

FAMILY PRIVACY AND ARTIFICIAL INTELLIGENCE

Keywords: Privacy, family, minors, artificial intelligence, codes of ethics

Schlüsselworte: Privatsphäre, Familie, Minderjährige, künstliche Intelligenz, Ethik-kodizes

Słowa kluczowe: prywatność, rodzina, nieletni, sztuczna inteligencja, kodeksy etyczne

Our digital society has made significant progress in valuing and protecting personal privacy, but it has also encouraged exhibitionism and the commercialization of the private sphere. Today, “digital communication wants to bring everything out into the open; people’s lives are combed over, laid bare, and bandied about, often anonymously”¹. In this way, “the right to privacy scarcely exists,” respect for others is lost, and everything becomes “a kind of spectacle” (FT 42).

When privacy is violated, the human being is reduced to a mere object². Generative artificial intelligence (AI) is further shaping the way individuals express their inner lives and how others gain access to private information. In this new context, we must recover the capacity for awe and reverence before the “sacred mystery” of every human being (FT 277), recognizing their “right to be themselves and to be different” (FT 218), and loving them “as if there were no one else in the world but him” (FT 193).

* Prof. dr Martín Carbajo-Núñez, OFM, moral theologian and specialist in social communication, professor at two Pontifical universities in Rome (Italy): Antonianum (PUA) and Alfonsianum (PUL), as well as FST – San Diego University, CA (USA), e-mail: mcarbajo@fst.edu , ORCID: <https://orcid.org/0000-0002-2814-5688>.

¹ Francis, “*Fratelli Tutti*”. *Encyclical letter* (Oct. 3, 2020), [next: FT], n. 42, AAS 112(2020), pp. 969-1074.

² We have explored this topic in several publications, for example: M. Carbajo-Núñez, *Intimidad y comunicación. Bases filosófico-teológicas para un encuentro en autenticidad*, “*Antonianum*” 82(2007), pp. 637-675; M. Carbajo-Núñez, *El espectáculo de la intimidad. Raíces históricas de la comunicación centrada en el yo*, “*El Ágora USB*” 12/2(2012), pp. 449-534; M. Carbajo-Núñez, *L’attenzione alla soggettività e l’appello alla coscienza nei codici deontologici del giornalismo europeo*, in: *Fedeli alla chiesa del Redentore. Scritti in onore di Sabatino Majorano*, ed. A.V. Amaranter, Bologna 2014, 129-143; M. Carbajo-Núñez, *The universal fraternity. Franciscan roots of Fratelli tutti*, Phoenix (AZ) 2023, chap. 5.

The commercialization of personal data is now one of the most profitable industries³. The digital footprints that individuals leave involuntarily during everyday activities, whether commercial or recreational, are automatically collected and stored indefinitely. Based on this computerized information, it is possible to construct a detailed profile of the individual, which can be used to influence their behaviour and drive them towards consumerism.

In the first part of this article, we will outline some conclusions from our studies of sixty national codes of journalistic ethics, drafted and adopted by journalists in forty-two European countries⁴. The aim is to understand how these professionals perceive the value of human privacy and how they seek to protect it⁵. We will then examine the challenges that AI poses to privacy within the family (ch. 2) and in the lives of minors (ch. 3), and finally propose strategies to address these challenges (ch. 4)⁶.

Table 1. European deontological documents included in this study

	Id.	Country	Title and Issuing Institution
1	c01	IFJ	International Federation of Journalists (Tirana)
	c02	Albania	Journalists' Code of Ethics
	c03	Germany	Code of Ethics and Rules of the Press Council
	c04	Armenia	Code of Ethics of the Yerevan Press Club
5	c05	Austria	Code of Ethics of the Press Council
	c06	Azerbaijan	Professional Ethics Code for Journalists
	c07a	Belgium	Code of Journalistic Principles
	c07b	Belgium	Recommendations of the Journalists' Association (AGJPB) on the Media Coverage of Non-Natives
	c08	Belarus	Professional Ethics Code of the Journalists' Union
10	c09a	Bosnia-Herz	Press Code
	c09b	Bosnia-Herz	Broadcasting Code of Conduct
	c10	Bulgaria	Ethics Code of Bulgarian Mass Media
	c11	Croatia	Ethics Code of the Journalists' Association

³ D. Feldman, E. Haber, *Measuring and protecting privacy in the Always-on era*, "Berkeley Technology Law Journal" 5(2020), pp. 197-249.

⁴ For statistical purposes, codes belonging to the same country are counted as a single unit.

⁵ Cf. P.P. Singh, *European codes of journalism ethics*, New Delhi 2018; S.A. Banning, *Standards of Work Today: Using History to Create a New Code of Journalism Ethics*, eBook, New-castle-upon-Tyne 2020; B. Miller, *Reporting by the code: journalistic ethics and responsibilities*, London 2024.

⁶ This article is based on the lecture delivered by Prof. Carbajo-Núñez at the 9th International Symposium on the Family, organized by the University of Warmia and Mazury in Olsztyn, Poland, on June 12, 2025.

	c12	Czech Rep.	Code of Conduct of the Publishers' Union
15	c12b	Czech Rep.	Ethics Code of the Journalists' Union
	c13	Denmark	Code of Conduct, Approved by Parliament and Adopted by the Journalists' Union
	c14	Slovakia	Ethics Code of the Journalists' Union
	c15	Slovenia	Code of the Journalists' Association and Union
	c16a	Spain	Code of the Federation of the Spanish Press (FAPE)
20	c16b	Spain	Deontological Code of the Catalonia College of Journalists
	c17	Estonia	Press Deontology Code
	c18	Finland	Code of Conduct of the Journalists' Union
	c19a	France	Code of the Journalists' Union
	c19b	France	Statute of the Right to Information
25	c19c	France	Norms and Practices of the Provincial Daily Press
	c20	Greece	Code of Ethics for Press and Audiovisual Sector
	c20b	Greece	Code of Ethics of the Pan-Hellenic Federation of Journalists
	c21	Hungary	Ethics Code of the National Association of Journalists
	c22	Ireland	Conduct Code of the National Union of Journalists
30	c23	Iceland	Journalistic Ethics Standards of the Press Council
	c24a	Italy	Ethics Code of the Press Order and Federation
	c24b	Italy	Treviso Charter on Information and Minors
	c24c	Italy	Code on Television and Minors
	c24d	Italy	Code on the Processing of Personal Data
35	c25	Latvia	Deontological Code of the Journalists' Union
	c26	Lithuania	Deontological Code of the Press and Broadcasting
	c27	Luxembourg	Deontological Code of the Press Council
	c28a	Macedonia	Journalists' Deontological Code
	c28b	Macedonia	Declaration of Editors and SEEMO Executives
40	c29a	Malta	Code of the Press Club and Broadcasting Institute
	c29b	Malta	<i>Deontological Code of the Press Club (TMPC)</i>
	c30	Moldova	Deontological Code of the Journalists' Union

	c31	Montenegro	Deontological Code of Journalists' Associations
	c32	Norway	Norwegian Press Code of Ethics
45	c33	Netherlands	Rules of the Journalists' College
	c34a	Poland	Code of the Journalists' Association (AJRP)
	c34b	Poland	Ethical Statute of Journalists, Editors, and Broadcasters
	c35a	Portugal	Deontological Code of the Journalists' Union
	c36	Romania	Deontological Code of the Press Club
50	c37a	Russia	Guidelines on News Coverage of Terrorism
	c37b	Russia	Journalists' Code of Ethics
	c38	Serbia	Code of the Independent Journalists' Association
	c39	Sweden	Code of the Press, Radio and Television Council
	c40	Switzerland	Declaration and Rules on Journalists' Rights and Duties
55	c41a	Turkey	Professional Principles Adopted by the Press Council
	c41b	Turkey	Deontological Code of the Journalists' Association
	c42a	UK	Code of Conduct of the National Union of Journalists (NUJ)
	c42b	UK	Press Complaints Commission (PCC) Code
	c42c	UK	Photographers' Association Guidelines on Working with Children
60	c42d	UK.ofcom	TOfcom Broadcasting Code (Editor's Code of Practice),
	c43	Ukraine	Journalist's Code of Ethics
	c44	Cyprus	Journalist's Code of Conduct
	c45a	Georgia	Journalist's Code of Ethics
	c45b	Georgia	Professional Standards for Mass Media
65	c46	<u>Kosovo</u>	Press Code

1. FAMILY PRIVACY IN THE ETHICAL CODES OF EUROPEAN JOURNALISM

Ethical self-regulation documents, commonly referred to as “codes of ethics”⁷, set out the guidelines that information professionals must follow in order to carry out their work responsibly, according to objective criteria of public service.

⁷ There is no uniform terminology to refer to them. In English, the most commonly used expressions are: ‘codes of ethics’, ‘codes of conduct’, and ‘codes of practice’. Although these terms are sometimes treated as synonyms, they actually have different meanings in practice. Cf. C. Fisher,

The rapid growth of digital journalism⁸ and artificial intelligence presents a new set of challenges. The role traditionally assigned to the press as a filter and guarantor of the right to information appears to have been weakened. Today, anyone can publish content on the internet without apparent restrictions⁹.

Respect for privacy and private life¹⁰ is addressed in 71.4% of European codes of ethics. These codes uphold the right of every person, whether natural or legal, to control their own information, both at the moment it is provided and in the subsequent phases of editing, publication, and storage. Below are some of the conclusions related specifically to the family sphere.

1.1. Ethical criteria for the collection, publication, and storage of information

During the data collection phase, informational intrusions into private spaces, including the family home, must be avoided. Additionally, individuals are recognized as having the right to exercise active control over the accuracy, use, and updating of their already-stored personal data.

78.5% of the codes require that information be obtained honestly. Exceptions to this rule are permitted only when the data collected is of significant public interest and there is no other way to obtain it without incurring serious risks. In any case, there must always be proportionality between the means employed and the social utility of the information being sought.

Once the information has been published, both the journalist and the news organization are obligated to correct any erroneous, incomplete, or distorted data and to facilitate the exercise of the right of reply.

Personal information always belongs to the individual to whom it refers. Consequently, renewed consent must be sought in order to use that information for purposes other than those for which it was originally collected. Furthermore, those who store such information are required to keep the individuals concerned informed of all relevant details (location, responsible parties, procedures) so they can effectively exercise control over their data.

The publication of personal data is not justified simply because it is accurate or accessible; it must also be relevant, and its disclosure must generate an “extraordinary social benefit”. It is therefore necessary to distinguish between “satisfying public curiosity” and “serving the public interest.” It is not uncommon for audiences to be interested in irrelevant or sensational aspects of private life, but such interest alone is not sufficient to render them matters of public concern.

A. Lovell, *Business ethics and values*, Essex 2003, p. 210; *Codes of ethics and ethical guidelines: emerging technologies, changing fields*, ed. K. Laas, M. Davis, E. Hildt, eBook, Cham 2022.

⁸ The first online newspaper, that is, one published regularly on the Internet, began in January 1994. Six years later, there were already more than 5,400 online newspapers. Cf. B. Gunter, *News and the Net*, London 2003, p. 143.

⁹ The so-called “weblogs” or simply “blogs” have become popular; they are a kind of online newspaper created by individuals. Cf. N. Miladi, *Global media ethics and the digital revolution*, London 2022.

¹⁰ Some codes distinguish between the “intimate sphere” and “privacy” (c12).

1.2. Protection of the privacy of children and young people

52.3% of the codes explicitly state that the protection of minors' privacy must take precedence over the informational value of the news, as minors are still vulnerable and impressionable individuals. Any intrusion into their private life that could cause trauma or negatively affect their future development must be avoided. The age range considered most protected varies depending on the code—up to fourteen, fifteen, sixteen, or eighteen years of age.

Minors must not be subjected to arbitrary interference or any form of violence, harm, psychological abuse, or exploitation. The fact that they are children of public figures does not justify a lower level of privacy protection.

Journalists must exercise particular caution when minors appear as victims, witnesses, or defendants in judicial proceedings, to avoid damaging their personality or hindering future social reintegration. For this reason, their names, photographs, or any data that could lead to their identification must not be published, especially in cases of sexual abuse¹¹. The publication of the names of missing minors requires explicit authorization from the competent authority. Likewise, sensitivity is required when reporting on family disputes or child custody cases (c17).

Programs broadcast during children's viewing hours must not disturb the psychological or moral balance of minors. In particular, all content that promotes discrimination, contempt towards individuals or groups, delegitimization of parental or educational figures, or the transgression of basic social norms must be avoided. Ambiguous representations of good and evil are also discouraged (c24c).

The participation of minors in the media is subject to strict restrictions in order to protect them from potentially traumatic experiences (c20, c24b). Although parental or guardian consent is always required (c17), this alone is not sufficient to legitimize every form of participation¹². Interviews dealing with family conflicts, divorces, adoptions (c09a), abductions, painful experiences, or criminal behaviour (c16a) are especially sensitive. Only topics related to sports are considered sufficiently harmless for children to participate in (c29b).

2. AI AND PRIVACY IN THE FAMILY SPHERE

The challenges to family privacy have increased with the development of AI. The massive extraction of data and the growing automation of decision-making demand a revision and update of the ethical principles outlined by media professionals in their respective codes of ethics.

Artificial intelligence encourages new forms of surveillance over the family, in some cases limiting its autonomy in decision-making. To face such challenges, not only is proper education for families essential, but also the support of an appropriate ethical and legal regulatory framework.

¹¹ Some codes allow the publication of such data in cases of homicide, serious crimes, or when it can be demonstrated that the public interest requires it (c32).

¹² (c42d/1). Some codes allow a minor to be interviewed if the aim is to protect the child's interests (c24a), or "if the minor is already under public scrutiny" (c17).

2.1. The paradox of the “smart” home

Internet of Things (IoT) devices, such as virtual assistants (Alexa, Google Home, Siri), security cameras, connected appliances, and smart toys, are transforming the family home into a “smart” home. While these technologies undeniably offer benefits in terms of convenience and efficiency, their use also poses significant risks to the privacy of family life.

These devices continuously collect data on the routines, habits, conversations, and preferences of household members. Such data can later be used to personalize advertising content, influence access to insurance, or serve as evidence in potential legal disputes. In 2023, Amazon acknowledged that recordings obtained through Alexa had been used to train AI models, even after some users had requested the deletion of those records¹³.

2.2. Assessment of Family Dynamics for Predictive Purposes

The functioning of AI and the conclusions it reaches are not necessarily objective or neutral, as they depend on the type of prior training and the criteria used to define what is considered a “normal” family life.

Some social, judicial, or healthcare services have begun using algorithms to analyse family dynamics, consumption patterns, locations, and social media activities in order to predict possible risks such as child neglect, marital breakdowns, or economic instability. Algorithmic scoring systems are used to classify the level of family “stability,” thereby influencing access to social benefits, bank loans, mortgages, or personal insurance¹⁴.

The use of these systems poses serious ethical risks. By labelling certain families as “at risk,” algorithms may reproduce structural prejudices, perpetuate social stereotypes, and amplify class, gender, or ethnic biases¹⁵. A paradigmatic case was the tax fraud scandal in the Netherlands, where a secret algorithm used discriminatory variables to falsely accuse thousands of families of fraud¹⁶. In the United States, sys-

¹³ Cf. Federal Trade Commission - Department of Justice, *FTC and DOJ Charge Amazon with Violating Children’s Privacy Law by Keeping Kids’ Alexa Voice Recordings Forever and Undermining Parents’ Deletion Requests* (31.05.2023), in *Federal Trade Commission* [on-line], <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever> (access: 5.06.2025).

¹⁴ “Redlining is an illegal practice in which lenders avoid providing services to individuals living in communities of color”: United States Department of Justice, *Press Release: Justice Department Announces New Initiative to Combat Redlining* (22.10.2021) in: *Archives U.S. Department of Justice* [on-line], <https://www.justice.gov/archives/opa/pr/justice-department-announces-new-initiative-combat-redlining> (5.06.2025).

¹⁵ Z. Obermeyer, B. Powers, Ch. Vogeli, S. Mullainathan, *Dissecting racial bias in an algorithm used to manage the health of populations*, “Science” 366/6464(2019), pp. 447-453; S. Ho, G. Burke, *Child welfare algorithm faces Justice Department scrutiny* (1.02.2023), in: *The Associated Press* [on-line], <https://apnews.com/article/justice-scrutinizes-pittsburgh-child-welfare-ai-tool-4f61f45bfc3245fd2556e886c2da988b> (access: 5.06.2025).

¹⁶ Council of Europe, *Netherlands - Report of the Childcare Allowance Parliamentary Inquiry Committee entitled “Unprecedented injustice” (Ongekend onrecht) Dec. 17, 2020*, in: *Council of Eu-*

tems like *eScore* have faced strong criticism for relying on potentially discriminatory data to evaluate creditworthiness¹⁷.

On another front, many “parental control” applications use AI technologies to monitor teenagers’ messages, locations, and social networks. Although they are presented as protective tools, their use can erode trust between parents and children and blur the line between protection and surveillance¹⁸. Apps like *Bark* or *mSpy*, which integrate voice recognition and geolocation, may extend covert monitoring practices within the domestic environment.

2.3. Deepfakes and the right to be forgotten

AI makes it increasingly difficult to preserve anonymity and the right to be forgotten, especially in sensitive areas such as medical records, legal cases, or academic files. Even when names and family details have been deleted, AI systems can re-identify individuals by cross-referencing databases and performing additional analyses.

Generative AI can revive content linked to past situations, thereby reinstating stigmas and affecting the reputation and well-being of those who have sought to rebuild their lives. The dispersion of personal and family data across remote servers or digital clouds prevents users from maintaining effective control over their own information, increasing the risk of unauthorized access or abusive uses.

AI also enables the creation of fake content with realistic appearance (*deepfakes*) from fragments of authentic data. These materials may include fictional narratives, recreations of family disputes, or manipulated sexualized scenes. The creation of synthetic pornography or the alteration of past images for purposes of blackmail constitutes a new form of digital violence with traumatic potential¹⁹, especially when minors are involved.

AI’s capacity to make content go viral presents an additional challenge: news once published with discretion may be amplified in contexts far removed from their original intent. For instance, an article about a custody dispute may resurface with new narratives and intentions. There have also been cases of deepfakes reconstructing crime scenes, making identifiable those minors whose identities were initially protected.

rope Portal [on-line], [https://www.coe.int/en/web/venice-commission/-/CDL-REF\(2021\)073-e](https://www.coe.int/en/web/venice-commission/-/CDL-REF(2021)073-e) (access: 5.06.2025).

¹⁷ Cf. Transparency Center, *CoreLogic Score*, in: *Core Logic - Commercial Express: Glossary* [on-line], https://twia.msbccommercial.com/Help/Content/Resources/Glossary/CoreLogic_Score.htm (access: 5.06.2025).

¹⁸ Cf. S. Feldstein, *State surveillance and implications for children*, “UNICEF Issue brief” 1 (August 2020), in: *United Nations Children’s Fund* [on-line], <https://www.unicef.org/innocenti/media/1136/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf> (31.08.2025); Federal Trade Commission, *A look behind the Screens: Examining the data practices of social media and video streaming services. Staff Report (September 2024)*, in: *Federal Trade Commission* [on-line] https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf (access: 5.06.2025).

¹⁹ Cf. H.P. Jondec Briones, et al., *El uso ilícito de las técnicas de inteligencia artificial y la necesidad de su regulación: el deepfake*, “*Vniversitas Jurídica*” 73(2024), in *Revistas: Pontificia Universidad Javeriana* [on-line], <https://doi.org/10.11144/Javeriana.vj73.uiti> (access: 5.06.2025).

2.4. Family disputes and algorithmic profile generation

The principle that journalists must act with sensitivity and respect when reporting on family disputes and child custody cases becomes even more necessary in a media environment shaped by AI technologies.

These tools have the capacity to identify patterns and family dynamics from a multitude of sources, such as social media, press releases, court records, and other public documents related to marital conflicts, divorces, or custody matters. This body of information is further expanded by photos, videos, and digital messages, sometimes shared by third parties unrelated to the core family unit.

Even if the content analysed by AI has been previously disclosed, its automated processing²⁰ can lead to disproportionate amplification. By analysing large volumes of data, AI systems can reconstruct detailed profiles that may stigmatize certain families.

Moreover, some algorithmic models can automatically generate sensationalist news content by extracting data from judicial archives without applying proper anonymization measures for minors involved.

3. CHALLENGES TO THE PRIVACY OF MINORS

Childhood represents the sector most exposed to emerging threats against family privacy. Risks such as reidentification, the perpetuation of stigmas, and the multiplication of surveillance vectors pose unprecedented challenges that require deep ethical and legal reflection. The following section analyses some representative cases.

3.1. Reidentification from anonymous data

The deontological codes of European journalism emphasize the need to protect the identity of minors in all reporting that could affect their personal development or future. This protection includes techniques such as pixelating faces or omitting names in graphic and written content.

However, recent advances in AI technologies have called into question the effectiveness of these traditional practices. Facial recognition tools and biometric data analysis are now capable of reversing anonymization processes, enabling the reidentification of minors based on images, locations, and contextual patterns. A landmark case was that of Clearview AI, which was sanctioned for collecting and analysing children's faces without consent²¹.

These algorithms not only identify faces in public or school settings but also enrich reconstructed profiles with additional information, such as geolocation, affiliation with specific educational institutions, or the child's family environment. The ability of these tools to cross-reference public and private databases significantly increases minors' exposure, even when basic anonymization measures have been applied.

²⁰ Cf. *Periodismo automatizado*, in: *Wikipedia: La enciclopedia libre* [on-line], https://es.wikipedia.org/wiki/Periodismo_automatizado?utm_source=chatgpt.com (access: 5.06.2025).

²¹ Cf. <https://es.euronews.com/next/2024/09/03/paises-bajos-multa-a-clearview-ai-por-construir-una-base-de-datos-ilegal> (access: June 5, 2025).

3.2. Automated profiles and algorithmic exposure of minors

Numerous educational and recreational applications designed for children integrate artificial intelligence systems capable of collecting and processing sensitive data related to their habits, cognitive, emotional, and social abilities. These systems allow for the construction of automated profiles, often without informed consent from parents or legal guardians.

This algorithmic processing follows a commercial logic that overrides the best interests of the child. As a result, reward and control dynamics are generated to encourage consumption, putting the emotional and social development of children at risk. It is striking that regulations such as the United States' Children's Online Privacy Protection Act (COPPA) prohibit the collection of personal data from children under thirteen, yet do not apply the same level of scrutiny to the collection and exploitation of AI-inferred data, such as emotions, personality traits, or communicative intentions²².

Moreover, various children's applications incorporate facial or voice recognition systems that analyse children's emotional reactions (joy, sadness, frustration) in order to dynamically tailor the content provided. These data can later be used for commercial or institutional purposes, for example, in targeted marketing campaigns. There is a risk that certain children may be prematurely classified as "problematic" or "potential offenders."

3.3. Minors involved in criminal acts

The deontological codes of European journalism establish the obligation to protect minors involved in criminal acts, whether as victims, witnesses, or alleged offenders. In this regard, the Code of the Federation of Associations of Journalists of Spain (FAPE) states that "journalists must refrain from interviewing, photographing, or recording minors on subjects related to criminal activities or matters falling within the sphere of privacy"²³.

The growing influence of AI in the information field introduces new risks that require enhanced protection for minors. For instance, algorithmic systems are capable of extracting information from judicial documents, databases, or partially anonymized content, and in some cases, identifying minors who have participated in criminal proceedings.

AI's ability to interlink scattered data, even after explicit references have been removed, significantly increases the risk of reidentification. Furthermore, the profiles generated by these systems may include predictive assessments of the minor's future behaviour, thereby contributing to stigmatization and social exclusion.

²² Code of Federal Regulations (United States), *Part 312: Children's Online Privacy Protection Rule* (22.04.2025), in: *ECFR: National Archives* [on-line], <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312> (5.06.2025).

²³ Federación de Asociaciones de Periodistas de España (next: FAPE), *Código deontológico*, in: *Federación de Asociaciones de Periodistas de España* [on-line], <https://fape.es/home/codigo-deontologico-1/> (access: 5.06.2025).

4. PROPOSALS FOR THE PROTECTION OF FAMILY PRIVACY

The following are some proposed lines of action aimed at protecting privacy from the risks associated with the use of AI in family contexts and childhood.

4.1. Improving algorithms to safeguard children's privacy

Respect for family privacy must guide the development of AI-managed systems, products, and services. In this regard, it is recommended to implement the *Privacy by Design and by Default* (PbD) approach, structured around the seven principles formulated by Ann Cavoukian²⁴. This involves limiting the collection of data on minors to what is strictly necessary, ensuring rigorous anonymization, and always obtaining informed and verifiable consent from those legally responsible for their care.

The use of AI to classify, monitor, or predict the behaviour of minors in sensitive areas, such as mental health, sexual orientation, or socioeconomic status, must be strictly avoided. Likewise, the collection of biometric data in spaces frequented by minors, such as classrooms, parks, or leisure centres, should be strictly restricted.

4.2. Mechanisms for redress and accountability

Once data has been collected, it is essential to establish strict protocols for its storage, access, and use, supervised through mandatory, periodic, and independent audits. These audits must verify compliance with international standards such as ISO/IEC 27090²⁵, ensure the right to be forgotten for minors, and promote digital education that enables children to consciously manage their digital footprint.

The European Union's Artificial Intelligence Act²⁶ explicitly recognizes the need to evaluate applications aimed at minors when these pose a high risk. Legal liability for developers significantly increases in cases where harm to minors occurs, requiring them to ensure robust anonymization and implement preventive filters to avoid generating content that mentions or stigmatizes children. Judicial data involving minors must never be used to train AI models, not even for statistical purposes.

Given the seriousness of potential violations of children's privacy, exemplary sanctions are warranted. Additionally, media outlets and news agencies must implement strict verification protocols and alert systems within their AI tools to ensure that the content generated does not include bias or improper references to schools, extracurricular activities, or family residences.

²⁴ A. Cavoukian, *Understanding How to Implement Privacy by Design, One Step at a Time*, "IEEE Consumer Electronics Magazine" 9(2020), pp. 78-82; I. Giannakakis, *Privacy by Design and By Default. A Practical Guide for the Digital Era*, Saarbrücken 2019.

²⁵ Cf. ISO/IEC DIS 27090, *Cybersecurity - Artificial Intelligence - Guidance for addressing security threats to artificial intelligence systems*, in: *IOS: International Organization for Standardization* [on-line] <https://www.iso.org/standard/56581.html> (access: 5.06.2025).

²⁶ Cf. *European Union's Artificial Intelligence Act* [on-line], <https://artificialintelligenceact.eu/es/> (access: 5.06.2025).

CONCLUSION

Morbid curiosity and the commercialization of private life pose a direct threat to human dignity and to the harmonious development of the person. Each individual must be able to integrate the new possibilities offered by the information society without losing an “embodied,” respectful, and genuinely human way of communicating.

The progressive expansion of artificial intelligence is transforming the home into an object of economic interest and technological intrusion. Devices designed to facilitate family life, such as household appliances, vehicles, sensors, and digital assistants, are now part of the Internet of Things (IoT), a network that constantly collects and exchanges information, turning the most intimate spaces of the home into valuable data sources for market logics.

In this context, the document *Antiqua et nova*, issued by the Dicasteries for the Doctrine of the Faith and for Culture and Education²⁷, proposes an ethical and relational reflection that calls for the rehumanization of technological and communicative processes.

Protecting family privacy, and especially safeguarding the best interests of the child, must take precedence over any supposed informational benefit or commercial interest. The aim is to ensure that children can grow up free from media exposure and digital stigmatization.

It is urgent to restore a balance between respect for privacy and genuine closeness to others. Just as we “take off our sandals” before “the sacred mystery of the other,”²⁸ we must also avoid leaving them in solitude, indifference, or anonymity.

As Pope Francis warns in *Fratelli tutti*, “respect for others disintegrates” when people are pushed aside, ignored, and at the same time, their lives are shamelessly invaded (FT 42). Technological intrusion into the domestic sphere, even into its most private spaces, demands the establishment of firm boundaries and the promotion of digital disconnection zones, where family relationships can flourish free from surveillance and quantification.

FAMILY PRIVACY AND ARTIFICIAL INTELLIGENCE

SUMMARY

The progressive expansion of artificial intelligence is transforming the home into an object of economic interest and technological intrusion. Devices designed to facilitate family life,

²⁷ DICASTERIO PARA LA DOCTRINA DE LA FE – DICASTERIO PARA LA CULTURA Y LA EDUCACIÓN, «*Antiqua et Nova*. Nota sobre la relación entre la inteligencia artificial y la inteligencia humana», en *Internet*: https://www.vatican.va/roman_curia/congregations/cfaith/documents/rc_ddf_doc_20

²⁸ FT 277. “we have to remove our sandals when standing on the ‘holy ground’ of our encounter with the one who speaks to me”. Francis, *Message for the 50th World Communications Day* (24.01.2016), OsRom 17(2016), p. 7.

such as household appliances, vehicles, sensors, and digital assistants are turning the most intimate spaces of the home into valuable data sources for market logics. Protecting family privacy, and especially safeguarding the best interests of the child, must take precedence over any supposed informational benefit or commercial interest. In fact, when privacy is violated, the human being is reduced to a mere object. In the first part, we will outline some conclusions on family privacy from our studies of sixty national codes of journalistic ethics, drafted and adopted by journalists in forty-two European countries. We will then examine the challenges that AI poses to privacy within the family (ch. 2) and in the lives of minors (ch. 3), and finally propose strategies to address these challenges (ch. 4).

FAMILIÄRE PRIVATSPHÄRE UND KÜNSTLICHE INTELLIGENZ

ZUSAMMENFASSUNG

Die fortschreitende Verbreitung künstlicher Intelligenz verwandelt das Zuhause in einen Gegenstand von wirtschaftlichem Interesse und technologischer Einmischung. Geräte, die das Familienleben erleichtern sollen, wie Haushaltsgeräte, Fahrzeuge, Sensoren und digitale Assistenten, machen die intimsten Bereiche des Zuhauses zu wertvollen Datenquellen für die Marktlogik. Der Schutz der Privatsphäre der Familie und insbesondere die Wahrung des Kindeswohls müssen Vorrang vor vermeintlichen Informationsvorteilen oder kommerziellen Interessen haben. Denn wenn die Privatsphäre verletzt wird, wird der Mensch zu einem bloßen Objekt degradiert. Im ersten Teil werden wir einige Schlussfolgerungen zum Thema Privatsphäre in der Familie aus unseren Studien zu sechzig nationalen journalistischen Ethikkodizes vorstellen, die von Journalisten in zweiundvierzig europäischen Ländern entworfen und verabschiedet wurden. Anschließend untersuchen wir die Herausforderungen, die KI für die Privatsphäre innerhalb der Familie (Kapitel 2) und im Leben von Minderjährigen (Kapitel 3) mit sich bringt, und schlagen schließlich Strategien zur Bewältigung dieser Herausforderungen vor (Kapitel 4).

PRYWATNOŚĆ RODZINY A SZTUCZNA INTELIGENCJA

PODSUMOWANIE

Postępujący rozwój sztucznej inteligencji zmienia dom w obiekt zainteresowania gospodarczego i technologicznej ingerencji. Urządzenia zaprojektowane w celu ułatwienia życia rodzinnego, takie jak sprzęt AGD, pojazdy, czujniki i asystenci cyfrowi, zamieniają najbardziej intymne przestrzenie domu w cenne źródła danych dla logiki rynkowej. Ochrona prywatności rodziny, a zwłaszcza ochrona najlepszego interesu dziecka, musi mieć pierwszeństwo przed wszelkimi domniemanymi korzyściami informacyjnymi lub interesami handlowymi. W rzeczywistości, gdy prywatność zostaje naruszona, człowiek zostaje zredukowany do zwykłego przedmiotu. W pierwszej części artykułu przedstawionych zostało kilka wniosków dotyczą-

cych prywatności rodziny, wynikających z badań sześćdziesięciu krajowych kodeksów etyki dziennikarskiej, opracowanych i przyjętych przez dziennikarzy w czterdziestu dwóch krajach europejskich. Następnie przeanalizowano wyzwania, jakie sztuczna inteligencja stawia przed prywatnością w rodzinie (rozd. 2) i w życiu nieletnich (rozd. 3), a na koniec zaproponowane zostały strategie rozwiązania tych wyzwań (rozd. 4).

BIBLIOGRAPHY

- Francis, "Fratelli Tutti". *Encyclical Letter* (October 3, 2020), *AAA* 112(2020), pp. 969–1074.
- Francis, *Message for the 50th World Communications Day* (24.01.2016), *OsRom* 17(2016), p. 7.
- Banning S.A., *Standards of Work Today: Using History to Create a New Code of Journalism Ethics*, eBook, Newcastle-upon-Tyne 2020.
- Carbajo-Núñez M., *El espectáculo de la intimidación. Raíces históricas de la comunicación centrada en el yo*, "El Ágora USB" 12/2(2012), pp. 449–534.
- Carbajo-Núñez M., *Intimidación y comunicación. Bases filosófico-teológicas para un encuentro en autenticidad*, "Antoniano" 82(2007), pp. 637–675.
- Carbajo-Núñez M., *L'attenzione alla soggettività e l'appello alla coscienza nei codici deontologici del giornalismo europeo*, in: *Fedeli alla chiesa del Redentore. Scritti in onore di Sabatino Majorano*, ed. A.V. Amarante, Bologna 2014, 129-143.
- Carbajo-Núñez M., *The Universal Fraternity. Franciscan Roots of Fratelli Tutti*, Phoenix (AZ) 2023.
- Cavoukian A., *Understanding How to Implement Privacy by Design, One Step at a Time*, "IEEE Consumer Electronics Magazine" 9(2020), pp. 78–82.
- Codes of ethics and ethical guidelines: emerging technologies, changing fields*, ed. K. Laas, M. Davis, E. Hildt, eBook, Cham 2022.
- Council of Europe, *Netherlands - Report of the Childcare Allowance Parliamentary Inquiry Committee entitled 'Unprecedented injustice' (Ongekend onrecht) December 17, 2020*, in: *Council of Europe Portal* [on-line], [https://www.coe.int/en/web/venice-commission/-/CDL-REF\(2021\)073-e](https://www.coe.int/en/web/venice-commission/-/CDL-REF(2021)073-e) (access: 5.06.2025).
- European Union's Artificial Intelligence Act* [on-line], <https://artificialintelligenceact.eu/es/> (access: 5.06.2025).
- Federación de Asociaciones de Periodistas de España (FAPE), *Código Deontológico*, in: *Federación de Asociaciones de Periodistas de España* [on-line], <https://fape.es/home/codigo-deontologico-1/> (access: 5.06.2025).
- Federal Trade Commission, *A Look behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services. Staff Report (September 2024)*, in: *Federal Trade Commission* [on-line], https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf (access: 5.06.2025).
- Federal Trade Commission - Department of Justice, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests* (31.05.2023), in: *Federal Trade Commission* [on-line], <https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge->

- e-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever (access: 5.06.2025).
- Feldman D., Eldar H., *Measuring and Protecting Privacy in the Always-on Era*, "Berkeley Technology Law Journal" 5(2020), pp. 197–249.
- Feldstein S., *State Surveillance and Implications for Children*, "UNICEF Issue Brief" 1(August 2020), in: *United Nations Children's Fund* [on-line], <https://www.unicef.org/innocenti/media/1136/file/UNICEF-Global-Insight-data-governance-surveillance-issue-brief-2020.pdf> (access: 31.08.2025).
- Fisher C., Lovell A., *Business Ethics and Values*, Essex 2003.
- Giannakakis I., *Privacy by Design and By Default. A Practical Guide for the Digital Era*, Saarbrücken 2019.
- Gunter B., *News and the Net*, London 2003.
- Ho S., Burke G., *Child Welfare Algorithm Faces Justice Department Scrutiny*, (1.02.2023), in: *The Associated Press* [on-line], <https://apnews.com/article/justice-scrutinizes-pittsburgh-child-welfare-ai-tool-4f61f45bfc3245fd2556e886c2da988b> (access: 5.06.2025).
- ISO/IEC DIS 27090, *Cybersecurity - Artificial Intelligence - Guidance for addressing security threats to artificial intelligence systems*, in: *IOS: International Organization for Standardization* [on-line] <https://www.iso.org/standard/56581.html> (access: 5.06.2025).
- Jondec Briones H.P., et al., *El Uso Ilícito de las Técnicas de Inteligencia Artificial y la Necesidad de su Regulación: El Deepfake*, "Vniversitas Jurídica" 73(2024), in: *Revistas: Pontificia Universidad Javeriana* [on-line], <https://doi.org/10.11144/Javeriana.vj73.uiti> (access: 5.06.2025).
- Miladi N., *Global media ethics and the digital revolution*, London 2022.
- Miller B., *Reporting by the code : journalistic ethics and responsibilities*, London 2024.
- Obermeyer Z., Powers B., Vogeli Ch., Mullainathan S., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, "Science" 366/6464(2019), pp. 447–453.
- Periodismo automatizado*, in: *Wikipedia: La enciclopedia libre* [on-line], https://es.wikipedia.org/wiki/Periodismo_automatizado?utm_source=chatgpt.com (access: 5.06.2025).
- Singh P.P., *European codes of journalism ethics*, New Delhi 2018.
- Transparency Center, *CoreLogic Score*, in: *Core Logic - Commercial Express: Glossary* [on-line], https://twia.msbcommercial.com/Help/Content/Resources/Glossary/CoreLogic_Score.htm (5.06.2025).
- Code of Federal Regulations (United States), *Part 312: Children's Online Privacy Protection Rule* (22.04.2025), in: *ECFR: National Archives* [on-line], <https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312> (5.06,2025).
- United States Department of Justice, *Press Release: Justice Department Announces New Initiative to Combat Redlining* (22.10.2021) in: *Archives U.S. Department of Justice* [on-line], <https://www.justice.gov/archives/opa/pr/justice-department-announces-new-initiative-combat-redlining> (5.06.2025).