Artificial intelligence and family privacy

December 26, 2025

An article by Prof. M. Carbajo-Núñez, published on the blog of the Alfonsiana Academy

The development of Artificial Intelligence [= AI] is increasing comfort in family life**[i]**, but it is also introducing new forms of domestic surveillance that can, at times, limit their autonomy in decision-making.

The paradox of the "smart home"

Devices connected to the Internet of Things (IoT), such as virtual assistants (Alexa, Google Home, Siri), security cameras, smart appliances, and interactive toys, are transforming the family environment into a "smart home." These technologies provide greater convenience and efficiency, but they also pose significant risks to the privacy of family life.

These devices continuously collect data on household members' routines, habits, conversations, and preferences. Such information may be later used to personalize advertising, influence insurance eligibility, or serve as evidence in potential legal disputes. In 2023, Amazon acknowledged that it had used Alexa's recordings to train AI models, even after some users had requested that those recordings be deleted.

Using AI to predict family dynamics

The conclusions generated by AI systems are not necessarily objective or neutral, as they depend on how these systems have been trained and on the criteria they have been given to define what constitutes a "normal" family life.

Some social services, judicial institutions, and healthcare providers have begun using algorithms to analyze family dynamics, consumption habits, geolocation patterns, and social media activity to predict risks such as child neglect, marital breakdown, or economic instability. Based on such data, these systems may classify families by their level of "stability," thereby influencing access to social

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it.
Ok No Privacy policy

Such practices raise serious ethical concerns. AI models can mistakenly label certain families as "high-risk," perpetuating structural biases, social stereotypes, and class, gender, or ethnic discrimination. A notorious example occurred in the Netherlands, where a secret algorithm used discriminatory criteria to falsely accuse thousands of families of tax fraud. In the United States, tools like *eScore* have likewise been accused of relying on potentially discriminatory data to assess families' creditworthiness.

In addition, many parental control applications use AI to monitor adolescents' messages and online activity. Although marketed as protective tools, they often create distrust between parents and children and blur the line between caring protection and outright surveillance. Apps such as Bark or mSpy, which incorporate voice recognition and geolocation features, can easily be used to exercise covert monitoring inside the home.

Family disputes and algorithmic profiling

AI tools can identify patterns and family dynamics by analyzing numerous sources, such as social networks, press articles, court records, and other public documents related to marital conflicts, divorce proceedings, or child custody cases. They may also process photos, videos, and digital messages shared by others outside the immediate family.

Even if the content was already public, AI can amplify it far beyond its original scope. By processing large volumes of data, AI systems can reconstruct detailed family profiles which can be potentially stigmatizing.

Some algorithmic models can even generate sensationalist news content by extracting data from court files without ensuring adequate protection for minors involved.

Conclusion

The rapid expansion of AI is transforming the home into a more comfortable space, but also into a site of economic exploitation and technological intrusion. Devices designed to make family life easier, such as household appliances, vehicles, sensors, and digital assistants, are now part of the broader IoT, a network that constantly collects and exchanges data. As a result, even the most intimate areas of the home can be transformed into valuable sources of information for commercialization.

Protecting family privacy, especially safeguarding minors, must take precedence over commercial interest or information advantages. Strict regulations are needed to shield the domestic sphere from unwanted technological intrusions, establishing clear digital-zones where family relationships can flourish without surveillance and quantification.

---

[i] These paragraphs are based on our article: Carbajo-Núñez Martín, «Family privacy and Artificial Intelligence», in *Studia Elbląskie* 26 (2025) 363-377.

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are happy with it.
Ok No Privacy policy