



Igor Zgoliński*

Wirtualna sala narad i inne nowe instrumenty postępowania karnego. Uwagi na tle zagrożeń i kosztów cyfryzacji

[Virtual Courtrooms and Other New Tools in Criminal Proceedings: Notes on the Risks and Costs of Digitization]

Abstract

This publication analyzes the critical issues surrounding the necessary digital reform of the justice system, using criminal proceedings as an example. It points out that digitization represents a fundamental paradigm shift in the concept of a fair trial—which must be accompanied by appropriate changes in the law. It also identifies the need to implement numerous new tools in criminal proceedings, including a virtual courtroom (conference room) for remote hearings. Specific amendments to criminal procedure regulations are proposed, emphasizing the necessity of a broader legislative revision covering exclusively digital issues. On the one hand, the digitization of criminal proceedings (*e-justice*) offers the potential to expedite proceedings and facilitate access to case files; on the other hand, however, it poses serious threats to the fairness of the trial. It also imposes significant financial burdens on the state. Key risks include: digital exclusion, the erosion of the principle of directness, and issues regarding the confidentiality of communications and the transparency of proceedings. A full understanding of these risks and the associated costs is essential for the *e-justice* system to effectively support the administration of justice.

Keywords: criminal proceedings, digitization, virtual courtroom (conference room), risks, costs.

Wstęp

Truizmem jest stwierdzenie, że cyfryzacja postępowań karnych (*e-justice*) może znacząco przyspieszyć przebieg postępowań karnych oraz ułatwić

* **Igor Zgoliński** – profesor uczelni, dr hab. nauk prawnych, Politechnika Bydgoska im. Jana i Jędrzeja Śniadeckich (afiliacja), sędzia SN; <https://orcid.org/0000-0002-5097-6170>; igor.zgolinski@pbs.edu.pl / associate professor, PhD in Law, post-doctoral degree, Bydgoszcz University of Science and Technology (affiliation); judge of the (Polish) Supreme Court.

stronom i innym podmiotom zainteresowanym dostęp do akt. Niewątpliwie należy dążyć do pełnej cyfryzacji, gdyż w tym kierunku zmierza postęp cywilizacyjny. W przypadku sądów usprawni to ich pracę i odwróci istniejący od czasów zaborów stan zbierania dokumentów papierowych, składania w poszczególne tomy akt, a następnie magazynowania i archiwizacji po zakończeniu postępowania.

Cyfryzacja jest przedsięwzięciem niezwykle skomplikowanym oraz kosztownym. Ma wiele odmian i generuje stałe wydatki, nieponoszone dotąd przez Skarb Państwa. Prócz wielu pozytywnych aspektów stwarza również wiele nowych poważnych zagrożeń. Z wymienionych powodów niezbędne staje się podjęcie próby określenia głównych zagrożeń oraz czynników powodujących zwiększenie wydatków na wymiar sprawiedliwości, a ponadto dokonanie ich stosownej analizy. Pozwoli to w przyszłości zniwelować niebezpieczeństwa związane z cyfryzacją, co niewątpliwie będzie pożytkiem dla podmiotów tworzących postęp w omawianej dziedzinie oraz uczestniczących w postępowaniach karnych. Przeanalizowanie obszarów wywołujących koszty pozwoli natomiast na zwizualizowanie skali problemu związanego z tym procesem i uświadomi źródła przyczyn, które ów postęp mogą (i będą) znacząco ograniczać. Celem analizy jest zatem przede wszystkim identyfikacja i wieloaspektowa analiza zagrożeń wynikających z informatyzacji procesu karnego, w tym wskazanie konfliktów między nowoczesną technologią a naczelnymi zasadami procesowymi¹ – z uwzględnieniem barier ekonomicznych. Badania dążą też do wypracowania postulatów legislacyjnych i technicznych, które pomogą zniwelować przyszłe ryzyka. W tekście zastosowano różne metody badawcze. Podstawowa jest metoda dogmatycznoprawna, a wspierają ją metody analityczno-badawcza, postulatyczna oraz analiza ryzyka.

Zagrożenia wynikające z cyfryzacji postępowania

W dobie implementacji systemów AI i postępującej cyfryzacji akt postępowania (e-akta) zagrożenia związane z cyfryzacją procesu karnego można podzielić na szereg obszarów. Każdy z nich generuje specyficzne ryzyka dla sprawowania wymiaru sprawiedliwości. W przypadku zagrożeń dla zasad rzetelnego procesu (fair trial) jako kluczowy postrzegać należy problem wykluczeń cyfrowych. Jest to problem nie tylko socjologiczny, gdzie został

¹ W literaturze przedmiotu wskazano już nawet na zasadę cyfryzacji, obowiązującą względem do instytucji prawnych określonych w k.p.k. – zob. szerzej: P. Czarnecki, *Zasada elektronizacji (cyfryzacji) procesu karnego* [w:] *W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi*, D. Szumiło-Kulczycka (red.), Warszawa 2022, ss. 440–443.

relatywnie dobrze zbadany², lecz stanowi również problem w cyfryzacji postępowań. Zawsze będzie kładł się cieniem nad tym mechanizmem. Społeczeństwo w dużej mierze nadal nie potrafi w odpowiedni sposób poruszać się po świecie cyfrowym i w pełni korzystać z udogodnień, które się z tym wiążą. Co więcej, brak odpowiedniego sprzętu lub jedynie owych umiejętności, zwłaszcza po stronie podejrzanego bądź oskarżonego, może prowadzić do nierówności w dostępie do sądu, do akt postępowania bądź do poszczególnych czynności procesowych. Przepaść cyfrowa może wręcz uniemożliwiać lub znacząco utrudniać realizację prawa do obrony, jeśli dostęp do dowodów, pism procesowych czy udział w czynnościach będzie wymagał specjalistycznej wiedzy technicznej lub odpowiedniego sprzętu. Konieczne jest zatem takie wdrażanie i udoskonalanie cyfryzacji postępowań, które będzie wiodło do wykreowania nie tylko narzędzi prostych w obsłudze od strony technicznej i niewymagających wysokiej jakości sprzętów, lecz również zapewniało alternatywny udział w tymże postępowaniu w formule tradycyjnej (dotychczasowej). Państwo musi więc utrzymywać model hybrydowy, gwarantujący prawo do tradycyjnego procesu osobom nieposiadającym kompetencji lub odpowiedniego sprzętu. W dobie dążenia do nowoczesności prawo do analogowego procesu powinno stać się nowym prawem człowieka, chroniącym przed wykluczeniem i błędami systemowymi. Wpisuje się ono bezsprzecznie w karnoprosesową zasadę równego traktowania stron i funkcjonalną regułę równouprawnienia³.

Kolejnym ważkim zagadnieniem z tej sfery jest potencjalne ograniczenie karnoprosesowej zasady bezpośredniości. Rozprawy zdalne mogą utrudniać sędziemu oraz pozostałym osobom (podmiotom) w niej uczestniczącym właściwą ocenę prowadzonych dowodów. Jest to szczególnie widoczne choćby w ramach oceny wiarygodności świadków (brak możliwości odczytania pełnej mowy ciała w obliczu niepełnego obrazu osoby składającej zeznania)⁴. Może to również prowadzić do osłabienia kontaktu obrońcy z mandantem (brak możliwości poufnej konsultacji w trakcie przesłuchania). Omawiana kwestia wydaje się trudna do zupełnego zniwelowania, gdyż rozprawy zdalne nawet przy zaawansowanej technologii, raczej nie są w stanie zastąpić bezpośredniego uczestnictwa i wrażeń (odczuć) z tym związanych. Pokusić się można o kilka uwag na tej płaszczyźnie. Celowe wydaje się

² Zob. np. S. Czetwertyński, A. Mroczek-Czetwertyńska, Wykluczenie cyfrowe w społeczeństwie informacyjnym, „Nauki Społeczne” 2012, 1, 5, ss. 116–127, M. Castells, Społeczeństwo sieci, Warszawa 2007, H.S. Dordick, G. Wang, The Information Society: A Retrospective View, Newbury Park 1993, J. Kujawski, Wykluczenie cyfrowe jako forma wykluczenia społecznego. Przypadek Polski, „Media i Społeczeństwo” 2018, 9, s. 252 i nn., R. Jedlińska, Wykluczenie cyfrowe w Polsce na tle krajów Unii Europejskiej, „Ekonomiczne Problemy Usług” 2018, 131, 2, ss. 225–236 i nn.

³ M. Rogacka-Rzewnicka, O równości, równouprawnieniu i równowadze procesowej w postępowaniu karnym [w:] W pogoni..., ss. 161–163.

⁴ J. Marszałek, M. Skwarcow, Użycie sztucznej inteligencji w postępowaniu karnym, „Przegląd Sądowy” 2025, 3, s. 63.

zwiększenie liczby kamer na salach rozpraw, które z różnych perspektyw przekazywałyby wizję oraz fonię – co w założeniu zwiększy transparentność przekazu i wzmocni zasadę bezpośredniości. Brak fizycznej obecności na sali sądowej osłabia wszakże empatię – w tym empatię sędziego – oraz utrudnia oskarżonemu aktywny udział w procesie (chodzi np. o trudność w przerwaniu wypowiedzi, by skonsultować się z obrońcą przez komunikator, podjęcie adekwatnej reakcji przez złożenie uzupełniających wyjaśnień itd.). Pamiętać trzeba, że cyfryzacja zmienia dynamikę sali rozpraw, co często uderza w najsłabszych uczestników postępowania. Problemem staje się zresztą nie tylko mały obraz, lecz i stale postępująca technologia wygładzania wizerunku. Algoritmy kompresji wideo i filtry AI (nawet te, które standardowo są umieszczone w komunikatorach) mogą maskować mikromimikę świadka, która dla obserwujących będzie sygnałem stresu lub objawem kłamstwa. Konieczne jest więc wprowadzenie określonego standardu „surowego sygnału wideo” w celach procesowych, wolnego od owych algorytmicznych upiększeń. Zasadę bezpośredniości wzmocniłoby natomiast wbudowanie przeglądarki akt podczas rozprawy zdalnej oraz w wirtualnej sali narad – uniemożliwiającej wykonywanie zrzutów ekranu (*watermarking*) i zapewniającej pełną kontrolę nad tym, kto w danej chwili ogląda dany dokument.

Wydaje się ponadto, że warto umieścić w narzędziach umożliwiających prowadzenie rozpraw zdalnych możliwość szybkiego przejścia do innego pokoju osób biorących w niej udział – w celu zapewnienia osobnej, niejako pozasądowej, komunikacji (wirtualna, cyfrowa sala narad). Bez wątpienia taka opcja powinna być zapewniona dla kontaktu obrońcy z oskarżonym, dla zachowania tajemnicy obrończej (*attorney-client privilege*). Do rozważenia pozostaje, czy winno się to odbywać za zgodą przewodniczącego, czy też bez. Mając na względzie specyfikę rozpraw zdalnych oraz możliwość równoległego porozumiewania się za pomocą innych środków komunikacji, uważam, że mogłoby to odbywać się niejako obok rozprawy, a więc bez zgody przewodniczącego. W sytuacjach skomplikowanych należałoby zarządzić do tego specjalną przerwę w rozprawie, co już wymaga zgody. Podobnej zgody będą wymagały inne sytuacje występujące na sali rozpraw, z reguły w sposób nagły i pilny, jak choćby: wniosek o dobrowolne poddanie się karze, potrzeba narady nad złożeniem dodatkowych wyjaśnień, sygnalizacji przez biegłych potrzeby przeprowadzenia dodatkowych czynności bądź dyskusji ze stronami postępowania. Możliwość ta prawdopodobnie nie będzie się cieszyła – przynajmniej na początku – dużym zainteresowaniem z uwagi na obawy używania narzędzia nowego i dodatkowo udzielonego przez sąd (ewentualnie organ ścigania bądź organ wykonawczy). Będzie to wywoływało przede wszystkim obawę braku zachowania tajności (*poufności*). Wirtualna sala narad będzie jednak miała zdecydowanie szersze wykorzystanie. Może służyć do narady składu orzekającego nad orzeczeniem oraz innych narad czy dyskusji

w toku postępowania. Może być też wykorzystywana – jak już wspomniano – przez biegłych, np. przez biegłego psychologa, do różnego typu rozmów z pokrzywdzonym bądź zebrania danych osobopoznawczych. Systemy e-justice powinny być więc projektowane w architekturze *end-to-end encryption* dla kanałów bocznych (E2EE), do których klucze deszyfrujące posiadałyby wyłącznie strony, a nie operator systemu. Innymi słowy, gdy osoby zalogują się do tej sali, wówczas ich urządzenia wymieniają wzajemnie klucze publiczne przez serwer, który nie będzie ich przechowywał w formie deszyfrującej (co jest znane np. z komunikatora Signal), a wiadomości na czacie bocznym będą szyfrowane kluczem sesyjnym odbiorcy na urządzeniu nadawcy. Uczestnicy mogą wówczas zweryfikować tożsamość rozmówców poprzez porównanie tzw. *safety numbers* (skrótów kryptograficznych kluczy publicznych) poza głównym kanałem.

Następna kwestia – nieodległa od powyżej omawianej – dotyczy potencjalnej obawy o naruszenie zasady jawności postępowania⁵. Jakkolwiek technologia umożliwia transmisję, to bariery techniczne lub błędy systemowe mogą *de facto* wykluczać publiczność z udziału w procesie, co także może w określonych sytuacjach godzić w transparentność wymiaru sprawiedliwości. Problem stanie się szczególnie nabrzmiały w kontekście postępowań cieszących się dużym zainteresowaniem opinii publicznej. *De lege lata* jest rozwiązywany za pomocą wydawania specjalnych kart wstępu, co ma przeciwdziałać zakłócaniu przebiegu rozprawy. W świecie cyfrowym antidotum mogłoby się okazać umożliwienie transmisji z otwartym dostępem (*open access*), rzecz jasna bez możliwości jakiegokolwiek ingerencji bądź czynnego uczestnictwa w postępowaniu.

Następnym obszarem zagrożeń są różnego typu ryzyka związane z dowodami cyfrowymi (*deepfakes*) i manipulacją danymi (zjawisko syntetycznych dowodów). Postępująca dostępność rozmaitych narzędzi AI pozwala na tworzenie realistycznych, acz przecież fałszywych obrazów, fotografii, nagrań wideo, audio czy dokumentów. Generuje to ryzyko wprowadzenia do procesu sfabrykowanych nagrań wideo lub audio, które są na pierwszy rzut oka niemożliwe do odróżnienia od prawdziwych. Wejdziemy więc w erę dowodu probabilistycznego, w której autentyczność nagrania czy dokumentu przestaje być oczywista. W konsekwencji w toku procesu niezbędne stanie się sięgnięcie do kolejnych dowodów (weryfikujących) w postaci specjalistycznych ekspertyz biegłych z zakresu informatyki śledczej. Wymuszać to będzie niekiedy prowadzenie wpadkowych, żmudnych postępowań, zmierzających jedynie do odróżnienia autentycznych dowodów od zaawansowanych manipulacji. Dowody cyfrowe są niezwykle podatne na różnego rodzaju modyfikacje. Brak ścisłych procedur (np. sum kontrolnych, *blockchain*) przy zabezpieczaniu da-

⁵ P. Czarnecki, *Rozprawa sądowa w Internecie. Postulat wprowadzenia możliwości transmisji (streamingu) rozpraw sądowych w rzetelnym procesie karnym*, „Prokuratura i Prawo” 2025, 3, s. 58.

nich może prowadzić do podważenia ich autentyczności oraz wiarygodności przed sądem. Poza tym dowody cyfrowe bywają „ulotne”, np. brak natychmiastowego zabezpieczenia sumy kontrolnej (*hash*) pliku pozwala na jego edycję na etapie zabezpieczania, co może wywołać zarzut manipulacji. Dane przechodzą też przez serwery różnych dostawców usług. Dużym ryzykiem jest np. uzyskanie dowodów z naruszeniem procedur międzynarodowych (np. bez stosownego wniosku o pomoc prawną), a to może prowadzić do niedopuszczalności wykorzystania takich dowodów. Uzyskanie danych z pominięciem procedur MLAT (*Mutual Legal Assistance Treaty*) lub bez uwzględnienia wyroków TSUE dotyczących retencji danych⁶ stwarza ryzyko uchylania wyroków w postępowaniu odwoławczym. Cyfryzacja bez uregulowania statusu dowodów z chmury może więc stać się generatorem przewlekłości postępowań. Tego typu sytuacje również będą bowiem wymagały stosownych weryfikacji procesowych, co będzie wpływało na ogólną sprawność postępowania. Nie wydaje się jednak, aby można było zupełnie uniknąć tego zjawiska. Jest ono nieuchronne. Pamiętać natomiast należy, że świadome wprowadzanie do postępowania karnego fałszywych dowodów winno być oceniane przez pryzmat naruszenia norm kodeksu karnego, który już obecnie przewiduje penalizację tego rodzaju zachowań (zob. art. 234 i 235 k.k.). Z drugiej strony pojawi się również wyraźne pole do nadmiernej inwigilacji, gdyż cyfryzacja umożliwia organom ścigania stosowanie metod w postaci „przeszukań zdalnych” czy też masowej analizy metadanych, w tym niezwiązanych ze sprawą. Działania te odbywają się w szarej strefie, dodatkowo w obliczu niedookreślonego stanu prawnego, co potęguje możliwość naruszania prawa do prywatności. Pilnego, wyprzedzającego wdrożenia wymagają zatem odpowiednie regulacje prawne (np. rozporządzenia), które wytyczą podstawowe reguły dla tego rodzaju czynności. Dane z polskich postępowań mogą być też przetwarzane na zagranicznych serwerach, a to implikuje pytania o suwerenność cyfrową wymiaru sprawiedliwości i faktyczną ochronę danych np. przed obcymi wywiadami⁷. W celu mitygowania tych zagrożeń kluczowe jest więc nie tylko stosowanie Aktu o sztucznej inteligencji (AI Act) – który klasyfikuje systemy AI stosowane w wymiarze sprawiedliwości jako systemy wysokiego ryzyka, wymagające najwyższego stopnia nadzoru ludzkiego – ale i jego wewnętrznie krajowe uszczegółowienie.

Zagadnieniem doniosłym z perspektywy cyfrowych zagrożeń są także różnego typu bolączki samych algorytmów sztucznej inteligencji (błąd algorytmiczny Bias). Systemy wspomagające decyzje (np. przy szacowaniu ryzyka prawdopodobieństwa popełnienia przestępstwa) mogą powielać różnego typu uprzedzenia historyczne (rasowe, majątkowe, terytorialne i inne), prowadząc

⁶ Na przykład wyrok z 8.04.2014 r. w sprawach połączonych C-293/12 i C-594/12.

⁷ Zob. P. Opitek, Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych, „Prokuratura i Prawo” 2018, 7–8, s. 65.

do niewłaściwych wyników, a w konsekwencji także orzeczeń. Brak przejrzystości działania algorytmów sprawia, że strony mogą nie zweryfikować tego, na jakiej podstawie system wygenerował dany wynik bądź sugestię. Godzi to też w rzetelność uzasadniania orzeczeń. Odmianą omawianej kwestii są tzw. halucynacje AI w analizie prawnej. Istnieje bowiem duże ryzyko bezkrytycznego korzystania przez organy stosujące prawo z systemów generatywnych, np. do streszczania akt, co może prowadzić do pominięcia kluczowych faktów lub „zmyślenia” przez AI nieistniejących okoliczności. Ważne z tej perspektywy jest ujawnienie kodów źródłowych, gdyż w przeciwnym razie zawsze będzie wywoływało to spory i podejrzenia o stronniczość.

Centralizacja akt w chmurze lub systemach sądowych stworzy natomiast wysokie ryzyko masowych wycieków danych osobowych pokrzywdzonych, świadków oraz innych danych tam zawartych. E-akta zawierają dane medyczne, intymne szczegóły z życia ofiar i dane świadków. Wyciek takich informacji może prowadzić do wtórnej wiktymizacji ofiar lub odwetu na świadkach. Niezależnie od powyższego ataki typu *ransomware* na systemy sądowe mogą sparaliżować pracę sądów, co może z kolei prowadzić do przedawnienia spraw lub zastoju, a nawet zawieszania postępowań z powodu braku dostępu do akt. Nie trzeba dodawać, że może też implikować konieczność prowadzenia postępowań odtworzeniowych. Zablockowanie dostępu do e-akt przez hakerów może sparaliżować tysiące spraw jednocześnie, prowadząc do jaskrawego naruszenia prawa do rozpoznania sprawy w rozsądnym terminie.

Nie będzie odkrywcze stwierdzenie, że od początku należy wdrożyć stały monitoring działania systemu, zadbać o bezpieczeństwo cyfrowe oraz ochronę prywatności. Polska zajmuje obecnie 6. miejsce na świecie w globalnym rankingu cyberbezpieczeństwa (*Cyber Defense Index*). Świadczy to o bardzo wysokim poziomie ogólnej cybernetycznej odporności państwa, aczkolwiek specyficzność wymiaru sprawiedliwości stwarza unikatowe wyzwania i potęguje prawdopodobieństwo ataków. Potwierdza to fakt, że Polska znajduje się też w czołówce najczęściej atakowanych krajów świata, głównie przez grupy powiązane z Rosją (np. *People's Cyber Army* czy *APT44*). Sądy są więc narażone na ataki blokujące dostęp do usług (DDoS) oraz liczne próby sabotażu danych. Problem ten staje się szczególnie istotny – zważywszy, że od marca 2026 r. sądownictwo przechodzi na nowy, bardziej rozległy zakresowo model cyfrowy, obejmujący m.in. e-apelacje. W bieżącym roku ma więc nastąpić swoisty przełom cyfrowy, dwustronna zaś komunikacja z sądem stać się standardem, a odbywać się przez portale informacyjne. Systemy te są chronione przez krajowe jednostki CSIRT (Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego), które już teraz odnotowują skokowy wzrost liczby ataków na infrastrukturę administracji publicznej. Polskie sądownictwo posiada co prawda solidną tarczę w postaci zaawansowanych systemów krajowych (NASK, CSIRT) i wysokiej pozycji w rankingach, jednak dynamiczna cyfry-

zacja e-apelacji oraz status Polski jako celu ataków hybrydowych sprawią, że bezpieczeństwo to będzie w stanie permanentnego testowania. Krytycznym wyzwaniem pozostaje tu zwłaszcza pełna implementacja unijnych standardów NIS2 w systemach sądowych. Mimo że Polska wdraża dyrektywę NIS2 (poprzez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa), proces ten stale napotyka na opóźnienia legislacyjne.

Wszystkie powyżej opisane aspekty wiążą się z obawami nie tylko o bezpieczeństwo, ale i stabilność techniczną infrastruktury wymiaru sprawiedliwości, przy relatywnie nieodległym i na pewno znacznym wzroście obrotu cyfrowego. Będzie to niewątpliwie niespotykanym dotąd wyzwaniem, nie tylko dla osób prowadzących postępowania, lecz również dla kadry administracyjnej, która powinna co najmniej od kilku lat przechodzić systematyczne szkolenia i nabywać odpowiednie kwalifikacje zawodowe. Brak tego typu działań zakreślonych na szeroką skalę systematycznie eskaluje krajowe zapóźnienie w obszarze cyfryzacji.

Koszty cyfryzacji postępowań

Zagadnienie kosztów cyfryzacji ma dwa oblicza. Z jednej strony są to wymierne wydatki, które winien ponieść Skarb Państwa na czynności z tym związane; z drugiej jednak strony na szali położona jest swoista korzyść społeczna w postaci usprawnienia postępowań, zapewnienia ich transparentności oraz zachowania właściwej relacji względem postępu cywilizacyjnego. Są to aspekty niewymierne, lecz ważniejsze niżli koszty finansowe. Faktyczne koszty cyfryzacji postępowań karnych będą ogromne i wydaje się, że nie jest możliwe ich bezdyskusyjne skonkretyzowanie, zwłaszcza pod kątem wysokości⁸. Jest to zagadnienie wysoce złożone, znacznie wykraczające poza np. sam zakup komputerów czy niezbędnych licencji. Faktyczne koszty będzie można ustalić dopiero po zakończeniu przetargów i pełnym wdrożeniu cyfryzacji, a i tak będą one systematycznie powiększane o koszty bezpieczeństwa, nadzoru (monitoringu) oraz stałego serwisowania i szkoleń. Z tych powodów nie jest możliwe szersze odniesienie się do tego aspektu w opracowaniu artykułowym. Zasadne jest natomiast określenie głównych czynników te koszty wywołujących.

Ujmując rzecz w skali makro: na samo wzmocnienie cyberbezpieczeństwa przeznaczono około 4 miliardów zł (dane z roku 2025), z czego część trafiła bezpośrednio do sektora publicznego i wymiaru sprawiedliwości. Znacznie większe koszty będzie jednak generował cały mechanizm, gdyż cyberbezpie-

⁸ I. Zgoliński, *Technology and Criminal Proceedings: An attempt to systematize the issue and determine the main directions of implementation*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych” 2025, 1, 73, s. 104.

czeństwo jest jedynie częścią cyfrowego usprawniania sądów. Jeśli chodzi o skalę wydatków w Polsce, to zgodnie z planami na lata 2024–2026 wydatki na samą transformację cyfrową wymiaru sprawiedliwości w Polsce szacuje się na setki milionów złotych rocznie. Przykładowo tylko na rozwój systemów informatycznych w sądach powszechnych przeznaczają się milionowe środki z Programu Operacyjnego Polska Cyfrowa oraz funduszy celowych Ministerstwa Sprawiedliwości.

Koszty cyfryzacji można ogólnie podzielić na koszty bezpośrednie (finansowe) oraz koszty pośrednie (systemowe). Bezpośrednie koszty finansowe (inwestycyjne), które dotąd były finansowane głównie z KPO (Krajowy Plan Odbudowy) oraz funduszy spójności to przede wszystkim infrastruktura sprzętowa. Niezbędne jest przecież wyposażenie sal rozpraw w systemy do wideokonferencji, kamery 4K, systemy nagłośnienia oraz bezpieczne terminale dla sędziów i protokolantów. Koszty generować będzie utworzenie państwowych chmur obliczeniowych do przechowywania – zapewne petabajtów⁹ – danych (nagrania z rozpraw, e-akta, dowody cyfrowe itp.). Do tego doliczyć należy jeszcze wydatki związane z energią i chłodzeniem owych data centers. Koszty te są akurat możliwe do generalnego oszacowania na podstawie szeregu czynników szczegółowych, takich jak: liczba sal rozpraw, konfiguracja kamer, rodzaj i liczba potrzebnego sprzętu itd. Trudne do oszacowania będą natomiast nakłady finansowe przeznaczane na stworzenie autorskich systemów (jak choćby Portal Informacyjny Sądów, systemy e-doręczeń, systemy dla wewnętrznego użytku sądownictwa na wzór np. *gaius-lex*) oraz licencje na narzędzia informatyki śledczej (w tym do łamania zabezpieczeń, jak np. Cellebrite). Cały ten ciąg działań wymagać będzie, rzecz jasna, zatrudnienia ekspertów z branży IT, których wynagrodzenia w sektorze prywatnym są znacznie wyższe, a to z kolei wymusi adekwatne podnoszenie stawek w administracji sądowej – dla zapewnienia konkurencyjności. W przeciwnym razie nastąpi zapaść kadrowa, co utrudni dokonanie procesu cyfryzacji (o ile go wręcz nie uniemożliwi).

Do drugiej grupy kosztów, tzw. kosztów operacyjnych (stricte procesowych), zaliczyć trzeba natomiast w pierwszej kolejności wydatki na biegłych informatyków. Wzrost liczby dowodów cyfrowych powoduje wzrost kosztów postępowań, gdyż zwiększy się liczebność opinii biegłych. Koszty generować będzie nadto konieczność przeszkolenia wielu osób, które można liczyć w tysiącach, a więc sędziów, prokuratorów oraz pracowników sekretariatów¹⁰. Chodzi tu głównie o szkolenia z obsługi nowych systemów oraz z zakresu zachowania cyberhigieny. Jeszcze większe wydatki implikować będzie zwykła

⁹ Jeden petabajt (PB) to około 500 miliardów stron standardowego tekstu drukowanego.

¹⁰ Edukacja ta ma charakter stały, wpisuje się w metamorfozę kulturową i progresywne zwiększanie kompetencji cyfrowych; zob. K. Kiejnich-Kruk, *Building blocks – strategia cyfryzacji wymiaru sprawiedliwości. Perspektywa estońska*, „Przegląd Sądowy” 2025, 3, s. 92.

digitalizacja akt archiwalnych, co wiąże się ze skanowaniem papierowych akt spraw będących w toku, aby mogły stać się częścią e-akt. Do tego wymaga stworzenia całej infrastruktury.

W skład kosztów cyfryzacji postępowań zaliczyć także wypada tzw. koszty ukryte. Istnieje duże ryzyko błędów sądowych, a więc także nieuchronnych kosztów odszkodowań, np. za niesłuszne skazania bądź stosowanie tymczasowego aresztowania, wynikłe np. z błędnych interpretacji dowodów cyfrowych lub błędów algorytmu AI wspierającego decyzje. Tego typu koszty wynikać mogą także z różnego rodzaju ataków cyfrowych, awarii systemów, problemów z logowaniem świadków na rozprawy zdalne czy ataków DDoS – które mogą paraliżować sądy, znacząco przewlekać postępowania i generować straty. Państwo będzie musiało ponadto ponieść również duże koszty zapewnienia punktów dostępu do sieci lub pomocy technicznej dla osób wykluczonych cyfrowo (starszych, ubogich), aby nie straciły one prawa do obrony (koszt Digital Divide).

Choć docelowo cyfryzacja ma przynieść długofalowe oszczędności (brak kosztów wysyłki papierowej, mniejsza liczba konwojów więziennych dzięki rozprawom zdalnym), to obecnie znajdujemy się w fazie początkowych – i bodaj najwyższych – nakładów inwestycyjnych, gdzie koszty utrzymania starych (papierowych) i nowych (cyfrowych) struktur nakładają się na siebie. Gdy się jednak zna praktykę, można gorzko stwierdzić, że w najbliższych latach będzie zapewne dochodziło do przerzucenia tych kosztów (co najmniej częściowego) na poszczególne jednostki organizacyjne wymiaru sprawiedliwości, bez zapewnienia im niezbędnego wsparcia informatycznego.

Wnioski de lege ferenda

Bez „cyfrowej gwarancji kodeksowej”, czyli uregulowania wprost w kodeksie postępowania karnego odpowiednich prawnych bezpieczników technologicznych, cyfryzacja może stać się narzędziem co prawda efektywnym, ale wadliwym sprawiedliwościowo. Przygotowanie konkretnych propozycji legislacyjnych wymaga z pewnością dogłębnego spojrzenia i opracowania konkretnego modelu¹¹, a następnie kompleksowego projektu zmian k.p.k. oraz szczegółowych rozporządzeń. Parę obszarów i kierunków zmian warto jednak wskazać, gdyż są niezbędne do mitygowania zidentyfikowanych zagrożeń. To zaledwie parę zmian, ale chodzi tutaj wyłącznie o zobrazowanie skali problemu, przed którym stoimy.

¹¹ M. Klubińska, *Czynności procesowe na odległość w procesie karnym – założenia modelowe* [w:] *Czynności procesowe na odległość w postępowaniu karnym*, M. Klubińska, A. Lach (red.), Warszawa 2025, s. 358.

Przed wszystkim są to gwarancje poufności komunikacji (zwłaszcza na linii obrońca–oskarżony). Należy wprowadzić przepisy gwarantujące nie-naruszalność komunikacji w trakcie zdalnego postępowania – jak choćby przepisu stanowiącego, że system teleinformatyczny sądu musi zapewniać funkcjonalność wydzielonego, szyfrowanego kanału komunikacji (tzw. wirtualnego/cyfrowego pokoju narad). Komunikacja ta byłaby wyłączona spod jakiegokolwiek nadzoru czy protokołowania, w tym pod rygorem pominięcia czynności procesowej, której narada dotyczyła. W rozdziale 43 k.p.k. (po art. 374 k.p.k.) można byłoby dodać przepis o treści następującej: „System teleinformatyczny służący do przeprowadzenia rozprawy na odległość musi zapewniać oskarżonemu i jego obrońcy funkcjonalność niezwłocznego i poufnego porozumiewania się w wydzielonym kanale komunikacji elektronicznej (cyfrowy pokój narad), niedostępnym dla pozostałych uczestników postępowania. Treść komunikacji wewnątrz tego kanału objęta jest bezwzględną tajemnicą i nie podlega utrwaleniu przez system”.

Konieczne wydaje się też doprecyzowanie, w jaki sposób weryfikowane będą dowody podatne na zaawansowaną manipulację. Dobrym krokiem byłoby przyjęcie, że autentyczność dowodów cyfrowych (audio, wideo, dokumentów) wygenerowanych lub zmodyfikowanych przez AI powinna zostać zweryfikowana przez biegłego z zakresu informatyki, akredytowanego przez odpowiedni organ (np. CLKP). Niezbędne jest też wprowadzenie obowiązku dołączania do akt *hash verification report* (raportu sumy kontrolnej) dla każdego kluczowego dowodu cyfrowego, potwierdzającego jego integralność od momentu zabezpieczenia. Należy nadto ustawowo zagwarantować, że postęp technologiczny nie pozbawi nikogo prawa do sprawiedliwego sądu – choćby przez wprowadzenie przepisu dającego oskarżonemu prawo do złożenia wniosku o prowadzenie postępowania w formie tradycyjnej (papierowej i stacjonarnej) w przypadku wykazania, że jego sytuacja osobista, zdrowotna lub brak dostępu do technologii uniemożliwia mu pełną realizację prawa do obrony w formie cyfrowej. Sąd miałby obowiązek przychylić się do takiego wniosku.

Podsumowanie

Powyższa analiza wiedzie do wniosku, że cyfryzacja postępowań karnych jawi się jako proces nieunikniony i cywilizacyjnie pożądany, który jednak w stadium wdrożeniowym generuje fundamentalne napięcia na linii: efektywność vs. rzetelność procesu. Kluczowe wnioski płynące z analizy obszarów zagrożeń i kosztów to możliwość ingerencji w fundamenty karnoprosesowe w postaci klasycznego rozumienia zasady bezpośredniości

oraz jawności. Ekonomicznym paradoksem cyfryzacji jest to, że jakkolwiek e-justice obiecuje oszczędności, to faktycznie generuje ogromne wydatki na cyberbezpieczeństwo, archiwizację danych w chmurze, aktualizację systemów oraz szkolenia. Są to koszty stałe, które Skarb Państwa będzie musiał ponosić bezterminowo, aby uniknąć paraliżu państwa. Pełny sukces cyfryzacji zależy zatem nie tyle od jakości kodów programistycznych, ile od stworzenia systemowych bezpieczników prawnych i zapewnienia funduszy finansowych sukcesywnie przeznaczanych na ten cel. Muszą one przede wszystkim chronić uczestników przed „dyktaturą algorytmu” i cyberatakami oraz zapewniać, że technologia pozostanie każdorazowo służebna wobec konstytucyjnych praw obywatelskich.

Całościowe podsumowanie problematyki cyfryzacji postępowań karnych (e-justice) wykazuje, że stoimy obecnie przed największą transformacją wymiaru sprawiedliwości od czasów kodyfikacji procedur¹². Technologia przestaje być tylko narzędziem, a staje się współuczestnikiem procesu. Cyfryzacja jest niezbędna, aby sądownictwo nie stało się „analogowym skansenem”. Pamiętać natomiast należy, że cyfryzacja nie może być celem samym w sobie, gdyż jest tylko środkiem do urzeczywistnienia sprawiedliwości. Sukces tego procesu zależy od tego, czy ustawodawca zdąży obudować technologię gwarancjami procesowymi, zanim systemy informatyczne na trwałe zmienią dynamikę sali rozpraw. Takich czynności nie ma jednak zbyt wiele i nie są planowane z logicznym wyprzedzeniem, zwłaszcza w powiązaniu z etapami wdrożeń cyfrowych. Wywołuje to obawy o powodzenie przedsięwzięcia cyfryzacji postępowań karnych oraz czyni niemożliwą próbę wyznaczenia jakiegokolwiek realnego terminu jej zakończenia.

Abstrakt

Publikacja stanowi analizę newralgicznych punktów niezbędnej cyfrowej reformy wymiaru sprawiedliwości na przykładzie postępowań karnych. Wskazano w niej, że cyfryzacja to fundamentalna zmiana paradygmatu rzetelnego procesu – co musi się wiązać ze stosownymi zmianami w prawie. Stwierdzono również potrzebę wdrożeń wielu nowych instrumentów w postępowaniu karnym, w tym wirtualnej sali narad dla rozpraw zdalnych. Zaproponowano konkretne zmiany w przepisach postępowania karnego, akcentując niezbędność szerszej nowelizacji – obejmującej wyłącznie zagadnienia cyfrowe. Cyfryzacja postępowań karnych (e-justice) z jednej bowiem strony oferuje przyspieszenie postępowań i ułatwienie dostępu do akt, z drugiej jednak stwarza poważne zagrożenia dla rzetelności procesu. Generuje też znaczne obciążenia finansowe dla państwa.

¹² A. Sołtysińska, *Digitalization of Criminal Justice* [w:] *Obywatel w centrum działań e-administracji w Unii Europejskiej*, S. Dudzik, I. Kawka, R. Śliwa (red.), Kraków 2023, s. 253.

Kluczowe zagrożenia obejmują: wykluczenie cyfrowe, osłabienie zasady bezpośredniości oraz problemy z poufnością komunikacji i jawnością postępowania. Pełne zrozumienie pól zagrożeń i ponoszonych kosztów jest niezbędne, aby system *e-justice* wydawnie wspierał wymiar sprawiedliwości.

Słowa kluczowe: postępowanie karne, cyfryzacja, wirtualna sala narad, zagrożenia, koszty.

BIBLIOGRAFIA

Castells A., Społeczeństwo sieci, Warszawa 2007.

Czarnecki P., Rozprawa sądowa w Internecie. Postulat wprowadzenia możliwości transmisji (streamingu) rozpraw sądowych w rzetelnym procesie karnym, „Prokuratura i Prawo” 2025, 3.

Czetwertyński S., Mroczek-Czetwertyńska A., Wykluczenie cyfrowe w społeczeństwie informacyjnym, „Nauki Społeczne” 2012, 1, 5.

Czynności procesowe na odległość w postępowaniu karnym, M. Klubińska, A. Lach (red.), Warszawa 2025.

Dordick H.S., Wang G., The Information Society: A Retrospective View, Newbury Park 1993.

Jedlińska R., Wykluczenie cyfrowe w Polsce na tle krajów Unii Europejskiej, „Ekonomiczne Problemy Usług” 2018, 131, 2.

Kiejnich-Kruk K., Building blocks – strategia cyfryzacji wymiaru sprawiedliwości. Perspektywa estońska, „Przegląd Sądowy” 2025, 3.

Kujawski J., Wykluczenie cyfrowe jako forma wykluczenia społecznego. Przypadek Polski, „Media i Społeczeństwo” 2018, 9.

Marszałek J., Skwarcow M., Użycie sztucznej inteligencji w postępowaniu karnym, „Przegląd Sądowy” 2025, 3.

Obywatel w centrum działań e-administracji w Unii Europejskiej, S. Dudzik, I. Kawka, R. Śliwa (red.), Kraków 2023.

Opitek P., Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych, „Prokuratura i Prawo” 2018, 7–8.

W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi, D. Szumiło-Kulczycka (red.), Warszawa 2022.

Zgoliński I., Technology and Criminal Proceedings: An attempt to systematize the issue and determine the main directions of implementation, „Europejski Przegląd Prawa i Stosunków Międzynarodowych” 2025, 1, 73.