SERIA PRAWO, NR 8 2022 (10)

OPINIE i ANALIZY

INSTYTUTU DE REPUBLICA

Rekomendacje dotyczące oceny dowodów elektronicznych w postępowaniach cywilnych i administracyjnych, ze szczególnym uwzględnieniem *blockchain* oraz *cloud computing*

DR HAB. MAREK ŚWIERCZYŃSKI, PROF. UCZ.
DR ZBIGNIEW WIĘCKOWSKI

INSTYTUT
De Republica

PRAWO

SERIA WYDAWNICZA „OPINIE I ANALIZY IDR" NR 10

OPINIE i ANALIZY

INSTYTUTU DE REPUBLICA

Rekomendacje dotyczące oceny dowodów elektronicznych w postępowaniach cywilnych i administracyjnych, ze szczególnym uwzględnieniem *blockchain* oraz *cloud computing*

DR HAB. MAREK ŚWIERCZYŃSKI, PROF. UCZ.
DR ZBIGNIEW WIĘCKOWSKI

INSTYTUT De Republica

SERIA PRAWO, NR 8 2022 (10)

Redakcja serii
dr hab. Bogumił Szmulik, prof. ucz.
dr Magdalena Maksymiuk
mgr Łukasz Gołąb

ISBN 978-83-67253-05-5 (online)

Wydawca
Instytut De Republica
ul. Belwederska 23 lok.1
00-761 Warszawa
+48 22 295 07 29
e-mail: instytut@iderepublica.pl
www.iderepublica.pl

Spis treści

Rekomendacje dotyczące oceny dowodów elektronicznych w postępowaniach cywilnych i administracyjnych, ze szczególnym uwzględnieniem *blockchain* oraz *cloud computing*

dr hab. Marek Świerczyński, prof. ucz.
dr Zbigniew Więckowski

Streszczenie

Wytyczne Rady Europy w sprawie dowodów elektronicznych w postępowaniu cywilnym i administracyjnym przyjęte zostały przez Komitet Ministrów Rady Europy 30 stycznia 2019 roku. Projekt wytycznych został opracowany przez Komitet Rady Europy – European Committee on Legal Co-operation (CDCJ). Celem wytycznych jest dostarczenie praktycznych wskazówek sądom i innym właściwym organom pełniącym funkcje orzecznicze, specjalistom, w tym prawnikom, oraz stronom postępowania w zakresie postępowania z dowodami elektronicznymi w postępowaniu cywilnym i administracyjnym. Wytyczne dotyczą między innymi zeznań ustnych składanych za pośrednictwem zdalnego łącza, wykorzystania, gromadzenia, przechowywania i archiwizacji dowodów elektronicznych.

Słowa kluczowe

dowody elektroniczne, metadane, blockchain, cloud computing

I. Przedmiot opinii

Przedmiotem rekomendacji jest analiza przyjętych 30 stycznia 2019 roku przez Komitet Ministrów Rady Europy wytycznych Rady Europy w sprawie dowodów elektronicznych w postępowaniach cywilnych i administracyjnych (wytyczne CDCJ). Celem wytycznych CDCJ jest dostarczenie państwom członkowskim praktycznych wskazówek w zakresie wykorzystania dowodów elektronicznych w postępowaniach cywilnych i administracyjnych.

Struktura dokumentu jest następująca. Uwagi wprowadzające (wstęp) zawarte zostały w pkt 4.1. Wnioski i rekomendacje zawarte w pkt III pełnią funkcję zakończenia przeprowadzonej analizy. Poszczególne zagadnienia prawne dotyczące dowodów elektronicznych zostały przedstawione w pkt 4.2 – 4.10. Poszczególne problemy zostały omówione przy uwzględnieniu stanowiska Rady Europy wyrażonego w wytycznych CDCJ.

Przedstawiona opinia ma na celu poprawę dostępu do wymiaru sprawiedliwości w dobie intensywnego rozwoju technologii informatycznych.

II. Stosowane skróty, źródła prawa oraz dokumenty europejskie

2.1. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz.U. 1993 nr 61 poz. 284, dalej jako Konwencja).

2.2. Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. 2003 nr 3 poz. 25, dalej jako Konwencja 108 lub w wersji zmodernizowanej jako Konwencja 108+).

2.3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. U. UE L 257 z 28. 8. 2014 r., s. 73–114, dalej jako Rozporządzenie eIDAS).

2.4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.E. L 119, 4. 5. 2016, s. 1–88, dalej jako RODO).

2.5. Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (CM(2018)169-add1final) and their Explanatory Memorandum (CM(2018)169-add2), dostępne na stronie https://www.coe.int/en/web/cdcj/activities/digital-evidence, dalej jako wytyczne CDCJ).

III. Główne rekomendacje

3.1. Wytyczne CDCJ porządkują terminologię prawniczą w zakresie dowodów elektronicznych. W dokumencie zdefiniowano pojęcie dowodu elektronicznego, metadanych oraz usług zaufania. Z uwagi na stały rozwój technologiczny, w wytycznych przyjęto szeroką definicję „dowodów elektronicznych".

3.2. Przy najbliższej rewizji wytycznych CDCJ wskazane jest zdefiniowanie pojęć: *blockchain* oraz *cloud computing*, z uwagi na ich ścisły związek z dowodami elektronicznymi oraz coraz większe znaczenie w obrocie prawnym.

3.3. Wytyczne CDCJ służą zwiększeniu zaufania sędziów i innych przedstawicieli zawodów prawniczych w odniesieniu do wykorzystania technologii informatycznych opartych na chmurze obliczeniowej (*cloud computing*).

3.4. Technologia *blockchain* służy skutecznemu zabezpieczaniu dowodów elektronicznych. Uniemożliwia modyfikację danych. *Blockchain* nadaje się do celów dowodowych, np. w zakresie sporów związanych z naruszaniem praw własności intelektualnej.

3.5. Rekomendujemy przyjęcie w zrewidowanych wytycznych CDCJ następującej definicji *blockchain*: „sekwencja bloków z informacją o operacjach wykonywanych w systemie zbudowanym na podstawie algorytmów zapisany w rozproszonym, zdecentralizowanym systemie informatycznym z wykorzystaniem kryptograficznych metod ochrony informacji".

3.6. Podejmując się oceny dowodów elektronicznych należy kierować się trzema głównymi zasadami przedstawionymi w wytycznych CDCJ: a) do roli sądu należy określenie znaczenia danego dowodu elektronicznego (w szczególności decyzja ta nie powinna być przerzucana na biegłego z zakresu technologii informatycznych), b) zasada neutralności dowodów elektronicznych oznacza brak ich dyskryminacji, jak też uprzywilejowania wobec innych środków dowodowych, c) strony powinny być równorzędnie traktowane, oznacza to między innymi zapewnienie możliwości zakwestionowania autentyczności dowodu elektronicznego.

3.7. Stosowane przez sądy metody przesłuchania świadków w trakcie rozprawy zdalnej powinny zabezpieczać przekaz obrazu lub dźwięku przed utratą danych, zniekształceniem lub nieuprawnionym ujawnieniem. Na tyle, na ile jest to technicznie możliwe, dowód na odległość powinien być przeprowadzany w taki sam sposób, w jaki przeprowadza się go w sądzie.

3.8. W przypadku gdy zeznanie wymaga zachowania poufności, konieczne jest zastosowanie środków lub rozwiązań technicznych ograniczających dostęp wyłącznie do osób uprawnionych. Ze względów bezpieczeństwa, stosowane systemy łączności, zarówno publiczne, jak i prywatne, powinny zapewniać szyfrowanie sygnału wideo w celu ochrony przed jego przechwyceniem, przez osoby nieuprawnione.

3.9. Dowody elektroniczne powinny być przedstawiane w ich oryginalnej postaci. W przypadku złożenia wydruku dowodu elektronicznego, sąd może zarządzić, na wniosek strony lub z własnej inicjatywy, dostarczenie oryginału dowodu elektronicznego. Metadane występujące w oryginalnej (cyfrowej) wersji dowodu elektronicznego mogą zapewnić kontekst niezbędny do właściwej oceny dowodu. Sądy powinny być świadome potencjalnej wartości dowodowej metadanych.

3.10. Wytyczne CDCJ odwołują się do dorobku unijnego, w szczególności rozporządzenia eIDAS, w odniesieniu do podpisów elektronicznych. Sądy powinny uwzględniać fakt wykorzystania w obrocie różnych rodzajów podpisów elektronicznych oraz ich odmiennej wartości dowodowej.

3.11. Sądy powinny kierować się wytycznymi CDCJ w zakresie procedur zarządzania procesem zbierania, przechowywania oraz archiwizacji dowodów elektronicznych. Dowody elektroniczne wymagają szczególnych środków ostrożności, ze względu na łatwość ich zmiany, uszkodzenia lub zniszczenia w wyniku niewłaściwego obchodzenia się z nimi.

3.12. Gromadzenie i przechowywanie dowodów elektronicznych wymaga od państw członkowskich Rady Europy przyjęcia specjalnych narzędzi i procedur w celu zapewnienia ich integralności, poufności oraz bezpieczeństwa.

3.13. W przypadku dowodów elektronicznych zwiększa się ryzyko generowania niepotrzebnej ilości danych, ze względu na łatwość ich pozyskania. Powyższe może utrudnić postępowanie dowodowe lub nawet uniemożliwić skuteczne jej przeprowadzenie. Aktywne zarządzanie danymi elektronicznymi przez sąd powinno odbywać się z poszanowaniem zasady proporcjonalności.

3.14. Sądy powinny przyjąć proaktywne podejście do ochrony integralności dowodów elektronicznych przed cyberzagrożeniami, w tym przed ich uszkodzeniem lub nieuprawnionym dostępem. Nieuprawnione osoby nie powinny mieć dostępu do dowodów elektronicznych. Przechowywane dowody elektroniczne mogą być powiązane ze znormalizowanymi metadanymi. W zakresie archiwizacji dowodów elektronicznych

aktualność zachowuje zalecenie Komitetu Ministrów Rady Europy w sprawie archiwizacji dokumentów elektronicznych w sektorze prawnym (Rec(2003)15).

3.15. Wytyczne CDCJ regulują migrację danych polegającą na zmianie nośnika pamięci w celu zachowania dostępności do dowodów elektronicznych. Zaniedbanie migracji może skutkować brakiem możliwości odczytania danych. Rekomendowanym rozwiązaniem jest migrowanie danych przy wykorzystaniu rozwiązań sieciowych, takich jak chmury obliczeniowe (*cloud computing*), które są stale udoskonalane wraz z postępem technologicznym.

3.16. Zaleca się, aby przy transgranicznym przeprowadzaniu dowodów elektronicznych, sądy ściśle współpracowały w tej kwestii, uwzględniając dotychczasowy dorobek unijnych rozporządzeń w tym zakresie.

3.17. Optymalizację procesu przekazywania dowodów elektronicznych za pomocą środków elektronicznych można osiągnąć poprzez wdrożenie wspólnych standardów technicznych i formatów plików oraz poprzez cyfryzację krajowych systemów sądowych i administracyjnych.

3.18. Wiedza dotycząca dowodów elektronicznych powinna być propagowana wśród sędziów oraz innych przedstawicieli zawodów prawniczych.

IV. Analiza prawna

4.1. Uwagi ogólne (wstęp)

4.1.1. Pandemia COVID-19 jest ogromnym wyzwaniem medycznym i logistycznym, o skali dotychczas niespotykanej we współczesnej historii świata. Stanowi moment przełomowy, którego konsekwencje trudno dziś przewidzieć. Przynosi zmiany w wielu obszarach naszego życia. Wśród negatywnych konsekwencji okresu pandemicznego, jak między innymi ból i śmierć bliskich osób, osamotnienie, zaburzenia psychiczne związane z izolacją, ograniczenia w swobodnym prowadzeniu działalności gospodarczej, na plan pierwszy wysuwa się co najmniej jeden obszar, którego rozwój obecna sytuacja wyłącznie wzmocniła, a jest nim sfera szeroko rozumianych nowych technologii informatycznych. Wymóg dystansu społecznego, izolacji, ograniczenia kontaktów towarzyskich wymusza szersze wykorzystanie technologii cyfrowych w społeczeństwie. Nauka zdalna, praca zdalna, korzystanie z dóbr kultury w sposób zdalny to przykłady aktywności, które choć znane były przed wybuchem pandemii, to jednak ich zasięg nie był tak powszechny, jak obecnie.

4.1.2. Pandemia COVID-19 wymusiła zmiany także w obszarze wymiaru sprawiedliwości, kiedy bardziej niż kiedykolwiek wcześniej konieczne stało się wykorzystywanie nowych narzędzi i metod przetwarzania oraz zarządzania dowodami elektronicznymi. Na szczególną uwagę zasługują wytyczne Rady Europy w sprawie dowodów elektronicznych w postępowaniu cywilnym i administracyjnym przyjęte przez Komitet Ministrów Rady Europy niespełna rok przed wybuchem pandemii w Europie, tj. 30 stycznia 2019 roku. Celem wytycznych jest dostarczenie praktycznych wskazówek dotyczących posługiwania się dowodami elektronicznymi w postępowaniach cywilnych i administracyjnych, sądom i innym właściwym organom pełniącym funkcje orzecznicze, specjalistom, w tym prawnikom, oraz stronom postępowania. Wytyczne dotyczą zeznań składanych zdalnie, zasad wykorzystania dowodów elektronicznych, gromadzenia, przejmowania i przekazywania dowodów, znaczenia, wiarygodności, przechowywania i zabezpieczania, archiwizacji, a także

podnoszenia świadomości społecznej w zakresie znaczenia dowodów elektronicznych oraz potrzeby przeprowadzenia szkoleń z tego zakresu w państwach członkowskich.

4.1.3. Wytyczne są pierwszym tego typu instrumentem o charakterze międzynarodowym, przygotowanym z myślą o wsparciu 47 państw członkowskich Rady Europy w dostosowaniu wymiaru sprawiedliwości do problematyki dowodów elektronicznych w postępowaniach cywilnych i administracyjnych. Przyjęte wytyczne stanowią ważny etap w procesie dostosowywania wymiaru sprawiedliwości do informatycznej rewolucji w wymiarze sprawiedliwości.

4.1.4. Zaletą wytycznych CDCJ jest ich przyjęcie w formie „prawa miękkiego" (*soft-law*). Narzucanie wiążących rozwiązań państwom członkowskim mogłyby skończyć się niepowodzeniem. To do państw członkowskich zależy czy i w jaki sposób wytyczne zostaną wdrożone w ich systemach prawnych.

4.1.5. CDCJ przygotował nie tylko tekst wytycznych, ale także *Explanatory Memorandum*, pełniący funkcję oficjalnego komentarza do wytycznych, w którym bardziej szczegółowo przedstawiono możliwości i warunki posługiwania się dowodami elektronicznymi w postępowaniach cywilnych i administracyjnych.

4.1.6. Uwzględniając specyfikę wszelkiego rodzaju aktów o charakterze międzynarodowym, zakładającym z samej swojej istoty konieczność osiągania licznych kompromisów, przyjęty tekst wytycznych należy ocenić pozytywnie. Dokument nie jest wolny od wad i niedociągnięć, istnieje jednak możliwość ich usunięcia na etapie rewizji wytycznych w przyszłości. Na ten moment, nie tylko przyjęcie dokumentu przez Radę Europy należy uznać za sukces tej organizacji, ale na uznanie zasługuje także przyjęta formuła instrumentu (*soft law*), która daje możliwość elastycznego dostosowania się państw członkowskich. Uwzględniono różnice w systemach prawnych państw członkowskich. Celem wytycznych nie jest ustanowienie wiążących norm prawnych (te pojawiłyby w przypadku przyjęcia konwencji) oraz harmonizacji ustawodawstw państw członkowskich, lecz przekazanie praktycznych wskazówek mających na celu wzmocnienie skuteczności i jakości wymiaru sprawiedliwości w obszarze dowodów elektronicznych. Wytyczne mogą być stosowane tylko w zakresie, w jakim nie są one sprzeczne z ustawodawstwem krajowym.

4.1.7. Jak wspomnieliśmy, do chwili obecnej istnieje niewiele norm na poziomie prawa międzynarodowego, europejskiego czy krajowego dotyczących dowodów elektronicznych. Z drugiej strony, co jest także jedną z konsekwencji pandemii, sądy są coraz częściej konfrontowane z koniecznością zajmowania się dowodami elektronicznymi. Tego typu dowody różnią się pod wieloma względami od dotychczas znanych rodzajów dowodów (potencjalna wartość dowodowa metadanych; łatwość, z jaką dowody elektroniczne mogą podlegać manipulacji i zniekształcaniu; udział podmiotów trzecich w gromadzeniu i archiwizacji dowodów elektronicznych, np. usługodawców

internetowych). W związku z tym istnieje uzasadniona potrzeba nie tylko poszerzania wiedzy na temat dowodów elektronicznych, lecz także zmiany przyjętego sposobu postępowania z nimi w postępowaniach cywilnych i administracyjnych.

4.2. Rekomendacje dotyczące terminologii w zakresie dowodów elektronicznych

4.2.1. W wytycznych CDCJ zdefiniowano kluczowe pojęcia, takie jak dowody elektroniczne, metadane oraz usługi zaufania. Za właściwe należy uznać również zdefiniowanie w zrewidowanej wersji wytycznych co najmniej dwóch dodatkowych pojęć: *blockchain* oraz *cloud computing*, ze względu na ich ścisły związek z dowodami elektronicznymi.

4.2.2. Z uwagi na stały rozwój technologiczny, w wytycznych przyjęto szeroką definicję „dow odów elektronicznych". Mogą przybierać one formę tekstu (e-mail, SMS), wideo, fotografii lub nagrań audio. Dane mogą pochodzić z różnych nośników lub metod dostępu, takich jak telefony komórkowe, strony internetowe, komputery pokładowe lub rejestratory GPS, w tym dane przechowywane w chmurze obliczeniowej.

4.2.3. Metadane oznaczają dane o innych danych (np. data i godzina utworzenia lub modyfikacji pliku lub dokumentu, data i godzina wysłania danych). Metadane zazwyczaj nie są bezpośrednio dostępne użytkownikom i wymagają podjęcia dodatkowych działań w celu ich ujawnienia.

4.2.4. Usługi zaufania pełnią ważną rolę w identyfikacji, uwierzytelnianiu i bezpieczeństwie obrotu elektronicznego. W wytycznych przyjęto definicję „usługi zaufania" sformułowaną w art. 3 pkt. 16 rozporządzenia eIDAS, tj. usługę elektroniczną świadczoną zazwyczaj za wynagrodzeniem i obejmującą tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

4.2.5. W przyjętej wersji wytycznych, nie pojawiły się definicje chmury obliczeniowej (*cloud computing*) oraz *blockchain,* i to pomimo prowadzonych w ramach CDCJ dyskusji na temat konieczności ich wprowadzenia. Ostatecznie do obu pojęć odpowiednie odwołanie znajdziemy jedynie w *Explanatory Memorandum*.

4.2.6. W zakresie *cloud computing* poruszony został wątek współdzielenia danych (chmury) czyli przechowywania określonych danych na różnych serwerach, które mogą znajdować się w różnych lokalizacjach fizycznych (powszechna technika bezpieczeństwa). Globalny charakter Internetu i rosnące znaczenie usług w chmurze obliczeniowej

sprawiają, że coraz trudniej jest zakładać, że dostęp do danych ma charakter ściśle krajowy. Potrzeba wzrostu świadomości i zaufania wśród sędziów i innych przedstawicieli zawodów prawniczych dla przechowywania dowodów elektronicznych w chmurach obliczeniowych. Należy zachęcać do bezpośredniej współpracy między sądami a dostawcami usług zaufania. Przy wyborze dostawcy należy brać pod uwagę takie czynniki, jak miejsce siedziby dostawcy usług, miejsce, w którym dane są przetwarzane oraz istnienie lokalnych przepisów regulujących dostęp do danych.

4.2.7. Technologię *blockchain* można zdefiniować jako księgę rozproszoną, która odnosi się do listy zapisów (bloków), które są ze sobą powiązane oraz zabezpieczone za pomocą kryptografii, w zdecentralizowanej sieci *peer-to-peer*. Funkcjonalność *blockchain* powoduje, że zapis cyfrowy jest odporny na modyfikację danych. Dane występujące w danym bloku nie mogą zostać zmienione wstecznie bez zmiany wszystkich kolejnych bloków, co wymaga zgody większości sieci. Dzięki temu *blockchain* nadaje się do celów dowodowych. Na przykład w § 1913 Vermont Rules of Evidence (USA) stwierdzono, że: „(1) Zapis cyfrowy zarejestrowany elektronicznie w blockchainie ma charakter samouwierzytelniający się zgodnie z Vermont Rule of Evidence 902, jeśli towarzyszy mu pisemne oświadczenie wykwalifikowanej osoby, złożone pod przysięgą, stwierdzające kwalifikacje osoby do złożenia poświadczenia oraz: (a) datę i godzinę wprowadzenia rekordu do blockchain; (b) datę i godzinę odebrania rekordu z blockchain; (c) potwierdzenie, że zapis był utrzymywany w blockchainie w ramach regularnie prowadzonej działalności". W Chinach, w wyroku z dnia 28 czerwca 2018 r., Sąd Internetowy w Hangzhou orzekł, że w rozpatrywanej przez niego sprawie (spór dotyczący własności intelektualnej) dane przechowywane na platformie *blockchain* były na tyle wiarygodne i wolne od zniekształcenia, że można było się na nich oprzeć i zostały zaakceptowane przez sąd jako wiarygodny dowód w prowadzonej sprawie.

4.2.8. Zdefiniowanie *blockchain* w tekście wytycznych okazało się zbyt dużym wyzwaniem dla CDCJ. Uważamy, że przy okazji rewizji wytycznych można wykorzystać definicję *blockchain* zaproponowaną w polskiej literaturze przez D. Szostka: „sekwencja bloków z informacją o operacjach wykonywanych w systemie zbudowanym na podstawie algorytmów zapisany w rozproszonym, zdecentralizowanym systemie informatycznym z wykorzystaniem kryptograficznych metod ochrony informacji"[1].

[1] D. Szostek, *Blockchain a prawo*, Warszawa 2018, s. 42.

4.3. Rekomendacje dotyczące głównych zasad postępowania z dowodami elektronicznymi

4.3.1. Przy formułowaniu głównych zasad postępowania z dowodami elektronicznymi należy kierować się trzema głównymi zasadami określonymi w wytycznych CDCJ.

1) Do decyzji sądu powinna należeć ocena wartości dowodowej danego dowodu elektronicznego.
2) Zasada neutralności dowodów elektronicznych oznacza z jednej strony brak dyskryminacji, a z drugiej uprzywilejowania dowodów elektronicznych w postępowaniach sądowych[2].
3) Wymóg równego traktowania stron postępowania w odniesieniu do dowodów elektronicznych oznacza w szczególności umożliwienie stronie zakwestionowania autentyczności danego dowodu elektronicznego[3].

4.4. Rekomendacje dotyczące zdalnych przesłuchań

4.4.1. Dowody ustne składane za pośrednictwem łącza zdalnego (nie obejmuje to uprzednio nagranych dowodów ustnych), uznawane są za dowód elektroniczny w świetle wytycznych CDCJ. Odnosi się to do dowodów ustnych składanych przy wykorzystaniu platformy wideokonferencyjnej (umożliwiającej transmisję zsynchronizowanego obrazu i dźwięku w czasie rzeczywistym). W wytycznych podkreślono, że nie wszystkie dowody ustne mogą być przeprowadzane za pośrednictwem łącza zdalnego. Może bowiem pojawić się konieczność stacjonarnego odebrania zeznań świadka i konieczność obserwacji jego zachowania podczas przesłuchania. Wadą połączenia zdalnego jest to, że niektórych reakcji świadka (w ramach komunikacji niewerbalnej) nie można w pełni zaobserwować. Ważne jest, aby sędziowie, prawnicy oraz personel pomocniczy byli świadomi możliwych różnic pomiędzy zeznaniami złożonymi osobiście, a zeznaniami składanymi na odległość.

4.4.2. W przypadku gdy zeznanie wymaga zachowania poufności, konieczne jest zastosowanie środków lub rozwiązań technicznych ograniczających dostęp wyłącznie dla osób

[2] „Chociaż art. 6 Konwencji gwarantuje prawo do rzetelnego procesu sądowego, nie określa on żadnych zasad dotyczących dopuszczalności dowodów lub sposobu ich oceny, które są zatem przede wszystkim kwestiami do uregulowania przez prawo krajowe i sądów krajowych". (zob. García Ruiz przeciwko Hiszpanii, nr 30544/96, paragraf 28).

[3] „Zasada równości stron [...] oznacza, że każda strona musi mieć zapewnioną rozsądną możliwość przedstawienia swojej sprawy – w tym swoich dowodów – w warunkach, które nie stawiają jej w znacząco niekorzystnej sytuacji w stosunku do jego przeciwnika." (zob. Letinčić przeciwko Chorwacji, nr 7183/11, pkt 48).

uprawnionych. Urządzenia zapewniające integralność przekazu telekomunikacyjnego zapewnią sądowi i stronom odpowiednią możliwość zdalnego przesłuchania świadka.

4.4.3. Wytyczne wymagają zwrócenia uwagi, aby zastosowana technologia umożliwiała zadawanie pytań w trakcie składania zeznań przez świadka (jeżeli przepisy proceduralne tak stanowią), zwłaszcza gdy dowód ma zasadnicze znaczenie dla rozstrzygnięcia sprawy. Wymóg ten nie może być spełniony, gdy transmisja jest zniekształcona z powodu słabej łączności lub gdy dostęp stron do środków technicznych jest ograniczony. Może to dawać niesprawiedliwą przewagę jednej ze stron. Na tyle, na ile jest to technicznie możliwe, dowód na odległość powinien być przeprowadzany w taki sam sposób, w jaki przeprowadza się go w sądzie.

4.4.4. Stosowane metody powinny odpowiednio zabezpieczać przekaz obrazu lub dźwięku przed utratą, zniekształceniem lub nieuprawnionym ujawnieniem. Sąd może sprawdzić tożsamość osoby składającej zeznanie, żądając od niej okazania odpowiedniego dokumentu, takiego jak ważny dowód osobisty, paszport lub prawo jazdy. Stosowanym w niektórych państwach rozwiązaniem jest łączenie ze świadkiem przy pomocy kontrolowanego połączenia, po poprawnej weryfikacji udzielonych odpowiedzi. Ewentualnie, połączenie byłoby możliwe poprzez weryfikację danych przez stronę internetową banku, w którym rachunek prowadzi dana osoba.

4.4.5. Ze względów bezpieczeństwa, stosowane systemy łączności, zarówno publiczne, jak i prywatne, powinny zapewniać co najmniej szyfrowanie sygnału wideo w celu ochrony przed przechwyceniem. Zgodnie z wytycznymi, możliwe jest otrzymanie dowodów za pośrednictwem połączenia prywatnego, jeżeli zezwala na to prawo krajowe, pod warunkiem, że zastosowane rozwiązania zapewniają wystarczające bezpieczeństwo techniczne i są zgodne z zabezpieczeniami proceduralnymi. Połączenie prywatne oznacza system łączności który nie jest oficjalnym, rządowym systemem stworzonym specjalnie w celu przeprowadzania dowodów w sądzie. Rekomendujemy, aby dowody elektroniczne były wgrywane do zabezpieczonego serwera danego sądu.

4.5. Rekomendacje dotyczące formatu dowodów elektronicznych

4.5.1. Dowody elektroniczne powinny być przedstawiane sądowi przez strony w ich oryginalnym formacie. W przypadku złożenia wydruku dowodu elektronicznego, sąd może zarządzić, na wniosek strony lub z własnej inicjatywy, dostarczenie oryginału dowodu elektronicznego przez właściwą osobę. Dane geolokalizacyjne są przykładem dowodu, który może mieć istotne znaczenie dla rozstrzygnięcia sprawy, pod warunkiem, że są one przedstawione w wersji oryginalnej – cyfrowej. Dostarczanie

wydruków dynamicznych stron internetowych czy transkrypcji głosowych nie jest zbieżne z naturą dowodów elektronicznych, które dostarczają między innymi tak cenne dane jakimi są metadane. Metadane zapewniają kontekst niezbędny do oceny dowodu (danych), a sądy powinny być świadome ich potencjalnej wartości dowodowej. Można je wykorzystać do prześledzenia i zidentyfikowania źródła i celu komunikacji, danych dotyczących urządzenia, które wygenerowało dowód elektroniczny, daty, godziny, czasu trwania i rodzaju połączenia. Metadane mogą być istotne jako dowody pośrednie (takie jak wskazanie najbardziej odpowiedniej wersji dokumentu) lub jako dowody bezpośrednie (np. dokument w formie pliku).

4.5.2. Postulat akceptowania wyłącznie plików w ich oryginalnym formacie, uzasadniony jest między innymi tym, że wydrukami dowodów elektronicznych można łatwo manipulować. Wydruk ekranu z przeglądarki internetowej nie jest wiarygodnym dowodem, ponieważ nie jest niczym innym jak kopią ekranu. Można go zmodyfikować w bardzo prosty sposób, ponieważ nie potrzeba do tego żadnego specjalnego oprogramowania ani sprzętu.

4.6. Rekomendacje dotyczące podpisów elektronicznych

4.6.1. W zakresie różnych rodzajów podpisów elektronicznych, wytyczne słusznie odwołują się do dorobku unijnego, w szczególności rozporządzenia eIDAS. „Zaawansowany podpis elektroniczny" oznacza podpis elektroniczny, który spełnia wymogi art. 26 rozporządzenia eIDAS. „Kwalifikowany podpis elektroniczny" oznacza zaawansowany podpis elektroniczny, który został złożony za pomocą specjalnego urządzenia przeznaczonego do tego celu, czyli posiadający „kwalifikowany certyfikat podpisu elektronicznego", tj. certyfikat wydany przez osobę fizyczną lub prawną, która świadczy jedną lub więcej kwalifikowanych usług zaufania („dostawca kwalifikowanych usług zaufania") i która jest do tego upoważniona przez właściwy organ nadzorczy.

4.6.2. Obecnie większość dowodów elektronicznych pozbawiona jest zaawansowanego lub kwalifikowanego podpisu elektronicznego i nie jest zabezpieczona w żaden inny sposób. Powinny one jednak być uznawane przez sądy za dowody elektroniczne (przy czym wartość dowodowa tych dowodów może być różna w zależności od konkretnego przypadku), biorąc pod uwagę na przykład różnorodne usługi zaufania związane z elektronicznym zarządzaniem dokumentami i identyfikacji sygnatariuszy, które są dostępne na całym świecie. Jednym z przykładów jest podpis biometryczny, czyli metoda uzyskiwania elektronicznej wersji podpisu własnoręcznego, w której osoba składa swój podpis na urządzeniu elektronicznym za pomocą specjalnego rysika

i podkładki. W zależności od obowiązującego prawa, sąd może uznać taki podpis biometryczny za równoważny z podpisem własnoręcznym.

4.7. Rekomendacje dotyczące gromadzenia, przechowywania i archiwizacji dowodów elektronicznych

4.7.1. Wytyczne CDCJ odnoszą się także do tak istotnej, szczególnie w kontekście konieczności powtórnego skorzystania z dowodów, kwestii jaką jest zarządzanie procesem zbierania, przechowywania oraz archiwizacji dowodów elektronicznych. Dowody elektroniczne wymagają szczególnych środków ostrożności, ze względu na swój charakter i łatwość z jaką mogą zostać zmienione, uszkodzone lub zniszczone w wyniku niewłaściwego obchodzenia się z nimi. W przeciwnym razie będą one bezużyteczne lub doprowadzą do nieścisłych wniosków.

4.7.2. Co do zasady, w postępowaniu cywilnym i administracyjnym to strony są odpowiedzialne za prawidłowe gromadzenie dowodów elektronicznych. Różne rodzaje danych mogą wymagać odpowiednich metod ich gromadzenia (szczególnie w kontekście przeciwdziałania naruszania integralności dowodów). W sprawach o istotnym znaczeniu, strony powinny rozważyć zebranie dowodów elektronicznych przy wsparciu informatyka lub notariusza. Potwierdzanie autentyczności dowodów elektronicznych mogą przeprowadzać także inni przedstawiciele zawodów prawniczych.

4.7.3. Należy zwrócić uwagę, że choć sędziowie oraz przedstawiciele zawodów prawniczych, zwiększyli swoją wiedzę i doświadczenie w zakresie postępowania z dowodami elektronicznymi, to nadal brakuje jednolitych standardów w tej dziedzinie. Gromadzenie i przechowywanie dowodów elektronicznych wymaga od państw członkowskich przyjęcia specjalnych narzędzi i procedur w kierunku zapewnienia ich integralności, poufności i bezpieczeństwa. Ważne, aby w ramach obowiązujących lub planowanych procedur uwzględniać konieczność tworzenia i archiwizowania kopii zapasowych (także w oryginalnym formacie) na wypadek, gdyby jeden ze sposobów przechowywania zawiódł.

4.7.4. W przypadku akceptowania dowodów elektronicznych przez sąd, wytyczne słusznie wskazują, że przyjmowanie ich jest uzasadnione tylko wówczas gdy jest to przydatne dla celów dowodowych. Istnieje ryzyko, że łatwość pozyskiwania dowodów elektronicznych przez stronę, może skutkować dużą ilością niepotrzebnych dowodów. Powyższe może utrudnić lub nawet uniemożliwić skuteczne postępowanie z nimi. Aktywne zarządzanie danymi powinno odbywać się z poszanowaniem zasady proporcjonalności. Każdy wniosek strony o przedstawienie dowodów elektronicznych powinien być rozpatrywany pod względem merytorycznym, w szczególności jego

przydatności dla celów dowodowych. Strony powinny być uprawnione do kwestionowania tego typu wniosków.

4.7.5. Wiarygodność dowodów elektronicznych może być kwestionowana z uwagi na oddzielenie tożsamości cyfrowej od tożsamości fizycznej. Zgodnie z wytycznymi, sądy powinny dążyć do ustalenia tożsamości twórcy danych elektronicznych. Wydaje się jednak zasadne pytanie, czy to jednak nie strona powołująca się na dany dowód nie powinna wykazać kto jest twórcą danych treści. W wytycznych słusznie wskazano na obiektywne sposoby ustalania tożsamości, gdy prawo właściwe milczy na ten temat (podpis elektroniczny, sprawdzenie adresu e-mail, z którego dokument został wysłany). Pomocą w zapewnianiu wiarygodności dowodów mogą służyć usługi zaufania. Najbardziej popularne wydają się być: certyfikowanie podpisów elektronicznych[4] oraz znakowanie czasem[5].

4.7.6. W zakresie, w jakim pozwala na to obowiązujące prawo i w zależności od uznania sądu, wytyczne zachęcają do przyjmowania jako dowodów wszelkiego rodzaju dowodów elektronicznych. Jeżeli dochodzi do sporu, strony zasadniczo określają kwestie istotne dla rozstrzygnięcia sprawy i – o ile jedna ze stron nie podniesie zarzutu braku autentyczności dowodu elektronicznego – sąd nie musi poruszać tej kwestii z własnej inicjatywy. Strona, która chce oprzeć się na dowodach elektronicznych może być zobowiązana do wykazania jego autentyczności – na przykład poprzez przedstawienie metadanych lub wystąpienie o stosowny nakaz prawny w celu uzyskania dodatkowych danych od innej osoby (np. dostawcy usług zaufania) gdy strona kwestionuje dowody elektroniczne. Wiarygodność danych elektronicznych można udowodnić w dowolny sposób, na przykład za pomocą kwalifikowanego podpisu elektronicznego lub innych podobnych metod identyfikacji, które zapewniają integralność danych. Do prawa właściwego należy wskazanie skutków prawnych podpisów elektronicznych, na przykład poprzez określenie, że tylko kwalifikowany podpis elektroniczny powinien mieć równoważny skutek prawny podpisowi odręcznemu (atramentowemu), lub poprzez wymóg, aby urządzenie służące do składania podpisu znajdowało się pod wyłączną kontrolą podpisującego. Choć wytyczne powstały w celu pomocy państwom członkowskim Rady Europy (47 państw) to dla zapewnienia integralności danych, wytyczne odwołują się do rejestru dostawców kwalifikowanych usług zaufania w UE.

[4] Certyfikaty do podpisów elektronicznych, czasami określane jako „cyfrowy identyfikator" danej osoby, mogą gwarantować zarówno autentyczność, jak i integralność danych. W przypadku gdy tożsamość osoby składającej podpis elektroniczny jest wątpliwa, sąd może zażądać od usługodawcy związanego z podpisem elektronicznym do złożenia oświadczenia dotyczącego kwestii, co do których jest on kompetentny do przedstawienia dowodów.

[5] Znakowanie czasem (poświadczenie czasu) jest mechanizmem, który umożliwia udowodnienie integralności danych. Dowodzi, że dane istniały w określonym momencie i nie zostały modyfikowane. Znacznik czasu jest cennym aspektem dowodu elektronicznego, ponieważ zawiera istotne metadane dotyczące momentu jego utworzenia.

4.7.7. Dodatkowego wyjaśnienia wymaga wytyczna dotycząca ciężaru dowodowego. Osoby wymagające szczególnej opieki, tj. konsumenci, dzieci, osoby niepełnosprawne mogą nie być technicznie lub ekonomicznie zdolne do dostarczenia dowodów elektronicznych. W takiej sytuacji, gdy korzystają oni z przepisów ustawowych, które ułatwiają lub przerzucają na drugą stronę ciężar dowodu, tego typu przepisy mają pierwszeństwo przed wytycznymi. W pełni zgadzamy się z opinią zawartą w wytycznych, że sądy powinny odgrywać aktywną rolę w sprawach, w które zaangażowane są osoby wymagające szczególnej opieki. Pomocne byłoby upowszechnianie zdalnego udziału w postępowaniu sądowym wśród osób potrzebujących wsparcia.

4.7.8. Wytyczne CDCJ uwzględniają również większą wartość dowodową publicznych (urzędowych) systemów elektronicznych generujących dowody elektroniczne. Utrwalonym standardem europejskim jest traktowanie danych z elektronicznych rejestrów publicznych jako dokumentów urzędowych.

4.7.9. Wytyczne CDCJ regulują również kwestie przechowywania i archiwizacji dowodów elektronicznych. Przechowywanie odnosi się do okresu trwania danego postępowania cywilnego lub administracyjnego, archiwizacja obejmuje czas po zakończeniu postępowania. Sąd może przechowywać dowody elektroniczne na przykład na urządzeniach przenośnych (kartach pamięci), serwerach, systemach kopii zapasowych lub innych miejscach przechowywania danych (w tym *cloud computing*). Dowody elektroniczne powinny być przechowywane i archiwizowane w ich oryginalnym formacie (tj. nie w formie wydruków), zgodnie z obowiązującym prawem.

4.7.10. Sądy powinny przyjąć proaktywne podejście do ochrony integralności dowodów elektronicznych przed cyberzagrożeniami, w tym przed uszkodzeniem lub nieuprawnionym dostępem. Skupiając się na zapobieganiu, sądy mogą zapobiec wpływowi cyberzagrożeń na integralność dowodów elektronicznych i zmniejszyć ogólne ryzyko związane z bezpieczeństwem cybernetycznym. Niezależnie od stosowanej metody przechowywania, nieupoważnione osoby nie powinny mieć dostępu do dowodów elektronicznych.

4.7.11. Przechowywane dowody elektroniczne mogą być powiązane ze znormalizowanymi metadanymi. Wdrożenie międzynarodowych norm dotyczących metadanych zapewnia pewien poziom spójności w przechowywaniu dowodów elektronicznych. Ponieważ tworzenie znormalizowanych metadanych może być trudne i czasochłonne, sądy mogą korzystać z narzędzi, które pomagają w generowaniu znormalizowanych metadanych[6].

[6] Dostępnych jest wiele narzędzi do tworzenia znormalizowanych metadanych. Na przykład narzędzie do zarządzania metadanymi może wygenerować plik XML (eXtensible Markup Language) zawierający metadane związane z dowodem elektronicznym. Pliki XML nie wymagają profesjonalnego oprogramowania. Narzędzie to może uprościć zarówno przechowywanie, jak i wyszukiwanie dowodów elektronicznych. W tym względzie

4.7.12. W zakresie archiwizacji, aktualność zachowuje zalecenie Komitetu Ministrów Rady Europy w sprawie archiwizacji dokumentów elektronicznych w sektorze prawnym (Rec(2003)15). Prawo krajowe zazwyczaj określa okresy przechowywania i techniczne warunki archiwizacji. Elektroniczny nośnik danych, jeżeli jest używany, powinien być zaopatrzony w certyfikat identyfikacyjny zawierający podstawowe dane o nim. Nośnik taki powinien być odpowiednio chroniony, w szczególności przed utratą, szkodliwym działaniem środków chemicznych, pola magnetycznego lub elektrycznego, ciepła, światła oraz przed uszkodzeniami mechanicznymi.

4.7.13. Zgodnie z wytycznymi, służby archiwizacyjne w sądach mogą weryfikować, ewentualnie z wykorzystaniem podpisu elektronicznego lub innych procedur elektronicznych, że dowody elektroniczne są archiwizowane przez wykwalifikowanych specjalistów lub właściwe organizacje oraz że dane nie zostały przez nich zmienione. Państwa członkowskie powinny zapewnić organizacjom, którym na mocy prawa powierzono obowiązek archiwizacji, środki niezbędne do archiwizowania dowodów elektronicznych.

4.8. Rekomendacje dotyczące migracji danych

4.8.1. Wytyczne CDCJ odnoszą się także do tak istotnej i wrażliwej kwestii jaką jest migracja danych, czyli zmiana nośnika pamięci w celu zachowania dostępności do dowodów elektronicznych. Zaniedbanie migracji może skutkować brakiem możliwości odczytania danych. Dokumenty elektroniczne mogą być archiwizowane poprzez okresowe przenoszenie danych z jednego nośnika na inny lub z jednego formatu na inny. Migracja powinna dotyczyć również metadanych dotyczących archiwizowanych dokumentów elektronicznych. Migracja na nowy nośnik pamięci powinna odbywać się regularnie, gdy jest to właściwe, ze względu na rozwój technologiczny.

4.8.2. Według wytycznych CDCJ należy unikać archiwizowania dowodów na płytach CD, DVD i innych dyskach optycznych, które stają się nieczytelne z powodu fizycznego lub chemicznego pogorszenia ich jakości. Przyczyny są różne – od utleniania warstwy odblaskowej po fizyczne ścieranie powierzchni lub krawędzi dysku, w tym widoczne zarysowania, aż po inne rodzaje reakcji z zanieczyszczeniami.

4.8.3. Warte rozważenia jest migrowanie danych do urządzeń sieciowych, takich jak chmury obliczeniowe, które są stale udoskonalane w wyniku rozwoju technologicznego nośnika i sprzętu. Archiwizacja w chmurze może również zapewnić większą kontrolę nad kosztami dzięki możliwości płacenia tylko za potrzebną przestrzeń.

---

należy przestrzegać międzynarodowych standardów stosowanych w odniesieniu do metadanych, takich jak te opublikowane przez Międzynarodową Organizację Normalizacyjną (ISO).

4.9. Rekomendacje dotyczące transgranicznej oceny dowodów elektronicznych

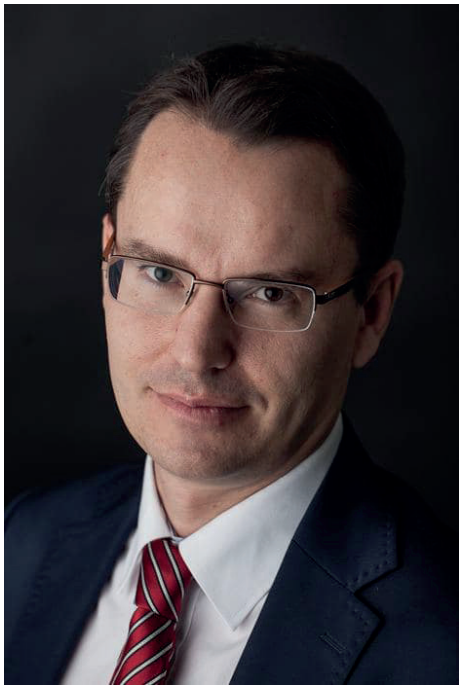
4.9.1. Choć posługiwanie się dowodami elektronicznymi ma często charakter ściśle krajowy, coraz częściej zdarza się, że obejmuje także inne kraje (element transgraniczny). Przykładem jest umiejscowienie w innym kraju infrastruktury wykorzystywanej do przetwarzania lub przechowywania danych, lub dostawcy, który umożliwia przechowywanie lub przetwarzanie danych.

4.9.2. Ponadto, istnieją znaczne odrębności pomiędzy krajowymi przepisami proceduralnymi dotyczącymi przeprowadzania dowodów za granicą. Sądy wykorzystujące tego typu dowody, powinny te różnice uwzględniać. Zaleca się, by przy transgranicznym przeprowadzaniu dowodów elektronicznych, sądy ściśle współpracowały w tej kwestii. Sąd wzywający powinien być informowany o zasadach proceduralnych stosowanych przez sąd wezwany, aby w razie potrzeby dostosować swoją ocenę dowodów elektronicznych. W szczególności przeprowadzanie dowodów za granicą nie powinno skutkować naruszeniem podstawowych zasad prawa procesowego.

4.9.3. Skuteczność postępowania ulega znaczącej poprawie, gdy możliwe jest przekazanie dowodów elektronicznych do innych sądów (również zagranicznych) w oryginalnym formacie (wraz metadanymi) zamiast ich drukowania i wysyłania. Optymalizację procesu przekazywania dowodów elektronicznych za pomocą środków elektronicznych można osiągnąć poprzez wdrożenie wspólnych standardów technicznych i formatów plików oraz poprzez cyfryzację krajowych systemów sądowych i administracyjnych. Uwzględniając wyższe ryzyko zniszczenia dowodów elektronicznych, należy przyjąć na szczeblu krajowym procedury, które pozwalają na bezpieczne przekazywanie dowodów elektronicznych. Przy przekazywaniu dowodów należy brać pod uwagę integralność danych i zasady bezpieczeństwa (dla zapewnienia właściwego przekazywania dowodów elektronicznych pomocne może okazać się skorzystania z usług zaufania). Jeżeli transmisja danych wymaga poufności, konieczne może być zastosowanie środków lub rozwiązań technicznych, takich jak szyfrowanie, które ograniczają dostęp do bezpiecznej komunikacji wyłącznie dla osób upoważnionych.

4.10. Rekomendacje dotyczące edukacji w zakresie dowodów elektronicznych

4.10.1. Wiedza o specyfice dowodów elektronicznych, jak i samych wytycznych CDCJ powinna być propagowana wśród sędziów oraz pozostałych przedstawicieli zawodów prawniczych. Możliwość wykorzystania dowodów elektronicznych w postępowaniach cywilnych i administracyjnych powinna być także propagowana w społeczeństwie. Zalecane są szkolenia, w trakcie których omawiane byłyby konkretne kwestie związane z dowodami elektronicznymi, takie jak znaczenie metadanych i znakowania czasem, wykorzystania chmury obliczeniowej lub *blockchain* w gromadzeniu dowodów oraz konieczność przedkładania dowodów elektronicznych w ich oryginalnym formacie, a nie jako zeskanowanych obrazów lub wydruków. Instruktaż w zakresie kwestii materialnych i proceduralnych w kontekście dowodów elektronicznych powinien być stałym elementem edukacji prawniczej.



Dr hab. Marek Świerczyński – prof. uczelni, adwokat w Kancelarii Prawnej Kieszkowska Rutkowska Kolasiński, konsultant Rady Europy ds. technologii informatycznych (CDCJ, CEPEJ), profesor nadzwyczajny w Instytucie Nauk Prawnych UKSW.
ORCID: 0000-0002-4079-0487

Dr Zbigniew Więckowski – adiunkt w Katedrze Prawa Cywilnego i Prawa Prywatnego Międzynarodowego INP UKSW, Zastępca Dyrektora Instytutu Nauk Prawnych Uniwersytetu Kardynała Stefana Wyszyńskiego.
ORCID: 0000-0001-7753-3743

INSTYTUT
De Republica

Pragniemy wspierać polskich naukowców i dzielić się ich dokonaniami. Do naszych głównych zadań należy uwolnienie potencjału polskiej nauki poprzez promocję i popularyzację rodzimej myśli badawczej z zakresu nauk humanistycznych i społecznych, a także wytworzenie mechanizmów i kapitału społecznego, który organizowałby się wokół idei państwowości.

Instytut De Republica jest nowoczesnym zapleczem eksperckim, promocyjnym i wydawniczym dla niedocenianych w kraju i poza jego granicami, a tak ważnych dla właściwego rozumienia historii i zjawisk społecznych, dziedzin nauki. Równie istotnym aspektem we wspomnianym zakresie jest współdziałanie z uczelniami wyższymi, instytutami badawczymi oraz analitycznymi z Polski i całego świata.