym wyróżniane były trzy rodzaje podpisów elektronicznych: a) podpis elektroniczny; b) zaawansowany podpis elektroniczny; c) kwalifikowany podpis elektroniczny. Akt unijny został implementowany do polskiego systemu prawnego w drodze ustawy z 18.9.2001 r. o podpisie elektronicznym[41]. Polska ustawa wprowadziła dwa rodzaje podpisów elektronicznych: podpis elektroniczny oraz bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego

[35] Dz. Urz. UE L Nr 257, s. 73; dalej jako: rozporządzenie Nr 910/2014.

[36] Więcej na ten temat: *Z. Pazdro*, Podpis w postępowaniu administracyjnym, RPiE 1935, Nr 1, s. 20; *S. Kruszelnicki*, Kodeks postępowania cywilnego z komentarzem, Poznań 1938, s. 338; wyrok SN z 1.3.1935 r. CIII 532/34, WP 1936, Nr 3 poz. 50.

[37] *Z. Radwański*, Zarys części ogólnej prawa cywilnego, Warszawa 1979, s. 175; *tenże*, Prawo zobowiązań, Warszawa 1986, s. 453; *B. Kaczmarek-Templin*, Dowód z dokumentu elektronicznego w procesie cywilnym, Warszawa 2012, s. 60 i n.; *D. Szostek*, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, Warszawa 2012, s. 77 i n.; uchwała SN z 23.4.1960 r. 3 CO 8/60, PiP 1960, Nr 11, s. 888–890.

[38] *K. Knoppek*, Dokument…, s. 38–41.

[39] *J. Jankowski*, Podpis elektroniczny w obrocie prawnym, Warszawa 2007, s. 32–33.

[40] Dz. Urz. UE L Nr 257, s. 73.

[41] Dz. U. Nr 130, poz. 1450 ze zm. – nieobow.; dalej jako: Podpis ElU.

kwalifikowanego certyfikatu. Rozporządzenie uchyliło wyżej wskazaną dyrektywę i od 1.7.2016 r. jest bezpośrednio stosowane we wszystkich państwach członkowskich UE. Wspomniany akt normatywny zrównał w skutkach prawnych kwalifikowany podpis elektroniczny z podpisem własnoręcznym. Zgodnie z art. 25 rozporządzenia Nr 910/2014 podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ma postać elektroniczną lub nie spełnia wymogów kwalifikowanych podpisów elektronicznych. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu, natomiast oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim powinien być uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich UE. Wskazane rozporządzenie wprowadza nowe oraz na nowo definiuje dotychczasowe pojęcia: podpis elektroniczny, zaawansowany podpis elektroniczny (dotychczas nieobecny w prawie polskim), kwalifikowany podpis elektroniczny (zastąpił bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem w rozumieniu art. 3 ust. 2 PodpisElU), pieczęć elektroniczną, zaawansowaną pieczęć elektroniczną (pojęcia niewystępujące do wejścia w życie rozporządzenia w prawie polskim).

W tej materii kluczowe znaczenie ma ustawa z 5.9.2016 r. o usługach zaufania oraz identyfikacji elektronicznej[42], określająca: a) krajową infrastrukturę zaufania; b) działalność dostawców usług zaufania, w tym zawieszanie certyfikatów podpisów elektronicznych i pieczęci elektronicznych; c) tryb notyfikacji elektronicznej; d) nadzór nad dostawcami usług zaufania. Przepisy wskazanej ustawy nie znajdują zastosowania do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników[43]. Walor podpisu nie przysługuje wszelkim jego odwzorowaniom mechanicznym np. przez kalkę, faksymile, pieczątkę i in.

Ponadto należy podkreślić, że waloru dokumentu w rozumieniu art. 245 KPC nie spełnia anonim. Jak zauważa *W. Berutowicz* na moc dowodową dokumentu niepodpisanego wpływ ma także okoliczność, czy wystawca dokumentu jest znany[44]. Ze swojej istoty składanie oświadczeń bez podpisu nie jest zachowaniem zasługującym na społeczną aprobatę i stąd anonim nie powinien być brany pod uwagę jako dowód w sprawie rozpoznawany przez sąd.

Elektroniczny dokument prywatny a konieczność informatyzacji postępowania cywilnego

Postępowanie dowodowe jest procesem złożonym przebiegającym wieloetapowo. Pierwszy etap obejmuje decyzje organu procesowego o dopuszczeniu danego środka dowodowego, kolejny zaś to jego przeprowadzenie na podstawie obowiązujących przepisów. Zadaniem postępowania dowodowego jest obiektywne ustalenie stanu faktycznego sprawy, na bazie którego zostanie wydane merytoryczne rozstrzygnięcie. W kontekście zagadnień związanych z wprowadzeniem do polskiego systemu prawa elektronicznego dokumentu prywatnego konieczne staje się zaakcentowanie zmian zachodzących w cywilnym postępowaniu sądowym, związanych z informatyzacją tego postępowania.

Na gruncie art. 233 KPC została unormowana zasada swobodnej oceny dowodów, która zgodnie ze stanowiskiem prezentowanym przez *A. Klich* została sformalizowana w minimalnym stopniu (poza niektórymi postępowaniami odrębnymi), przez zobowiązanie sądu do wszechstronnego rozważenia zebranego materiału[45]. Artykuł 233 § 1 KPC przy uwzględnieniu treści art. 328 § 2 KPC nakładają na sąd orzekający obowiązki: a) wszechstronnego rozważenia materiału zebranego w sprawie; b) uwzględnienia wszystkich dowodów przeprowadzonych w postępowaniu; c) skonkretyzowania okoliczności towarzyszących przeprowadzeniu poszczególnych dowodów mających znaczenie dla oceny ich mocy i wiarygodności; d) wskazania jednoznacznego kryterium argumentacji pozwalającej na weryfikację oceny w przedmiocie uznania dowodu za wiarygodny bądź też jego zdyskwalifikowanie; e) przytoczenia w uzasadnieniu zaskarżonego orzeczenia dowodów, na których oparł się sąd, i przyczyn, dla których innym dowodom odmówił wiarygodności[46]. Granice swobodnej oceny dowodów wyznaczają normy obowiązującego prawa. Ponadto ocena ta powinna być poparta doświadczeniem życiowym, regułami logicznego myślenia oraz pewnym poziomem świadomości prawnej sądu rozpoznającego konkretną sprawę.

Procesowe znaczenie elektronicznych dowodów prywatnych w postępowaniu cywilnym jest związane z możliwością

[42] T.j. Dz.U. z 2019 r. poz. 162 ze zm.

[43] *K. Flaga-Gieruszyńska*, [w:] *A. Zieliński* (red.), Kodeks postępowania cywilnego…, s. 500.

[44] *W. Berutowicz*, Postępowania cywilne, Warszawa 1996, s. 196.

[45] *A. Klich*, Dowód z opinii biegłego w postępowaniu cywilnym. Biegły lekarz, Warszawa 2016, s. 17.

[46] *K. Flaga-Gieruszyńska*, [w:] *A. Zieliński* (red.), Kodeks postępowania cywilnego…, s. 478.

zapoznania się z nimi przez sąd, w konsekwencji decyzjami o ich dopuszczeniu i przeprowadzeniu na podstawie obowiązujących przepisów. Czynności organu procesowego związane z dowodami uzyskanymi z mediów elektronicznych, w tym elektronicznego dokumentu prywatnego, wymagają odpowiedniej infrastruktury teleinformatycznej, w którą powinny być wyposażone jednostki wymiaru sprawiedliwości. Z tego punktu widzenia należy podkreślić służebną rolę informatyzacji dla przebiegu postępowania cywilnego oraz dla organizacji wymiaru sprawiedliwości. Zadanie to może realizować sprzęt dedykowany utrwalaniu przebiegu postępowania. Ponadto należy dostrzegać konieczność modyfikowania infrastruktury sądownictwa, uzupełniając ją o nowoczesne technologie. Problematykę związaną z pozyskiwaniem przez sąd informatycznych nośników danych, na których zapisana jest treść podlegająca osądowi, regulują art. 254 § 2^1 i 2^2 KPC. Zgodnie z nimi sąd w razie potrzeby może wezwać wystawcę dokumentu sporządzonego w postaci elektronicznej do jego uzupełnienia. Należy przy tym podkreślić, że przepis ten jest błędnie sformułowany, ponieważ odnosi się do udostępnienia informatycznego nośnika danych, na którym ten dokument został zapisany, a zgodnie z ustawową definicją to właśnie ten nośnik jest dokumentem. Podobnie niepoprawnie jest skonstruowany przepis, który określa, że uwolnić się od tego obowiązku może wyłącznie ten, kto na pytanie, czy dokument sporządzono na tym informatycznym nośniku danych lub czy pochodzi on od niego, mógłby jako świadek odmówić zeznań.

Zgodnie z zasadą bezpośredniości sąd, który ma wydać wyrok w danej sprawie cywilnej, powinien zetknąć się bezpośrednio z całym zgromadzonym w niej materiałem, będącym podstawą rozstrzygnięcia. Implikuje to konieczność przeprowadzenia dowodu bezpośrednio przed sądem orzekającym. Według *K. Flagi-Gieruszyńskiej* zasada ta nie ma charakteru bezwzględnego ze względów praktycznych oraz z uwagi na reguły ekonomiki procesowej[47]. Stąd też na gruncie postępowania cywilnego występują wyjątki od wskazanej zasady, które nie powinny być wykładane rozszerzająco. Zdaniem tej Autorki wyjątki od zasady bezpośredniości nie dotyczą postępowania dowodowego w ogólności, gdyż odnosić się mogą wyłącznie do poszczególnych środków dowodowych, tj. charakteru dowodu albo względu na poważne niedogodności, lub niewspółmierności kosztów w stosunku do przedmiotu sporu (art. 235 § 1 KPC)[48].

Pierwsze ze wskazanych kryteriów odnosi się do charakteru dowodu, jego właściwości fizycznych i innych. Zgodnie z art. 235 § 2 KPC sąd orzekający może postanowić o przeprowadzeniu takiego dowodu na odległość przy użyciu urządzeń technicznych umożliwiających dokonanie czynności. Drugi przypadek odnosi się do reguł ekonomiki procesowej, nakazującej eliminację kosztów zbędnych lub niewspółmiernych do wartości przedmiotu sporu.

W kontekście wyżej przedstawionych zagadnień należy zaakcentować ich nierozerwalny związek z koniecznością informatyzacji postępowania cywilnego wynikający z prawa do rzetelnego procesu sądowego definiowanego w art. 6 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[49]. W Rekomendacji Komitetu Ministrów Rady Europy dotyczącej czynności sądowych i innych czynności prawnych na rzecz obywateli poprzez wykorzystanie nowych technologii, już w 2001 r. przedstawiono konkretne działania służące poprawie funkcjonowania sądownictwa dzięki wykorzystaniu komunikacji elektronicznej[50]. Dostrzegając ów związek, polski ustawodawca uzupełniał przepisy Kodeksu postępowania cywilnego o kolejne regulacje dopuszczające możliwość wykorzystywania nowoczesnych technologii. Wprowadzane rozwiązania charakteryzowały się jednak rozwiązaniami selektywnymi, sprowadzającymi się do przypadków dopuszczenia możliwości elektronicznego przeprowadzenia konkretnych czynności w konkretnych postępowaniach[51]. Wiele z wprowadzanych zmian związanych było i jest z koniecznością dostosowania polskiego prawa do prawa UE, np. wyżej przedstawionego rozporządzenia Nr 910/2014.

Podsumowanie

Elektroniczny dokument prywatny nie modyfikuje w istotny sposób dokumentu w postaci tradycyjnej (papierowej), ponieważ nie prowadzi do eliminacji elementów konstytuujących jego treść. Prowadzi to do wniosku, że podlega on takim samym rygorom jak jego tradycyjny odpowiednik. Wprowadzenie do ustawy procesowej elektronicznego dokumentu prywatnego jest związane z dostrzeżeniem przez ustawodawcę konieczności zmian zachodzących w społeczeństwie związanych z rozwojem nauki oraz postępem w dziedzinach informatyzacji i cyfryzacji oraz obowiązkiem dostosowania polskiego prawa do prawa międzynarodowego, w tym wynikających z przepisów UE.

Z tego też względu należy zaakcentować konieczność uwzględnienia zmian technologicznych w obrębie funk-

[47] *Ibidem*, s. 483.

[48] *Ibidem*, s. 484.

[49] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 4.11.1950 r., Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.

[50] Communicl of Europe Committee of Ministers Recommendation Rec (2001) of 28 th February 2001 on the divery of cort and other legal services to the citizen torugh the use of new technologies;https:/wod.coe.int/ViewDoc.jsp?id=188899 Strategia modernizacji przestrzeni sprawiedliwości w Polsce&Site=COE (dostęp z 8.1.2019 r.).

[51] *A. Kościółek*, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Teoria i praktyka, Warszawa 2016, s. 45.

cjonowania wymiaru sprawiedliwości. Należy podkreślić potrzebę popularyzowania i funkcjonowania systemów informatycznych w oparciu na najnowsze rozwiązania technologiczne, które są niezbędne do przedstawienia organowi procesowemu dowodów, mających swoje źródło w mediach elektronicznych. Z pewnością wpłynie to pozytywnie na zwiększenie zaufania obywateli do wymiaru sprawiedliwości, którzy wstępując na drogę sądową, realizują przysługujące im konstytucyjne prawo do sądu. Ponadto poprawi również efektywność pracy jednostek organizacyjnych sądów i przyczyni się do usprawnienia procedur, co może przełożyć się pozytywnie na ekonomikę całego postępowania.

Słowa kluczowe: dowód, dokument, informatyzacja.

Proof from private a electronic document regarding civil procedure

The subject of the present study are issues connected with the definition of a concept of a "private electronic document". At the same time, the author discusses issues regarding admissibility and proof of a private electronic document in the context of necessity of computerization of a civil procedure.

Keywords: proof, document, computerization.

Kryteria dopuszczalności stosowania monitoringu w miejscu pracy oraz związane z tym obowiązki pracodawcy w świetle reformy ochrony danych osobowych

Olga Dąbrowska[1]

Celem niniejszego opracowania jest analiza regulacji dotyczących stosowania monitoringu w miejscu pracy, wprowadzonych do polskiego porządku prawnego wskutek reformy ochrony danych osobowych. Wyjaśniwszy pojęcie i rodzaje monitoringu, autorka wskazuje i omawia podstawy prawne wdrożenia przez pracodawcę poszczególnych form monitoringu, formułuje warunki dopuszczalności ich stosowania oraz opisuje związane z tym obowiązki pracodawcy. Rozważania autorki opierają się na analizie przepisów prawa pracy i prawa ochrony danych osobowych, a także poglądów wyrażonych przez doktrynę, orzecznictwo, organy regulacyjne czy organizacje międzynarodowe.

Uwagi wstępne

Dynamiczny postęp technologiczny, w szczególności rozwój i łatwa dostępność nowoczesnych środków komunikacji elektronicznej oraz systemów umożliwiających automatyczne gromadzenie danych, dostarcza pracodawcom szeroki katalog narzędzi ułatwiających kontrolowanie działań pracownika. Jako najpopularniejsze formy takiej kontroli wskazać można monitoring wizyjny, monitoring systemów informatycznych (w tym kontrolę komunikatorów, poczty elektronicznej i analizę odwiedzanych witryn internetowych), kontrolę dostępu i czasu pracy, sprawdzanie wykazu połączeń telefonicznych oraz śledzenie geolokalizacji[2]. Zastosowanie nowoczesnych środków monitorujących pozwala pracodawcy zapisywać i analizować duże ilości danych, a w rezultacie relatywnie niskim kosztem osiągnąć korzystne z punktu widzenia ochrony własnego interesu cele, takie jak zapobieganie naruszeniom obowiązków pracowniczych, przestępstwom, nieuprawnionemu ujawnieniu tajemnicy przedsiębiorstwa i naruszeniom dobrego imienia pracodawcy czy zapewnienie odpowiedniej jakości produkcji i usług – co sprawia, że monitoring stał się powszechnym narzędziem kontroli pracowników. Niezależnie jednak od powodów, dla których pracodawca decyduje się na zastosowanie opisanych narzędzi w swoim zakładzie pracy, sposób, w jaki realizuje on swój interes, nie może nadmiernie ograniczać prawa do prywatności i ochrony danych osobowych podmiotów monitorowanych. Istnieje więc potrzeba określenia warunków i ograniczeń wykorzystania narzędzi monitorujących w miejscu pracy – tak aby zapewnić poszanowanie godności oraz prawnie uzasadnionych interesów osób monitorowanych, czyli pracowników.

Od 25.5.2018 r. podstawowym aktem prawnym regulującym w UE kwestie związane z ochroną danych osobowych jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[3]. O ile wybór rozporządzenia jako instrumentu prawnego reformy powinien zakładać zupełne ujednolicenie sektora ochrony danych w ramach UE[4], o tyle jednak w niektórych obszarach RODO pozostawia państwom członkowskim pewien zakres swobody legislacyjnej. Jednym z przepisów będących wyrazem takiej swobody jest art. 88 RODO, który przewiduje możliwość zawarcia bardziej szczegółowych zasad w przepisach krajowych lub porozumieniach zbiorowych w przypadku przetwarzania danych osobowych w związku z zatrudnieniem[5]. Te krajowe regulacje w świetle art. 88 ust. 2 RODO muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych

[1] Studentka V roku prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] Więcej o rodzajach monitoringu: *D. Dörre-Nowak*, Monitoring w miejscu pracy a prawo do prywatności, [w:] Praca i zabezpieczenie społeczne, 2004, Nr 9, s. 8; *M. Kuba*, Prawne formy kontroli pracownika w miejscu pracy, Warszawa 2014, s. 276; *M. Wujczyk*, Prawo pracownika do ochrony prywatności, Warszawa 2012, s. 309.

[3] Dz.Urz. UE L Nr 199, s. 1, dalej jako: RODO.

[4] *M. Kawecki*, [w:] *M. Kawecki*, *T. Osieja* (red.), Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, Warszawa 2017, s. 4.

[5] Zgodnie z art. 88 ust. 1 RODO, Państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy; zob. również motyw 155 preambuły do RODO.

osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy. Polski prawodawca, dostrzegając potrzebę szczegółowego unormowania tej materii ze względu na specyfikę stosunku pracy, na mocy delegacji zawartej w art. 88 RODO znowelizował przepisy dotyczące przetwarzania danych osobowych pracowników w związku z zatrudnieniem. Uchwaloną 10.5.2018 r. ustawą o ochronie danych osobowych[6] dodano do Kodeksu pracy art. 22^2 i 22^3, dotykające bezpośrednio kwestii stosowania monitoringu w miejscu pracy, jednocześnie realizując podnoszone od dawna postulaty doktryny o zasadności przyjęcia kompleksowej regulacji w tym przedmiocie[7].

Pojęcie monitoringu

Rozważania należy rozpocząć od wyjaśnienia pojęcia monitoringu będącego przedmiotem regulacji omawianych art. 22^2 i 22^3 KP. Do 25.5.2018 r. w polskim porządku prawnym nie istniała definicja legalna monitoringu, a próby zdefiniowania tego pojęcia podejmowano poprzez odwoływanie się do definicji formułowanych przez organy nadzorcze, organizacje międzynarodowe, orzecznictwo czy piśmiennictwo. I tak według *Information Comissioner*[8] monitoring w miejscu pracy powinien być rozumiany jako czynności podejmowane w celu gromadzenia informacji o pracownikach poprzez poddanie ich obserwacji, zarówno bezpośredniej, jak i pośredniej, także przy użyciu środków elektronicznych[9]. Międzynarodowa Organizacja Pracy z kolei wskazuje, że monitoring obejmuje w szczególności stosowanie takich urządzeń, jak: komputery, kamery, sprzęt wideo, aparaty dźwiękowe, telefony i inne środki komunikacji, a także stosowanie różnych metod ustalania tożsamości i lokalizacji oraz innych form nadzoru[10]. W literaturze przedmiotu podnosi się, co zresztą nietrudno zauważyć w przywołanych powyżej definicjach, że pojęcie monitoringu należy odnosić do kontroli pracownika za pomocą nowoczesnych środków technicznych[11]. Wskazuje się przy tym, że monitoring nacechowany jest raczej stałością i systematycznością działań oraz ma pozwalać na bieżąco weryfikować stan faktyczny[12]. Większość wymienionych cech znajduje odzwierciedlenie w nowelizacji Kodeksu pracy, która do polskiego porządku prawnego wprowadza dwie nowe definicje: monitoringu oraz monitoringu poczty elektronicznej. Zgodnie z treścią art. 22^2 § 1 KP, mianem monitoringu określa się szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu. Tak sformułowana definicja sugeruje, że pojęcie to odnosi się wyłącznie do nadzoru przy użyciu wyżej wymienionych środków, którymi najczęściej będą zapewne kamery przemysłowe. Jednocześnie jednak w następnym art. 22^3 § 1 KP stanowi się o monitoringu poczty elektronicznej oraz innych jego formach. Nie jest do końca zrozumiałe, dlaczego prawodawca najpierw pojęcie monitoringu odnosi wyłącznie do nadzoru za pomocą środków umożliwiających rejestrację obrazu, a następnie tego samego pojęcia używa w kontekście kontroli poczty elektronicznej i innych form nadzoru pracowników. Wydaje się, że z tego względu bardziej trafne byłoby w art. 22^2 KP zastąpienie słowa „monitoring" wyrażeniem „monitoring wizyjny" – zwłaszcza że dla każdej ze zdefiniowanych form monitoringu istnieją odrębne podstawy prawne ich stosowania. Stąd na potrzeby niniejszego opracowania, pod ogólnym pojęciem monitoringu będą rozumiane wszelkie jego formy, natomiast monitoring przy użyciu środków umożliwiających rejestrację obrazu będzie określany jako monitoring wizyjny. W tym miejscu należy podkreślić, że nowa regulacja Kodeksu pracy nie jest ograniczona wyłącznie do form monitoringu zdefiniowanych wprost, art. 22^3 § 4 przewiduje bowiem możliwość wdrożenia również innych form monitoringu poprzez odpowiednie stosowanie przepisów o monitoringu poczty elektronicznej. Podstawy prawne stosowania poszczególnych form monitoringu zostaną szczegółowo opisane w dalszej części opracowania.

Monitoring a przetwarzanie danych osobowych – regulacja podstaw prawnych przetwarzania danych osobowych pochodzących z monitoringu przez pracodawcę

Stosowanie monitoringu daje pracodawcy techniczną możliwość zbierania rozmaitych informacji o pracowniku, takich jak: jego wizerunek, treść prowadzonej przez niego korespondencji, identyfikatory w systemach informatycznych, odwiedzane strony internetowe, czas pracy, odciski palca czy dane o lokalizacji. Powstaje pytanie, kiedy informacje te należy zakwalifikować jako dane osobowe w rozumieniu art. 4 ust. 1 RODO[13]. Przy dokonywaniu takiej kwalifikacji bierze się pod

[6] Dz.U. poz. 1000 ze zm.

[7] *M. Kuba*, Monitoring w miejscu pracy – refleksje na tle aktualnego stanu prawnego, Krytyka Prawa, tom 6, Warszawa 2014, s. 561 i 569.

[8] Information Commissioner to brytyjski urząd będący odpowiednikiem polskiego Prezesa Urzędu Ochrony Danych Osobowych.

[9] The Employment Practices Code, UK Information Commissioner's Office, Wilmslow 2011, s. 59.

[10] Protection of workers' personal data, International Labour Organisation, Geneva 1997, pkt 3.3; dalej jako: Kodeks Praktyk MOP.

[11] *M. Wujczyk*, Prawo…, s. 308–309.

[12] *M. Kuba*, Prawne…, s. 275.

[13] Zgodnie z treścią art. 4 pkt 1 RODO „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

uwagę wszelkie sposoby oraz inne informacje, jakimi może posłużyć się dany podmiot w celu zidentyfikowania określonej osoby[14]. Pracodawca, dysponując szczegółowymi informacjami o pracowniku (w tym niekiedy jego zdjęciami), zgromadzonymi w dokumentacji kadrowej i systemach informatycznych służących zarządzaniu zasobami ludzkimi, niemal w każdym przypadku będzie miał możliwość identyfikacji pracowników podlegających monitoringowi, która to możliwość jest kluczowym czynnikiem dla zakwalifikowania informacji jako danej osobowej. Oznacza to więc, że w ramach kontroli sprawowanej za pomocą monitoringu dochodzi do przetwarzania danych osobowych pracowników przez pracodawcę, nawet bowiem gdyby pracodawca nie wykorzystywał wtórnie danych pochodzących z monitoringu, to za przetwarzanie danych należy uznać już samą czynność ich gromadzenia[15]. Nie budzi przy tym wątpliwości, że pracodawca będzie występował tu w roli administratora danych osobowych, ponieważ to on jest podmiotem decydującym o celach i sposobach przetwarzania danych pracowniczych[16], co oczywiście nie wyklucza możliwości ich powierzenia podmiotom trzecim (takim jak dostawcy systemów informatycznych czy agencje ochrony) na mocy odpowiednich porozumień o powierzeniu przetwarzania[17]. Rodzi to zatem konieczność respektowania przez pracodawcę przepisów o ochronie danych osobowych. Powołane wyżej przepisy Kodeksu pracy są szczególną regulacją sektorową wprowadzoną na mocy delegacji zawartej w art. 88 RODO, co oznacza, że w zakresie przetwarzania danych w kontekście zatrudnienia będą miały one pierwszeństwo przed przepisami ogólnymi RODO. W regulacji tej znajdziemy m.in. szczególną podstawę prawną przetwarzania, ściśle określony termin retencji (przechowywania) danych czy określenie sposobu realizacji obowiązku informacyjnego o stosowaniu monitoringu. Jednak w przypadkach nieuregulowanych przez przepisy szczególne zastosowanie znajdą pozostałe przepisy RODO.

Podnieść należy, że dotychczasowy brak kompleksowej regulacji kwestii związanych z monitoringiem budził poważne zastrzeżenia oraz spotykał się z licznymi głosami krytyki i postulatami o konieczności ustanowienia odpowiednich przepisów w tej materii[18]. Przed 25.5.2018 r. podstawowymi aktami prawnymi znajdującymi zastosowanie dla przetwarzania danych osobowych w stosunkach pracy były Kodeks pracy i ustawa z 29.8.1997 r. o ochronie danych osobowych, przy czym regulacje kodeksowe w zasadzie ograniczały się do treści art. 22^1, który w kwestiach w nim nieuregulowanych odsyła do przepisów o ochronie danych osobowych. W § 1 i 2 omawianego artykułu ustanawia się zamknięty katalog danych, do których żądania uprawniony jest pracodawca[19]. Należy w tym miejscu zaznaczyć, że choć omawiany art. 22^1 KP upoważnia pracodawcę jedynie do żądania danych osobowych, to z treści artykułu wywodzi się również uprawnienie do przetwarzania danych jako konsekwencji ich gromadzenia[20]. Domaganie się wszelkich danych osobowych nieobjętych przedmiotowym katalogiem musi natomiast, zgodnie z § 4, znajdować podstawę w odrębnych, powszechnie obowiązujących przepisach prawa. Tak sformułowana treść art. 22^1 KP z jednej strony stanowi o prawach pracodawcy, a z drugiej służy ochronie życia prywatnego pracownika, mając na celu utrudnienie lub uniemożliwienie dyskryminowania pracowników ze względu na kryteria zabronione przepisami prawa pracy[21]. W konsekwencji znacznego ograniczenia przez ustawodawcę zakresu danych, do których żądania pracodawca jest uprawniony, liczne spory rodzi kwestia pozyskiwania z inicjatywy pracodawcy danych niemieszczących się w katalogu z art. 22^1 § 1 i 2 KP, jeśli pracownik wyraził na to zgodę. Pogląd o niedopuszczalności takich działań wydaje się dominujący i znajduje uzasadnienie w licznych decyzjach GIODO oraz orzecznictwie[22]. Naczelny Sąd Administracyjny w jednym z wyroków stanął na stanowisku, że wyrażona na prośbę pracodawcy pisemna zgoda pracownika na pobranie i przetworzenie jego danych osobowych narusza prawa pracownika i swobodę wyrażenia przez niego woli, uzasadniając swój pogląd w ten sposób, że brak równowagi w relacji pracodawca – pracownik stawia pod znakiem zapytania dobrowolność w wyrażeniu zgody na

[14] *P. Litwiński*, [w:] *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018, komentarz do art. 4, nb 3.

[15] Zgodnie z art. 4 pkt 2 RODO, „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

[16] W myśl art. 4 pkt 7 RODO, administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

[17] Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystania monitoringu wizyjnego, Urząd Ochrony Danych Osobowych, Warszawa 2018, s. 14–15; dalej jako: Wskazówki PUODO.

[18] *M. Kuba*, Monitoring…, s. 561 i 569.

[19] O zamkniętym charakterze tego katalogu: *A.M. Świątkowski*, Kodeks pracy. Komentarz, Warszawa 2018, art. 22^1, nb 2; *A. Malinowski*, Kodeks pracy, Warszawa 2015, art. 22^1, nb 1; *G. Sibiga*, Zakres stosowania ustawy o ochronie danych osobowych do przetwarzania danych pracowników i osób ubiegających się o zatrudnienie, MoPr 2012, Nr 3, s. 125.

[20] *M. Frąckowiak*, *T. Świeboda*, Ochrona danych osobowych pracownika w perspektywie RODO i przepisów dotyczących monitoringu wizyjnego stosowanego przez pracodawcę, MoPr 2018, Nr 7, s. 9; *G. Sibiga*, Zakres…, s. 124.

[21] *A.M. Świątkowski*, Kodeks…, komentarz do art. 22^1, nb 2.

[22] Zob. m.in.: decyzja GIODO z 29.3.2011 r., Nr DIS/DEC–249/14067/11; decyzja GIODO z 15.12.2009 r., Nr DIS/DEC–1261/46988/09; decyzja GIODO z 19.5.2009 r., Nr DOLIS/DEC-400/09, decyzja GIODO z 19.5.2006 r., Nr GI-DEC-DIS-163/06/481; zob. również stanowiska GIODO dostępne na stronach: https://giodo.gov.pl/pl/348/971, https://giodo.gov.pl/pl/348/2962 (dostęp z dnia 10.12.2018 r.).

pobieranie i przetworzenie danych osobowych[23]. Pojawiały się jednak negatywne oceny tak ukształtowanej linii interpretacyjnej jako nienadążającej za potrzebami rynku pracy i stawiającej niepotrzebne granice w rozwoju nowych technologii[24]. Podnoszono również, że nie wydaje się uzasadnione przyjmowanie z góry założenia o braku możliwości wyrażenia przez pracownika zgody spełniającej kryteria stawiane przez prawo ochrony danych, a w konsekwencji niedopuszczalności przetwarzania danych przez pracodawcę na zasadach ogólnych[25]. Dlatego warto zaznaczyć, że podnoszony w doktrynie postulat o wprowadzeniu zgody pracownika jako podstawy przekazania pracodawcy innych danych niż objęte dyspozycją art. 22^1 § 1 i 2 KP[26], został uwzględniony w procesie dostosowywania brzmienia obowiązujących przepisów prawa pracy do postanowień RODO. Jeśli bowiem ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 zostanie podpisana przez Prezydenta RP[27], już wkrótce do Kodeksu pracy zostanie dodany art. 22^{1a}, zgodnie z którym zgoda osoby ubiegającej się o zatrudnienie lub pracownika będzie mogła stanowić, z pewnymi wyjątkami, podstawę przetwarzania przez pracodawcę danych osobowych innych niż skatalogowane w art. 22^1 KP, niezależnie od tego, czy ich pozyskanie nastąpi z inicjatywy pracodawcy czy pracownika. W świetle poczynionych wyżej uwag zmianę taką należy ocenić jako pozytywną, gdyż kładzie kres wielu problemom interpretacyjnym związanym z brakiem kompleksowej regulacji w tym przedmiocie.

Przesłanki dopuszczalności poszczególnych form monitoringu po 25.5.2018 r.

Zanim szczegółowo opisane zostaną przesłanki dopuszczalności poszczególnych form monitoringu wprowadzonych w drodze nowelizacji Kodeksu pracy wraz z reformą ochrony danych, wypada pokrótce przybliżyć, jak dotychczas doktryna kształtowała warunki, których spełnienie czyniło monitoring dopuszczalnym. Otóż zaliczało się do nich[28]:

1. Zgodność z prawem – za niedopuszczalne uznawano stosowanie monitoringu polegającego na wykorzystaniu metod sprzecznych z prawem.
2. Istnienie usprawiedliwionego celu – wdrożenie monitoringu musiało mieć swoją wyraźną i uzasadnioną przyczynę.
3. Proporcjonalność – wybrany środek nadzoru powinien być proporcjonalny do założonego celu, jaki monitoring miał spełniać.
4. Transparentność – konieczne było określenie jasnych reguł stosowania monitoringu oraz stopnia jego ingerencji w prywatność pracowników.
5. Spełnienie wymogów określonych w przepisach o ochronie danych osobowych.

Nie ulega wątpliwości, że wszelkie formy monitoringu z punktu widzenia ochrony pracownika mogą potencjalnie stanowić zagrożenie dla jego dóbr osobistych. Dlatego zanim pracodawca wdroży szczególny system nadzoru w swoim zakładzie pracy, powinien on zidentyfikować jego cel (np. poprawa bezpieczeństwa), a następnie dobrać środki i sposób użytkowania monitoringu odpowiednio do założonego celu[29]. Monitoring nie może bowiem prowadzić do nadmiernej ingerencji w sferę osobistą pracownika lub do pozyskiwania jego danych osobowych w zakresie wykraczającym ponad niezbędne potrzeby pracodawcy[30]. Z podobnego założenia wyszedł ustawodawca, dając w przyjętych przepisach wyraz zasadom celowości i proporcjonalności. W myśl art. 22^2 § 1 KP pracodawca może wprowadzić monitoring wizyjny, jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Monitoring poczty elektronicznej zaś, zgodnie z art. 22^3 § 1 KP, może być przez pracodawcę wprowadzony, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Omawiane przepisy zawierają enumeratywne wyliczenie przyczyn uzasadniających wprowadzenie szczególnego nadzoru nad pracownikami w postaci monitoringu. Brak więc podstaw do zastosowania monitoringu przez pracodawcę w celach innych niż wyrażone *explicite* w Kodeksie pracy. Taki też pogląd wyraził Prezes Urzędu Ochrony Danych Osobowych, uzasadniając swoje stanowisko w ten sposób, że możliwość stosowania określonych narzędzi kontroli pracownika, co do zasady, powinna być określona w ustawie, wraz z gwarancjami zabezpieczającymi pracowników przed ich nadużywaniem ze strony administratora[31]. Ponadto w obu przepisach wyraźnie posłużono się kryterium niezbędności. Należy je rozumieć tak, że monitoring może być wprowadzony tylko wtedy, kiedy inne, mniej inwazyjne metody zapewniania bezpieczeństwa są niewystarczające, a wskazanych celów nie można osiągnąć w inny sposób niż przez

[23] Zob. wyrok NSA z 1.12.2009 r., I OSK 249/09, Legalis.

[24] *A. Malinowski*, Kodeks…, komentarz do art. 22^1, nb 5; podobny pogląd wyrażono w wyroku WSA w Warszawie z 27.11.2008 r., II SA/Wa 903/08, Legalis.

[25] *M. Wujczyk*, Prawo…, s. 170–171.

[26] *Ibidem*, s. 178.

[27] Na dzień sporządzenia niniejszego opracowania ustawa oczekuje na podpis Prezydenta RP – została ona uchwalona przez Sejm 21.2.2019 r. oraz przyjęta przez Senat bez poprawek 21.3.2019 r.; tekst ustawy dostępny jest na stronie: http://orka.sejm.gov.pl/opinie8.nsf/dok?OpenAgent&3050_u (dostęp z 22.3.2019 r.).

[28] *A. Lach*, Monitorowanie pracownika w miejscu pracy, MoPr 2004, Nr 10, s. 267–268.

[29] *M. Kuba*, Monitoring…, s. 568.

[30] Wskazówki PUODO, s. 13.

[31] *Ibidem*, s. 19–20.

wybraną formę monitoringu[32]. Wybrana forma monitoringu musi więc pozostawać w stosunku proporcjonalności do założonego celu, z uwzględnieniem potrzeby ochrony prawa do prywatności i ochrony danych osobowych pracowników. Zasady celowości i niezbędności są elementem wspólnym dla regulacji monitoringu wizyjnego i monitoringu poczty elektronicznej, natomiast na szerszą uwagę zasługują również regulacje szczególne, odnoszące się do poszczególnych form monitoringu uwzględnionych w Kodeksie pracy.

1. Monitoring wizyjny

Z uwagi na fakt, że monitoring wizyjny uważa się za jeden ze sposobów kontroli najsilniej ingerujących w prywatność pracownika[33] oraz ze względu na szczegółowość ustawowej regulacji, to właśnie tej formie monitoringu poświęcona będzie znaczna część dalszych rozważań. W ustawie wskazano wyczerpująco cztery przypadki, w których zastosowanie przez pracodawcę środków technicznych umożliwiających rejestrację obrazu będzie uzasadnione. Są to: bezpieczeństwo pracowników, ochrona mienia, kontrola produkcji lub zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Nie budzi wątpliwości zasadność uznania ochrony bezpieczeństwa pracowników za uzasadniony cel stosowania monitoringu, wszak już na gruncie regulacji sprzed 25.5.2018 r. względy bezpieczeństwa kwalifikowano jako mieszczące się w formule zgodnego z prawem celu kontroli pracownika[34]. Wątpliwości może budzić natomiast objęcie dyspozycją przepisu wyłącznie pracowników. Na terenie zakładu pracy lub wokół niego mogą bowiem przebywać nie tylko osoby trzecie takie jak klienci, kontrahenci, dostawcy itp., ale również osoby świadczące na rzecz pracodawcy usługi lub pracę na podstawie innej niż stosunek pracy (np. zleceniobiorcy, samozatrudnieni). Wydaje się, że zasadne byłoby więc sformułowanie przepisu w sposób mający na celu zapewnienie bezpieczeństwa wszystkich osób przebywających na terenie zakładu pracy lub wokół niego, a nie tylko pracowników. Drugą okolicznością uzasadniającą wprowadzenie monitoringu wizyjnego w miejscu pracy jest ochrona mienia. Jeśli przyjąć znaczenie nadane temu zwrotowi w ustawie z 22.8.1997 r. o ochronie osób i mienia[35], należy rozumieć je jako działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony. Ponieważ ustawodawca nie wskazał, o czyje mienie chodzi, należy raczej przyjąć, że wprowadzenie monitoringu wizyjnego uzasadniać będzie ochrona mienia nie tylko należącego do pracodawcy, ale również do pracowników, zleceniobiorców czy osób trzecich[36]. Okoliczność ta została więc ujęta w sposób bardzo szeroki. Kolejną przesłanką, której sformułowanie może nastręczać pewnych trudności interpretacyjnych, jest kontrola produkcji. Powstaje bowiem pytanie, jak ową kontrolę produkcji rozumieć – czy wyłącznie jako monitoring procesów produkcyjnych zapewniający ich prawidłowy, nieprzerwany przebieg oraz kontrolowanie ewentualnych nieprawidłowości, czy również jako kontrola wydajności produkcji i efektywności świadczonej pracy (popularna np. w magazynach, dużych halach produkcyjnych i montażowych), która potencjalnie mogłaby stanowić podstawę oceny pracownika. Rozstrzygnięcie problemu utrudnia fakt, że omawiane przepisy obowiązują zaledwie kilka miesięcy, nie zdążyła się więc wykształcić w tym zakresie jakakolwiek linia orzecznicza. W doktrynie pojawiają się głosy poparcia dla szerszego rozumienia tego zwrotu[37], jednak w opublikowanych przez Prezesa Urzędu Ochrony Danych Osobowych wskazówkach dotyczących wykorzystania monitoringu wizyjnego, wyraźnie stanął on na stanowisku, że niedopuszczalne jest stosowanie monitoringu jako środka nadzoru nad jakością wykonywanej pracy[38]. Taka interpretacja wydaje się zgodna nie tylko z literalnym brzmieniem przepisu, który wyraźnie stanowi nie o „kontroli świadczonej pracy", a „kontroli produkcji", ale również z zaleceniami Grupy Roboczej Artykułu 29[39]. Ostatnią przesłanką stanowiącą podstawę do wprowadzenia środków technicznych umożliwiających rejestrację obrazu jest zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Słusznie wskazuje się, że o ile cel ten nie budzi zastrzeżeń, o tyle przedmiotowa forma monitoringu nie wydaje się odpowiednia w kontekście ochrony informacji[40], zwłaszcza że przepisy o monitoringu nie zezwalają co do zasady na nagrywanie dźwięku towarzyszącego zdarzeniom, a zgodnie z poglądem Prezesa Urzędu Ochrony Danych Osobowych stosowanie rejestracji dźwięku może zostać uznane za nadmiarową formę przetwarzania danych, wiązać się z odpowiedzialnością administracyjną i cywilną, a nawet karną[41]. Właściwszym środkiem służącym ochronie informacji wydaje się monitoring poczty elektronicznej.

Z podjęciem decyzji o wdrożeniu monitoringu nieodłącznie wiąże się konieczność określenia jego celu, zakresu oraz sposobu zastosowania. Zgodnie z art. 22^2 § 6 KP ustala się je w układzie zbiorowym pracy bądź w regulaminie pracy, a jeśli pracodawca nie jest objęty układem zbiorowym pracy lub nie

[32] *K. Jaśkowski*, *E. Maniewska*, Komentarz aktualizowany do Kodeksu pracy, Lex/el. 2018, art. 22^2, 22^3, nb 2.2; wskazówki PUODO, s. 22.

[33] *M. Wujczyk*, Prawo…, s. 318.

[34] *M. Kuba*, Monitoring…, s. 565.

[35] T.j. Dz.U. z 2018 r. poz. 2142 ze zm.

[36] *M. Kuba*, [w:] *K.W. Baran* (red.), Kodeks pracy. Komentarz, Warszawa 2018, art. 22^2, nb 4.4.

[37] *M. Frąckowiak*, *T. Świeboda*, Ochrona…, s. 13.

[38] Wskazówki PUODO, s. 19–20; podobny pogląd wyrażono w Kodeksie Praktyk MOP, pkt 5.4.

[39] Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, Article 29 Data Protection Working Party, Brussels 2004, s. 25; dalej jako: WP89 4/2004.

[40] *M. Kuba*, [w:] *K.W. Baran* (red.), Kodeks…, komentarz do art. 22^2, nb 4.6.

[41] Wskazówki PUODO, s. 26.

jest obowiązany do ustalenia regulaminu pracy – w obwieszczeniu. Pracodawca nie zawsze zatem będzie uprawniony do samodzielnego określenia celu, zakresu i sposobu zastosowania monitoringu, gdyż na gruncie przepisów Kodeksu pracy wprowadzenie oraz zmiana dwóch pierwszych dokumentów wymaga uzgodnienia z zakładową organizacją związkową[42]. Ustawa nie precyzuje terminu wydania czy daty wejścia w życie obwieszczenia o monitoringu, podobnie jak nie określa terminu na dostosowanie treści układu zbiorowego pracy lub regulaminu. Ustalając taki termin, pracodawca powinien jednak mieć na względzie, że w myśl art. 22^2 § 7 KP poinformowanie pracowników o wprowadzeniu monitoringu musi nastąpić nie później niż dwa tygodnie przez jego uruchomieniem. Ponadto każdorazowo przed dopuszczeniem pracownika do pracy pracodawca powinien przekazać mu na piśmie te same informacje, które ma obowiązek zamieścić w regulaminie pracy, układzie zbiorowym lub obwieszczeniu (art. 22^2 § 8 KP). Obowiązek informacyjny może być więc realizowany bądź w trybie zbiorowym, bądź indywidualnym – zależnie od tego, czy informacja jest przekazywana pracownikowi pozostającemu już w stosunku pracy, czy nowo zatrudnionemu. Niezależnie od powyższego na pracodawcy spoczywa również obowiązek oznaczenia pomieszczeń i terenu objętych monitoringiem wizyjnym w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem (art. 22^2 § 9 KP). Osoby pozostające w obszarze monitorowanym muszą bowiem mieć świadomość, że miejsce ich pobytu jest obserwowane za pomocą kamer. Jak wskazuje Prezes Urzędu Ochrony Danych Osobowych, znaki takie powinny być dostępne przed wejściem w obszar obserwowany, w niezbyt dużej odległości od nadzorowanych miejsc. Ponadto powinny być widoczne, syntetyczne, umieszczone w sposób trwały, zaś wymiary tablic muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer[43]. Nie jest jednak wystarczające oznaczenie obszaru objętego monitoringiem wyłącznie piktogramami, gdyż spełnienie obowiązku w sposób określony w § 9 nie konsumuje obowiązku informacyjnego ustanowionego w art. 13 RODO, wynikającego z pełnionej przez pracodawcę funkcji administratora danych. Pełna informacja o monitoringu, obejmująca wszystkie wymogi z art. 13 RODO, powinna być zamieszczona w miejscu monitorowanym, np. na tablicach albo w formie dokumentu dostępnego na recepcji czy też u przedstawiciela administratora[44]. Oznacza to możliwość realizacji obowiązku informacyjnego poprzez podanie informacji podstawowych i uzupełnienie ich w kolejnych warstwach informacyjnych, co z praktycznego punktu widzenia wydaje się bardzo dogodnym wyjściem z uwagi na obszerność klauzul informacyjnych zgodnych z wymogami RODO. Na podstawie opisanych czynności informacyjnych sformułować można zasadę jawności monitoringu wizyjnego, której wprowadzenie bez wątpienia należy ocenić pozytywnie. Wszak tylko pracownik świadomy bycia obserwowanym jest w stanie chronić się przed nadmierną ingerencją w jego prywatność przez pracodawcę. Na istotne znaczenie realizacji obowiązku informacyjnego wskazuje Europejski Trybunał Praw Człowieka w wyroku w sprawie Lopez Ribalda i inni przeciwko Hiszpanii[45]. W przedmiotowym stanie faktycznym skarżące były kasjerkami w sieci supermarketów. Wobec podejrzenia ich o kradzież miejsce ich pracy objęto monitoringiem wizyjnym, jednak nie ujawniono lokalizacji części kamer. W opinii Trybunału doszło więc do naruszenia prawa do poszanowania życia prywatnego i rodzinnego ustanowionego w art. 8 Konwencji ochronie praw człowieka i podstawowych wolności[46]. Warto również nadmienić, że wprowadzenie wymogu jawności monitoringu wizyjnego od dawna było postulowane przez Grupę Roboczą Artykułu 29[47] oraz Międzynarodową Organizację Pracy[48].

Interesy pracodawcy nie mogą w sposób nadmierny ograniczać dóbr osobistych pracownika, w szczególności jego prawa do prywatności i ochrony danych oraz uzasadnionego oczekiwania co do zapewnienia intymności. Ustawodawca daje temu wyraz w art. 22^2 § 2 KP, ustanawiając zakaz prowadzenia monitoringu wizyjnego w pomieszczeniach sanitarnych, szatniach, stołówkach, palarniach i pomieszczeniach udostępnianych zakładowej organizacji związkowej. Dopuszcza się jednak odejście od tego zakazu, gdy jest to niezbędne do realizacji celu wprowadzenia monitoringu oraz nie narusza to godności i innych dóbr osobistych pracownika – co jest możliwe w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób (np. oprogramowania zamazującego określone fragmenty kadrowanego obrazu[49]). Pomieszczenia domyślnie wyłączone spod monitoringu wizyjnego mogą zatem być nim objęte tylko wyjątkowo, a nadzór taki powinien być ograniczony czasowo – może to np. oznaczać tymczasowe objęcie nadzorem kamer szafek, do których ktoś usiłował się włamać albo dokonał z nich kradzieży[50]. Zawsze jednak pracodawca powinien rozważnie podchodzić do kwestii monitorowania miejsc zakazanych, wyważając sprzeczne interesy obu stron stosunku pracy.

W art. 22^1 § 3–5 KP uregulowano również w sposób szczególny okres retencji (przechowywania) danych utrwalonych w postaci nagrań obrazu. Wynosi on co do zasady trzy miesiące od dnia nagrania. Jedynie w przypadku gdy nagrania

[42] Por. art. 104^2 i 241^9 KP.
[43] Wskazówki PUODO, s. 14, 20.
[44] *Ibidem*, s. 14.
[45] Wyrok Europejskiego Trybunału Praw Człowieka z 9.1.2018 r. w sprawie López Ribalda i inni przeciwko Hiszpanii, skarga nr 1874/13.
[46] Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r., Dz.U. z 1993 r. Nr 61, poz. 284.
[47] WP89 4/2004, s. 22.
[48] Kodeks Praktyk MOP, pkt 6.14.
[49] Wskazówki PUODO, s. 26.
[50] *Ibidem*, s. 27.

obrazu stanowią lub mogą stanowić dowód w postępowaniu prowadzonym na podstawie prawa, o czym pracodawca powziął wiadomość, termin ten ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Wyjątek ten ma zapewne na celu zabezpieczenie nagrań utrwalających incydenty, których odtworzenie może mieć znaczenie dla celów dowodowych. Po upływie wskazanych terminów, jeśli przepisy odrębne nie stanowią inaczej, dane osobowe uzyskane w wyniku nagrania muszą ulec zniszczeniu. Powyższe regulacje stanowią więc uszczegółowienie wyrażonej w art. 5 ust. 1 lit. e RODO zasady ograniczenia czasowego, zgodnie z którą dane muszą być przechowywane w formie umożliwiającej identyfikację podmiotu danych, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

2. Monitoring poczty elektronicznej

Drugą formą monitoringu, uregulowaną wprost w art. 22^3 znowelizowanego Kodeksu pracy, jest kontrola służbowej poczty elektronicznej pracownika. Unormowanie to jest o tyle istotne, że stanowi ograniczenie wolności i tajemnicy komunikowania się, którym ustawodawca nadał szczególną rangę poprzez objęcie ich konstytucyjną ochroną i których ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony[51]. W świetle omawianej regulacji pracodawca może wprowadzić monitoring poczty elektronicznej, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Należy zwrócić uwagę, że wskutek posłużenia się przez ustawodawcę spójnikiem oraz wymagane jest spełnienie obu przesłanek jednocześnie – monitoring poczty elektronicznej pracownika będzie zatem dopuszczalny wyłącznie wówczas, gdy jego zastosowanie będzie niezbędne zarówno do zapewnienia odpowiedniej organizacji pracy, jak i dla właściwego użytkowania udostępnionych pracownikowi narzędzi. Wydaje się, że sposób sformułowania celów przedmiotowej formy monitoringu nie wymaga szerszego komentarza – chronią one interes pracodawcy w tym, aby pracownicy jak najpełniej wykorzystali czas pracy na wykonywanie swoich obowiązków, a także aby odpowiednio korzystali z udostępnionych im w tym celu narzędzi[52]. Jak sygnalizowano już powyżej, można jedynie mieć zastrzeżenia co do nieuwzględnienia monitoringu poczty elektronicznej jako środka mającego na celu ochronę istotnych dla pracodawcy informacji. Wszak w dobie powszechnej informatyzacji ogromne ilości danych są przechowywane przez pracodawców w formie elektronicznej, a ich ujawnienie za pośrednictwem poczty elektronicznej poza system informatyczny pracodawcy może być niezwykle łatwe. Dziwi również, dlaczego ustawodawca ogranicza zakres regulacji wyłącznie do poczty elektronicznej, nie obejmując nią innych metod komunikacji służbowej, np. wiadomości SMS, komunikatorów w postaci aplikacji na telefon czy rozmów telefonicznych. Jak wskazuje *M. Kuba*, wprawdzie objęcie monitoringiem również tych innych metod komunikacji jest możliwe na podstawie art. 22^3 § 4 KP, odsyłającego do odpowiedniego stosowania przepisów o monitoringu poczty elektronicznej, jednak zasadność ich unormowania wprost podyktowana jest szczególną doniosłością tajemnicy komunikacji oraz warunkami jej ograniczenia[53].

W myśl art. 22^3 § 2 KP monitoring poczty elektronicznej nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika. Przy wytyczaniu granic owej tajemnicy może jednak powstać wątpliwość co do dopuszczalnego zakresu kontroli pracodawcy, w szczególności gdy w elektronicznej skrzynce pocztowej znajdują się zarówno wiadomości o charakterze służbowym, jak i prywatnym. Niektórzy autorzy podzielają pogląd, że nie można a *priori* zakładać, że każda wiadomość wysłana lub odebrana przy użyciu sprzętu służbowego ma charakter komunikacji służbowej, więc w razie przypadkowego natknięcia się przez pracodawcę na wiadomość o charakterze prywatnym, nie będzie on uprawiony do przeczytania takiej wiadomości w całości, nawet przy istnieniu zakazu korzystania z poczty służbowej do celów prywatnych[54]. Inni zaś proponują domniemanie, że o ile brak wyraźnego oznaczenia prywatnego charakteru korespondencji, o tyle prowadzona jest ona w imieniu pracodawcy, zatem nie może być mowy o jakiejkolwiek poufności korespondencji prowadzonej ze służbowej skrzynki pracownika (z domniemania takiego jednak nie mógłby korzystać pracodawca zakazujący używania służbowej poczty elektronicznej dla celów prywatnych)[55]. Wydaje się więc, że najdogodniejszym wyjściem dla pracodawcy jest wprowadzenie zakazu korzystania z poczty służbowej do celów prywatnych.

Doniosłe znaczenie dla ochrony dóbr osobistych pracownika ma również realizacja zasady jawności. Obowiązek informacyjny w przypadku stosowania monitoringu poczty elektronicznej ukształtowano na wzór przepisów o monitoringu wizyjnym poprzez ich odpowiednie zastosowanie (art. 22^3 § 3 KP). Oznacza to, że podobnie jak przy monitoringu wizyjnym, cele, zakres oraz sposób zastosowania monitoringu muszą zostać określone w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, a w przypadku nowo zatrudnionego pracownika – przekazane mu na piśmie. Ponadto informacja o wprowadzeniu monitoringu

[51] Zob. treść art. 49 Konstytucji RP.

[52] Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców, Urząd Ochrony Danych Osobowych, Warszawa 2018, s. 34.

[53] *M. Kuba*, [w:] *K.W. Baran* (red.), Kodeks…, komentarz do art. 22^3, nb 3.1.

[54] *Ibidem*, nb 4.1.

[55] *E. Suknarowska-Drzewiecka*, [w:] *K. Walczak* (red.), Kodeks pracy. Komentarz, Warszawa 2018, art. 22^3, nb 3.

poczty elektronicznej musi zostać przekazana pracownikom nie później niż dwa tygodnie przed jego uruchomieniem, a miejsca monitorowane muszą być oznaczone w sposób widoczny i czytelny. Zastanawia jedynie, w jaki sposób pracodawca miałby spełnić ten ostatni wymóg. Przykładowo przychodzą tu na myśl stosowne oznaczenia na ekranach lub skrzynkach pocztowych pracowników.

Odnośnie pozostałych form monitoringu, odpowiednie zastosowanie znajdą przepisy o monitoringu poczty elektronicznej, jednak pod warunkiem że ich zastosowanie jest niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Do takich form kontroli można zaliczyć między innymi monitoring systemów informatycznych oraz aktywności pracowników w Internecie, stosowanie urządzeń GPS w samochodach służbowych czy ewidencjonowanie czasu pracy przy użyciu zautomatyzowanych narzędzi.

3. Inne obowiązki pracodawcy związane ze stosowaniem monitoringu w miejscu pracy

Poza warunkami legalności stosowania monitoringu w miejscu pracy i związanymi z tym obowiązkami ustanowionymi Kodeksu pracy pracodawca musi również spełnić wiele wymogów prawnych włożonych na niego przez RODO z racji pełnienia roli administratora danych osobowych pracowników. Pracodawca obowiązany jest w szczególności:

1) przestrzegać zasad dotyczących przetwarzania danych osobowych, ustanowionych w art. 5 RODO – istotne znaczenie ma tu zwłaszcza zasada rozliczalności, nakazująca administratorowi być w stanie wykazać przestrzeganie innych zasad przetwarzania;
2) realizować wobec podmiotów danych obowiązek informacyjny w myśl art. 13–14 RODO – jak już wskazano, realizacja obowiązków informacyjnych wynikających z Kodeksu pracy nie konsumuje tych ustanowionych w rozporządzeniu;
3) umożliwiać osobom, których dane dotyczą, realizację praw przyznanych im w art. 15–22 RODO – tj. prawa dostępu, prawa do sprostowania lub usunięcia danych, prawa do ograniczenia przetwarzania, prawa do przenoszenia danych;
4) zapewnić bezpieczeństwo danych poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać, zgłaszanie naruszeń ochrony danych organowi nadzorczemu oraz zawiadamianie podmiotów danych o takich naruszeniach (art. 32–34 RODO).

Ponadto, w sytuacjach określonych w RODO, pracodawca ma również obowiązek przeprowadzenia skutków planowanych operacji przetwarzania dla ochrony danych, powołania inspektora ochrony danych osobowych czy prowadzenia rejestru czynności przetwarzania.

Podsumowanie

Konkludując, można stwierdzić, że pomimo istnienia pewnych niedoskonałości w treści art. 22^2 i 22^3 KP sam fakt ich włączenia do Kodeksu pracy należy ocenić pozytywnie. Objęcie kompleksową regulacją kwestii związanych ze stosowaniem monitoringu w miejscu pracy było bowiem w dotychczasowym stanie prawnym pożądane z punktu widzenia ochrony prywatności i danych osobowych pracownika.

Słowa kluczowe: monitoring w miejscu pracy, dane osobowe, RODO, Rozporządzenie Ogólne o Ochronie Danych Osobowych, Kodeks pracy, pracodawca, administrator, pracownik, podmiot danych, reforma ochrony danych osobowych, prywatność w miejscu pracy.

Criteria of admissibility to use video surveillance in a workplace and duties of an employer in the light of reform on personal data protection

The aim of this paper is to analyze the regulations concerning the use of video surveillance in a workplace, introduced into Polish legal system as a result of personal data protection law reform. The author explains the concept and types of video surveillance, indicates and discusses legal grounds for introducing particular forms of monitoring by an employer, formulates their admissibility requirements and describes obligations of an employer. The author's reflections are based on the analysis of labour law and personal data protection law provisions, as well as the views expressed by scholars, jurisprudence, regulatory bodies and international organizations.

Keywords: video surveillance in a workplace, personal data, GDPR, General Data Protection Regulation, labour code, employer, administrator, employee, subject of data, personal data protection reform, privacy in a workplace.

Dowód z opinii biegłego a ustalenie konkurencyjnego charakteru produkcji – audycji telewizyjnych

adw. *Aleksandra Glanc-Walkiewicz*[1]

Celem niniejszego artykułu jest odpowiedź na pytanie, czy możliwe jest ustalenie charakteru danej audycji telewizyjnej jako utworu audiowizualnego i tym samym zaszeregowanie jej do danego gatunku w oparciu na dowód z opinii biegłego w procesie sądowym (czy też na podstawie innego środka dowodowego). Kwestia ta może być przydatna dla rozstrzygnięcia sprawy o zapłatę kary umownej za naruszenie przez twórcę wobec producenta zakazu konkurencji polegające na wykonaniu dzieła autorskiego, np. reżyserii, na rzecz innego podmiotu konkurującego na rynku usług audiowizualnych w zakresie gatunku utworu audiowizualnego/audycji telewizyjnej.

Uwagi wstępne

Problem prawny, jaki wiąże się z ustaleniem charakteru danej audycji telewizyjnej, może wynikać ze sporu dotyczącego roszczenia producenta o zapłatę kary umownej przeciwko wykonawcy dzieła autorskiego w postaci reżyserii odcinków audycji telewizyjnej z tytułu naruszenia zakazu konkurencji. Ważne jest przy tym ustalenie, czy udział tego twórcy (reżysera) w produkcji na rzecz innego podmiotu konkurencyjnego dotyczył produkcji o tożsamym charakterze, objętej klauzulą zakazu konkurencji, czyli utworu audiowizualnego, np. w postaci audycji telewizyjnej z gatunku paradokumentu. W tym celu konieczna staje się identyfikacja obu produkcji pod kątem zakwalifikowania ich do gatunku serialu paradokumentalnego.

Istotne znaczenie dla tej kwestia ma zagadnienie, czy jedynym albo też podstawowym dowodem oferowanym w takiej sprawie powinien być dowód z opinii biegłego. Jeżeli tak, to jaką specjalizację ma posiadać biegły? Czy wystarczający będzie dowód z opinii jednego biegłego, zespołu biegłych czy też konieczne jest posłużenie się dowodem z opinii instytutu naukowo-badawczego? Należy jednak rozważyć, czy dowód taki w przedstawionym procesie jest zbędny, gdyż ocena przynależności obu seriali do gatunku paradokumentu nie wymaga wiedzy specjalnej.

Już na początku rozważań można postawić tezę, że dowód z opinii biegłego w takim procesie może okazać się nieprzydatny, chociaż analiza orzecznictwa sądów w takich procesach wskazuje na to, że ten dowód jest często stosowany, zwykle z inicjatywy samej strony procesu, zgodnie z art. 6 KC.

Dowód z opinii biegłego

Należy przypomnieć, że zgodnie z art. 278 KPC biegłego sądowego powołuje się w wypadkach wymagających wiadomości specjalnych. Dowód z opinii biegłego, z uwagi na wymóg wiadomości specjalnych, jest dowodem tego rodzaju, że nie może być zastąpiony inną czynnością dowodową, np. zeznaniem świadka, czy innymi środkami dowodowymi, gdyż te środki nie niosą odpowiednich wiadomości specjalnych, mających wpływ na rozstrzygnięcie sporu cywilnego. Dowód taki jest dopuszczalny w sytuacji, gdy nie może być zastąpiony przez jakikolwiek inny środek dowodowy, np. zeznania świadków, dowód z dokumentów, informacje uzyskane od określonego podmiotu, instytucji. Opinia biegłego może być zastąpiona przez zeznania świadka, który posiada wiedzę specjalną np. lekarza, ale dowód taki nie może być uznawany za opinię biegłego, przy czym może być wzięty pod uwagę przez sąd przy ocenie przydatności opinii biegłego sądowego w sprawie i uzasadniać zasięgnięcie opinii biegłego lub biegłych[2].

Opinia biegłego najczęściej dotyczy zagadnień wymagających szczegółowych informacji z różnorodnych dziedzin nauki. Sąd, opierając się na opinii biegłego wyspecjalizowanego w konkretnej dziedzinie, rozstrzyga wątpliwości pojawiające się w toku procesu w celu właściwego ustalenia stanu faktycznego sprawy. Ustawodawca uzależnia zatem przeprowadzenie dowodu z opinii biegłego od konieczności posiadania tzw. wiadomości specjalnych. Pojęcie to nie zostało jednak zdefiniowane, ponieważ nie jest możliwe jednoznaczne ustalenie definicji legalnej. Wynika to z tego, że kryteria do ustalenia tego pojęcia są uzależnione okolicznościami danej sprawy i stopniem jej skomplikowania, uzasadniającym skorzystanie z pomocy podmiotu mającego wiedzę specjalną. Ustawodawca pozostawia więc sądowi, ewentualnie stronom, decyzję co do zdefiniowania potrzeby skorzystania z opinii biegłego[3]. Biegłych sądowych powołuje się w sytuacji, gdy potrzebna jest

[1] Adwokat w ORA we Wrocławiu, wcześniej sędzia orzekający w wydziale cywilnym Sądu Rejonowego i Okręgowego we Wrocławiu, specjalista z zakresu prawa własności intelektualnej, zwłaszcza utworów audiowizualnych.

[2] Tak SN w wyroku z 5.2.1976 r., ICR 264/74, niepubl.

[3] *A. Klich*, Pojęcie wiadomości specjalnych w tzw. Cywilnych procesach lekarskich, [w:] *R. Sztychmiller, M. Różański* (red.), Dowodzenie w sprawach cywilnych, gospodarczych i administracyjnych, Olsztyn 2014, s. 96–97.

wiedza z poszczególnych dziedzin nauki np. techniki, sztuki, rzemiosła, a także innych umiejętności. Oczywiście wiedza prawnicza, poza prawem obcym, jest wyłączona z tych dziedzin wiedzy, ponieważ sąd jest specjalistą z zakresu prawa. Konieczne jest posłużenie się biegłymi, którzy posiadają umiejętności powiązane z ich wykształceniem właściwym dla określonej dziedziny wiedzy, a także z zawodem wykonywanym w danej dziedzinie[4]. Wiadomości specjalne nie muszą mieć naukowego charakteru, mogą być także wynikiem wiedzy uzyskanej w ramach praktyki[5].

Utwór audiowizualny i jego cechy

Należy stwierdzić, że w celu ustalenia, czy oba utwory audiowizualne, a dokładnie audycje telewizyjne w postaci seriali przynależą do gatunku paradokumentu, a zatem czy są wobec siebie konkurencyjne, wymagana jest wiedza specjalna, dziedziną tą będzie zaś filmoznawstwo. Istnieje jednak wiele kwalifikatorów pozwalających – po przeprowadzeniu porównania – na wyróżnienie spośród innych utworów audiowizualnych gatunku paradokumentu. Do kwalifikatorów tych można zaliczyć[6] cechy specyficzne gatunku paradokumentu na podstawie jego definicji, a także cechy dotyczące technik produkcji i doboru obsady w serialu paradokumentalnym.

Istotne znaczenie dla ustalenia przez sąd przynależności danego utworu audiowizualnego do paradokumentu ma także klasyfikacja audycji telewizyjnych z określeniem przynależności do gatunku dokonywana przez Państwową Wyższą Szkołę Filmową, Telewizyjną i Teatralną im. Leona Schillera w Łodzi[7].

Paradokument jako utwór audiowizualny

W końcu informacja na temat zakwalifikowania danego utworu audiowizualnego do określonego gatunku wynika także z taksowania[8] i repartycji tzw. tantiem producenckich (należnych producentom utworów audiowizualnych) przez OZZ (organizacje zbiorowego zarządzania prawami autorskimi – w odniesieniu do utworów audiowizualnych – SFP – ZAPA/Stowarzyszenie Filmowców Polskich – Związek Autorów i Producentów Audiowizualnych) po uprzednim zainkasowaniu opłat od podmiotów korzystających z tych utworów na polu eksploatacji nadawanie – odtwarzanie – w zależności od zakwalifikowania przez SFP – ZAPA utworu do danego gatunku (w tym serialu paradokumentalnego).

I tak, jeśli idzie o serial paradokumentalny to, jak każda audycja telewizyjna, jest on utworem audiowizualnym. Regulacje rozdziału 6 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych[9] (art. 69–73), statuują utwór audiowizualny jako dzieło współautorskie, czyli takie, w przypadku których działania twórców są ukierunkowane na stworzenie wspólnego dzieła jako jednolitego bytu artystycznego (w odróżnieniu od dzieła zbiorowego w rozumieniu art. 11, charakteryzującego się odrębnością poszczególnych elementów składowych). Wprowadzenie do ustawy o prawie autorskim kategorii utworów audiowizualnych wynikało z potrzeby stworzenia pojęcia pojemnego, które pozwalałoby na objęcie nowych rodzajów twórczości audiowizualnej. W związku z art. 2 ust. 1 konwencji berneńskiej pierwotny zakres tego pojęcia tworzą utwory filmowe oraz zrównane z nimi utwory wyrażone w podobny sposób. Poza tym zakresem pozostają natomiast rozbieżności co do kwalifikacji poszczególnych rodzajów utworów audiowizualnych. Nie jest bowiem możliwe stworzenie klasycznej definicji tego pojęcia. Nie ma zatem możliwości jednoznacznej klasyfikacji dzieł audiowizualnych[10]. Ustawodawca w art. 1 ust. 1 pkt 9 PrAutU wskazuje wśród utworów audiowizualnych także utwory filmowe. Istotnym zagadnieniem prawnym jest ustalenie kręgu jego współtwórców. Z utworem współautorskim mamy do czynienia wówczas, gdy działania twórców są ukierunkowane na stworzenie wspólnego dzieła. Istotne znaczenie ma zatem element woli kreowania utworu audiowizualnego jako jednolitego działa artystycznego. Przykładowo jeżeli utwór literacki został zaadaptowany do utworu audiowizualnego, to adaptacja będzie jedynie utworem zależnym w stosunku do pierwowzoru literackiego. Podobnie rzecz się ma w przypadku zapożyczeń do utworów audiowizualnych utworów już wcześniej istniejących, głównie muzycznych, plastycznych, fotograficznych[11].

---

[4] *J. Turek*, Dopuszczenie dowodu z opinii biegłego, [w:] *J. Turek* (red.), Rola biegłego we współczesnym procesie, Warszawa 2002, s. 12.

[5] *A. Jarocha*, Wiadomości specjalne jako przedmiot dowodu z opinii biegłych, [w:] *B. Guzik*, *P. Wiliński* (red.), Prawo wobec wyzwań współczesności, t. 6, Poznań 2010, s. 275 i n.

[6] Kwalifikatory zidentyfikowane przez autora.

[7] Internetowa Baza Filmu Polskiego – FILMPOLSKI.PL.

[8] Ustalania wysokości tantiem.

[9] T.j. Dz.U. z 2018 r. poz. 1191 ze zm.; dalej jako: PrAutU.

[10] *M. Bukowski*, [w:] *D. Flisak* (red.), Prawo autorskie i prawa pokrewne. Komentarz, Warszawa 2015, s. 915.

[11] *Ibidem*, s. 918; szerzej zob. w wyroku TK z 24.5.2006 r., K 5/05, OTK-A 2006, Nr 5, poz. 59. TK stwierdził, że: „w istocie o tym, czy wkład konkretnej osoby w proces produkcji dzieła audiowizualnego jest rezultatem twórczości, a tym samym czy tę osobę należy zaliczyć do grona współtwórców tego działa, decyduje w ostatniej instancji okoliczności konkretnego przypadku. W odniesieniu do reżysera, scenarzysty, autora adaptacji utworu literackiego, kompozytora muzyki filmowej i operatora obrazu pozytywna odpowiedź na to pytanie w zasadzie nie powinna budzić wątpliwości, skoro o ich statusie współtwórców przesądził ustawodawca. Poza tym występują cal rzesze osób uczestniczących w produkcji audiowizualnej, których praca nie wykazuje cech twórczości autorskiej. Pomiędzy nimi a grupą uznanych przez ustawę za współtwórców działa audiowizualnego znajdują się niejednokrotna kategoria osób, których status jako ewentualnych współtwórców takich dzieł nie jest przesadzony i budzi spory doktrynalne". Por. wyrok SN z 5.4.2002r., III RN 133/01, OSNAPiUS 2002, Nr 12, poz. 281 w zakresie nieuznania kierownika produkcji za współautora dzieła audiowizualnego.

Na marginesie zasadniczych rozważań należy wskazać, że nowelizacja ustawy z 9.9.2000 r. doprowadziła do istotnej zmiany w zakresie wynagrodzenia za utwór audiowizualny. Zrezygnowano bowiem przez uchylenie ust. 1 i 2 art. 70 ustawy z nabycia utworów przez producenta dzieła audiowizualnego oraz domniemania nabycia praw do utworów stworzonych na zamówienie producenta (ust. 2). Obecnie art. 70 ust. 1 PrAutU stwarza domniemanie prawne, zgodnie z którym producent utworu audiowizualnego nabywa na mocy umowy o stworzenie dzieła albo umowy o wykorzystywanie już istniejącego utworu wyłączne prawa majątkowe do eksploatacji tych utworów w ramach utworu audiowizualnego jako całości. Powyższa redakcja powoduje wątpliwość, komu należy się prawo autorskie do dzieła audiowizualnego. Stąd trzeba przyjąć, że prawa autorskie przysługują współtwórcom utworu audiowizualnego, jak również wiodącą rolę odgrywa tu nadal producent tego utworu[12].

Słownik języka polskiego PWN definiuje paradokument jako „film fabularny zrealizowany w konwencji filmu dokumentalnego, oparty na faktach". Według tego słownika przedrostek „para" jest to pierwszy człon wyrazów złożonych, oznaczający: niby, prawie, wyrażający podobieństwo do tego, co jest określane drugą częścią złożenia. Zgodnie z tą definicją, serial oparty na faktach, zrealizowany w konwencji filmu dokumentalnego, ma znamiona paradokumentu. Stwarza on bowiem pozór prawdziwości oglądanych treści, czyli ostatecznie można uznać, że serial paradokumentalny jest „utworem fabularnym stanowiącym podzieloną na odcinki, a więc rozłożoną w czasie, całość dramaturgiczną, w której przedstawiona jest wielowątkowa historia zamkniętej grupy pierwszo- i drugoplanowych bohaterów". Stylem i formą naśladuje dokument, ale nie prezentuje autentycznych wydarzeń i prawdziwych osób, lecz opiera się na faktach. Definicja ta jest przydatna, ponieważ wskazuje ogólny kontekst znaczeniowy samego pojęcia „paradokument".

Obecnie można zatem prześledzić cechy charakteryzujące serial paradokumentalny. Okazuje się, że praktyka wykształciła już wiele cech pozwalających wyróżnić serial paradokumentalny (paradokument) i w ten sposób odróżnić go od innych dzieł audiowizualnych w oparciu na specyfikę technicznych aspektów produkcji oraz dobór obsady. W szczególności gatunek ten wyróżnia się następującymi charakterystycznymi cechami: „setki" – wywiady/wypowiedzi bohaterów do kamery, lub do niewidocznej osoby zza kamery (np. do domniemanego redaktora/dziennikarza); następnie „setkom" towarzyszy co chwilę pojawiająca się u dołu ekranu „belka", charakterystyczny dla programów informacyjnych, publicystycznych i filmów dokumentalnych pasek informacyjny podkreślający najważniejsze treści: imię i nazwisko bohatera, zawód, jego wiek; ponadto „setki", które zawierają „belkę" informacyjną, są komentarzem do prezentowanych wydarzeń, widzowi uzupełnia dzięki nim wiedzę o bohaterach. Ten element konstrukcji paradokumentu ma na celu uwiarygodnienie autentyczności pokazywanych osób i sytuacji, wzmocnienie złudzenia ich dziania się »tu i teraz«. Następną cechą paradokumentu jest charakterystyczny „narrator", czyli podmiot, który komentuje zza kadru wydarzenia, co ma potęgować wrażenie autentyczności prezentowanych na ekranie sytuacji. Narrator ma na celu informowanie widza o tym, co widzi na ekranie, a nawet streszczanie całości dotychczasowej fabuły. Ponadto należy zauważyć, że sposób filmowania paradokumentu jest inny, czyli kamera jest bardziej dynamiczna, podobnie jak w filmie dokumentalnym. Kolorystyka obrazu nie ma znaczenia. Filmuje się z reguły na dwie kamery. Należy też podkreślić, że w konwencji paradokumentu zakłada się uczestnictwo niezawodowych aktorów, chociaż nie ma przeciwwskazań obsadzania w paradokumentach i zawodowych aktorów, byleby aktor taki był nieznany i nierozpoznawalny. Do niektórych większych ról są obsadzeni jednak absolwenci wydziału lalkarskiego PWST, czyli lalkarze nieposiadający dyplomu aktora teatru, telewizji i kina, czy też aktorzy – amatorzy. Udział niezawodowych aktorów wpisuje się więc w konwencję paradokumentu.

Paradokument zatem, co wynika z powyższych uwag, łączy w sobie techniki filmów dokumentalnych i fabularnych, jest określoną formułą gatunkową, realizacyjną i produkcyjną. Nie sposób przy tym mówić aktualnie o paradokumencie w czystej i pierwotnej jego postaci. Serial paradokumentalny jako gatunek ewoluuje, przybiera różne odsłony, co wiąże się również ze swoistą dla tego typu gatunku nomenklaturą. Serialem paradokumentalnym jest również *scripted – reality* (ang.), który wyewoluował z pierwotnej postaci paradokumentu (serialu paradokumentalnego). W *scripted – reality* występują bowiem ci sami aktorzy, podczas gdy w postaci podstawowej występują aktorzy zmieniający się. To nie wpływa jednak w żaden sposób na kwalifikację audycji jako paradokumentu/serialu paradokumentalnego/ *scripted – reality.*

[12] *M. Czajkowska-Dąbrowska*, [w:] *J. Barta*, *R. Markiewicz* (red.), Prawo autorskie i prawa pokrewne, Warszawa 2011, s. 428. Zob. także, *J. Szczotak*, Utwory audiowizualne stan oczekiwania na nowelizację prawa autorskiego, PS 2009, Nr 1, s. 31; *A. Nowicka*, System prawa prywatnego, s. 113; *E. Traple*, Prawo współpracy dzieła audiowizualnego do udziału w dochodach z eksploatacji tego dzieła w polskim prawie autorskim, ZNUJ, z. 69, s. 47 i n.; *P. Ślęzak*, Wynagrodzenie twórców filmowych i artystów wykonawców z tytułu rozpowszechniania utworu, PiP 2008, z. 10, s. 88.

Rola organizacji zbiorowego zarządzania prawami autorskimi w kwalifikacji utworów audiowizualnych

Obecnie w polskiej praktyce rynku audiowizualnych produkcji filmowych kwalifikacja serialu jako serialu paradokumentalnego została dokonana przez Państwową Wyższą Szkołę Filmową, Telewizyjną i Teatralną im. Leona Schillera w Łodzi (właściciela największej Internetowej Bazy Filmu Polskiego – Filmpolski.pl) oraz przez Związek Autorów i Producentów Audiowizualnych (SFP-ZAPA). Wskazanym powyżej podmiotom można przydać walor ekspertów, których opinia, recenzja, kwalifikacja powinna być i jest traktowana jako wiążąca m.in. w środowisku producenckim. Należy zauważyć, że podstawowym elementem działalności SFP-ZAPA[13] jest właściwa identyfikacja dzieł audiowizualnych, pozwalająca na szybkie wypłaty należnych autorom i producentom tantiem, a także wspieranie walki z piractwem w obrocie utworami filmowymi. ZAPA oprócz twórców utworów audiowizualnych chroni również ich producentów[14]. Producenci, zgłaszając się do ZAPA, powierzają jej autorskie prawa majątkowe do wyprodukowanych utworów oraz prawa pokrewne do wideogramów. Członkami tej organizacji są także ci, którzy prawa autorskie do utworu audiowizualnego nabyli w drodze umowy z producentem, np. dystrybutorzy. ZAPA pobiera dla twórców i producentów filmowych i telewizyjnych tantiemy autorskie i producenckie z następujących pól: dystrybucji kinowej, dystrybucji wideokaset i DVD (Blue Ray), nadań telewizyjnych, najmu i publicznego odtwarzania, czystych nośników oraz reemisji kablowej i satelitarnej w Polsce i za granicą.

ZAPA negocjuje i inkasuje wynagrodzenie należne producentom i innym dysponentom praw autorskich (np. dystrybutorom), a następnie pieniądze otrzymane od podmiotów korzystających z tychże praw dzieli pomiędzy swoich uprawnionych. W znacznej części są to tantiemy z tytułu reemisji kablowej i satelitarnej. Producenci wideogramów otrzymują dodatkowo wynagrodzenie z tytułu czystych nośników. Należności tych uprawnień nie mogą dochodzić indywidualnie od użytkowników, a jedynie za pośrednictwem właściwej organizacji.

Utworami audiowizualnymi chronionymi przez ZAPA są: filmy i seriale fabularne, filmy i seriale dokumentalne, filmy i seriale animowane, filmy i seriale lalkowe, telenowele i *sitcomy*, telenowele paradokumentalne, teatry telewizji, dokumenty fabularyzowane, fabularyzowane rekonstrukcje sądowe, *scripted reality* i animacje 3D.

Podział tantiem pomiędzy współtwórców utworu audiowizualnego dokonywany jest według zasad ustalonych w uchwale Rady Administracyjnej SFP – ZAPA Nr 7 z 4.2.2008 r. Organizacja ta określa zatem gatunek utworu audiowizualnego i – na podstawie własnych regulaminów repartycji tantiem – przyznaje wynagrodzenia podawane w prawomocnie zatwierdzanych tabelach wynagrodzeń, m.in. w oparciu na przedstawiane jej przez dystrybutora/emitenta lub producenta tzw. metryki praw autorskich i praw pokrewnych dotyczące danego odcinka audycji, a określające: tytuł i czas emisyjny audycji, autorów scenariusza, reżysera, tytuły wykorzystanych w audycji drobnych utworów słownych, muzycznych i słowno-muzycznych, czas ich emisji oraz imiona i nazwiska ich autorów, imiona i nazwiska artystów wykonawców i tytuły wykonywanych przez nich utworów i ról/piosenek, czas emisji artystycznych wykonań i organizacje zbiorowego zarządzania reprezentujące poszczególnych autorów wykorzystanych utworów, artystów wykonawców oraz producentów wykorzystanych fonogramów. Z kolei producent w umowie z emitentem (np. stacją TV) zobowiązuje się – co do zasady – dostarczyć emitentowi wykaz informacji o audycji (zwany dalej „wyciągiem z ewidencji audycji"), wymienionych w § 4 rozporządzenia Krajowej Rady Radiofonii i Telewizji z 12.7.2011 r. w sprawie sposobu prowadzenia przez nadawcę ewidencji czasu nadawania audycji wytworzonych pierwotnie w języku polskim, audycji europejskich i audycji europejskich wytworzonych przez producentów niezależnych oraz czasu jej przechowywania[15], określającym nazwę programu, w którym rozpowszechniono audycję, nazwę nadawcy, okres sprawozdawczy, tytuł audycji, dzień, miesiąc, rok, godzinę rozpoczęcia rozpowszechnienia audycji w programie, rzeczywisty czas trwania audycji, rok produkcji audycji, nazwę producenta audycji.

Kwalifikacja utworów audiowizualnych a tantiemy

Każdy utwór audiowizualny zakwalifikowany zostaje jako gatunek i za taki ma określone w procentach tantiemy (w tym producenckie). To daje jednocześnie wyraz temu, z jakim ga-

[13] SFP-ZAPA – Stowarzyszenie Filmowców Polskich – Związek Autorów i Producentów Audiowizualnych jest właściwą organizacją zbiorowego zarządzania prawami autorskimi (OZZ). Działa na podstawie zezwolenia Ministra Kultury i Dziedzictwa Narodowego (tak obecnie).

[14] Organizacja zbiorowego zarządzania, zgodnie z art. 70 ust. 3 PrAutU stanowi, że obowiązek zapłaty wynagrodzenia z ust. 2^1 tego przepisu obciąża korzystającego z utworu audiowizualnego. W pierwotnym brzmieniu ustawy podmiotem zobowiązanym był producent utworu audiowizualnego. Zmiana podmiotu zobowiązanego doprowadziła do rozszczepienia warunków eksploatacyjnych utworu audiowizualnego. Zmiana ta mogła być korzystna, gdyby towarzyszyła jej sprawna redystrybucja, ale poprzez zatwierdzenie tabel wynagrodzenia. Obecnie OZZ, w tym przypadku ZAPA, posługuje się niezatwierdzonymi tabelami wynagrodzeń, co jest niekorzystne dla rynku i powoduje zagrożenie dla wykorzystywania przez OZZ pozycji dominującej w relacji z podmiotami korzystającymi, zob. więcej: *M. Bukowski*, [w:] *D. Flisak* (red.), Prawo autorskie…, s. 930.

[15] Dz.U. Nr 160, poz. 962.

tunkiem utworu audiowizualnego – np. audycji – telewizyjnej mamy do czynienia. Paradokument – czyli *scripted reality*, otrzymuje zawsze określony procent tantiem (inny niż np. serial fabularny, a to właśnie na tle, czy konkurujący serial ma charakter fabularnego, czy paradokumentalnego, powstał spór). Tantiemy producenckie w przypadku obu paradokumentów są identyczne, w przypadku zaś paradokumentu i fabuły – różne. Wyżej przedstawione wyliczenie stanowi zarazem o gradacji procentowej tantiem producenckich (im wyżej w hierarchii ZAPA – tym tantiemy wyższe).

Po dokonaniu analizy powyższego zagadnienia należy stwierdzić, że dowód z opinii biegłego, tym bardziej z zakresu sztuki filmowej i telewizyjnej, którego trudno szukać na listach biegłych sądów okręgowych, a zatem powoływanego co najwyżej *ad hoc* – może okazać się niepotrzebny w procesie mającym na celu ustalenie zasadności powództwa o zapłatę kar umownych z tytułu naruszenia zakazu konkurencji poprzez wykonanie na rzecz innego podmiotu produkcji konkurencyjnej.

Można stwierdzić, że ustalenie, do jakiego gatunku audycji telewizyjnej należy zakwalifikować oba utwory audiowizualne, w szczególności, czy oba seriale należą do gatunku paradokumentu, czy też tylko jeden z nich, a drugi to np. gatunek serialu fabularnego – nie wymaga wiedzy specjalnej biegłych, ponieważ powyższe ustalenia można poczynić w oparciu na inne środki dowodowe wskazujące w sposób wyraźny na podobieństwa bądź różnice obu audycji telewizyjnych (odtworzenie charakterystycznych obrazów z nagrań utrwalonych na nośnikach DVD/blue ray/video, pomocniczo zeznania świadków – osób biorących udział w produkcji), a przez to rozpoznanie cech charakterystycznych danego gatunku w rozumieniu technik realizacyjnych, produkcyjnych czy doboru obsady. Dokumentem prywatnym może być np. decyzja o zakwalifikowanie danego utworu audiowizualnego do danego gatunku w tabelach SAP ZAPA, ponieważ na ich podstawie dokonuje się wypłata wynagrodzeń, o których mowa w art. 70 PrAutU.

Informacja pochodząca od Państwowej Wyższej Szkoły Filmowej, Telewizyjnej i Teatralnej im. Leona Schillera w Łodzi

W końcu ustalenia powinny mieć na względzie miarodajne informacje podawane na stronach internetowych przez Państwową Wyższą Szkołę Filmową, Telewizyjną i Teatralną im. Leona Schillera w Łodzi (właściciela największej Internetowej Bazy Filmu Polskiego – Filmpolski.pl) oraz przez Związek Autorów i Producentów Audiowizualnych (SFP – ZAPA). Informacje te powinny być poczytywane za miarodajne, ponieważ wskazanym powyżej podmiotom należy w pełni przypisać walor instytucji eksperckich. Jednak informacja zamieszczona na powyższej bazie internetowej Filmu Polskiego stanowi także dokument prywatny będący dowodem w sprawie. Nie zawiera on jednak oświadczenia woli, a oświadczenie wiedzy i w ten sposób zbliża się do wypowiedzi biegłego. Nie ma także przeszkód, aby sąd zlecił przeprowadzenie dowodu właśnie wykładowcom Państwowej Wyższej Szkoły Filmowej, Telewizyjnej i Teatralnej im. Leona Schillera w Łodzi, i wówczas ich wypowiedź będzie miała walor opinii biegłego sądowego. Jednakże opinia ta zostanie sporządzona właśnie przy wykorzystaniu, w zasadniczej dla opracowania opinii części, wyżej wymienionej bazy wiedzy.

Pismo pochodzące od PWSFTiT jest niewątpliwie dokumentem w rozumieniu przepisów Kodeksu postępowania cywilnego. Przepisy Kodeksu postępowania cywilnego nie zawierają definicji „dokumentu". W szerokim znaczeniu dokument należy rozumieć jako każdy przedmiot, w którym zawarta jest jakaś myśl, przejaw ludzkiej działalności, w szczególności plany, szkice, rysunki, fotografie[16]. Dokumentami w węższym znaczeniu są dokumenty urzędowe i prywatne w rozumieniu Kodeksu postępowania cywilnego[17]. W rezultacie nowelizacji Kodeksu cywilnego dokonanej mocą ustawy z 10.7.2015 r. wprowadzono w art. 77^3 definicję dokumentu, przyjmując, że dokumentem jest nośnik informacji umożliwiający zapoznanie się z jej treścią. Natomiast stosownie do art. 77^2 KC, do zachowania dokumentowej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie. Stąd też legalna definicja dokumentu zerwała z tradycyjnym rozumieniem tego pojęcia jako informacji utrwalonej wyłącznie w postaci pisma, dając w ten sposób wyraz szerokiemu ujęciu dokumentu[18]. W kontekście definicji pojęcia dokumentu można wyróżnić dokumenty zawierające tekst (sporządzone za pomocą znaków alfabetu i reguł językowych) oraz inne dokumenty. Do tych pierwszych znajdą zastosowanie przepisy art. 244 KPC i n., natomiast do innych dokumentów odnosi się art. 308 KPC. Ustawodawca przyjął, że konstytutywną cechą dokumentu jest jego intelektualna zawartość, czyli informacja – treść, obejmująca różnego rodzaju oświadczenia, w tym oświadczenia woli. Treść ta musi zostać odpowiednio utrwalona w sposób umożliwiający jej odtworzenie. Dla istnienia dokumentu nie ma znaczenia, czy jest on podpisany. Podpis nie jest zatem koniecznym elementem dokumentu[19].

[16] *W. Miszewski*, Proces cywilny w zarysie. Część pierwsza, Warszawa–Łódź 1946, s. 173.

[17] *K. Piasecki*, Postępowanie sporne rozpoznawcze, Warszawa 2011, wyd. 3, s. 261.

[18] Zob. *D. Szostek*, Nowe ujęcie dokumentu w prawie prywatnym, Warszawa 2012, s. 250; *tenże*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Komentarz, Warszawa 2016, s. 150.

[19] *A. Góra-Błaszczykowska*, [w:] *A. Góra-Błaszczykowska* (red.), Kodeks postępowania cywilnego. Komentarz, t. I, Legalis/el. 2016, nb 1.

Następnie należy stwierdzić, że nadal zachowano w Kodeksie postępowania cywilnego podział na dokumenty urzędowe i prywatne z uwagi na kryterium podmiotowe, czyli jaki podmiot sporządza dokument, i tak, z art. 244 KPC wynika, że dokumenty urzędowe, sporządzone w przepisanej formie przez powołane do tego organy władzy publicznej i inne organy państwowe w zakresie ich działania, stanowią dowód tego, co zostało w nich urzędowo zaświadczone (art. 244 § 1). Natomiast powyższy przepis ma zastosowanie odpowiednie do dokumentów urzędowych sporządzonych przez podmioty, inne niż wymienione w § 1, w zakresie zleconych im przez ustawę zadań z dziedziny administracji publicznej.

W tym stanie rzeczy powyższa regulacja normuje formalną moc dowodową dokumentów urzędowych. Polega ona na domniemaniu zgodności z prawdą oświadczenia uprawnionego organu, zawartego w pochodzącym od niego dokumencie. Przepis określa warunki, jakie musi spełniać pismo, aby uznać je za dokument urzędowy. Otóż pismo musi być sporządzone we właściwej formie przez organy władzy publicznej i inne organy państwowe (pochodzenie dokumentu) oraz musi być sporządzone przez wymienione organy w zakresie ich działania (treść dokumentu należąca do właściwości danego organu). W piśmiennictwie przeprowadzono następujący podział dokumentów, które korzystają z przypisanej dokumentom urzędowym mocy dowodowej:

1) dokumenty urzędowe sporządzone w przepisanej formie przez powołane do tego organy władzy publicznej i inne organy państwowe w zakresie ich działania;
2) dokumenty urzędowe sporządzone przez organizacje zawodowe, samorządowe, spółdzielcze i inne organizacje pozarządowe w zakresie zleconych im przez ustawę spraw z dziedziny administracji publicznej;
3) dokumenty, które ustawa zrównuje z dokumentami urzędowymi pod względem przypisanej im mocy dowodowej[20].

Z uwagi na kryterium treści dokumentu urzędowego można wyróżnić tzw. dokumenty dyspozytywne (konstytutywne) i deklaratywne. Pierwsze obejmują bezpośrednio określoną czynność prawną i stanowią jej dowód; wymienione jako drugie odnoszą się w swojej treści do leżących poza nią m.in. okoliczności, stanów, wycinków rzeczywistości[21]. W zakres pojęcia organów władzy publicznej należy zaliczyć zarówno organy państwowe, jak i organy samorządu terytorialnego (gminy, powiatu, województwa). W tym kontekście nie można uznać szkoły wyższej, nawet państwowej, jako organu władzy publicznej. Szkoła wyższa nie realizuje bowiem funkcji władczej państwa, a jedynie realizuje zadania edukacyjne państwa.

Pismo, aby uzyskać przymiot dokumentu urzędowego, musi być sporządzone „w zakresie działania" organu – wystawcy. Na zakres działania organu składa się jego właściwość rzeczowa i miejscowa (terytorialna). W przypadku naruszenia przez organ właściwości miejscowej przy sporządzaniu dokumentu utrzyma on charakter dokumentu urzędowego. Natomiast wydanie dokumentu z przekroczeniem zakresu kompetencji rzeczowej powoduje, że traci on przymiot dokumentu urzędowego. W drugim z wymienionych przypadku dokument należy traktować jako dokument prywatny. Należy podkreślić, że organy władzy publicznej występują także w obrocie prywatnoprawnym, tj. poza sferą imperium, jednakże dokumenty wydane w tym zakresie nie są dokumentami urzędowymi w świetle art. 244 KPC.

Podsumowanie

W związku z powyższymi rozważaniami nie można uznać dokumentu sporządzonego przez PWSFTiT za dokument urzędowy, ponieważ szkoła wyższa nie jest organem administracji publicznej ani też na podstawie odrębnych przepisów nie realizuje funkcji z zakresu administracji publicznej[22]. Stąd też dokument wystawiony przez szkołę wyższą stanowi jedynie dokument prywatny, ale o charakterze deklaratywnym, czyli potwierdzającym pewien stan faktyczny (oświadczenie wiedzy).

Kolejnym istotnym kwalifikatorem jest wysokość/pułap przyznawanych za dany gatunek tantiem producenckich – fundamentalnym elementem aktywności SFP ZAPA jest właściwa identyfikacja dzieł audiowizualnych, pozwalająca na szybkie wypłaty należnych autorom i producentom tantiem, a także wspieranie walki z piractwem w obrocie utworami filmowymi.

A zatem należy uznać, że w sytuacji gdy baza wiedzy: FILMPOLSKI.PL, jak też ZAPA.ORG.PL, przypisują danej audycji określony charakter i klasyfikują ją jako określony gatunek – nie ma potrzeby odwoływania się do opinii biegłego czy tym bardziej dowodu z opinii instytutu naukowego lub naukowo-badawczego (art. 290 KPC), ponieważ biegły/zespół biegłych *ad hoc* najpewniej musiałby rekrutować się spośród specjalistów Szkoły lub członków Organizacji, a zatem powieliłby w istocie kwalifikację podmiotu, z którego się wywodzi.

Najważniejsze natomiast jest to – i o tym nigdy nie należy zapominać, iż dowód z opinii biegłego podlega ocenie sądu w całokształcie materiału zgromadzonego w sprawie na tych samych zasadach co inne dowody. Natomiast to sąd jest ostatecznie najwyższym biegłym w sprawie.

[20] Tak *M. Manowska*, Postępowanie nakazowe i upominawcze, Warszawa 2001, s. 86.

[21] Zob. *K. Piasecki*, Postępowanie sporne…, s. 262.

[22] *A. Bednarczyk-Płachta*, Status szkoły wyższej jako podmiotu administracji publicznej, Warszawa 2016, s. 17. Autorka uznała, że szkoły wyższe w Polsce, bez względu na ich status prawny, należy określać jako podmioty zewnętrzne względem organów administracji publicznej, niepowiązane z nią hierarchicznie i organizacyjnie, co powoduje niemożność utożsamiania ich organów z organami administracyjnymi.

Słowa kluczowe: opinia biegłego, dowód, konkurencyjny charakter, audycja telewizyjna, utwór audiowizualny, serial paradokumentalny, kwalifikatory, tantiemy producenckie.

Proof from an expert opinion and determination of the competitive nature of production – television programs

The aim of the present study is to answer the question whether it is possible to determine the competitive nature of a given television program as an audiovisual piece of work, and at the same time to categorize it to a given genre based on the proof from an expert opinion in a court case (or based on other means of proof). This issue may be useful in order to settle a case of penal sum regarding violation of a non-compete clause by a creator in regard to a producer, which depends on creating a piece of work, e.g. direction, for another person who competes on the market of audiovisual services within the scope of genre of an audiovisual piece of work/television program.

Keywords: expert opinion, proof, competitive nature, TV program, audiovisual piece of work, pseudo-documentary, qualifiers, producer royalties.

Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom

r.pr. *Marta Kruk*[1]

Celem niniejszego opracowania jest usystematyzowanie oraz analiza obowiązków dostawców usług cyfrowych wynikających z przepisów o krajowym systemie cyberbezpieczeństwa. W opracowaniu skupiono się także na wskazaniu, jakie podmioty są uznawane za dostawców usług cyfrowych w rozumieniu tej ustawy. Analizy obowiązków dokonano, odwołując się do odpowiednich przepisów prawa unijnego. Zwrócono także uwagę na odmienności w zakresie koniecznych do zrealizowania obowiązków związanych z wystąpieniem zdarzeń mogących mieć negatywny wpływ na cyberbezpieczeństwo wynikające z kwalifikacji takich incydentów jako istotne czy krytyczne oraz na kary, jakie mogą wiązać się z niedopełnieniem przez dostawców usług cyfrowych obowiązków wynikających z ustawy.

Uwagi wstępne

Ponad 55% ludności na całym świecie korzysta obecnie z Internetu, przy czym w samej Europie wskaźnik ten wynosi 85%. Statystyki prowadzone od 2000 r. pokazują stały wzrost w tej dziedzinie[2]. Przyczyną tego zjawiska jest ciągły rozwój świata nowych technologii w świecie cyfrowym, gdzie kolejne nowości innowacyjne i technologiczne stają się codziennością życia. Tendencja ta powoduje, że za główny kierunek rozwoju i wzrostu gospodarczego UE uznano stworzenie jednolitego rynku cyfrowego. Zakłada on wykorzystanie w cyberprzestrzeni nowych technologii takich jak Internet rzeczy (IoT), łączność 5G, przetwarzanie danych i informacji w chmurze czy też dzięki technologiom *big data*[3].

Dynamiczny rozwój nowych technologii cyfrowych stał się podstawą wyodrębnienia cyberbezpieczeństwa jako nowej i samodzielnej dyscypliny naukowej, której nie można analizować wyłącznie w kategoriach technologicznych[4]. Immanentną częścią ekosystemu cyberbezpieczeństwa są bowiem kategorie organizacyjne, ekonomiczne, prawne, społeczne czy współpracy międzynarodowej o zasięgu globalnym[5]. Wykorzystywanie nowych technologii niewątpliwie niesie za sobą korzyści, ale też powoduje liczne i ulegające ciągłej przemianie zagrożenia dla poszczególnych osób fizycznych i prawnych, ogółu ludności, instytucji czy państw. Z jednej strony, skala incydentów w cyberprzestrzeni i ich skutki powodują olbrzymie straty zarówno w gospodarkach państw europejskich, jak i w prowadzonej działalności gospodarczej w sektorze prywatnym, czy też poważne zagrożenie dla zdrowia i mienia obywateli UE[6]. Ryzyko związane z cyberprzestępczością systematycznie wzrasta, powodując podważenie zaufania osób fizycznych do nowych technologii w świecie cyfrowym[7].

Z drugiej strony, nie ma już możliwości odwrotu z obranej drogi rozwoju i odcięcia się czy rezygnacji z wykorzystywania nowych technologii czy to przez rządy państw, w rozwoju gospodarki, w sektorze użyteczności publicznej, sektorze prywatnym czy wreszcie w bieżącym życiu przez osoby fizyczne. Stąd konieczne jest zagwarantowanie bezpieczeństwa obywatelom UE w coraz bardziej obecnej w codziennym życiu cyberprzestrzeni. Ponieważ skala i rodzaje cyberprzestępstw nieustannie ewoluują, pamiętać należy, że nie jest możliwe zapewnienie w 100% odpornych na zagrożenia systemów teleinformatycznych czy też 100% idealnych rozwiązań organizacyjno-prawnych. Odpowiedzialność za zapewnienie cyberbezpieczeństwa obywatelom nie może spoczywać wyłącznie na rządach państw UE, ponieważ cyfrowego świata nie kontroluje wyłącznie sektor publiczny[8]. Aby osiągnąć zakła-

[1] Autorka jest partnerem Kancelarii Prawnej VenaGroup we Wrocławiu oraz rzecznikiem prasowym Okręgowej Izby Radców Prawnych we Wrocławiu.

[2] Zob. https://www.internetworldstats.com/stats.htm (dostęp z 23.1.2019 r.).

[3] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia jednolitego rynku cyfrowego dla Europy", COM(2015) 192 final.

[4] *C. Banasiński*, Cyberbezpieczeństwo w Unii Europejskiej – kierunki regulacji, [w:] *J. Jagielski*, *D. Kijowski* (red.), Prawo administracyjne wobec współczesnych wyzwań. Księga jubileuszowa dedykowana profesorowi Markowi Wierzbowskiemu, Legalis/el. 2018.

[5] *M. Olszewska*, Cyberbezpieczeństwo jako przedmiot analizy przestrzennej, [w:] *G. Szpor*, *K. Czaplicki* (red.), Internet. Informacja przestrzenna. Spatial information, Legalis/el. 2018.

[6] *M.-T. Holzleitner*, *J. Reichl*, European provisions for cyber security in the smart grid – an overview of the NIS-directive, [w:] Elektrotechnik & Informationstechnik, Springer Verlag Wien 2017.

[7] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, [w:] *J. Gołaczyński* (red.), Wybrane dobre praktyki w zakresie usług elektronicznych, Legalis/el. 2016.

[8] *M. Olszewska*, Cyberbezpieczeństwo jako przedmiot analizy przestrzennej, Legalis/el. 2018.

dany cel, niezbędne jest zaangażowanie sektora prywatnego oraz osób fizycznych[9]. Większość elementów sieci i systemów teleinformatycznych związanych chociażby z tworzeniem, zarządzaniem i rozwojem Internetu czy też część istotnej infrastruktury krytycznej należy do sektora prywatnego. Zasadnicza jest więc zwiększona odpowiedzialność sektora prywatnego i jego zaangażowanie w zapewnienie bezpieczeństwa w cyberprzestrzeni[10]. Pamiętać należy, że równie istotny jest aspekt informacyjny i edukacja konsumentów związana z ich aktywnością w świecie cyfrowym oraz dotyczącym tej aktywności zagrożeniem cyberprzestępstwami[11].

Z powyższych rozważań wynika, że skoro nie jest możliwa całkowita eliminacja zagrożeń związanych z cyberprzestępczością, jedynym słusznym rozwiązaniem jest podjęcie działań minimalizujących niebezpieczeństwo wystąpienia incydentów w świecie cyfrowym oraz maksymalnie ograniczających ryzyko strat z nimi związanych[12]. Konieczne jest zapewnienie gwarancji bezpieczeństwa i poufności informacji na poziomie technicznym w cyberprzestrzeni. Kolejno, równie istotne jest zagwarantowanie nienaruszalności systemów teleinformatycznych poprzez zapewnienie i monitorowanie ich odporności na incydenty oraz zapewnienie stałej ich dostępności, a także przechowywanych i przetwarzanych w nich zasobów[13]. Działania te muszą obejmować nie tylko krytyczną infrastrukturę teleinformatyczną w sektorze publicznym, ale również sektor prywatny. Konieczna jest współpraca, wymiana informacji i doświadczeń pomiędzy poszczególnymi sektorami w zakresie monitorowania incydentów, sposobów reagowania na nie, określania ich przyczyn, prowadzenia analiz związanych z ich wystąpieniem, wyciągania wniosków i podejmowania działań na przyszłość w celu wyeliminowania ich ponownego wystąpienia[14].

W UE na gruncie prawa skutek ten ma zostać osiągnięty przez wprowadzone w 2016 r. prawodawstwo – stosowane od 25.5.2018 r. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[15] oraz dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[16], która miała zostać wdrożona przez państwa członkowskie UE do 9.5.2018 r. Przyjęcie wskazanych dwóch aktów prawnych stanowi wprost realizację strategii jednolitego rynku cyfrowego, której celem jest m.in. zwiększenie zaufania obywateli wspólnoty europejskiej względem usług cyfrowych i poprawa ich bezpieczeństwa[17]. Wspomnieć należy, że oprócz wskazanych aktów prawnych ramy i podstawy prawne zwalczania cyberprzestępczości tworzy dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 12.8.2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW[18]. Dyrektywa NIS nakłada na państwa członkowskie UE obowiązek poszerzenia ich współpracy w kwestii zapewnienia cyberbezpieczeństwa oraz zwalczania cyberprzestępczości. Dyrektywa ta ustanawia nowe obowiązki dla państw członkowskich w zakresie opracowania, wdrożenia i stosowania strategii bezpieczeństwa sieci i systemów informatycznych, rozwijając współpracę w tym zakresie w ramach wspólnoty, oraz tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT)[19]. Wreszcie dyrektywa NIS wprowadza nowe standardy dotyczące odporności systemów informatycznych na ataki hakerskie w kluczowych sektorach gospodarki, w zakresie świadczenia usług kluczowych oraz usług cyfrowych, takich jak wyszukiwarki, przechowywanie danych w chmurze czy internetowe platformy handlowe[20].

Wpływ ustawy o krajowym systemie cyberbezpieczeństwa na działalność dostawców usług cyfrowych

Dnia 28.8.2018 r. weszła w życie ustawa implementująca do polskiego porządku prawnego dyrektywę NIS, czyli ustawa z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa[21] określająca organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy,

[9] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, Legalis/el. 2016.

[10] Tamże, Legalis el./2016. Zob. także: *K. Szczepanowska-Kozłowska*, *J. Ostrowska*, Poland Chapter 22, [w:] Global Legal Group, The International Comparative Legal Guide to: Cybersecurity 2018 1-st Edition, A practical cross-border insight into cybersecurity work, Global Legal Group 2018, s. 141 i n.

[11] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, Legalis/el. 2016.

[12] *T. Tołpa*, *J. Protasiewicz*, *M. Kozłowski*, *B. Bułkszas*, Zagrożenia, nadużycia i bezpieczeństwo w systemach informatycznych a granice ochrony praw podstawowych, Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne 2015, s. 542.

[13] *M.-T. Holzleitner*, *J. Reichl*, European provisions for cyber security in the smart grid – an overview of the NIS-directive, Springer Verlag Wien 2017.

[14] *S. Kotecka*, Strategie i dobre praktyki dotyczące bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych i ochrony przed ich nieuprawnionym ujawnieniem, Legalis/el. 2016.

[15] Dz.Urz. UE L Nr 199, s. 1, dalej jako: RODO.

[16] Dz.Urz. UE L Nr 194, s. 1; dalej jako: dyrektywa NIS.

[17] *M. Olszewska*, Cyberbezpieczeństwo jako przedmiot analizy przestrzennej, Legalis/el.2018.

[18] Dz.Urz. UE L Nr 218, s. 8.

[19] Art. 1 ust. 2 dyrektywy NIS.

[20] *M. Siemaszkiewicz*, Internet rzeczy – wyzwania cyberbezpieczeństwa, Edukacja Prawnicza 2018, Nr 1, s. 51 i n.

[21] Dz.U. poz. 1560; dalej jako: KrajSysCybU.

a także wskazująca zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej[22]. Zasadniczym celem tej ustawy jest stworzenie krajowego systemu cyberbezpieczeństwa mającego zapewnić cyberbezpieczeństwo na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów[23]. Kluczowe z punktu widzenia nowej regulacji pojęcie cyberbezpieczeństwa zostało zdefiniowane w art. 2 pkt 4 KrajSysCybU. W myśl tego przepisu cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Dostawcy usług cyfrowych objęci Krajowym Systemem Cyberbezpieczeństwa

Artykuł 4 KrajSysCybU zawiera wyliczenie podmiotów, które objęte zostały Krajowym Systemem Cyberbezpieczeństwa. Zgodnie z pkt 2 tego przepisu do tego systemu zalicza się także dostawców usług cyfrowych.

Warto zwrócić uwagę, że zgodnie z art. 1 ust. 2 KrajSysCybU jej przepisów nie stosuje się do przedsiębiorców telekomunikacyjnych[24] – w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, a także do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[25], oraz podmiotów wykonujących działalność leczniczą tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

W rozumieniu art. 17 ust. 1 KrajSysCybU dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową. Podobnie jak w dyrektywie NIS, w ustawie o krajowym systemie cyberbezpieczeństwa za dostawców usług cyfrowych, w myśl tego przepisu, nie są uważani mikroprzedsiębiorcy[26] i mali przedsiębiorcy[27]. Powodem wyłączenia tych podmiotów z kategorii dostawców usług cyfrowych może być fakt, że wymagane ustawą o krajowym systemie cyberbezpieczeństwa środki bezpieczeństwa oraz nałożone obowiązki mogą stanowić dla nich nieproporcjonalne obciążenie[28]. Kolejno wskazać należy, że w myśl art. 2 pkt 15 KrajSysCybU usługą cyfrową jest usługa świadczona drogą elektroniczną w rozumieniu przepisów ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną[29], wymieniona w załączniku Nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa.

Analiza ww. załącznika Nr 2 oraz przepisów będących przedmiotem odesłania ustawowego pozwala na zdefiniowanie usługi cyfrowej jako usługi, która jest usługą internetowej platformy handlowej, usługą przetwarzania w chmurze lub usługą wyszukiwarki internetowej, i która świadczona jest bez jednoczesnej obecności stron (na odległość) poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej (w rozumieniu prawa telekomunikacyjnego), tj. za pomocą systemów transmisyjnych oraz urządzeń komutacyjnych lub przekierowujących, a także innych zasobów, w tym nieaktywnych elementów sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.

Przywołane w powyższej definicji kategorie usług cyfrowych zostały zdefiniowane ustawowo w załączniku Nr 2 do ustawy o krajowym systemie cyberbezpieczeństwa. Zgodnie z tym załącznikiem internetowa platforma handlowa to usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na

[22] Art. 1 ust. 1 KrajSysCybU.

[23] Art. 3 KrajSysCybU.

[24] O których mowa w ustawie z 16.7.2004 r. – Prawo telekomunikacyjne, t.j. Dz.U. z 2018 r. poz. 1954 ze zm.

[25] Dz.Urz. UE L Nr 257, s. 73; dalej jako: rozporządzenie eIDAS. Usługi zaufania to zgodnie z art. 3 pkt 16 rozporządzenie eIDAS usługi elektroniczne zazwyczaj świadczone za wynagrodzeniem i obejmujące: a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

[26] W myśl art. 7 ust. 1 pkt 1 ustawy z 6.3.2018 r. – Prawo przedsiębiorców (Dz.U. poz. 646 ze zm.; dalej jako: PrPrzedsU) mikroprzedsiębiorcy to przedsiębiorcy, którzy w co najmniej jednym roku z dwóch ostatnich lat obrotowych zatrudniali średniorocznie mniej niż 10 pracowników oraz osiągnęli roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 2 mln euro, lub sumy aktywów ich bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 mln euro.

[27] Zgodnie z art. 7 ust. 1 pkt 2 PrPrzedsU mali przedsiębiorcy to przedsiębiorcy, którzy w co najmniej jednym roku z dwóch ostatnich lat obrotowych zatrudniali średniorocznie mniej niż 50 pracowników oraz osiągnęli roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych nieprzekraczający równowartości w złotych 10 mln euro, lub sumy aktywów ich bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 10 mln euro, i którzy nie są mikroprzedsiębiorcami.

[28] *M.-T. Holzleitner, J. Reichl*, European provisions for cyber security in the smart grid – an overview of the NIS-directive, Springer Verlag Wien 2017.

[29] Dz.U. z 2017 r. poz. 1219 ze zm.

stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy korzystającej z usług świadczonych przez internetową platformę handlową. Usługę przetwarzania w chmurze ustawodawca zdefiniował jako usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników, natomiast wyszukiwarka internetowa to usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiająca w wyniku odnośniki odnoszące się do informacji związanych z zapytaniem.

Należy zauważyć, że przytoczona powyżej ustawowa definicja internetowej platformy handlowej jest stosunkowo nieostra i jej interpretacja w praktyce może budzić zasadnicze wątpliwości. W celu jej uzupełnienia należy sięgnąć posiłkowo do treści motywu 15 preambuły dyrektywy NIS, zgodnie z którym internetowa platforma handlowa umożliwia konsumentom i przedsiębiorcom handlowym zawieranie umów sprzedaży lub umów o świadczenie usług online z przedsiębiorcami handlowymi i jest ostatecznym miejscem zawierania tych umów. W przypadku gdy możliwe jest ostateczne zawarcie umowy, nie powinna ona obejmować usług online, które spełniają wyłącznie funkcję pośredniczącą wobec usług stron trzecich. Nie powinna zatem obejmować usług online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego w celu zakupu produktu. W opinii autorki, w kontekście treści motywu 15 dyrektywy 2016/1148, a także z uwagi na *ratio legis* analizowanej regulacji, należy również uznać, że działalność przedsiębiorców handlowych pośredniczących w sprzedaży towarów i świadczeniu usług za pośrednictwem własnej internetowej platformy handlowej, która jest ostatecznym miejscem zawierania umów, we wskazanym zakresie zawiera się w istocie rzeczy w definicji usługi cyfrowej internetowej platformy handlowej.

Jak rozumieć definicję usługi przetwarzania w chmurze? Po pierwsze, posiłkując się motywem 17 dyrektywy NIS, można przyjąć, że zakres pojęcia „zasoby obliczeniowe" obejmuje sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi. Zgodnie z tym motywem pojęcie „skalowalne" odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów, jako reakcja na fluktuacje zapotrzebowania. Natomiast pojęcie „elastyczny zbiór" charakteryzuje zasoby obliczeniowe, które są przydzielane i uwalniane zależnie do zapotrzebowania, aby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia. „Wspólne wykorzystywanie przez wielu użytkowników" polega natomiast na dzieleniu przez wielu użytkowników wspólnego dostępu do usługi, jednak przetwarzanie w ramach tej usługi odbywa się oddzielnie dla każdego z użytkowników, przy jednoczesnym świadczeniu usługi z tego samego sprzętu elektronicznego.

Jak z kolei wskazano w motywie 16, definicja wyszukiwarki internetowej nie powinna obejmować funkcji wyszukiwania, które ograniczają się do treści na konkretnej stronie internetowej, bez względu na to, czy funkcja wyszukiwania jest zapewniana przez wyszukiwarkę zewnętrzną. Co więcej, podobnie jak w przypadku definicji internetowej platformy handlowej, tak również w zakresie definicji wyszukiwarki internetowej nie powinny znajdować się usługi online, które porównują cenę poszczególnych produktów lub usług różnych przedsiębiorców handlowych, a następnie przekierowują użytkownika do preferowanego przedsiębiorcy handlowego, aby tam dokonał zakupu produktu.

Obowiązki dostawców usług cyfrowych

Wskazać należy więc, że zgodnie z art. 17 ust. 2 zd. 1 KrajSysCybU dostawca usługi cyfrowej jest obowiązany podejmować właściwe i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki zarządzania ryzykiem zostały określone w rozporządzeniu wykonawczym Komisji (UE) 2018/151 z 30.1.2018 r. ustanawiającym zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi rodzajami ryzyka dla bezpieczeństwa sieci i systemów informatycznych oraz parametrów służących do określenia, czy incydent ma istotny wpływ[30]. W rozporządzeniu tym doprecyzowane zostały również elementy, jakie mają zostać uwzględnione przez dostawców usług cyfrowych przy określaniu i przedsiębraniu środków mających na celu zapewnienie poziomu bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez nich w kontekście oferowania usług cyfrowych, jak również parametry, które należy wziąć pod uwagę w celu ustalenia, czy incydent ma istotny wpływ na świadczenie tych usług.

W myśl art. 17 ust. 2 zd. 2 KrajSysCybU środki zarządzania ryzykiem, a więc skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka[31] zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają bezpieczeństwo systemów informacyjnych i obiektów, postępowanie w przypadku obsługi incydentu, zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej, monitorowanie, audyt i testowanie, najnowszy stan wiedzy, w tym zgodność

[30] Dz.Urz. UE L Nr 26, s. 48; dalej jako: rozporządzenie Nr 2018/151.
[31] Art. 2 pkt 19 KrajSysCybU.

z normami, międzynarodowymi, o których mowa w rozporządzeniu Nr 2018/151.

1. Bezpieczeństwo systemów informacyjnych i obiektów

W myśl art. 2 ust. 1 rozporządzenia Nr 2018/151 bezpieczeństwo sieci i systemów informatycznych oraz ich środowiska fizycznego obejmuje następujące elementy:

- systematyczne zarządzanie sieciami i systemami informatycznymi, co oznacza mapowanie systemów informatycznych oraz ustanowienie zestawu odpowiednich polityk w zakresie zarządzania bezpieczeństwem informacji, w tym analiz ryzyka, zasobów ludzkich, bezpieczeństwa operacji, architektury bezpieczeństwa, zabezpieczenia danych i zarządzania cyklem życia systemu oraz, w stosownych przypadkach, szyfrowania i zarządzania nim;
- bezpieczeństwo fizyczne i środowiskowe, które oznacza dostępność zestawu środków mających na celu ochronę bezpieczeństwa sieci i systemów informatycznych dostawców usług cyfrowych przed szkodami z zastosowaniem całościowego podejścia do kwestii zagrożeń opartego na analizie ryzyka, które uwzględnia np. awarie systemu, błędy ludzkie, działania złośliwe bądź zjawiska naturalne;
- bezpieczeństwo dostaw oznacza ustanowienie oraz utrzymywanie odpowiednich polityk w celu zagwarantowania dostępności oraz, w stosownych przypadkach, identyfikowalności krytycznych dostaw wykorzystywanych do świadczenia usług;
- kontrole dostępu do sieci i systemów informatycznych, co oznacza dostępność zestawu środków, które mają zagwarantować, że dostęp fizyczny i dostęp logiczny do sieci i systemów informatycznych, w tym administracyjne bezpieczeństwo sieci i systemów informatycznych, są uprawnione i ograniczone w oparciu na wymogi dotyczące prowadzenia działalności i bezpieczeństwa.

2. Postępowanie w przypadku obsługi incydentu

Zgodnie z art. 2 ust. pkt 10 KrajSysCybU obsługa incydentu to czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu. W odniesieniu do postępowania w przypadku incydentu środki przedsiębrane przez dostawcę usług cyfrowych, zgodnie z art. 2 ust. 2 rozporządzenia Nr 2018/151, obejmują:

- utrzymywanie i testowanie procesów oraz procedur wykrywania w celu zapewnienia terminowej i odpowiedniej wiedzy na temat nietypowych zdarzeń;
- procesy i polityki dotyczące zgłaszania incydentów oraz identyfikowania niedociągnięć i słabych punktów w jego systemach informatycznych;
- reagowanie zgodnie z ustanowionymi procedurami oraz składanie sprawozdań z wyników przedsięwziętych środków;
- ocenę powagi danego incydentu, dokumentowanie wiedzy uzyskanej z analizy incydentów oraz gromadzenie odpowiednich informacji, które mogą stanowić dowody i wspierać proces ciągłego doskonalenia.

3. Zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej

Zarządzanie ciągłością działania, w myśl art. 2 ust. 3 rozporządzenia wykonawczego 2018/151, oznacza zdolność do utrzymania lub, w razie potrzeby, przywrócenia realizacji usług na uprzednio określonych dopuszczalnych poziomach, po wystąpieniu zakłócenia, i obejmuje:

- ustanowienie i stosowanie planów awaryjnych w oparciu o analizę wpływu na działalność w celu zapewnienia ciągłości usług świadczonych przez dostawców usług cyfrowych, co jest oceniane i testowane w regularnych odstępach czasu, np. przez ćwiczenia;
- zdolności w zakresie przywracania gotowości do pracy po katastrofie, które są oceniane i testowane w regularnych odstępach czasu, na przykład przez ćwiczenia.

4. Monitorowanie, audyt i testowanie

Monitorowanie, audyt i testowanie, w myśl art. 2 ust. 4 rozporządzenia wykonawczego 2018/151, obejmują ustanowienie i utrzymywanie polityk w zakresie:

- przeprowadzania zaplanowanej sekwencji obserwacji lub pomiarów w celu dokonania oceny, czy sieci i systemy informatyczne działają zgodnie z zamierzeniem;
- inspekcji i weryfikacji mających na celu sprawdzenie, czy stosuje się normę lub zbiór wytycznych, czy rejestry są dokładne, a także czy realizowane są cele w zakresie efektywności i skuteczności;
- procesu mającego na celu ujawnienie wad mechanizmów bezpieczeństwa sieci i systemów informatycznych, które służą ochronie danych i utrzymaniu funkcjonalności zgodnie z zamierzeniem. Tego rodzaju proces obejmuje procesy techniczne i personel zaangażowany w przepływ operacji.

5. Najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi

Normy międzynarodowe, zgodnie z art. 2 ust. 5 rozporządzenia Nr 2018/151, oznaczają normy przyjęte przez międzynarodową jednostkę normalizacyjną, o której mowa w art. 2 ust. 1 lit. a) rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 1025/2012, tj. Międzynarodową Organizację Normalizacyjną (ISO), Międzynarodową Komisję Elektrotechniczną (IEC) i Międzynarodowy Związek Telekomunikacyjny (ITU). Stosowane mogą być również europejskie lub uznane

międzynarodowe normy i specyfikacje mające znaczenie dla bezpieczeństwa sieci i systemów informatycznych, w tym istniejące normy krajowe.

6. Środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową

W myśl art. 17 ust. 3 KrajSysCybU dostawca usługi cyfrowej podejmuje ponadto środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi. Ciągłość ta może mieć wpływ na kluczową działalność gospodarczą i społeczną w UE, wszak zakłócenie usług cyfrowych mogłoby uniemożliwić świadczenie innych usług, które są od nich zależne[32]. W dzisiejszych czasach, gdy z usług cyfrowych korzystają niemal wszyscy przedsiębiorcy, przerwanie ciągłości świadczenia takich usług mogłoby znacząco utrudnić funkcjonowanie takich przedsiębiorców, a także, co również podkreślono w motywie 48 preambuł dyrektywy NIS, znacząco wpłynąć na ich uczestnictwo w rynku wewnętrznym i handlu transgranicznym w Unii.

Pozostałe obowiązki związane z wystąpieniem incydentów w cyberprzestrzeni oraz ich odmienność w zależności od rodzajów incydentów

Należy zauważyć, że na gruncie przepisów ustawy o krajowym systemie cyberbezpieczeństwa szczególną rolę odgrywają obowiązki dostawców usług cyfrowych dotyczące reakcji na wystąpienie incydentów. W pierwszej kolejności należy wskazać, że zgodnie z art. 18 ust. 1 pkt 1 KrajSysCybU, dostawca usługi cyfrowej przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów.

W rozumieniu art. 2 pkt 5 KrajSysCybU incydentem jest zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Ustawa o krajowym systemie cyberbezpieczeństwa definiuje także szczególne kategorie incydentów, które mogą mieć niekorzystny wpływ na odporność systemów informacyjnych dostawców usług cyfrowych.

Po pierwsze, wyróżnia się incydent istotny, czyli taki, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia Nr 2018/151[33]. Zgodnie z tym przepisem dany incydent uznaje się za mający istotny wpływ, jeżeli zaistniała co najmniej jedna z wymienionych w nim przesłanek. Będziemy mieć zatem do czynienia z incydentem istotnym, gdy usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 000 000 użytkownikogodzin[34] bądź też gdy incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług, oferowanych bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w UE. Incydent istotny nastąpi także wtedy, gdy spowoduje ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych lub gdy wyrządził co najmniej jednemu użytkownikowi w UE stratę materialną, której wysokość przekracza 1 000 000 euro.

Po drugie, ustawa wprowadza również kategorię incydentu krytycznego. Jest to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT GOV, CSIRT MON, CSIRT NASK[35].

Wreszcie na gruncie analizowanej regulacji wyróżnić można również kategorię incydentów zwykłych, tj. takich zdarzeń, które mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo, ale nie są ani incydentami krytycznymi, ani incydentami istotnymi.

Szczególną uwagę zwrócić należy na dodatkowe obowiązki przedsiębiorców związane z wystąpieniem incydentów istotnych i incydentów krytycznych. Stąd odróżnić należy dwa rodzaje postępowania w przypadku wystąpienia incydentów, w zależności od tego, czy zachodzi incydent zwykły, czy też incydent istotny lub krytyczny. Dopiero bowiem sklasyfikowanie incydentu jako incydentu istotnego czy też krytycznego pociąga za sobą odmienności w zakresie postępowania z nim w postaci dodatkowych obowiązków omówionych w dalszej części rozważań.

W myśl art. 18 ust. 2 KrajSysCybU w celu sklasyfikowania incydentu jako istotnego dostawca usługi cyfrowej uwzględnia w szczególności liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; czas trwania incydentu; zasięg geograficzny obszaru, którego dotyczy incydent; zakres zakłócenia funkcjonowania usługi; zakres wpływu incydentu na działalność gospodarczą i społeczną. Dostawca usługi cyfrowej, zgodnie z art. 18 ust. 3 KrajSysCybU, klasyfikując incydent jako istotny, ocenia istotność wpływu incydentu na świadczenie usługi cyfrowej na podstawie parametrów, o których mowa powyżej, oraz progów określonych w rozporządzeniu wykonawczym 2018/151.

[32] Motyw 48 preambuły dyrektywy NIS.

[33] Art. 1 pkt 7 KrajSysCybU.

[34] Pojęcie „użytkownikogodziny" odnosi się do liczby dotkniętych incydentem użytkowników w Unii przez okres sześćdziesięciu minut

[35] Art. 1 pkt 6 KrajSysCybU.

Tab. 1. Parametry i odpowiednie progi, jakie należy wziąć pod uwagę w celu określenia, czy wpływ incydentu jest istotny

Parametr	Progi
Liczba użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług	Dostawca usług cyfrowych musi być w stanie oszacować jedną z następujących liczb: 1) liczba dotkniętych incydentem osób fizycznych i osób prawnych, z którymi zawarto umowę na świadczenie danej usługi, lub 2) liczba dotkniętych incydentem użytkowników, którzy korzystali z tej usługi, na podstawie w szczególności wcześniejszych danych o ruchu.
Czas trwania incydentu	Dostawca usług cyfrowych musi ustalić okres, jaki upływa od zakłócenia właściwego świadczenia usługi pod względem jej dostępności, autentyczności, integralności lub poufności, do czasu przywrócenia stanu normalnego.
Zasięg geograficzny obszaru, którego dotyczy incydent	Dostawca usług cyfrowych musi być w stanie ustalić, czy dany incydent ma wpływ na świadczenie jego usług w poszczególnych państwach członkowskich.
Zakres zakłócenia funkcjonowania usługi	Zakres ten dostawca usług cyfrowych powinien mierzyć w odniesieniu do jednego lub większej liczby następujących aspektów osłabionych w wyniku danego incydentu: dostępność, autentyczność, integralność lub poufność danych lub powiązanych usług.
Zakres wpływu incydentu na działalność gospodarczą i społeczną	Dostawca usług cyfrowych musi być w stanie – w oparciu na wskazówki, takie jak charakter jego stosunków umownych z klientem lub, w stosownych przypadkach, potencjalna liczba użytkowników dotkniętych incydentem – stwierdzić, czy incydent spowodował znaczne straty materialne bądź niematerialne dla użytkowników, na przykład odnośnie do zdrowia, bezpieczeństwa lub uszkodzenia mienia.

W przypadku gdy analiza powyższych parametrów pozwoli na ustalenie, iż dany incydent nie spełnia przesłanek uznania go za incydent istotny, uznać należy, że zaistniałe zdarzenie ma charakter incydentu zwykłego i konsekwentnie nie rodzi ono po stronie dostawcy usługi cyfrowej żadnych obowiązków ponad te, jakie wynikają z przedstawionej powyżej definicji obsługi incydentu. Powyższe oznacza, że w sytuacji uznania zdarzenia za incydent zwykły dostawca usług cyfrowych obowiązany będzie wyłącznie dokonać priorytetyzacji, a także podjąć działania naprawcze i ograniczyć skutki incydentu zgodnie z procedurami, które wdrożył, realizując obowiązek, o którym mowa w art. 17 ust. 2 pkt 2 oraz art. 17 ust. 3 KrajSysCybU.

Szczególne obowiązki dostawców usług cyfrowych związane z kategorią incydentów istotnych i incydentów krytycznych

Zgodnie z art. 18 KrajSysCybU dostawca usługi cyfrowej klasyfikując incydent jako istotny jest obowiązany zgłosić go niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego organu, tj. CSIRT GOV, CSIRT MON lub CSIRT NASK. Zgłoszenie, o którym mowa powyżej, jest przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji[36]. Informacje, które przedsiębiorca musi zawrzeć w zgłoszeniu, wskazano w art. 19 ust. 1 KrajSysCybU. Zgłaszając incydent, należy przede wszystkim opisać przyczynę i źródło incydentu, jego wpływ na świadczenie usługi cyfrowej, w tym liczbę użytkowników, których dotknął, czas trwania incydentu, jego zasięg geograficzny, zakres zakłócenia funkcjonowania usługi cyfrowej oraz zakres wpływu incydentu na działalność gospodarczą i społeczną. Oprócz tego przedsiębiorca ma obowiązek przedstawić w zgłoszeniu informacje umożliwiające właściwemu CSIRT określenie, czy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich UE. Wreszcie należy także przedstawić podjęte działania zapobiegawcze i naprawcze.

Należy podkreślić, że dostawca usługi cyfrowej obowiązany jest przekazać informacje znane mu w chwili dokonywania zgłoszenia. Informacje te dostawca usług cyfrowych uzupełnia następnie w trakcie obsługi incydentu istotnego[37]. Co ważne, jak wynika z brzmienia art. 19 ust. 3 KrajSysCybU, obowiązek przekazania w niezbędnym zakresie informacji stanowiących tajemnice prawnie chronione, w tym stanowiących tajemnicę przedsiębiorstwa, powstaje, wyłącznie gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Właściwy CSIRT może zwrócić się do dostawcy usługi cyfrowej o uzupełnienie zgło-

[36] Art. 18 ust. 5 KrajSysCybU.
[37] Art. 19 ust. 2 KrajSysCybU.

szenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań ustawowych. Należy pamiętać, że informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, dostawcy usług cyfrowych mają obowiązek odpowiednio oznaczyć w zgłoszeniu[38].

Podkreślenia wymaga fakt, że zgodnie z brzmieniem art. 18 ust. 4 KrajSysCybU dostawca usługi cyfrowej nie ma obowiązku dokonania zgłoszenia, o którym mowa wyżej, gdy nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej. Powyższe oznacza, że w braku możliwości oceny istotności wpływu incydentu na świadczenie usługi cyfrowej incydent będzie obsługiwany tak jak incydent zwykły.

Zgodnie z art. 18 ust. 1 pkt 5 KrajSysCybU dostawca usług cyfrowych zapewnia obsługę incydentu istotnego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.

Na dostawcy usługi cyfrowej spoczywa również obowiązek usunięcia, w wyznaczonym terminie, podatności, czyli właściwości systemu informacyjnego, które mogą być wykorzystane przez zagrożenie cyberbezpieczeństwa, tj. przez potencjalną przyczynę wystąpienia incydentu[39], a które doprowadziły lub mogłyby doprowadzić do incydentu istotnego, na wezwanie organu właściwego do spraw cyberbezpieczeństwa, jeśli z wnioskiem o takie wezwanie w trakcie koordynacji obsługi incydentu istotnego wystąpi CSIRT MON, CSIRT NASK lub CSIRT GOV[40]. W przypadku uznania zgłoszonego incydentu istotnego za incydent krytyczny przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV dostawca usług cyfrowych jest obowiązany ponadto zapewnić w niezbędnym zakresie dostęp do informacji dla właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV o incydentach zakwalifikowanych jako krytyczne[41]. Co więcej, w myśl art. 18 ust. 1 pkt 7 KrajSysCybU dostawca usługi cyfrowej przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora. Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy (m.in. przewoźnicy lotniczy, przedsiębiorstwa energetyczne, banki krajowe, podmioty lecznicze), posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej[42]. Należy wskazać również, że usługą kluczową jest usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych[43], tj. m.in. transport lotniczy pasażerski, udzielanie opieki zdrowotnej.

Warto ponadto zwrócić uwagę na możliwość dobrowolnego przekazywania właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV informacji nieobjętych ustawowym obowiązkiem informacyjnym. W myśl art. 20 KrajSysCybU dostawca usługi cyfrowej może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV również informacje o incydentach innych niż istotne (tj. o incydentach zwykłych), a także o zagrożeniach cyberbezpieczeństwa, szacowaniu ryzyka, podatnościach oraz wykorzystywanych technologiach. Informacje te są przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania ich w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Kary za niedopełnienie obowiązków

Należy podkreślić, że w przepisach ustawy o krajowym systemie cyberbezpieczeństwa przewidziane zostały kary pieniężne, nakładane w drodze decyzji organu właściwego do spraw cyberbezpieczeństwa za naruszenie przez dostawcę usług cyfrowych ustawowo określonych obowiązków. W przypadku gdy dostawca usług cyfrowych nie wykonuje obowiązku zgłoszenia incydentu istotnego, podlega karze pieniężnej do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego[44]. Jeżeli dostawca usług cyfrowych nie wykonuje obowiązku obsługi incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, m.in. obowiązku przekazania niezbędnych danych, w tym danych osobowych, podlega karze pieniężnej do 20 000 zł[45]. Ponadto gdy dostawca usług cyfrowych nie usuwa w wyznaczonym terminie podatności, które doprowadziły lub mogłyby doprowadzić do incydentu istotnego, na wezwanie organu właściwego do spraw cyberbezpieczeństwa, jeśli z wnioskiem o takie wezwanie w trakcie koordynacji obsługi incydentu istotnego wystąpi CSIRT MON, CSIRT NASK lub CSIRT GOV, podlega karze pieniężnej do 20 000 zł[46]. Co istotne, kary, o których mowa powyżej, mogą zostać nałożone, również w przypadku gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli organ właściwy do spraw cyberbezpieczeństwa uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia[47].

Jakkolwiek określone powyżej przypadki naruszeń stanowią katalog zamknięty, a konsekwentnie niedopełnienie innych obowiązków niż wskazane powyżej co do zasady nie

[38] Art. 19 ust. 4 i 5 KrajSysCybU.
[39] Art. 2 pkt 11 i 17 KrajSysCybU.
[40] Art. 18 ust. 1 pkt 6 KrajSysCybU.
[41] Art. 18 ust. 1 pkt 2 KrajSysCybU.
[42] Art. 5 ust. 1 KrajSysCybU.
[43] Art. 2 pkt 16 KrajSysCybU.
[44] Art. 73 ust. 2 pkt 1 w zw. z art. 73 ust. 3 pkt 12 KrajSysCybU.
[45] Art. 73 ust. 2 pkt 2 w zw. z art. 73 ust. 3 pkt 13 KrajSysCybU.
[46] Art. 73 ust. 2 pkt 3 w zw. z art. 73 ust. 3 pkt 13 KrajSysCybU.
[47] Art. 76 KrajSysCybU.

pociąga za sobą odpowiedzialności finansowej, w przepisach ustawy o krajowym systemie cyberbezpieczeństwa przewidziana została wyjątkowa odpowiedzialność uzależniona od czasu trwania naruszenia i jego skutków. Należy bowiem podkreślić, że jeśli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo dostawca usługi cyfrowej uporczywie narusza przepisy ustawy, powodując: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi; 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych – organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 1 000 000 zł[48]. Literalne brzmienie powyższego przepisu (możliwość jego zastosowania w wypadku „uporczywego naruszenia przepisów ustawy") uzasadnia pogląd, że dotyczy on naruszenia jakichkolwiek przepisów, jeśli naruszenie to jest uporczywe i wypełnia chociażby jedną z przesłanek wskazanych w pkt 1 lub 2 powyżej.

Podsumowanie

Analiza przepisów ustawy o krajowym systemie cyberbezpieczeństwa implementującej dyrektywę NIS prowadzi do wniosku, że wiele podmiotów sektora prywatnego spełnia przesłanki kwalifikujące ich uznanie za dostawcę usług cyfrowych w rozumieniu przepisów ustawy. Konstatacja ta pociąga za sobą konsekwencje w postaci objęcia tej kategorii dostawców usług cyfrowych krajowym systemem cyberbezpieczeństwa i nałożenia nań obowiązków w zakresie zarządzania ryzykiem, zapobiegania i minimalizacji wpływu incydentów na usługę cyfrową, a także ich obsługi. Pamiętać należy, że celem regulacji ustawowej jest wypracowanie niezbędnych reguł postępowania w celu lepszego zapewnienia cyberbezpieczeństwa, a przez to zapewnienie ciągłości świadczenia usług cyfrowych. Nawet jeśli usługi cyfrowe świadczone przez dostawców sektora prywatnego nie są usługami podstawowymi dla ogółu ludności, zapewnienie ich ciągłości może mieć wpływ na kluczową działalność gospodarczą i społeczną nie tylko konkretnego kraju UE, ale także całej wspólnoty. Nie może umknąć uwadze, że zakłócenie usług cyfrowych mogłoby uniemożliwić świadczenie innych usług, które są od nich zależne, a które to mogą być usługami podstawowymi dla gospodarki i społeczeństwa UE. W porównaniu do RODO, którego głównym celem jest ochrona danych osobowych podmiotów prywatnych, ustawa o krajowym systemie cyberbezpieczeństwa kładzie główny nacisk na zapewnienie bezpieczeństwa sieci i systemów teleinformatycznych. W akcie tym ustawodawca stosuje wiele podobnych mechanizmów związanych z identyfikowaniem, szacowaniem i zarządzaniem ryzykiem oraz powiela znaczną część obowiązków określonych w RODO. Istotna różnica dotyczy wyłączenia w ustawie o krajowym systemie cyberbezpieczeństwa mikroprzedsiębiorców i małych przedsiębiorców z konieczności stosowania środków bezpieczeństwa i realizacji obowiązków tam określonych. Fakt ten może wynikać z nieproporcjonalności obowiązków i związanych z nimi nierozerwalnie ciężarów, które to byłyby za wysokie w odniesieniu do wielkości tych przedsiębiorców. Trudno zatem stwierdzić, że nałożone obowiązki będą wysoce uciążliwe dla określonej w ustawie o krajowym systemie cyberbezpieczeństwa kategorii dostawców usług cyfrowych.

[48] Art. 73 ust. 5 KrajSysCybU.

Słowa kluczowe: cyberbezpieczeństwo, dostawcy usług cyfrowych, krajowy system cyberbezpieczeństwa, obowiązki dostawców usług cyfrowych

Obligations of digital service providers under the act on the national cybersecurity system as an element of improvement of security in the digital world and prevention of cybercrime

The aim of the present study is to systematize and analyze the obligations of digital service providers under the national cybersecurity system. The study also focuses on identifying which entities are considered as providers of digital services within the meaning of this act. The analysis of the obligations refers to the relevant provisions of EU law. The author also pays attention to the differences in the scope of obligations necessary to perform which are related to the occurrence of events that may have a negative impact on cybersecurity connected with qualifications of such incidents as significant or critical and to penalties that may result from the failure of digital service providers to fulfil their obligations under the act.

Keywords: cybersecurity, digital service providers, national cybersecurity system, obligations of digital service providers.

Critical Analysis of the „Mosaic Principle" Under Art. 7 Para 2 Brussels Ibis Regulation for Disputes Arising out of Non-Contractual Obligations on the Internet[1]

Ph.D. *Tereza Kyselovská*[2]

This article analyzes the „mosaic principle" under Art. 7 Para 2 Brussels Ibis Regulation for disputes arising out of non-contractual obligations on the Internet, online defamation and online infringements of copyright in particular. The subject of the analysis are decisions of the Court of Justice of the EU, namely *Shevill, eDate, Bolagsupplysningen*, *Pinckney* and *Hejduk*. The aforementioned decisions are critically analyzed in terms of the nature of dissemination of information on the Internet and the appropriateness and usefulness of their interpretation in the context of the objectives and principles underlying the Brussels Ibis Regulation.

Introduction

Internet and modern communication technologies have changed the way information is distributed and shared. In the „printed age" it was possible to predict and limit reach of published information. Nowadays, in the „Internet age", the dissemination of information is relatively easy and fast; it is possible to share information with unlimited number of people. On the Internet, there are no borders as we know them from the „physical" world. This development creates many legal challenges. On the Internet, it is relatively „easy" to enter into private law relationship with international (cross-border) element. These legal relationships are governed by the private international law rules (hereinafter referred to as PIL). The PIL rules are deeply rooted in the principle of territoriality; they „anchor" legal conduct to a territory of a particular state in order to determine competent court and law applicable. This is particularly difficult in case of legal conduct on the Internet[3].

This article is aimed at the analysis of one of the problematic areas, i.e. jurisdictional rules for disputes arising out of non-contractual obligations on the Internet (online infringements of privacy, online defamation and online infringements of copyright). In order to determine the court, which has international jurisdiction, it is necessary to answer following questions: Where can the claimant sue the infringer for alleged online infringement if the infringed information is accessible everywhere on the Internet? What types of remedies and amount of damages is possible to claim at that *forum*? In case of damage that occurred on the territory of several states, how could the remedy be divided among all potential *forums*?

To answers these questions it is necessary to analyze PIL and jurisdictional rules[4]. However, the majority of EU PIL rules were created in the „print age". For this reason, these rules are „technologically neutral" and do not consider rather specific characteristics of the Internet. Therefore, it is necessary to turn to case law of the Court of Justice of the European Union (hereinafter referred to as „CJEU") and its interpretation of the relevant jurisdictional rules contained in relevant EU jurisdictional rules.

The aim of this article is a critical analysis of the case law of the CJEU regarding interpretation of jurisdictional rules for disputes arising out of non-contractual obligations on the Internet. This analysis will be focused in Article 7 Para 2 of the Brussels Ibis Regulation[5] containing jurisdictional rule „place where the harmful event occurred or may occur". According to the CJEU, this rule consists of the place of the casual event and place of the damage. The „place of the damage" criterion is highly problematic. On numerous occasions, the CJEU has interpreted it as every place where the Internet content can be accessed, i.e. using „the mosaic principle". The aim of this article is to test this criterion with regards to the principles the EU jurisdictional rules and Brussels Ibis Regulation.

[1] This article is part of a project of the Masaryk University MUNI/A/1141/2017.

[2] The author holds position of associate professor at the Department of International and European Law, Faculty of Law, Masaryk University in Brno, Czech Republic. In her research, she specializes in private international law, intellectual property rights and electronization. She teaches courses in European private international law, international commercial law and arbitration.

[3] For analysis of other challenges the PIL faces in the Internet era, see for instance *T. Kyselovská*, Působnost práva na internetu, [in:] *R. Polčák* et al., Právo informačních technologií, Praha 2018, s. 29–64, p. 36; *T. Kyselovská*, Elektronizace a její vliv na vybrané aspekty evropského mezinárodního práva soukromého, [in:] *N. Rozehnalová, J. Valdhans, K. Drličková, T. Kyselovská*, Mezinárodní právo soukromé Evropské unie (Nařízení Řím I, Nařízení Řím II, Nařízení Brusel I), Praha 2013, p. 411–439; *T. Kyselovská*, Vybrané otázky vlivu elektronizace na evropské mezinárodní právo soukromé a procesní: (se zaměřením na princip teritoriality a pravidla pro založení mezinárodní příslušnosti soudu ve sporech vyplývajících ze smluvních závazkových vztahů), Brno 2014, p. 228. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia; sv. č. 487.

[4] This article deals only with European private international law rules, i.e. relevant EU regulations.

[5] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

This article will focus on the most relevant judgments, namely *Bier*,[6] *Shevill*,[7] *eDate*,[8] *Bolagsupplysningen*[9] (for online defamation); and *Pinckney*[10] and *Hejduk*[11] (for infringements of copyright).

For the purposes of this article, five research questions will be analyzed: Is the interpretation of the CJEU in compliance with the goals and principles of the Brussels Ibis Regulation and its provisions? Has the CJEU taken into account the specific characteristics of the Internet and the way in which information is distributed online? Is the mosaic principle in compliance with the principles of legal certainty and predictability under the Brussels Ibis? Does the interpretation of the CJEU result in favoring special jurisdictional rules in Article 7 Para 2 instead of the general jurisdictional rule in Article 4 of the Brussels Ibis Regulation?

Based on these five research questions, the goal of this article is to verify or refuse following working hypothesis: The mosaic approach used in Article 7 Para 2 Brussels Ibis Regulation is contrary to the principles of legal certainty and predictability for disputes arising out of non-contractual obligations on the Internet.

Structure of this article follows the research questions and working hypothesis. The article is structured into six parts. In the second part, brief description of jurisdictional rules in the Brussels Ibis Regulation for disputes arising out of non-contractual relationships is introduced. The third part deals with the development of the CJEU case law regarding interpretation on Art. 7 Para 2 (defamation in printed media, defamation on the Internet, infringement of copyright on the Internet). The fourth part contains critical analysis of the mosaic principle. The fifth part introduces possible solutions instead of the mosaic principle. The sixth part contains conclusion and verification of the working hypothesis.

The author of this article hopes this text will contribute to the discussion in this area of law and will be a relevant asset for both legal theory and practice.

International jurisdiction of courts in disputes arising out of non-contractual obligations

Rules for international jurisdiction of courts for disputes arising out of non-contractual obligations with international element are provided for in Article 4 and Article 7 Para 2 Brussels Ibis Regulation.

Article 4 Brussels Ibis Regulations contains general rule of jurisdiction. The general rule is based on the domicile of the defendant. Domicile of legal persons is autonomously defined in Art. 63. Domicile of natural persons is determined under Art. 62 Para 1 according to *lex fori*.

The Brussels Ibis Regulation allows for several exemptions from the general rule. One of these exemptions is special jurisdictional rule in Article 7[12].

Article 7 Para 2 Brussels Ibis Regulation[13] prescribes rules for international jurisdiction of courts in matters relating to tort, delict or quasi-delict. It is applicable, *inter alia*, to disputes arising out defamation and violations of privacy and infringements of intellectual property rights. Under this provision, a person domiciled in a Member State may be sued in the courts of another Member State „where the harmful event occurred or may occur". The reason for this special (alternative) rule is a close connection between the court and the action. Its objective is to ensure legal certainty and predictability for the defendant[14]; sound administration of justice, effectivity in evidentiary matters[15] and procedural economy[16]. This provision shall be interpreted autonomously[17]. It derogates from the general rule of the defendant's domicile; therefore, it shall be interpreted also restrictively and in consideration of the purpose of the special jurisdictional rules[18].

[6] Judgment of the Court of 30 November 1976. Handelskwekerij G.J. Bier BV v. Mines de potasse d'Alsace SA. Case 21–76.

[7] Judgment of the Court of 7 March 1995. Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA. Case C-68/93(hereinafter referred to as Shevill).

[8] Judgment of the Court (Grand Chamber) of 25 October 2011. eDate Advertising GmbH and Others v X and Société MGN LIMITED. Joined Cases C-509/09 and C-161/10 (hereinafter referred to as eDate).

[9] Judgment of the Court (Grand Chamber) of 17 October 2017. Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB. Case C-194/16 (hereinafter referred to as Bolagsupplysningen).

[10] Judgment of the Court (Fourth Chamber) of 3 October 2013. Peter Pinckney v KDG Mediatech AG. Case C-170/12 (hereinafter referred to as Pinckney).

[11] Judgment of the Court (Fourth Chamber) of 22 January 2015. Pez Hejduk v EnergieAgentur.NRW GmbH. Case C-441/13 (hereinafter referred to as Hejduk).

[12] This type of jurisdiction is in the Czech legal literature called as alternative jurisdiction, because it better describes its meaning and purpose, [in:] *J. Valdhans*, Nařízení Brusel I (alternativní příslušnost), [in:] *N. Rozehnalová, J. Valdhans, K. Drličková, T. Kyselovská*, Mezinárodní právo soukromé Evropské unie (Nařízení Řím I, Nařízení Řím II, Nařízení Brusel I), Praha 2013, p. 224–265. Also, see Preamble to the Brussels Ibis Regulation, Para 16, where the term „alternative grounds of jurisdiction" is used.

[13] This Article is based on the analysis of the CJEU case law regarding „predecessors" of the Brussels Ibis Regulation. Legal rules contained in Art. 7 Para 2 Brussels Ibis Regulation is similar to the Art. 5 Para 3 Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Regulation); resp. Art. 5 Para 3 1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters (Brussels I Convention).

[14] This objective is important, in particular, in disputes concerning non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation, [in:] Preamble to the Brussels Ibis Regulation, Para 16.

[15] Bolagsupplysningen, Para 27, Pinckney, Paras 27–28.

[16] Preamble to Brussels Ibis Regulation, Para 16. From case law, see for instance Bier, Para 11; Shevill, Para 19; *eDate*, Para 40; Bolagsupplysningen, Para 26.

[17] Bolagsupplysningen, Para. 25; eDate, Para 38; Pinckney, Para 23.

[18] *J. Valdhans*, Nařízení…, p. 224; Hejduk, Para 17; Pinckney, Paras 24–25.

Development of the CJEU case law

The Court of Justice of the EU has had several opportunities to interpret the criterion „place where the harmful event occurred or may occur". First, in judgment *Bier*, the CJEU laid down the fundamental principle underlying this provision. In judgment *Shevill* the interpretation was further developed for disputes arising out of defamation and violations of privacy in print media. In case of online defamation and violations of privacy the CJEU interpreted this provision in judgments *eDate* and *Bolagsupplysningen*. For infringements of intellectual property rights and copyright in particular, judgments in *Pinckney* and *Hejduk* will be also critically analyzed.

1. Setting the Scene – Judgments in *Bier* and *Shevill*

The expression „place where the harmful event occurred or may occur" was interpreted for the first time in 1976 in judgment *Bier*. According to the CJEU, this expression was intended to cover both the place where the damage occurred (*forum damni infecti*) and the place of the event giving rise to it (*forum delicti commissi*). It is up to the claimant, which courts he would choose; he has the option for either of these places[19]. Thus, the claimant has an „alternative within alternative jurisdictional rules".

This interpretation was further developed in 1996 in judgment *Shevill*. The *Shevill* case concerned defamation in printed media (newspaper) that were distributed in several Member States. The CJEU confirmed that the claimant could bring an action before courts where the illegal conduct occurred[20]. Courts of the place of the illegal conduct are competent to decide on the entire harm and damages. As another possibility, the claimant could bring an action for damages against the publisher also before the courts of each Member State in which the publication was distributed and where the victim claimed to have suffered injury to his reputation. These courts, however, have jurisdiction to rule solely in respect of the harm caused on the Member State of the court seized[21]. This type of territorially limited jurisdiction for damages is called „the mosaic principle" (*Mosaiktheorie*)[22].

The CJEU was aware of possible problems and challenges the mosaic approach might bring; courts in different Member States would decide about different aspects of one dispute. The CJEU, however, reasoned that the claimant has the possibility to file an action claiming full amount of damages before either court of the publisher's domicile (Art. 4) or the court of place where the event giving rise to the damages occurred, generally at the place of the publisher's domicile (Art. 7 Para 2), again claiming full amount of damages[23].

To sum up, in disputes arising out of defamation and violations of personality rights in printed media, combining outcomes of the judgments in *Bier* and *Shevill*, the claimant could bring proceedings before following courts:

1) Article 4: defendant's domicile – full amount of damages.
2) Article 7 Para 2: place of the illegal conduct giving rise to damage (i.e. place of publication) – full amount of damages.
3) Article 7 Para 2: place of the actual damage (i.e. states of distribution; place, where the claimant has suffered injury to his reputation) – territorially limited amount of damages.

2. The Scene is Set for Online Defamation – Judgments in *eDate* and *Bolagsupplysningen*

With the widespread use of the Internet, distribution and publication of information has changed. As Advocate General Bobek ironically stated: „As inevitably happens in the era of anonymous Internet bravery, universally known for its genteel style, subtle understanding, and moderation…"[24], on the Internet, any data can be distributed freely and without any limitations.

In 2011, for the first time, the CJEU dealt with the applicability and interpretation of the special jurisdictional rules in Art. 7 Para 2 Brussels Ibis Regulation for disputes arising out of online defamation and violations of privacy on the Internet in judgment *eDate*. Thus, the CJEU had the opportunity to be both the „inventor of new and innovator of existing rules"[25].

---

[19] Pinckney, Para 18; Coty German, Para 46; *P. Mankowski*, Art. 5, [in:] *U. Magnus, P. Mankowski*, Brussels I Regulation. European Commentaries on Private International Law. Sellier. European Law Publishers 2007, p. 190.

[20] Place of the illegal conduct will be, in most cases, the same as the place of the defendant's domicile. For the purpose of the „place of the harmful act" is essential the place the wrongdoer, not the place of the actual publication. Shevill, Para 24.

For online cases, the CJEU has repeatedly adjudicated that the place of the casual event is identical with the place of domicile of an information society service provider. See Hejduk, Paras 23–26; Wintersteiger, Paras 34–38; eDate, Paras 42–43.

[21] Shevill, Paras 30–31; Bolagsupplysningen, Para 31; *T. Rauscher*, Europäisches Zivilprozess- und Kollisionsrecht EuZPR/EUIPR. Kommentar. Band I. Brüssel Ia-VO. 4. Auflage, Köln 2016, p. 343.

[22] According to *P. Mankowski*: „The mosaic principle provides a very effective counter-incentive against forum shopping by supposed or alleged victims and thus effectively safeguards the legitimate jurisdictional interests on the alleged wrongdoer's side." [in:] *P. Mankowski*, Art. 5…, p. 194.

[23] Shevill, Para 32.

[24] Opinion of Advocate General Michal Bobek delivered on 13 July 2017. Bolagsupplysningen OÜ a Ingrid Ilsjan against Svensk Handel AB. C-194/16. Para 1.

[25] „In this case, the CJEU is indeed both an inventor and innovator. […] the CJEU may be said to adhere to proactive innovation rather than reactive.", [in:] *U. Maunsbach*, The CJEU as an Innovator – a New Perspective on the Development of Internet Related Case law. *Masaryk University Journal of Law and Technology* [online]. 2017, vol. 11:1, p. 85–86 [cit. 12.8.2018]. Available at: https://journals.muni.cz/mujlt/article/view/6669.

In *eDate*, the CJEU confirmed the applicability of jurisdictional criterion in Art. 7 Para 2 for disputes arising out of defamation and privacy violations on the Internet. According to the CJEU, it is possible to bring proceedings to courts of the place of the damage (i.e. the mosaic principle) or courts of the place of the event giving rise to the damage (place of the publication)[26].

However, problem with the mosaic principle on the Internet is, that following the place of the damage criterion it is possible to bring proceedings to courts of every State from which territory of the information was accessible[27]. These courts can rule only on the amount of damages that occurred within their territory[28]. The CJEU, somehow, tried to respond to the worldwide distribution of information on the Internet, the seriousness of the damage and protection of fundamental rights and freedoms[29]. For these reasons, the CJEU created a third jurisdiction „limb" for the Art. 7 Para 2, the „center of interest", „Mittelpunkt der Interessen" of the claimant[30]. Center of interest of the claimant (natural person) will usually be in the Member State of his domicile. However, it could also be a State where the person does not have his habitual residence, but pursues a professional activity or established any other particularly close link with that State. Courts in the State of the center of interest have jurisdiction in respect to all the damage caused[31].

To summarize this decision, in disputes arising out of defamation and violations of personality rights on the Internet via website, combining judgments in *Bier*, *Shevill* and *eDate*, the claimant could choose and bring action before four courts. In three courts it is possible to claim full damages, in third court it is possible to claim only territorially limited damages.

1) Article 4: defendant's domicile – full amount of damages.
2) Article 7 Para 2: place of the illegal conduct giving rise to damage (i.e. place of publication) – full amount of damages.
3) Article 7 Para 2: place of the actual damage (i.e. states of distribution; place, where the claimant has suffered injury to his reputation) – territorially limited amount of damages.
4) Article 7 Para 2: center of interest[32] – full amount of damages.

Judgment in *eDate* has been criticized. Firstly, the CJEU automatically applied the mosaic principle to the Internet, without considerations as to the practical problems with determination of the amount of damages for the respective territory; strengthening possible *forum shopping* and pro-claimant approach[33]. In this decision, The CJEU weakened the principle of *actor sequitur forum rei*; the center of interest allows claimant to bring proceedings claiming full amount of damages to his „home" court. In the vast majority of cases, the center of interest will be situated in the place where the claimant (the harmed person) is domiciled. Thus, the CJEU stressed the application of the principle *forum actoris*[34]. The decision of the CJEU might be interpreted that the victim has only one center of interest. However, this is not entirely correct view; one person could have more than one center of interest in different States[35].

In 2017, the CJEU further developed its interpretation of „place of the harmful act" in case of online defamation in *Bolagsupplysningen*. This case differs from the previous one in two important aspects: a legal person (not a natural person) claimed primarily rectification and removal of information made accessible on the Internet and only secondarily claimed damages for the alleged harm to their reputation[36].

In *Bolagsupplysningen*, the CJEU decided on the material scope of Art. Para 2 Brussels Ibis Regulation. The CJEU confirmed that the special jurisdictional rule is applicable, regardless whether the damage allegedly suffered is material or non-material in nature[37]; and that the criterion center of interest is applicable to both natural and legal persons[38]. For

[26] eDate, Para 41; Bolagsupplysningen, Para 29.

[27] eDate, Para 51. The CJEU in this respect changed its initial interpretation. In Shevill, the information should have been actively distributed in printed form and be available on the territory on the state; in eDate, it was sufficient that the information is or has been available.

[28] eDate, Paras 51-52.

[29] Opinion of Advocate General Cruz Villalón delivered on 29 March 2011. eDate Advertising GmbH vs. X (C-509/09) and Olivier Martinez and Robert Martinez vs. MGN Limited (C-161/10). Joined cases C-509/09 and C-161/10; Opinion of AG Michal Bobek in Bolagsupplysningen, Para 36.

[30] According to *U. Maunschach*, the CJEU found inspiration for „centre of interest" in *common law* and its principles, [in:] *U. Maunsbach*, The CJEU…, p. 85.

[31] eDate, Para 52; Bolagsupplysningen, Para 32.

[32] Questionable in this respect is whether the criterion „centre of interest" creates a third, independent jurisdictional rule within the Article 7 Para 2, or is it a second „limb" of the place of damage. In the first case, we had to question what is the legal base for this new jurisdictional rule. This is more of a theoretical and doctrinal issue that has no real consequences for the result in this case. However, it is interesting and important question in the context of the approach of the CJEU to the interpretation of the special jurisdictional rules in the Brussels Ibis Regulation, [in:] *T. Lutzi*, Internet Cases in EU Private International Law – Developing a Coherent Approach. International and Comparative Law Quarterly [online]. 2017, vol. 66, p. 695 [last visited 18.12.2018]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2988596.

[33] eDate, Para 49.

[34] Opinion of AG Villalón in Hejduk, Para 26. The structure of jurisdictional rules in the Brussels Ibis Regulation does not, with the exception of the special jurisdiction, prioritize the domicile of the claimant. *T. Lutzi*, Internet…, p. 696.

[35] In eDate, the CJEU used the term „center of interest" as one single center, not „centers", which would indicate possible multiplicity of these centers. However, the Advocate General Bobek stated that both natural and legal persons might have more than one center of interest in respect of a particular claim. This interpretation could lead to further fragmentation of claims, thus decreasing legal predictability and certainty of the parties. Opinion of AG Bobek in Bolagsupplysningen, Para 116.

[36] In Shevill and eDate it was natural persons who claimed primarily damages for violations of privacy and defamation.

[37] Bolagsupplysningen, Para 36.

[38] AG Bobek extensively analyzed the issue whether legal persons also have some personality rights. Based on analysis of the case law of the European Court of Human Rights and CJEU, he concluded that they do; some Member States even expressly protect their good name or reputation. Opinion of AG Bobek in Bolagsupplysningen, Para 58.

natural persons, their center of interest generally corresponds to the Member State of their habitual residence (unless other factors establish particularly close link with another Member State)[39]. For legal persons, in general, it is the place where their commercial reputation is most firmly established. In other words, where they carry out the main part of their economic activities. This place will generally coincide with the place of their registered office or seat; the location of that office is not, however, in itself, a conclusive criterion for the purpose of the center of interest[40].

Secondly, the CJEU decided on the jurisdictional rule itself and confirmed the previous decision in *eDate*. The CJEU maintained (to some degree) the mosaic principle. The claimant may bring his action before the courts of each Member State of which territory online content is or has been available. These courts have jurisdiction only in respect of the harm caused in the territory of the Member State of the court seized[41]. However, the CJEU took into consideration the ubiquitous nature of content place online and universal scope of distribution of information. The application for the rectification and removal of information published online could be only a single and indivisible act. Therefore, such a request can only be made before a court with jurisdiction to rule on the entirety of an application for compensation for the damage[42]. The claim for rectification and removal of information placed online cannot be brought before the courts of each Member State in which the information is or was accessible[43].

To summarize the decision in *Bolagsupplysningen*, the CJEU confirmed and slightly adjusted its interpretation in *Shevill* and *eDate*. The claimant could choose and bring the action before four courts. In three courts, it is possible to claim full damages, including rectification and removal of information placed online. Jurisdiction of the fourth court to decide on damages is territorially limited.

1) Article 4: defendant's domicile – full amount of damages, including rectification and removal of content placed online.
2) Article 7 Para 2: place of the illegal conduct giving rise to damage (i.e. place of publication) – full amount of damages, including rectification and removal of content placed online.
3) Article 7 Para 2: place of the actual damage (i.e. states of distribution; place, where the claimant has suffered injury to his reputation) – territorially limited amount of damages.
4) Article 7 Para 2: center of interest – full amount of damages, including rectification and removal of content placed online.

The decision in *Bolagsupplysningen* has also been criticized[44]. The main issue is that the CJEU maintained the mosaic principle, even if in modified form. The CJEU unfortunately did not follow AG Bobek's suggestion to revisit the scope of Art. 7 Para 2 and to disregard the mosaic principle all-together[45].

3. The Curious Case Continues for Online Infringements of Copyright – Judgments in *Pinckney* and *Hejduk*

The interpretation of „place of the harmful act" for disputes arising out of the infringement of copyright on the Internet was the core of two decisions of the CJEU. In 2013, the CJEU rendered judgment in *Pinckney*; in 2015, judgment in *Hejduk*. In both cases, the CJEU followed the previous case law in *Shevill* and *eDate*, with emphasis on the difference between intellectual property rights and personality rights.

In *Pinckney*, the claimant (author and composer residing in France) claimed infringement of his copyright to 12 songs recorded on a vinyl record. These songs were reproduced without his consent on a CD pressed in Austria by company Mediatech; then marketed in UK company through different Internet websites accessible in France. The claimant brought proceedings against Madiatech in France according to Art. 7 Para 2 Brussels Ibis Regulation, seeking compensation for damage sustained because of the infringement of his copyright.

In *Hejduk*, the claimant, a professional photographer residing in Austria, claimed infringement of her copyright on her photographs, which were made available on a German website by the German based defendant without her consent. The claimant brought proceedings in her home court in Austria, arguing the jurisdiction was based on the Art. 7 Para 2.

In both cases, the CJEU pointed out that the copyright law is in the EU harmonized according to the Directive 2001/29 and they are subject to the principle of territoriality[46]. As to the application of the Art. 7 Para 2, the CJEU followed its judgment in *Wintersteiger*[47] and stated that the casual event

[39] Bolagsupplysningen, Para 40; eDate, Para 49.
[40] Bolagsupplysningen, Para 41.
[41] Bolagsupplysningen, Para 47.
[42] Bolagsupplysningen, Para 48.
[43] Bolagsupplysningen, Para 49.
[44] For more in-depth analysis and criticism of this CJEU judgment, see *T. Kyselovská*, Kritická analýza judikatury Soudního dvora EU ve věcech určení mezinárodní příslušnosti soudů v případě pomluvy a porušení osobnostních práv na internetu, Časopis pro právní vědu a praxi, Masarykova univerzita, 2018, XXVI, 4/2018, p. 589–610. doi:10.5817/CPVP2018-4-1.
[45] Advocate General Bobek argued that the place where the harm occurred should be limited to one jurisdiction. That is, before the courts of the Member State in which its center of interests is located. At these courts, the claimant could claim the entirety of the harm sustained. Opinion of AG Bobek in Bolagsupplysningen, Paras 96–97.
[46] Hejduk, Para 22; Pinckney, Para 39.
[47] Judgment of the Court, 19 April 2012. Wintersteiger AG v Products 4U Sondermaschinenbau GmbH. Case C-523/10.

took place at the seat of the infringing company[48]; i.e. Austria and the UK in *Pinckney*, and Germany in *Hejduk*.

The crucial question, however, was, where is the place of the actual damage; i.e. whether it is France in *Pinckney*, resp. Austria in *Hejduk*. The CJEU stated that the location of the place where the damage occurred in a particular Member State is subject to the right whose infringement is alleged is protected in that Member State[49]. The CJEU further stated that if the infringement is being made through a publication on a website, there is no requirement that this website is „directed" to the Member State where the damage occurred[50]. The mere accessibility of the content protected by copyright is sufficient[51].

In this judgment, the CJEU confirmed the applicability of the mosaic principle. The court, seized on the basis of the place where the alleged damage occurred, has jurisdiction only to rule on the damage caused within that Member State[52].

To summarize, the *Pinckney* and *Hejduk* judgments, in disputes arising out of online infringements of copyright, the claimant could choose and bring action before three courts. In two courts it is possible to claim full damages, in third court it is possible to claim only territorially limited damages.

1) Article 4: defendant's domicile – full amount of damages.
2) Article 7 Para 2: place of the illegal conduct giving rise to damage (i.e. place of the infringing company) – full amount of damages.
3) Article 7 Para 2: place of the actual damage (i.e. states where the content prohibited by copyright laws is available) – territorially limited amount of damages.

These two decisions were substantially criticized. In *Hejduk*, the CJEU blindly followed its ruling in *Pinckney*. Unfortunately, the CJEU did not adopt more restrictive interpretation of Art. 7 Para 2, as proposed by the Advocate General Villalón[53]. The AG Villalón suggested that none of the criteria – the center of interest of the alleged victim's interest, the direction of the website to a specific Member State and the territoriality principle – should be applied[54]. Rather, he proposed that in case of delocalized damage, the Art. 7 Para 2 shall be interpreted that the jurisdiction rests only with the courts for the place where the event giving rise to the damage occurred. This would be often the place where the defendant (the infringer) is established or domiciled.

It is obvious, that the CJEU is building a system of international jurisdiction in intellectual property cases. However, the interpretation of Art. 7 Para 2 may vary according to the nature of the right allegedly infringed[55]. Therefore, the mosaic approach was not applied in the *Wintersteiger* case, where an alleged online infringement of a national trademark was at issue. The CJEU declined to localize the place where the damage occurred at the place where the relevant website can be accessed. The CJEU held that the place where the damage occurred is the Member State where the national trademark is registered; the entire damage can be claimed only there.

Unlike national trademark rights, copyright law is protected in every Member State according to the relevant national law without registration. For copyright infringement, the CJEU established the jurisdictional rule that the mere accessibility of a website is sufficient to establish jurisdiction under Art. 7 Para 2. This rule is not subjected to any limitations, e.g. „targeting" or „directing" of activities. Rather, the CJEU upheld the mosaic principle created in *Shevill* as a certain form of limitation.

Critical Analysis of the Mosaic Principle for Online Infringements of privacy rights and copyright law – *cui bono*?

From the analysis in the previous parts, it is clear that the mosaic approach was used primarily for damages in connection with defamation and violations of privacy and personality rights under Article 7 Para 2 Brussels Ibis Regulation. Later, it was used for online infringements of copyright law[56]. Presumably, it could be used also regarding violations of other territorially protected IP rights[57].

In the author's opinion the mosaic principle causes more practical problems, therefore, it is time to reconsider it. The mosaic principle is very problematic; not only in the „offline" context, but especially on the Internet.

To analyze this problem it is necessary to distinguish the characteristics of privacy rights and copyright. Both of these areas of law are governed by different principles. Copyright is ubiquitous only in the sense that it is attached to the right holder wherever he or she might be. It is attached to the manifestation of the creation of human

[48] Hejduk, Para 26. Furthermore, „the allegation of an infringement of an intellectual and industrial property right, in respect of which the protection granted by registration is limited to the territory of the Member State of registration, must be brought before the courts of that State. It is the courts of the Member State of registration which are the best placed to ascertain whether the right at issue has been infringed", [in:] Pinckney, Para 37.

[49] Hejduk, Para 29; Pinckney, Para 33. Copyright rights are protected in all Member States subject to the territoriality principle. Hejduk, Para 30.

[50] Hejduk, Paras 31 to 33; Pinckney, Para 42.

[51] Hejduk, Para 34.

[52] Hejduk, Paras 35 to 37; Pinckney, Para 45.

[53] Opinion of Advocate General Villalón delivered on 11 September 2014. Pez Hejduk v EnergieAgentur.NRW GmbH. Case C-441/13. Para 33 et seq.

[54] Opinion of AG Villalón in Hejduk, Para 48.

[55] Hejduk, Para 26; Pinckney, Para 32.

[56] The mosaic principle was used also in unfair competition law disputes in Judgment of the Court (Third Chamber) of 21 December 2016. Concurrence Sàrl v Samsung Electronics France SAS and Amazon Services Europe Sàrl. Case C-618/15.

[57] The CJEU refused application of the mosaic principles in disputes arising out of infringements of trademarks in Wintersteiger, Para 25. See also *T. Lutzi*, Internet…, p. 691.

mind. It protects the exploitation of the copyright work within a certain territory.

On the other hand, privacy rights and copyright share some similarities. They are both ubiquitous rights, the nature of which is linked to the person itself and are protected in every Member State without the need for registration.

As was stated before, the territoriality principle[58] that the mosaic principle relies on, is problematic[59]. Especially if mere access to the website is sufficient to establish jurisdiction. This could lead to excessive *forum shopping*. Therefore, the main issue is the application of mosaic principle in the context of the Internet.

In some legal literature it is still argued that if a person posts or uploads information on the Internet, he does it knowing that the information might reach a worldwide audience; therefore, if a dispute arises, he can expect to be sued in multiple *fora* and under multiple laws applicable[60].

This argument is, in the author's opinion, not valid anymore. The mosaic principle was applied in *Shevill* for distribution of information in the printed media. The harm caused in offline infringement could be easily quantified. In 1995, when *Shevill* judgment was rendered, the Internet was not as widely used as today. Internet changed „rules of the game", distribution is not relevant factor any more. Internet changed the ways we share, publish and consume information. Information on the Internet is readily available, for unlimited number of people, in a wide range of languages thanks to automatic translators, „irrespective of any intention on the part of the person who placed it in regard to its consultation beyond that person's Member State of establishment and outside of that person's control"[61]. Many distribution channels, services and platforms are based on the Internet and online activity[62]. Services like Uber, AirBnB, Wikipedia could not exist without the Internet. These services are run not only by professionals. The fact that a person uses the Internet to reach his customers does not automatically mean that he intends to reach worldwide audience[63].

Both private international law and intellectual property rights (copyright) are traditionally rooted in the principle of territoriality. Therefore, the idea of territorially limited jurisdiction of courts (the mosaic principle) as to the amount of claimed only on the territory of that particular state, damages is, theoretically, in accordance with this principle. On the other hand, the mosaic principle leads to possible jurisdiction of courts of all 28 Member States. Information published online is available, thus, capable of infringing a person's rights, in all of them. Even a few „hits" on a website, where the information is published, might establish jurisdiction of courts of that State[64].

The mosaic principle creates a multiplicity of potential *forums*. Thus, in the context of online activity, it is not in accordance with several legal principles governing private international law and Brussels Ibis Regulation in particular.

The multiplicity of potential *forums* is contrary to the principle of legal certainty and predictability of jurisdictional rules[65]. It gives the claimant an advantage to choose the most suitable forum for him; i.e. his own forum or any of the 28 Member States. It disproportionately supports *forum shopping*[66]. The defendant cannot predict where he might be sued. This amounts to the risk of harassment[67]. In practice, it will not be as common for the claimant to file a suit at multiple courts in different States; however it could be a part of his deterrent procedural strategy.

The mosaic principle is contrary to the principle of *actor sequitur forum rei* (the claimant must follow the *forum* of the thing in the dispute, i.e. the defendant's domicile)[68].

The multiplicity of *forums* leads to multiplicity of applicable laws. However, this problem is more relevant in defamation

[58] The territoriality principle was the key criterion in Wintersteiger, Para 30; Pinckney, Para 39; and Hejduk, Para 22.

[59] Opinion of AG Villalón in Hejduk, Paras 33–40, Opinion of AG Jääskinen in Coty Germany, Para 68.

[60] See Dow Jones & Company Inc. v. Gutnick (2002) 210 CLR 575, [in:] *D. Svantesson*, Solving the Jurisdiction Puzzle, Oxford 2017, p. 97–98.

[61] eDate, Para 45.

[62] *T. Lutzi*, Internet…, p. 700. The accessibility ot information can be limited using geoblocking technologies, see *D. Svantesson*, Solving…, p. 201 et seq. However, even these technologies are not without flaws and might lead to restrictions on the EU internal market. For these reasons, the EU adopted Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC

[63] It is possible to limit some types of services to a particular territory, e.g. vis paid subscription (e-publications, e-books), registration (to research databases), declaration of non-delivery (Amazon, eBay). Many services are based on free access to information (e.g. Wikipedia, TripAdvisor etc.), [in:] *T. Lutzi*, Internet…, p. 701.

[64] According to the AG Villalón: „While it is true that the number and origin of „hits" on a website may be indicative of a particular territorial impact, they are, in any event, sources which do not provide sufficient guarantees for the purpose of establishing conclusively and definitely that unlawful damage has occurred." Opinion of AG Villalón in eDate, Para 50. See also Hejduk, Para 34; Pinckney, Para 44.

[65] Preamble to Brussels Ibis Regulation, Para 15; Opinion of AG Bobek in Bolagsupplysningen, Para 79.

[66] *Forum shopping* is usually associated with negative connotations. Such an approach is not appropriate. Brussels Ibis Regulation provides for *forum shopping*, because apart from general jurisdictional rule it contains also special jurisdictional rules (Art. 7) and prorogation of jurisdiction (Art. 25). However, in the context of the Internet, the mosaic principle leads to *ad absurdum* application of *forum shopping*. Therefore, it is contrary to the principle of legal certainty and predictability.

[67] Opinion of AG Bobek in Bolagsupplysningen, Para 88; similarly, *C. Vanleenhove*, The European Court of Justice in Bolagsupplysningen: The Brussels I Recast Regulation's jurisdictional rules for online infringement of personality rights further clarified. *Computer Law & Security Review* [online]. 2018, no. 34, p. 643 [cit. 17.8.2018]. Available at: https://biblio.ugent.be/publication/8561503.

[68] The system of jurisdictional rules in the Brussels Ibis Regulation is based on general rule (defendant's domicile) and exceptions from this rule. One of these exceptions is protection of a weaker party (sections 3 to 5). These special rules take precedence before general rule. Preamble to the Brussels Ibis Regulation, Para 18.

and violations of privacy disputes[69] rather than in copyright infringements (the latter being governed by *lex loci protectionis* according to Article 8 Para 1 Rome II Regulation).

The mosaic principle is contrary to the principle of sound administration of justice. The mere fact that the information is accessible in every Member State leads to the risk of defendant to be sued in any of these States.

According to some authors, the mosaic principle indicates a degree of bias of the CJEU in favor of protecting the victim (especially in defamation cases)[70]. However, interests of the claimant and the defendant should be considered equally. The aim of the special jurisdictional rules in Art. 7 is not to protect the weaker party (as in the case of consumer or employment contracts)[71]. Their purpose is to offer alternative grounds of jurisdiction based on a close connection between the court and the action ("principle of proximity")[72]. This goal, however, is not ensured in case of 28 potential fora that the claimant might choose from. Additionally, in case of information available online, it is practically very difficult to establish the amount of damage that occurred within the relevant territory of the competent court. Due to the delocalized nature of the damage, the courts could decide only „in respect of a fraction of damage suffered, thereby depriving the court of an overall view of the damage, which could impede the global assessment of the context of the case of which that court is seized. The benefit afforded by the proximity of the court to the facts of the case thus disappears, and with it the usefulness of [Art. 7 Para 2 Brussels Ibis Regulation]"[73].

The mosaic principle leads to fragmentation of the claims within all the possible *forums*. Each court will be competent to decide about the damages limited to the national territory concerned. This, in the light of the Internet, is „difficult if not impossible to exercise"[74].

The mosaic principle leads to an issue of dissonance between the scope of the jurisdiction and the remedies sought (e.g. court injunction, preliminary measures)[75]. Courts that have jurisdiction to decide about territorially limited damages cannot decide about removal of information from the Internet. This can be done only once; it is not possible to remove only a part of infringing content. In other words, it limits the competent court in respect of types of remedies that it may issue. In copyright infringements cases the claimant usually claims for the material to be taken down. The question is whether the partially competent court should be also reflected at the level of partial competence to issue an injunction. Is it possible to ask the defendant to delete only a proportional part of the content? As AG Bobek clearly stated, „provided that a court of a Member State is competent to hear an extra-contractual/tortious action for damages, it should also be entitled to rule on issue of all the remedies that are available under national law [not only damages]"[76].

Moreover, each of the competent courts will decide on claims with the same object[77]. This could enhance the risk of irreconcilable judgments. The Brussels Ibis Regulation is based on the principle of procedure economy and harmonious administration of justice[78] that is ensured by rules on lis pendens (Arts. 29 to 34) and concentration of claims (Art. 8). Question is how could the lis pendens rules solve the situation if there is one proceeding claiming „full" damages (in courts of the illegal conduct that lead to the damage) and several proceedings claiming „partial" damages (territorially limited damages claimed in courts where the damage occurred)[79].

Another problematic question is the effect *res iudicata* in case of judgment awarding full amount of damages and its relationship to possible subsequent claim for damages under one or more of the partial jurisdictions[80].

The mosaic principle is contrary to the requirement of restrictive interpretation of special jurisdictional rules in the Brussels Ibis Regulation. In the author's opinion, the application of the mosaic principle in the context of Internet infringements is fruitless. The CJEU is trying to apply existing rules and their interpretation to online activity. The main objection to the mosaic principle is the multiplicity of *forums* it creates. The CJEU should have resorted to its former case law; in case there could be multiple possible *forums* or it could be difficult to establish them, it is necessary to refuse the application of special jurisdictional rules and „return" to the general jurisdictional rule based on the defendant's domicile[81].

[69] Conflict-of-law rules for non-contractual relationships are contained in Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007, on the law applicable to non-contractual obligations (Rome II Regulation). However, non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation are excluded from its scope (Art. 1 Para 2 letter g). The applicable law shall be determined according to the national private international law rules.

[70] *C. Vanleenhove*, The European…, p. 646.

[71] Bolagsupplysningen, Para 39; similarly in Opinion of AG Bobek in Bolagsupplysningen, Paras 61 to 69.

[72] Bolagsupplysningen, Para 39.

[73] Opinion of GA Villalón, Pez Hejduk, Para 44.

[74] Opinion of AG Bobek, Bolagsupplysningen, Para 80.

[75] Opinion of AG Bobek, Bolagsupplysningen, Para 123.

[76] Opinion of AG Bobek, Bolagsupplysningen, Para 129.

[77] *T. Lutzi*, Internet…, p. 695.

[78] Preamble to Brussels Ibis Regulation, Para 21.

[79] *Lis pendens* and related actions are regulated in Art. 30 et seq. Brussels Ibis Regulation. See also Preamble to Brussels Ibis Regulation, Para 21; *T. Lutzi*, Internet…, p. 695.

[80] Opinion of AG Bobek, Bolagsupplysningen, Para 82.

[81] The requirement of restrictive interpretation of special jurisdictional rules stems from, see e.g. Judgment of the Court of 19 February 2002. Besix SA v Wasserreinigungsbau Alfred Kretzschmar GmbH & Co. KG (WABAG) and Planungs- und Forschungsgesellschaft Dipl. Ing. W. Kretzschmar GmbH & KG (Plafog). Case C-256/00.

This decision dealt with the interpretation of Art. 7 Para 1 letter a) Brussels Ibis Regulation (jurisdiction for contractual relationships and criterion place of performance). Nevertheless, its conclusions are applicable also to Art. 7 Para 2. According to the CJEU, in case „where the place of performance of the obligation in question cannot be determined because it consists in an undertaking not to do something which is not subject to any geographical limit and is therefore characterized by a multiplicity of places of performance. In such a case, jurisdiction can be determined only by application of the general criterion laid down in the first paragraph of Article [4 of the Brussels Ibis Regulation]", [in:] Besix, Para 55.

As resulting from the aforementioned analysis the mosaic principle does not serve the legitimate interest of any party and is contrary to the objectives of predictability and sound administration of justice governing the Brussels Ibis Regulation[82].

Proposed *de lege ferenda* solutions instead of the mosaic principle

The mosaic principle in the context of the Internet is useless for both online defamation and online infringement of copyright law. The claimant will usually claim the full amount of damages in one court; there is no practical need for partial damages at several different courts.

There is a need for a criterion limiting the EU-wide jurisdiction which the CJEU created with the aforementioned case law. The aim of this article is not only to criticize the current status quo, but also present some ideas *de lege ferenda*. In the author's opinion the answer could be the judgment in *Bolagsupplysningen,* resp. the Opinion of AG Bobek.

In case of delocalized damage on the Internet caused by infringement of copyright the mosaic principle should be abolished. The CJEU should exclude the possibility to sue in the courts of the State where the damage occurred. The CJEU should limit jurisdiction under Art. 7 Para 2 Brussels Ibis Regulation only to the courts of the State, where the event giving rise to the damage occurred. This exclusion still allows the claimant to sue according to the Art. 4 Brussels Ibis Regulation, i.e. in the defendant's domicile (for full amount of damages). In most of infringement cases, both criteria (defendant's domicile and place, where the illegal conduct occurred) will lead to the same court[83]. As Lutzi pointed out: „Instead of bending and twisting the interpretation of these provisions until they can be applied to Internet cases, the approach […] would allow the courts to disregard these provisions altogether where their application would lead to results that cannot be justified by the considerations that underline them. Instead, one would naturally fall back to criteria that do not raise these difficulties – the place of acting in Article 7 (2), the place of establishment in Article 7 (5), or the domicile of the defendant"[84].

The main advantage of this solution would be for the claimant to be able to claim the whole damage at one place and would not be forced to initiate various proceedings in order to receive compensation for the same infringement which is almost impossible to be quantified.

Also, the claimant could sue at the place of his or her „center of interest". Admittedly, the „center of interest" criterion was created for an infringement of personality rights. However, as was stated before, personality rights and copyright share many similarities. Under the „center of interest" criterion the claimant is entitled to sue for full amount of damages, as would be the majority of cases in practice.

Conclusion

The mosaic principle under Art. 7 Para 2 Brussels Ibis Regulation brought many legal issues. Disregarding this principle will increase legal predictability and certainty determining jurisdiction in disputes arising out of non-contractual obligations in general, and copyright infringements in particular.

In the introductory part of this article several research questions were presented. Based on the above analysis it is possible to conclude that the interpretation of the CJEU in *eDate*, *Bolagsupplysningen***,** *Pinckney* and *Hejduk* is not in accordance with goals and principles governing Brussels Ibis Regulation. The CJEU did not consider the characteristics of the Internet and the mode of distribution and accessibility of the information online. The mosaic principle is contrary to the principle of legal certainty and predictability. It favors special jurisdictional rules before general rule and is detriment to both claimant and defendant.

The analysis in this article verified the working hypothesis: The mosaic approach used in Article 7 Para 2 Brussels Ibis Regulation is contrary to the principles of legal certainty and predictability for disputes arising out of non-contractual obligations on the Internet.

[82] Opinion of AG Bobek, Bolagsupplysningen, Para 90.
[83] Opinion of AG Villalón in Hejduk, Para 45.
[84] *T. Lutzi*, Internet…, p. 711.

Keywords: Jurisdiction, Brussels Ibis Regulation, non-contractual obligations, place of harmful event, center of interest, mosaic principle, defamation, infringement of personality rights, infringement of intellectual property rights, copyright, online, Internet, case law, Court of Justice of the EU, *Shevill, eDate, Bolagsupplysningen Pinckney*, *Hejduk*

WYMOGI EDYTORSKIE:

- język publikacji: polski, angielski, niemiecki, rosyjski;
- edytor tekstu Word (format .doc lub .docx);
- styl czcionki: Times New Roman;
- wielkość czcionki: tekst główny – 12 pkt, przypis – 10 pkt;
- interlinia: 1,5 wiersza (w przypadku przypisów – 1 wiersz);
- objętość artykułu: do 30 000 tys. znaków ze spacjami;
- marginesy: standardowe – wszystkie 2,5 cm;
- przypisy dolne: odsyłaczami przypisów powinny być cyfry arabskie; odsyłacz należy umieścić bezpośrednio po fragmencie, do którego odnosi się przypis (przed kropką kończącą zdanie);
- należy dołączyć słowa kluczowe w języku polskim i angielskim;
- tytuł powinien być napisany czcionką Times New Roman 14 pkt (czcionka pogrubiona);
- tekst powinien składać się z następujących części: lid (streszczenie ok. 1500 znaków ze spacjami), uwagi wstępne, rozwinięcie (z podziałem na zatytułowane części), podsumowanie;
- do artykułu należy załączyć także lid (streszczenie) w języku angielskim (ok. 1500 znaków ze spacjami);
- śródtytuły nie powinny być numerowane, lecz pogrubione;
- należy dołączyć notę biograficzną (ok. 800 znaków ze spacjami);
- prosimy o wskazanie afiliacji.

Powoływane w przypisach pozycje bibliograficzne prosimy pisać według wzoru:

Inicjał. Nazwisko, Tytuł, ew. numer wydania, tom, część itp., miejsce i rok wydania, a następnie cytowane strony skrótem „s.", np.: *J. Kowalski*, Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku kolejnego powołania się **bezpośrednio** na cytowaną pozycję:

Ibidem, s. 15–16.

Powołanie kolejny raz, gdy cytujemy tylko jedną pozycję danego autora:

J. Kowalski, *op. cit*., s. 29–20.

Kolejne powołanie, gdy cytuje się kilka pozycji danego autora, zawiera pierwsze wyrazy tytułu, np.:

J. Kowalski, Jak pisać..., s. 28–29.

W przypadku **prac pod redakcją**, jeśli powoływana publikacja stanowi część całości:

P. Igrek, Cytowanie, [w:] *J. Kowalski* (red.), Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku publikacji w czasopismach tytuł czasopisma zastępuje nazwę wydawnictwa, po nim następuje rok (rocznik), przecinek, następnie numer (nr) w ramach rocznika ewentualnie także numer od początku wydawania pisma i numer strony:

J. Kowalski, Jak pisać przypisy?, Wiadomości Tekściarskie 2006, Nr 28 (236), s. 7.

Kilka kwestii specjalistycznych:

1. Oczekiwane oznaczenie ustawy wygląda następująco: Dz.U. z 2006 r. Nr 28, poz. 456.
2. Publikator prosimy podawać jedynie przy pierwszym przywołaniu aktu prawnego. Wówczas nazwę aktu i datę (miesiąc słownie) podajemy w tekście głównym (np. ustawa z 13.4.2003 r. o zasadach pisania artykułów), w przypisie zaś publikator (np. t.j. Dz.U. z 2006 r. Nr 28, poz. 456).
3. Zapisując artykuł, ustęp, punkt aktu prawnego, skrótów nie oddzielamy przecinkami, tak więc: art. 28 ust. 59 pkt (bez kropki!) 36, a nie: art. 28, ust. 59, pkt. 36.
4. W przypadku orzeczeń sądowych prosimy o zastosowanie następujących oznaczeń: Wyrok SN z 11.5.2011 r., I CA 123/11, OSNCP 2011, Nr 8, poz. 34. Nazwę orzeczenia i jego datę prosimy podać w tekście głównym (np. wyrok SN z 11.5.2011 r.), natomiast w przypisie publikator (I CA 123/11, OSNCP 2011, Nr 8, poz. 34).

Harmonogram publikacji:

Nr 1 – teksty do końca stycznia, druk luty/marzec
Nr 2 – teksty do końca kwietnia, druk maj/czerwiec
Nr 3 – teksty do końca lipca, druk sierpień/wrzesień
Nr 4 – teksty do końca października, druk listopad/grudzień

Osoba do kontaktu: dr *Aleksandra Klich*, e-mail: pme@beck.pl

EDITORIAL REQUIREMENTS:

- language of publication: Polish, English, German, Russian;
- text editor MS Word (.doc or .docx);
- font style: Times New Roman;
- font size: main text – 12 pts, footnote – 10 pts;
- line spacing: 1.5 line (for footnotes – 1 row);
- volume of the article: up to 30,000 characters with spaces;
- margins: standard – all 2.5 cm;
- footnotes: cross-referenced footnotes should be Arabic numerals; reference should be placed immediately after the passage to which the footnote regards (before the full stop ending a sentence);
- article must be attached with key words in Polish and English;
- the title should be written in Times New Roman 14 pts (bold);
- text should consist of following parts: lead (summary, around 1500 characters with spaces), initial comments, amplification (with a division into parts with titles), summation;
- article should also be attached with a lead (summary) in English (around 1500 characters with spaces);
- intertitles should not be numbered, but bold;
- article must be attached with a biographical note (approx. 800 characters including spaces);
- please indicate affiliation.

The referenced sources should adhere to the following style:

Initial(s). Last name, Title, edition number if applicable, volume, part, etc., place and year of publication, followed by the page(s) referred to with the 'p. (pp.)' abbreviation, e.g.: *J. Kowalski*, How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For subsequent reference made **directly** to the cited item:

Ibidem, p. 15–16.

Further reference, when several positions by a given author are being cited, include the first words of the title, e.g.:

J. Kowalski, How to..., p. 28–29.

For edited volumes, when the publication referenced forms a part of the whole:

P. Igrek, Citing, [in:] *J. Kowalski* (ed.), How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For publications in periodicals, the title of the periodical replaces the name of the publisher, followed by the year, comma, then the number (No.) within the year, possibly the consecutive number and page numbers:

J. Kowalski, How to do references?, Editorial news 2006, No. 28 (236) p. 7.

A few technical issues:

a. Expected indication of a legal act goes as follows: Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April on the rules of writing articles), and the publishing body shall be given in the footnote (e.g. Journal of Laws of 2006, No. 28, item 456).
b. When writing article, paragraph, point of a legal act, abbreviations should not be separated by commas, that is: art. 28 par. 59 point (no full stop!) 36, not: art. 28, par. 59, pt. 36).
c. For court judgements, please use the following indications: Judgement of the Supreme Court of 11.5.2011, I CA 123/11, OSNCP 2011, No. 8, item 34. Mind that the appelative of the judgement and its date should be indicated in the main text (e.g. Judgement of the Supreme Court of 11.5.2011), and the publishing body in the footnote (I CA 123/11, OSNCP 2011, No. 8, item 34).

Publication schedule (deadlines):

No. 1 – submitting manuscripts – end of January (print – February/March)
No. 2 – submitting manuscripts – end of April (print – May/June)
No. 3 – submitting manuscripts – end of July (print – August/September)
No. 4 – submitting manuscripts – end of October (print – November/December)

Contact Person: *Aleksandra Klich* PhD, e-mail: pme@beck.pl