



CHILD PORNOGRAPHY IN HUNGARIAN CRIMINAL LAW: OFFENDER CATEGORIES AND THE INVESTIGATIVE POTENTIAL OF ARTIFICIAL INTELLIGENCE

KISS, ESZTER¹ – CZEBE, ANDRÁS²

ABSTRACT

This article examines the Hungarian offence of child pornography from criminal-law, criminological, comparative-law, and technological perspectives. It outlines the development of the Hungarian legal framework under the influence of international and European norms, and compares it with the regulation in Germany, the United Kingdom, the United States, and Japan. The article also argues that the term paedophile is often used inaccurately in legal and public discourse, since not all offenders involved in child pornography cases fall within that clinical category. Against this background, it considers whether artificial-intelligence-based image recognition may assist criminal investigations involving child sexual abuse material. It concludes that such systems may be legally and practically useful in Hungary, provided that they remain subject to clear statutory regulation, meaningful human oversight, and strict data-protection safeguards.

KEYWORDS Child pornography; child sexual abuse material; artificial intelligence; criminal investigation; Hungarian criminal law

1. Introduction

As children gain access to smartphones and social media at an increasingly early age, the digital environment has become a significant site of sexual exploitation involving minors (NMHH, 2021). The digital environment has become a space of heightened vulnerability for minors (Hottó, 2024). This development has created new opportunities for offenders to obtain sexualized images of children through deception, coercion, and online manipulation (Mezei, 2021). In Hungary, such conduct is criminalized under Sections 204 and 204/A of Act C of 2012 on the Criminal Code.

¹ Graduate Law Student at Széchenyi István University, Deák Ferenc Faculty of Law and Political Sciences, Győr, Hungary.

² Associate Professor at Széchenyi István University, Deák Ferenc Faculty of Law and Political Sciences, Department of Criminal Law, Győr, Hungary.

This article examines the phenomenon from criminal law, criminological, and criminalistics perspectives. It proceeds from two premises. First, offences involving child sexual abuse material are characterised by substantial latency, as child victims are often intimidated into silence. Second, the investigation of such cases is highly resource-intensive because authorities must review large volumes of digital data, creating both practical burdens and risks of human error.

Against this background, the article explores whether artificial intelligence, especially machine-learning-based image recognition, may assist in the detection of child sexual abuse material, including pseudo-pornographic content. It further analyses the domestic and international legal framework and considers whether limited automation could improve the efficiency of criminal investigations, allowing law enforcement to concentrate more resources on identifying and prosecuting high-risk offenders.

2. The Evolution of the Hungarian Offence of Child Pornography

The current Hungarian regulation of child pornography is the result of a gradual convergence between domestic criminal law, international child-protection instruments, and European Union standards. At the international level, the 1989 UN Convention on the Rights of the Child established the basic obligation to protect children from sexual exploitation, including their use in pornographic performances and materials. This framework was later reinforced by the Optional Protocol on the sale of children, child prostitution and child pornography, as well as by the Council of Europe's Lanzarote Convention. At the European level, both Framework Decision 2004/68/JHA and, subsequently, Directive 2011/93/EU required Member States to adopt broader and more effective measures against the sexual exploitation of children, including offences committed through digital technologies (Csapucha, 2020).

Hungary incorporated these developments gradually. The broader child-rights orientation of the Convention was reflected in domestic law through the Child Protection Act of 1997 (Honti, 1998), while criminal-law protection developed through successive amendments to the Criminal Code. Child pornography first became a distinct criminal offence in Hungary in 1997. The original provision focused primarily on the production and distribution of prohibited pornographic recordings involving children, but the regulation remained relatively narrow in scope. In the following years, the legislature progressively expanded the range of punishable conduct to include, inter alia, acquisition, possession, offering, transfer, and making such material accessible to others.

This legislative development reflected a broader conceptual shift. Hungarian law moved away from an obscenity-centred understanding of pornography and

increasingly framed the offence in terms of the protection of minors from sexual exploitation (Csapucha, 2020). That shift became more pronounced after Hungary's accession to the European Union and the growing influence of international and European standards. A major restructuring took place in 2007, when the earlier offence was replaced by a provision more clearly centred on pornographic depictions of persons under eighteen and better aligned with Hungary's external legal obligations (Kovács, 2018).

The current Criminal Code, adopted in 2012, preserved the core structure of the earlier offence but repositioned it within a reconceptualised chapter on sexual offences. The most important recent reform came in 2021. The legislature separated offences relating to pornographic recordings from those involving pornographic performances, now regulated in Sections 204 and 204/A of the Criminal Code. The amendment also broadened the statutory concept of a pornographic recording to include realistic depictions of non-existent persons, thereby moving Hungarian law closer to the wider European approach to pseudo- or virtual child pornography. At the same time, penalties were increased, new aggravating circumstances were introduced, and certain limited privileged rules were retained for offenders aged between fourteen and eighteen (Tóth, 2025).

The present Hungarian framework extends beyond the definition of the offence itself. In addition to the criminalisation of production, distribution, possession, and related conduct, the law imposes mandatory permanent disqualification from occupations or activities involving authority over minors, and recent constitutional and statutory changes have further restricted access to individual presidential clemency in offences committed against children. Taken together, these developments show a clear legislative trend toward broader criminalisation, stricter sanctioning, and closer alignment with international and European child-protection standards (Commission Recommendation (EU) 2024/1238).

3. Comparative Legal Perspectives

National legal systems differ in terminology, structure, and legislative technique, yet a common regulatory pattern can be identified across jurisdictions. In each of the legal systems examined below, child pornography is criminalised through rules covering at least production, distribution, and possession, while digital dissemination has become an increasingly central concern. At the same time, important differences remain regarding protected age groups, the treatment of virtual or synthetic material, and the relationship between child protection and competing constitutional or cultural considerations.



3.1. *Germany*

German law provides one of the clearest examples of differentiated regulation. The Criminal Code distinguishes between child-pornographic content and youth-pornographic content, thereby separating depictions involving children under fourteen from those involving adolescents aged fourteen to seventeen (StGB, §§ 184b–184c). This age-based bifurcation gives the German framework a high degree of internal precision. It also criminalises a broad range of conduct, including dissemination, making content publicly accessible, procurement, and possession, while extending liability to realistic depictions. Although German law remains among the stricter European regimes, recent reform has demonstrated a willingness to recalibrate penalties without abandoning the overall protective structure (Witting, 2019).

3.2. *United Kingdom*

The United Kingdom regulates the field through several statutes rather than through a single codified offence (Coroners and Justice Act 2009; Criminal Justice Act 1988; Criminal Justice and Public Order Act 1994; Protection of Children Act 1978; Sexual Offences Act 2003). The British framework criminalises the taking, making, distribution, and possession of indecent images of children, and later amendments expanded the regime to include pseudo-photographs and related forms of visual representation. A notable feature of the British model is its practical categorisation of images by seriousness, which plays an important role in sentencing (Iemelianenko & Dmytruk, 2025). Compared with the German model, the British approach is less conceptually unified, but it is still mature, comprehensive, and highly adaptable to technological developments.

3.3. *United States*

The United States presents a different model, shaped not only by legislation but also by constitutional adjudication. Federal law criminalises the production, distribution, and possession of child pornography (18 U.S.C. ch. 110, §§ 2251, 2252, 2252A, 2256), and the Supreme Court has made clear that visual depictions involving real minors do not enjoy First Amendment protection (Ashcroft v. Free Speech Coalition, 2002; New York v. Ferber, 1982; Osborne v. Ohio, 1990). At the same time, constitutional limits have constrained attempts to regulate virtual or synthetic material too broadly (Niculescu, 2024). As a result, the American framework is broader than a purely real-child-only approach, but it remains heavily influenced by free-speech doctrine and by the distinction between actual minors, indistinguishable synthetic depictions, and protected expression (Palomares, 2024).

3.4. Japan

Japan regulates child pornography through a special statute rather than through its Penal Code ([Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children](#), arts. 2, 7). The statutory framework criminalises possession, production, provision, and online dissemination, and defines a child as a person under eighteen. Its most distinctive feature, however, lies in its narrower treatment of virtual material ([Galbraith, 2011](#)). Japanese law remains focused primarily on depictions of actual children, while wholly fictional or artificially created depictions have remained more weakly regulated than in several Western jurisdictions ([Takeuchi, 2015](#)). This reflects a different balance between child protection, legal policy, and broader cultural considerations.

3.5. Comparative Findings

From a comparative perspective, the four legal systems illustrate different regulatory priorities. Germany offers the clearest age-based distinction and one of the most systematic statutory models. The United Kingdom demonstrates a fragmented but functionally comprehensive regulatory approach. The United States shows how constitutional constraints can shape the limits of criminalisation, especially in relation to synthetic content. Japan, by contrast, remains comparatively restrictive in its treatment of wholly artificial depictions, revealing a narrower conception of the protected legal interest.

For Hungarian law, these comparisons suggest two broader conclusions. First, the international trend clearly favours broad criminalisation and adaptation to digital forms of offending. Second, the greatest divergence among legal systems now concerns pseudo-, virtual, and AI-generated material. This issue is especially relevant for the present article, because it is precisely in this area that questions of technological development, offender differentiation, and future criminal investigation most closely intersect.

4. Offender Categories, Terminological Precision, and Investigative Risk

A central analytical difficulty in this field lies in the widespread but imprecise use of the term paedophile. The term does not belong to criminal law as such; rather, it originates in clinical psychiatry and refers to a specific pattern of sexual interest subject to diagnostic criteria. It therefore cannot be used accurately as a blanket label for all persons who commit sexual offences against minors, including offences involving child pornography. The routine conflation of psychiatric diagnosis and criminal offending obscures important differences among

perpetrators and may distort both legal analysis and criminal policy (Erdélyi, 2022).

This distinction is particularly important in cases involving child sexual abuse material. Available research suggests that only a part of the broader offender population meets the diagnostic criteria for paedophilia, even if the proportion may be higher among offenders involved in child pornography than among contact offenders more generally. Conversely, not every person with a clinically relevant sexual interest in children commits a criminal offence. The relationship between diagnosis and offending is therefore significant, but not identical (Szabó & Virág, 2023).

A more differentiated criminological approach reveals that offenders in this field are far from homogeneous. The literature distinguishes, among others, compulsive users of pornography, situational or opportunistic offenders, and those whose sexual interest is preferentially and persistently directed toward children. These groups differ in motivation, degree of danger, responsiveness to treatment, and likelihood of reoffending (Weiss, 2020). From the perspective of criminal investigation, such differences are not merely theoretical. They bear directly on the assessment of risk, the likelihood of related offending, and the level of investigative attention required in individual cases.

Table 1: Number of Child Pornography Offenses Committed by Registered Offenders in Hungary
(Ministry of the Interior, Criminal Records Authority, n.d.)

Age group	2020	2021	2022	2023	2024
1. Children (0–13)	16	40	39	181	41
2. Juveniles (14–17)	76	151	79	128	113
3. Young adults (18–24)	55	66	66	72	59
4. Adults (25–59)	100	125	140	228	136
5. Elderly (60+)	6	10	12	8	8
Total	253	392	336	617	357

The issue becomes even more complex in relation to juvenile offenders (see Table 1). A significant proportion of detected child pornography cases involve minors or young persons who exchange self-generated sexual images within peer groups or engage in related conduct without fitting any meaningful clinical notion of paedophilia. In such cases, the indiscriminate use of the term paedophile is not only scientifically inaccurate but also normatively misleading. It collapses crucial distinctions between exploitative offending by adults and unlawful but qualitatively different conduct among adolescents (Csendes-Erdei, 2024).

This terminological problem has practical consequences. If all offenders are treated as if they belonged to a single high-risk category, law-enforcement resources may be allocated inefficiently, and investigative strategies may fail to reflect actual levels of danger. By contrast, recognising the heterogeneity of the offender population makes it possible to distinguish between lower-complexity cases and cases involving a greater likelihood of coercion, repeated offending, or broader sexual exploitation. That distinction is central to the present article, because it helps explain why technological assistance may be most useful in the preliminary sorting and assessment of less complex cases, while higher-risk cases continue to require intensive human investigation.

For this reason, greater terminological precision is necessary. In legal analysis, it is preferable to refer to offenders involved in child pornography or child sexual abuse material, rather than to use paedophile as a generic category. Such precision is not simply a matter of language; it is essential to a more differentiated and more effective investigative response.

5. Artificial Intelligence as an Investigative Tool

Against the background outlined above, the relevance of artificial intelligence in this field lies not in replacing human judgment, but in assisting criminal investigation where very large volumes of digital material must be processed. For the purposes of this article, AI is understood in a functional sense: as a machine-based system capable of analysing inputs and generating outputs that support prediction, classification, or decision-making ([Artificial Intelligence Act, art. 3, point 1](#)). In the present context, the relevant question is whether such systems can help law enforcement authorities identify, filter, and prioritise potentially relevant material in cases involving child pornography.

The most important technological field for this purpose is computer vision. Computer vision enables machines to process and interpret visual inputs such as images and videos, while contemporary image-classification tasks are typically performed through deep-learning methods ([Szeliski, 2022](#)). For the present analysis, the technical details need not be examined exhaustively. What matters is that such systems can be trained to recognise visual patterns and classify content at scale, including material that may be relevant to criminal investigation.

This technological capacity is particularly significant in child pornography cases. Investigations in this field often require the review of very large datasets, including thousands of images, videos, and digital communications. This creates not only a quantitative burden but also a substantial psychological burden for investigators. In such cases, AI may serve as a triage instrument: it can support

the preliminary filtering of digital evidence, reduce the volume of material requiring immediate manual review, and assist in the prioritisation of files that are more likely to be relevant from a criminal-law perspective (Lee et al., 2020).

At the same time, the use of AI in this field must be approached with caution. A system trained to detect child pornography can improve efficiency, but it cannot itself determine criminal liability or replace evidentiary assessment by competent authorities. Error rates remain a central concern, especially in relation to false positives and false negatives (Kaferanis et al., 2023). A false positive may burden the investigation with irrelevant material, while a false negative may result in the overlooking of evidence of serious abuse. For this reason, AI can only be justified here as an assistive tool operating under meaningful human supervision.

This cautious conclusion is supported by a German pilot project. The project demonstrated that AI-assisted image recognition may achieve a high rate of successful detection, while also revealing the continued need for human verification and further refinement. Its significance lies less in the promise of full automation than in showing that AI may already have practical value in the initial sorting and assessment of digital material (Brodowski et al., 2023).

From the perspective of the present article, the main implication is clear. If offender populations and case profiles are heterogeneous, then investigative responses should also be differentiated. AI may be most useful in supporting the preliminary assessment of less complex or lower-risk cases, where the goal is not to replace human investigation but to reduce unnecessary burdens and allow law enforcement authorities to concentrate more resources on cases involving coercion, repeated offending, or other indicators of heightened danger.

6. Conditions for AI-Assisted Implementation in Hungary

The possible use of AI-assisted image recognition in Hungary must be assessed within a multi-layered legal framework. The relevant question is not whether such a system is technologically conceivable, but whether it could be introduced in a manner consistent with EU law, Hungarian criminal law, criminal procedure, and data-protection requirements. From this perspective, the issue is best approached through four interrelated dimensions: EU regulatory requirements, substantive criminal law, procedural law, and data protection.

6.1. EU Regulatory Requirements

At EU level, the primary legal framework is provided by the Artificial Intelligence Act. A system used by or on behalf of law enforcement authorities to assist in the assessment of digital evidence would very likely fall within the category of high-

risk AI systems. This classification has significant legal consequences. Such systems must satisfy requirements relating to risk management, technical documentation, logging, traceability, accuracy, human oversight, and post-deployment monitoring. Their use therefore presupposes not merely technological functionality, but a structured governance framework capable of ensuring transparency, accountability, and legal control.

For the purposes of the present article, one consequence is particularly important: the AI Act does not authorise autonomous decision-making in criminal investigation. Rather, it permits the use of such systems only within a framework that preserves meaningful human supervision. Accordingly, any Hungarian implementation would have to be designed from the outset as an assistive mechanism rather than as a substitute for the evidentiary judgment of investigators, prosecutors, or courts.

6.2. *Substantive Criminal-Law Issues*

From the perspective of substantive criminal law, the principal difficulty lies not in the definition of the offence itself, but in the handling of illicit material for the purposes of training, testing, and operating the system. Under Hungarian law, the acquisition and possession of child pornography are themselves punishable forms of conduct. This creates an obvious tension where the development or operation of an AI system requires access to unlawful material.

A functional legal solution is conceivable, but only if accompanied by clear statutory authorisation. In principle, the social harmfulness normally associated with such conduct is absent where the material is handled exclusively for legitimate law-enforcement purposes under strict control. Even so, legal certainty would be better served by an explicit statutory basis exempting authorised actors from criminal liability under clearly defined conditions. Such a solution would also be consistent with the broader logic already visible in legal systems that recognise limited exceptions for official investigative or professional purposes.

6.3. *Procedural-Law Issues*

Hungarian criminal procedure offers a plausible framework within which such a system could operate. Electronic data may constitute evidence, may be seized, may be made temporarily inaccessible, and may also be subject to orders preserving digital material. Within this procedural context, AI could function as a support instrument for the identification, sorting, and prioritisation of potentially relevant files.

Its role, however, must remain limited. AI may indicate that a dataset is likely to contain child pornography, or conversely that it is unlikely to contain relevant material, thereby assisting investigators in directing their efforts more efficiently. It may also facilitate the structured storage and retrieval of evidence. Yet it cannot replace the procedural guarantees attached to the evaluation of evidence. Hungarian criminal procedure excludes unlawfully obtained evidence, and any AI-assisted handling of digital material must therefore preserve evidential integrity, verifiability, and the possibility of subsequent human review. The legal acceptability of such a system depends not only on what it detects, but also on whether its operation can be reconstructed, explained, and validated within the evidentiary process.

6.4. *Data Protection*

Data protection is an equally central condition of lawful implementation. In this field, the relevant material will often contain personal data of the most sensitive kind, including data concerning sex life and images of children, who are entitled to heightened legal protection. In Hungary, the general data-protection framework is supplemented, for law-enforcement purposes, by the specific rules applicable to criminal data processing. Any AI-assisted system would therefore have to comply with strict requirements concerning purpose limitation, data minimisation, access control, logging, storage limitation, and system security.

The use of AI does not reduce these obligations; on the contrary, it intensifies them. Automated or semi-automated processing introduces additional risks, including unauthorised access, data leakage, model extraction, and the possibility that sensitive material might be reconstructed or misused. For that reason, any domestic implementation would require not only formal legal authorisation but also robust technical and organisational safeguards. It may be argued that a properly designed system could, in some respects, improve protection by reducing the number of individuals exposed to the original material. Even so, that advantage would be acceptable only if the integrity, confidentiality, and evidentiary usability of the data remained fully protected.

6.5. *Conditions for Lawful Implementation*

Taken together, these considerations suggest that AI-assisted detection of child pornography could be introduced in Hungary in principle, but only under strict legal conditions. First, the system would have to remain an assistive tool rather than an autonomous decision-maker. Second, its operation would require a clear statutory basis governing the lawful handling of illicit material by authorised actors. Third, its procedural use would have to preserve evidential integrity, traceability, and the possibility of meaningful human verification.

Fourth, its design and deployment would need to satisfy the stringent requirements of EU AI regulation and criminal-data protection.

The decisive point is therefore not whether AI can be used at all, but under what conditions it can be used lawfully and responsibly. If those conditions are met, AI may become a valuable investigative aid in Hungary, especially in the preliminary assessment and prioritisation of digital material. If they are not, its use would risk undermining both procedural fairness and the protection of the sensitive data that such investigations inevitably involve.

7. Conclusion

This article has argued that the Hungarian offence of child pornography can no longer be examined solely as a matter of substantive criminal law. Its current form is the product of international child-protection standards, European legal harmonisation, domestic legislative development, and the growing impact of digital technologies on both offending and enforcement. At the same time, comparative analysis shows that important differences remain across jurisdictions, especially in the treatment of virtual or synthetic depictions.

A second central conclusion concerns the offender population. The routine use of the term paedophile in legal and public discourse is analytically misleading, because it obscures the heterogeneity of offenders involved in child pornography cases. Greater terminological precision is therefore necessary, not only for conceptual clarity but also because different offender profiles may require different investigative responses.

Against that background, artificial intelligence appears to offer a limited but significant opportunity. AI-assisted image recognition may help law enforcement authorities filter, sort, and prioritise large volumes of digital material, thereby reducing investigative burdens and allowing greater concentration on cases involving heightened risk. Its value lies in assistance, not substitution: it cannot replace human legal judgment, evidentiary evaluation, or procedural guarantees.

From a Hungarian perspective, the use of such systems appears legally conceivable in principle, but only under strict conditions. Any implementation would require a clear statutory basis, full compliance with EU requirements on high-risk AI systems, procedural safeguards ensuring evidential integrity and human review, and a robust data-protection framework capable of protecting highly sensitive material. If these conditions are met, AI may become a useful investigative instrument in the detection of offences involving child sexual abuse material.

References

- [1] Act C of 2012 on the Criminal Code.
- [2] Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (Act No. 52 of 1999).
- [3] Act XXXI of 1997 on the Protection of Children and the Administration of Guardianship.
- [4] Brodowski, D., Hartmann, M. & Sorge, C. (2023). Automatisierung in der Strafrechtspflege: Legal Tech, KI und eine „hybride Cloud“ im Einsatz gegen Kindesmissbrauch. *Neue Juristische Wochenschrift (NJW)*, 2023(9), 583–588. <https://doi.org/10.22028/D291-39216>
- [5] Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child, 2024 O.J. (L, 2024/1238).
- [6] Convention on the Rights of the Child, November 20, 1989, 1577 U.N.T.S. 3.
- [7] Coroners and Justice Act 2009.
- [8] Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, 2004 O.J. (L 13) 44–48.
- [9] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse [Lanzarote Convention], C.E.T.S. No. 201 (2007).
- [10] Criminal Justice Act 1988.
- [11] Criminal Justice and Public Order Act 1994.
- [12] Csapucha, B. (2020). A gyermekpornográfia hazai büntetőjogi szabályozása, s a jelenség ellen folytatott küzdelem a nemzetközi dokumentumok tükrében. *Büntetőjogi Szemle*, 9(1), 13–22. https://ujbtk.hu/wp-content/uploads/lapszam/BSz_202001_13-22o_Csapucha.pdf
- [13] Csendes-Erdei, E. (2024, March 6). Meglepő magyar kutatás: 183 pedofil bűnelkövető közül csak kettő volt valóban pedofil. *hvg360*. https://hvg.hu/360/20240306_pedofil_pedofolia_jog_szexualis_bantalmazas_pszichiatria_kriminologia_szabo_judit_virag_gyorgy_okri
- [14] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, 2011 O.J. (L 335) 1–14.
- [15] Erdélyi, Á. (2022). Valóban pedofilok-e a „pedofil” elkövetők? *Magyar Rendészet*, 22(3), 69–82. <https://doi.org/10.32577/mr.2022.3.4>
- [16] Galbraith, P. W. (2011). Lolicon: The reality of “virtual child pornography” in Japan. *Image & Narrative*, 12(1), 83–119.
- [17] Honti, H. (1998). A gyermekvédelmi törvény a nemzetközi jog és a gyakorlat tükrében. *Esély*, 10(6), 60–69. https://www.esely.org/kiadvanyok/1998_6/agyermekvedelmi_torveny.pdf
- [18] Hottó, I. (2024). The connections between cybercrime and family crisis and their impact on children, along with their potential criminal law implications. *Gubernaculum et Administratio*, 2(30), 189–204. <https://doi.org/10.16926/gea.2024.02.02.11>
- [19] Iemelianenko, V. & Dmytruk, M. (2025). Combating child pornography: International legal regulation and experience of Ukraine and foreign countries. *Theory and Practice of Jurisprudence*, 1(25), 174–197. [https://doi.org/10.21564/2225-6555.2024.1\(25\).306612](https://doi.org/10.21564/2225-6555.2024.1(25).306612)
- [20] Kaferanis, D., Sachoulidou, A. & Turksen, U. (2023). Artificial intelligence in law enforcement settings. *eucrim*, (1), 60–66. <https://eucrim.eu/articles/artificial-intelligence-in-law-enforcement-settings/>
- [21] Kovács, I. (2018). Kiberbiztonság?! Gyermek szexuális kizsákmányolása az interneten, azaz gyermekpornográfia Magyarországon, különös tekintettel a nemzetközi iOCTA, és INHOPE értékeléseire. *Rendvédelem*, 7(1), 178–267. https://epa.oszk.hu/03300/03353/00012/pdf/EPA03353_rendvedelem_2018_1_178-267.pdf

- [22] Lee, H.-E., Ermakova, T., Ververis, V. & Fabian, B. (2020). Detecting child sexual abuse material: A comprehensive survey. *Forensic Science International: Digital Investigation*, 34, 301022. <https://doi.org/10.1016/j.fsidi.2020.301022>
- [23] Mezei, K. (2021). Az online gyermekpornográfia és a büntetőjog. *Ügyészek Lapja*, 28(4), 19–30. https://real.mtak.hu/135281/1/mezei_UL_2021_4beliv.pdf
- [24] Ministry of the Interior, Criminal Records Authority.
- [25] Niculescu, B. (2024). Some aspects of comparative law regarding child pseudopornography and virtual child pornography. *Challenges of the Knowledge Society*, 17(1), 60–71. <https://doaj.org/article/2531cc0cc3134912a637ff43c28bfa17>
- [26] NMHH. (2021). *Digital parenting kutatás 7-16 éves gyermekekkel és szüleikkel*. https://nmhh.hu/dokumentum/224270/NMHH_PSYMA_7_16_eves_2021_KUTATASI_JELENTES.pdf
- [27] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, May 25, 2000, 2171 U.N.T.S. 227.
- [28] Palomares, N. (2024). Child pornography: A growing threat for forensic science in the digital age. *Themis: Research Journal of Justice Studies and Forensic Science*, 12(1), Article 3. <https://doi.org/10.55917/2324-6561.1122>
- [29] Protection of Children Act 1978.
- [30] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
- [31] Sexual Offences Act 2003.
- [32] Strafgesetzbuch (StGB).
- [33] Supreme Court of the United States. *Ashcroft v. Free Speech Coalition*. Judgment of April 16, 2002. No. 00-795. 535 U.S. 234.
- [34] Supreme Court of the United States. *New York v. Ferber*. Judgment of July 2, 1982. No. 81-55. 458 U.S. 747.
- [35] Supreme Court of the United States. *Osborne v. Ohio*. Judgment of April 18, 1990. No. 88-5986. 495 U.S. 103.
- [36] Szabó, J. & Virág, G. (2023). Bűnözők? Betegek? Gondolatok a pedofiáliáról és a szexuális bűnelkövetésről. *Ügyészeti Szemle*, 8(1), 4–16. <https://ugyesszegiszemle.hu/pdf/2023-01.pdf>
- [37] Szeliski, R. (2022). *Computer vision: Algorithms and applications* (2nd ed.). Springer Cham. <https://doi.org/10.1007/978-3-030-34372-9>
- [38] Takeuchi, C. L. (2015). Regulating lolicon: Toward Japanese compliance with its international legal obligations to ban virtual child pornography. *Georgia Journal of International and Comparative Law*, 44(1), 195. <https://digitalcommons.law.uga.edu/gjicl/vol44/iss1/7>
- [39] Tóth, A. B. (2025). A gyermekek sérelmére elkövetett bűncselekmények hatályos szabályozása és kodifikációs tendenciái. *Jogi Fórum*. https://www.jogiforum.hu/wp-content/uploads/2025/05/toth-anna_a-gyermekek-serelmere-elkovetett-buncselekmenyek_jogi-forum.pdf
- [40] United States Code, Title 18, Chapter 110 (18 U.S.C. ch. 110).
- [41] Weiss, R. B. (2020, November 17). Understanding users of child pornography. *Psychology Today*. <https://www.psychologytoday.com/ca/blog/love-and-sex-in-the-digital-age/202011/understanding-users-child-pornography>
- [42] Witting, S. K. (2019). Regulating bodies: The moral panic of child sexuality in the digital era. *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft / Critical Quarterly for Legislation and Law / Revue critique trimestrielle de jurisprudence et de législation*, 102(1), 5–38. <https://www.jstor.org/stable/26799645>

