JOURNAL OF MODERN SCIENCE

2/66/2026

www.jomswsge.com

DOI: 10.13166/jms/226336

Weronika Pielak-Sitek
WSGE Academy of Applied Sciences
in Józefów, Poland
ORCID iD: 0000-0003-2823-9083

AUTHENTICITY AND RELIABILITY OF EVIDENCE IN JUDICIAL PROCEEDINGS IN THE ERA OF GENERATIVE ARTIFICIAL INTELLIGENCE: A POLISH AND EUROPEAN UNION PERSPECTIVE

AUTENTYCZNOŚĆ I WIARYGODNOŚĆ DOWODÓW W POSTĘPOWANIU SĄDOWYM W ERZE GENERATYWNEJ SZTUCZNEJ INTELIGENCJI: PERSPEKTYWA POLSKA I UNIJNA

Abstract

Purpose: *The article asks whether Polish and European Union evidence law can secure the reliability of evidence that may have been fabricated with generative artificial intelligence (GenAI) – from deepfakes to synthetic documents and electronic signatures.*

Methods: *It applies the legal-dogmatic method to the Polish procedural codes and EU law, using the United States as a heuristic reference point rather than a full comparator and analysing the European case law binding on Poland.*

Results: *Polish law has no dedicated regime for electronic or AI-generated evidence: such material is admitted and assessed under the free-evaluation principle, with authentication delegated to a court-appointed expert (*biegły*). EU law adds two functional layers – the eIDAS trust-service presumptions and equivalence rules (confined to the cryptographic container, not the content) and the AI Act's marking duties (which fabricators will not observe).*

Discussion: *The continental model relocates rather than removes the gatekeeping problem; the fair-trial right to challenge evidence (Article 6 ECHR) is the decisive safeguard.* De lege ferenda *proposals for Poland and the EU are advanced.*

Keywords: *generative artificial intelligence, deepfake, digital evidence, authentication of evidence, EU AI Act, eIDAS, free evaluation of evidence*

Streszczenie

Cel: *Artykuł bada, czy polskie i unijne prawo dowodowe może zapewnić wiarygodność dowodów, które mogły zostać sfabrykowane za pomocą generatywnej sztucznej inteligencji (GenAI) – od deepfake'ów po syntetyczne dokumenty i podpisy elektroniczne.*

Metody: *Zastosowano metodę dogmatycznoprawną wobec polskich kodeksów procesowych i prawa UE, traktując prawo Stanów Zjednoczonych jako heurystyczny punkt odniesienia, a nie pełnoprawny komparator, oraz analizując orzecznictwo europejskie wiążące Polskę.*

Wyniki: *Prawo polskie nie zawiera odrębnego reżimu dla dowodu elektronicznego ani wytworzonego przez AI: materiał taki jest dopuszczany i oceniany w ramach swobodnej oceny dowodów, a uwierzytelnienie powierza się biegłemu. Prawo UE dodaje dwie warstwy funkcjonalne – domniemania autentyczności z eIDAS (model przerzucenia ciężaru ograniczony do warstwy kryptograficznej, nie treści) oraz obowiązki oznaczania z aktu o AI (których sprawcy nie będą przestrzegać).*

Dyskusja: *Model kontynentalny przemieszcza, a nie usuwa problem kontroli dowodu; decydującą gwarancją jest prawo do zakwestionowania dowodu (art. 6 EKPC). Przedstawiono postulaty de lege ferenda dla Polski i UE.*

Słowa kluczowe: *generatywna sztuczna inteligencja, deepfake, dowód elektroniczny, uwierzytelnianie dowodów, akt o sztucznej inteligencji, eIDAS, swobodna ocena dowodów*

Introduction

Forgery and procedural safeguards have always evolved together; generative artificial intelligence breaks the pattern. Fingerprinting, DNA and digital forensics improved the capacity to *detect* fraud; generative models improve the capacity to *commit* it. The result is a *verification asymmetry*: a convincing fabrication may cost a single prompt; disproving it may require costly forensic analysis, if possible at all (Łabuz et al., 2025). Text, image, audio, video, even authenticating metadata can now be synthesised (Bernacka, 2025; Garcia Vera, 2024) – at worst cross-modally, with mutually corroborating channels generated together to defeat the cross-referencing on which forensics relies.

Scholarship is dominated by the United States, whose Federal Rules of Evidence presuppose adversarial *gatekeeping*: threshold filters of authenticity (Rule 901) and reliability (Rule 702), judge-administered before the fact-finder weighs the exhibit (Delfino, 2023). The thesis defended here is that Poland and the European Union possess *no* bespoke regime for synthetic-media evidence: AI fabrication is triaged through free evaluation, the court-appointed expert (*biegły*), the eIDAS presumptions, the AI Act's marking duties, and the fair-trial right to contest evidence under Article 6 of the European Convention on Human Rights (ECHR). This reactive architecture relocates the authentication problem rather than removing it and leaves it exposed to the *liar's dividend* – the bad-faith denunciation of genuine evidence as fake (Chesney & Citron, 2019). The reform proposed is accordingly *de lege ferenda* and civil-procedural.

Research methods

The study is doctrinal. It applies the legal-dogmatic method to the Polish procedural codes – the Code of Criminal Procedure (*k.p.k.*), the Code of Civil Procedure (*k.p.c.*), the Code of Administrative Procedure (*k.p.a.*) and the Civil Code (*k.c.*) – and to directly applicable EU law, to reconstruct how each treats the authenticity and probative value of potentially AI-fabricated evidence. The United States is used not as a full comparator but as a heuristic foil: its Federal Rules of Evidence supply the most developed vocabulary for synthetic-media evidence – front-loaded, threshold gatekeeping – and throw the continental design into relief; the article surveys no American case law, drawing on that system only through secondary literature. The European case law is selected by one criterion: leading ECtHR and CJEU authorities, binding on Poland, on the admission and contestation of unlawfully obtained, covert or digital evidence – the setting into which a disputed synthetic exhibit will fall. The analysis starts with the EU framework, turns to Polish evidence law and that case law, and ends with *de lege ferenda* proposals.

The European Union framework for AI-generated evidence

European Union law leaves the admissibility of evidence to national procedure, yet shapes how synthetic media reach the courtroom.

The AI Act: transparency, marking and justice as high risk

Regulation (EU) 2024/1689 (the AI Act) applies directly in Poland (Artificial Intelligence Act, 2024): under Article 50(2) providers of generative systems must mark synthetic audio, image, video and text in machine-readable form; under Article 50(4) deployers must disclose deepfakes and AI-generated text on matters of public interest. Both duties bind only from 2 August 2026, leaving earlier material unmarked; the proposed Digital Omnibus on AI (COM(2025) 836; provisional agreement May 2026) would grant generative systems already on the market before that date a transitional period to comply with Article 50(2), widening the unmarked window (Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 (*Digital Omnibus on AI*), 2025). Even afterwards a mark or its absence is at most a circumstance to weigh: a fabricator will not mark evidence; law-enforcement and artistic exemptions leave much relevant content lawfully unmarked; and marks can be stripped, as the Commission's Code of Practice concedes (European Commission, AI Office (DG CNECT), 2026). A minority of image generators implement robust marking, fewer adequately label deepfakes (Rijsbosch et al., 2025), and a mark can even be affixed to authentic content to discredit it. Annex III(8), classifying AI assisting a judicial authority as high-risk, reaches the court's tools, not the fabricated evidence before it.

eIDAS and the presumption of authenticity as a burden-shifting model

Regulation (EU) No 910/2014 (eIDAS) attaches genuine rebuttable presumptions to a qualified electronic seal (integrity and correct origin, Art. 35(2)) and a qualified timestamp (accurate time, Art. 41(2)); a qualified electronic signature carries the *equivalent legal effect* of a handwritten signature (Art. 25(2)) – an equivalence rule, not a presumption (Regulation (EU) No 910/2014 (eIDAS), 2014). The true presumptions shift the evidential burden to the challenger without extinguishing the right to contest; the evidential *value* of a qualified signature remains nationally governed – V.B. Trade OOD (2024) confirmed Article 25 does not harmonise it, subject to effectiveness. Regulation (EU) 2024/1183 (*eIDAS 2.0*) adds the European Digital Identity Wallet (eIDAS 2.0 (European Digital Identity Framework), 2024). But eIDAS authenticates the *signing act*, not the *content*: AI-generated material wrapped in valid trust services can inherit unwarranted credibility, while unsigned synthetic media have no anchor at all.

Cross-border acquisition and data protection

The e-Evidence Regulation (EU) 2023/1543 (applicable from 18 August 2026) governs cross-border access, not downstream authentication: a file delivered under a European Production Order must still be authenticated by the Polish court, the more so as provenance metadata can itself be synthetic (E-Evidence Regulation, 2023). The GDPR bears on integrity mainly through its accuracy principle (Art. 5(1)(d)); whether data gathered in breach may be adduced turns not on any bar in the Regulation but on the fair-trial balance struck in NTH Haustechnik (C-484/24) (2026) (Section 5) (GDPR, 2016).

Polish evidence law under generative-AI stress

Polish law has no statutory definition of, or dedicated regime for, *electronic evidence,* let alone AI-generated evidence. Digital exhibits, deepfakes included, are admitted under general rules and assessed under free evaluation (Michalik & Zaremba, 2025). What Poland lacks is not admissibility screening – evidentiary prohibitions (*zakazy dowodowe*) and grounds for refusing evidence exist (Art. 170 § 1 k.p.k.; Art. 235[2] k.p.c.) – but an authenticity – or reliability-based threshold analogous to US Rules 901 and 702. Art. 168a k.p.k. points the other way: subject to enumerated exceptions, it bars excluding evidence *solely* because it was obtained unlawfully – a rule about the manner of obtaining, not the authenticity of content.

Criminal procedure (k.p.k.)

Criminal procedure follows a mixed, strongly inquisitorial model: Article 2 § 2 imposes material truth, Article 7 free but reasoned evaluation of all evidence, with no *Daubert*-style reliability filter (Kodeks Postępowania Karnego (k.p.k.), 1997). Where a material circumstance requires specialist knowledge (*wiadomości specjalne*), the court *must* appoint an expert (*biegły*) under Article 193 § 1; whether a recording is synthetic is a paradigm case, making authentication court-driven, not a party burden. Because the prosecution bears the burden of proof, evidence is taken *ex officio* (Art. 167) and unresolved doubt resolved *in dubio pro reo* (Art. 5 § 2), the burden analysis below concerns civil, not criminal, procedure. Polish criminal law has no dedicated *AI falsification* offence; deepfakes are reached through forgery (Art. 270 k.k., a deepfake possibly qualifying as a *dokument* under Art. 115 § 14 k.k.) and fraud (Art. 286 § 1), while a fake meant to direct proceedings against a person engages Art. 235 k.k., not Art. 233, confined to false testimony and expert opinions (Garcia Vera, 2024; Kodeks Karny (k.k.), 1997).

Civil procedure (k.p.c.) and the Civil Code

Civil procedure, by contrast, is adversarial: expert evidence under Article 278 k.p.c. is in practice contingent on a party's motion and advance of costs, with no material-truth mandate (Kodeks Postępowania Cywilnego (k.p.c.), 1964). Article 77³ k.c. defines a document functionally – any carrier of information permitting acquaintance with its content, no signature required (Kodeks Cywilny (k.c.), 1964). Article 243¹ k.p.c. confines the documentary-evidence provisions to documents containing text and identifying their issuer; a non-textual deepfake video therefore enters through Article 308 (records of image or sound, assessed under the inspection and document rules) or the residual Article 309 (Uliasz, 2023). Article 245 presumes the signatory of a signed private document made the declaration; under Article 253 the denier of their own document must prove its falsity, the proponent of a third-party document its genuineness. Article 254 supplies the examination mechanism; Article 255 penalises bad-faith challenges. An unsigned AI-generated file enjoys no presumption at all, its weight left to free evaluation under Article 233 § 1 (Michalik & Zaremba, 2025).

Article 253 does not, however, reach the unsigned synthetic media of Article 308. Hence the *de lege ferenda* claim: the logic of its second sentence should extend to these non-textual exhibits outside Article 243¹, so that once a party raises specific, articulable grounds for suspecting fabrication – a threshold a bare denial cannot meet – the burden of substantiating genuineness shifts to the *proponent*. Doctrine points towards, but does not yet compel, this allocation for textual media: in Wyrok Sądu Apelacyjnego w Warszawie (2017) the Warsaw Court of Appeal held a printout's easy modifiability goes to weight, not admissibility, and the literature leaves unsettled who must establish an electronic document's authenticity once credibly disputed (Gołaczyński, 2023; Uliasz, 2023). The eIDAS presumptions bind Poland by the Regulation's direct applicability (Art. 288 TFEU), not through Article 78¹ k.c. – which governs only the electronic *form* of juridical acts – or the 2016 Trust Services Act, an organisational statute (Kodeks Cywilny (k.c.), 1964, Ustawa o Usługach Zaufania Oraz Identyfikacji Elektronicznej, 2016). Table 1 maps the resulting allocation.

Table 1. *Allocation of the authenticity burden across categories of exhibit (Polish civil procedure and the eIDAS layer)*

Exhibit	Governing rule	Presumption / burden
Signed private document, own	Art. 245; 253 s. 1 k.p.c.	Presumption the signatory declared; the denier of their own document must prove its falsity.
Signed private document, third party	Art. 253 s. 2 k.p.c.	Proponent bears the burden of proving genuineness.
Unsigned synthetic media (deepfake image, sound, video)	Art. 308 k.p.c. (outside Art. 243[1])	No presumption; free evaluation (Art. 233 § 1). *De lege ferenda*: burden shifts to the proponent on a specific challenge.
Official document	Art. 76 k.p.a.	Rebuttable presumption of authenticity and truth.
Qualified e-signature, seal or timestamp	eIDAS Art. 25(2); 35(2); 41(2)	Equivalence (signature) or rebuttable presumption shifting the burden to the challenger – container, not content.

Administrative procedure (k.p.a.) and the constitutional frame

Administrative procedure has an open evidentiary catalogue and free assessment (Arts. 75 § 1, 80 k.p.a.); its pressure point is the rebuttable presumption for official documents (Art. 76), which a fabricated *official* PDF borrows unless rebutted (Kodeks Postępowania Administracyjnego (k.p.a.), 1960). Underpinning all three procedures, the Constitution guarantees the right to a court (Art. 45), defence rights (Art. 42) and privacy (Arts. 47, 51); read with Article 6 ECHR, these anchor the right to challenge authenticity. The Charter's Articles 47–48 (Art. 52(3) CFR) reinforce this only within the scope of EU law (Art. 51(1) CFR) – as with GDPR data, e-Evidence or AI-Act systems – so a purely domestic civil dispute falls outside the Charter, leaving Article 6 ECHR alone, which itself does not reach every administrative dispute.

European case law: the fair-trial right to challenge evidence

Neither the ECtHR nor the CJEU has yet ruled on a deepfake, but their case law fixes the terms on which suspect synthetic evidence will be litigated. With one exception, exclusion is not automatic: using a statement obtained in breach of Article 3 ECHR, or real evidence obtained by torture, renders proceedings automatically unfair (Gäfgen v. Germany [GC], 2010); for merely unlawful, unreliable or manipulable evidence – and real evidence from ill-treatment short of torture – there is no per se exclusionary rule. The question is whether the proceedings *as a whole* were fair, turning on a genuine opportunity to challenge the evidence and on its quality and reliability – a test originating in Schenk v. Switzerland (1988) and consolidated in Jalloh v. Germany [GC] (2006).

In Yüksel Yalçınkaya v. Türkiye [GC] (2023) the Grand Chamber found an Article 6 § 1 violation because the applicant could not effectively access or challenge the integrity and reliability of the electronic data grounding his conviction – the closest analogue for possibly synthetic evidence. Bykov v. Russia [GC] (2009) found no violation because the applicant could contest a corroborated covert recording. Where authenticity turns on expertise, Khodorkovskiy and Lebedev v. Russia (2013) required that the defence be able to cross-examine prosecution experts and adduce counter-expertise; Salabiaku v. France (1988), by analogy from its criminal-limb rule, confines presumptions within reasonable limits preserving the rights of the defence, so any authenticity presumption must remain rebuttable. For the court-appointed-expert model Polish law relies on, Mantovanelli v. France (1997) adds a civil-limb requirement: effective party participation in producing a decisive court-commissioned report.

The CJEU converges from national procedural autonomy bounded by effectiveness. In M.N. (EncroChat) (2024) the Grand Chamber held that where a defendant cannot comment effectively on evidence apt to have a preponderant influence on the findings, the national court must disregard it; anchored in Article 14(7) EIO Directive (EIO Directive, 2014), its extension to a purely domestic synthetic exhibit is an analogy through effectiveness, not a direct holding. NTH Haustechnik (C-484/24) (2026) confirmed that personal data gathered in breach of the GDPR is not automatically inadmissible: admissibility turns on foreseeable national rules and the fair-trial balance, EU law laying down no exclusionary rule (subject to equivalence and effectiveness); for tainted or synthetic evidence the control point remains national procedure.

Assessment and proposals de lege ferenda

The continental model compared

The US model is front-loaded: threshold screens of authenticity (Rule 901, with a drafted deepfake Rule 901(c) held in reserve) and reliability (Rule 702, with Rule 707 proposed, public comment closed February 2026), cleared by the proponent before a lay jury weighs the exhibit (Capra, 2024; Delfino, 2023). Polish procedure is back-loaded: the professional judge admits and weighs (Section 4), and nothing forces *biegły* authentication before the exhibit enters the court's reasoning. Continental law can codify burden-shifting, as eIDAS shows, but only for cryptographic provenance, not content (Regulation (EU) No 910/2014 (eIDAS), 2014); Poland's Act on Artificial Intelligence Systems, passed by the Sejm in June 2026 and awaiting signature, repeats the pattern: a supervisory architecture, no evidentiary rule (Ustawa o Systemach Sztucznej Inteligencji, 2026).

Recommendations

Early Polish scholarship argued for categorically excluding deepfakes from civil proceedings as unlawfully created material (Kaczmarek-Templin, 2019); the present proposal takes the opposite route – admission under free evaluation disciplined by a calibrated burden-shift, aligning with Michalik & Zaremba (2025). The measures below work within that architecture; the first parallels – without borrowing – the trigger of the proposed US Rule 901(c). *First, a rebuttable authenticity challenge in civil procedure.* Article 253 k.p.c., flanked by Article 254's examination mechanism and Article 255's bad-faith sanction, already shifts the genuineness burden for contested third-party private documents but not for the unsigned synthetic media of Article 308. The proposal extends that logic: on specific, articulable grounds that an exhibit may be AI-generated – mere invocation of deepfakes being insufficient – the burden of substantiating genuineness shifts to the proponent, dischargeable through provenance, a qualified signature, corroboration, or expert opinion (Michalik & Zaremba, 2025). That specificity threshold guards against the *liar's dividend* without loading provenance costs onto honest litigants. *Second, expert authentication for contested synthetic media.* A *biegły* is obligatory in criminal procedure (Art. 193 k.p.k.) but party-driven in civil (Art. 278 k.p.c.); the reform makes court-appointed authentication the default in a credible manipulation dispute, with adversarially testable conclusions, consistent with Khodorkovskiy and Lebedev v. Russia (2013) and, for the civil expert, Mantovanelli v. France (1997). *Third, marking as a weighed indicator, not a presumption.* Courts should weigh an AI Act Article 50 mark as one circumstance within free evaluation, never conclusive, given watermarking's non-adoption and fragility (Rijsbosch et al., 2025). The affirmative infrastructures differ by layer: cryptographic *content* provenance (C2PA, JPEG Trust) for the media themselves, the eIDAS 2.0 wallet for the *signed-document* subset alone (eIDAS 2.0 (European Digital Identity Framework), 2024). *Fourth, institutional capacity.* Forensic-IT expert panels, judicial training, and provenance-aware e-filing would let courts deliver the authentication the codes envisage.

Limitations

Three limits qualify the argument. First, it is doctrinal, not empirical: no public data show how often Polish courts confront disputed synthetic media. Second, the expert-authentication default presupposes forensic capacity and funding that Polish courts and parties often lack – under Article 278 k.p.c. the cost advance can fall on the litigant least able to bear it – so its value depends on the capacity just urged. Third, the burden-shift invites two objections: well-resourced counsel may manufacture *articulable* doubts, with Article 255's sanction (today confined to document challenges) the intended but untested check; and the shift must be squared with the persuasion burden that Article 6 k.c. and Article 232 k.p.c. keep on the party asserting the fact. The proposal does not reverse that ultimate burden; it adds a defined evidentiary trigger and means of discharge – a modest predictability gain set against the *liar's dividend*.

Conclusions

Generative artificial intelligence sharpens an old problem – ensuring evidence is what it purports to be – because fabrication is now cheaper than verification. Neither Poland nor the European Union has a purpose-built regime for synthetic-media evidence: Polish procedure admits digital exhibits under general rules, leaves them to free evaluation and delegates authentication to a court-appointed expert, setting no authenticity-based admissibility threshold, while the EU adds only marking duties the fabricator will not observe and eIDAS presumptions that reach the cryptographic container, not the content. Under the fair-trial case law of the ECtHR and the CJEU, the decisive safeguard is the effective right to challenge, not exclusion.

The continental architecture moves the gatekeeping problem rather than removing it: its material-truth mandate and mandatory court-driven expert inquiry are genuine strengths, but nothing forces authentication before an exhibit enters the court's reasoning. The proposals advanced above answer that gap from within the existing Polish and EU framework, without importing the American gatekeeping model. They share a premise: when any proof can be produced with a prompt, the integrity of proceedings depends less on new admissibility filters than on preserving a genuine, well-resourced opportunity to contest what evidence purports to show.

References

Bernacka, J. (2025). Problematyka prawna technologii deepfake – analiza legalności tworzenia i rozpowszechniania deepfake'ów po uchwaleniu AI Act. *Prawo i Więź*, *58*(5), 671–694. https://doi.org/10.36128/hg1acq35

Bykov v. Russia [GC]. (2009). *Application no. 4378/02, judgment of 10 March 2009, ECHR 2009*.

Capra, D. J. (2024). Deepfakes reach the advisory committee on evidence rules. *Fordham Law Review*, *92*(19), 2491–2506. https://fordhamlawreview.org/wp-content/uploads/2024/05/Vol.-92_19_Capra-2491-2506.pdf

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, *107*, 1753–1820.

Delfino, R. A. (2023). Deepfakes on trial: A call to expand the trial judge's gatekeeping role to protect legal proceedings from technological fakery. *Hastings Law Journal*, *74*(2), 293–360. https://repository.uclawsf.edu/hastings_law_journal/vol74/iss2/3/

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters (2014).

European Commission, AI Office (DG CNECT). (2026). *Code of practice on marking and labelling of AI-generated content*.

Gäfgen v. Germany [GC]. (2010). *Application no. 22978/05, judgment of 1 June 2010, ECHR 2010*.

Garcia Vera, G. (2024). Deep fake – postęp technologiczny a prawo karne. *Acta Iuridica Resoviensia*, (1 (44)), 39–53. https://doi.org/10.15584/actaires.2024.1.3

Gołaczyński, J. (2023). Pojęcie dokumentu elektronicznego w prawie cywilnym. *Przegląd Prawa i Administracji, Acta Universitatis Wratislaviensis*, *133*, 33–56. https://doi.org/10.19195/0137-1134.133.3

Jalloh v. Germany [GC]. (2006). *Application no. 54810/00, judgment of 11 July 2006, ECHR 2006-IX*.

Kaczmarek-Templin, B. (2019). Deepfake i jego walor dowodowy w procesach cywilnych. In K. Flaga-Gieruszyńska, J. Gołaczyński, & D. Szostek (Eds.), *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane* (pp. 95–102). C.H. Beck.

Khodorkovskiy and Lebedev v. Russia. (2013). *Applications nos. 11082/06 and 13772/05, judgment of 25 July 2013*.

Kodeks Cywilny (k.c.). Dz.U. 1964 nr 16 poz. 93; t.j. Dz.U. 2026 poz. 795 (1964).

Kodeks Karny (k.k.). Dz.U. 1997 nr 88 poz. 553; t.j. Dz.U. 2025 poz. 383 (1997).

Kodeks Postępowania Administracyjnego (k.p.a.). Dz.U. 1960 nr 30 poz. 168; t.j. Dz.U. 2025 poz. 1691 (1960).

Kodeks Postępowania Cywilnego (k.p.c.). Dz.U. 1964 nr 43 poz. 296; t.j. Dz.U. 2026 poz. 468 (1964).

Kodeks Postępowania Karnego (k.p.k.). Dz.U. 1997 nr 89 poz. 555; t.j. Dz.U. 2026 poz. 490 (1997).

Łabuz, M., Małecki, M., & Mika-Łabuz, K. (2025). Dziecięca pornografia w formie deep fakes – problemy wykładni na gruncie polskiego prawa karnego i propozycje legislacyjne. *Prawo w Działaniu*, *61*, 54–84. https://doi.org/10.32041/pwd.6103

Mantovanelli v. France. (1997). *Application no. 21497/93, judgment of 18 March 1997*.

Michalik, P., & Zaremba, P. (2025). Deepfake jako dowód w procesie cywilnym – rozważania na tle polskiego postępowania cywilnego. *Prawo i Więź*, *57*(4). https://doi.org/10.36128/PRIW.VI57.1206

M.N. (EncroChat). (2024). *Case C-670/22, ECLI:EU:C:2024:372, judgment of 30 April 2024*.

NTH Haustechnik (C-484/24). (2026). *Case C-484/24, ECLI:EU:C:2026:496, judgment of 18 June 2026, on the GDPR and the admissibility of unlawfully obtained personal data as evidence*.

Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 (*Digital Omnibus on AI*), Commission Proposal (COM) COM(2025) 836 final (2025).

Regulation (EU) 2016/679 (General Data Protection Regulation), L 119 Official Journal of the European Union 1 (2016).

Regulation (EU) 2023/1543 (e-Evidence Regulation), L 191 Official Journal of the European Union 118 (2023).

Regulation (EU) 2024/1183 (European Digital Identity Framework, eIDAS 2.0) (2024).

Regulation (EU) 2024/1689 (Artificial Intelligence Act), Regulation 2024/1689 (2024).

Regulation (EU) No 910/2014 (eIDAS), L 257 Official Journal of the European Union 73 (2014).

Rijsbosch, B., Dijck, G. van, & Kollnig, K. (2025). *Missing the mark: Adoption of watermarking for generative AI systems in practice and implications under the new EU AI act*. https://arxiv.org/abs/2503.18156

Salabiaku v. France. (1988). *Application no. 10519/83, judgment of 7 October 1988*.

Schenk v. Switzerland. (1988). *Application no. 10862/84, judgment of 12 July 1988*.

Uliasz, M. (2023). Dowód z dokumentu według art. 308 k.p.c. *Przegląd Prawa i Administracji, Acta Universitatis Wratislaviensis No 4149*, *133*, 175–191. https://doi.org/10.19195/0137-1134.133.12

Ustawa o Systemach Sztucznej Inteligencji [Act on Artificial Intelligence Systems], Government bill / druk sejmowy Druk nr 2443 (2026).

Ustawa o Usługach Zaufania Oraz Identyfikacji Elektronicznej. Dz.U. 2016 poz. 1579; t.j. Dz.U. 2024 poz. 1725 (2016).

V.B. Trade OOD. (2024). *Case C-466/22, ECLI:EU:C:2024:185, judgment of 29 February 2024, on Article 25 of Regulation (EU) No 910/2014 (eIDAS)*.

Wyrok Sądu Apelacyjnego w Warszawie. (2017). *sygn. I ACa 2111/15, judgment of 13 January 2017 – computer printouts and screenshots as other evidence under art. 308–309 k.p.c., assessed under free evaluation*.

Yüksel Yalçınkaya v. Türkiye [GC]. (2023). *Application no. 15669/20, judgment of 26 September 2023*.