POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

No. 53 (2685), 7 AUGUST 2026 © PISM

BULLETIN

# Bans on children’s access to social media as a way to regulate digital platforms

Aleksandra Wójtowicz

A growing number of countries are taking steps to restrict access to social media by children and teenagers. Australia became the first country in the world to introduce a ban (in force since December 2025) on persons under the age of 16 holding accounts on popular social media services. In June this year, the United Kingdom announced an analogous measure, and further countries—including EU members, among them Poland—are considering similar initiatives. Restricting children’s access to platforms has become one of the few politically acceptable ways of regulating big tech, although research shows that the effectiveness of such measures is limited.

In the EU, children’s online safety is regulated primarily by the Digital Services Act (DSA). Its Article 28 obliges online platforms accessible to minors to ensure high levels of privacy and safety, while very large online platforms (VLOPs) must actively mitigate systemic risks, including threats to minors’ mental health. However, the DSA neither sets a minimum age for users nor explicitly mandates age verification—in July 2025, the European Commission clarified these obligations in its guidelines on the protection of minors, pointing to appropriate age-assurance mechanisms as a means of ensuring compliance with the regulation. In practice, the age limit is set by the platforms’ own terms of service: officially, Meta (Facebook, Instagram), TikTok and X require users to be at least 13 years old. However, these age restrictions are widely known as being easy to circumvent, and for years the platforms were not effectively held to account for enforcing them, which the findings of the Commission’s investigation into Meta confirmed.

**Reasons for introducing bans**. The popularity of bans on children’s use of platforms stems from three overlapping factors. The first is the widespread conviction that social media poses serious risks—from behavioural addictions and mental health problems (such as depression, sleep disorders and body-image issues), to cyberbullying, harmful content, and adults with malicious intentions. The second factor is very high public support. According to the UK government, nine out of ten parents support a ban. In Poland, in an IBRiS poll from February this year, 77% of respondents supported the introduction of a ban on the use of social media by children under the age of 15, including a majority of voters of all the main political parties. Regulations of this kind are even gaining acceptance in the US, where children’s online safety has been promoted by Melania Trump, the Kids Online Safety Act is being processed in Congress, and similar state-level laws have been adopted in Utah, Texas and Louisiana, among others. Finally, “protecting children” is currently the easiest political route to regulating digital platforms. Given intensive lobbying by big tech and pressure from the US administration, which sees European digital rules as a barrier to the growth of American companies, it is easier to introduce provisions concerning minors than directly regulating the platforms.

**Countries introducing bans**. Australia pioneered the legal approach with the Online Safety Amendment (Social Media Minimum Age) Act 2024, in force since 10 December 2025, which prohibits persons under the age of 16 from holding accounts on the main social media platforms (including Facebook, Instagram, TikTok, YouTube, Snapchat and X), with no possibility of circumventing the ban even with parental consent. Responsibility for verification rests with the platforms, which must take “reasonable steps” to prevent minors from using their services or face fines of up to €31 million—Australia is currently planning to raise the fines to €68 million. Since the act entered into force, the platforms have removed access from around 4.7 million accounts identified as belonging to persons under the age of 16. On 15 June this year, the United Kingdom announced the introduction of a total ban for those under 16, which includes the platforms mentioned above. The ban is due to enter into force at the beginning of 2027. Similar regulations have been adopted or announced by further countries: Indonesia (deactivation of the accounts of persons under 16 from March this year), Malaysia (a ban for those under 16), Turkey (under 15), and in the EU, countries including Greece (a ban for those under 15 from January 2027), Denmark, France and Norway. Work on restrictions is also under way in Canada and Spain, as well as in Poland, where the Ministry of Digital Affairs and the Ministry of National Education are jointly drafting new legislation.

**Models for the ban**. The solutions adopted differ in three respects. The first aspect is the responsible entity—in most cases, the digital platforms face fines for failing to exercise due diligence in verifying users' age. An alternative model shifts responsibility to the level of app stores, which should not offer designated applications to persons below a specified age. The second element is the age limit, which is set at 13, 14, 15 or 16, depending on the governing legal order. The third aspect is the method of verification: is it carried out by the social media platform itself (user declaration, submission of an identity document, biometric analysis), by an app store, or by an external tool? In the EU, the Commission has developed an age-verification app to fulfil this role, based on the specifications of the European Digital Identity Wallet (eID), which member states are required to implement by the end of 2026. This is, however, only a Commission recommendation, so while states may—and to a large extent plan to—adopt it, they face no financial consequences for failing to act. The EC solution makes it possible to confirm that the age threshold has been met without disclosing the user's identity or date of birth to the platform. By contrast, the stance of the platforms themselves is more controversial: companies such as Meta are actively lobbying for mandatory age verification through their systems, as if it is carried out using their own tools or covers the entire ecosystem, it will give them broader access to data. To prove entitlement to use a service, every user—not only minors—would have to verify their age. In that case, these regulations would need to be brought into line with the GDPR.

So far, there is a lack of definitive data on the most effective model of ban. Preliminary data from Australia indicates that children aged between 10 and 15 continue to use social media. This, however, is considered to be largely due to the failure of platforms to implement effective age-verification measures—despite the ban, they reportedly either failed to check the age of users or wrongly classified them as older.

**The EU's first steps**. The European Union also plans to regulate minors' access to social media. In mid-July, the Commission received the report of a special panel on children's online safety. The report presented the impact of social media on children, including addictive mechanisms, as the platforms are designed to make users spend as much time on them as possible. On this basis, the report's authors developed recommendations for further EU action. At the end of 2026, the Commission will decide what steps to take in this matter. It has already announced that it will focus primarily on limiting those aspects of social media that make them harmful to children, such as the addictive autoplay of short video content or the *infinite scroll*, which continually loads new content when the user scrolls to the bottom of the page.

**Conclusions and recommendations**. The trend towards banning children from accessing social media will continue to grow. In the coming years, further countries—likely including all EU members—will introduce regulations along these lines, and the direction of these changes may soon be set by the European Commission by legislating in this area. At the same time, regulating minors' access will be used as a substitute for regulating big tech directly. In the context of child-protection measures, it is also worth promoting other rules, for example those concerning incitement to violence and online hate speech, which would allow the genuine enforcement of the DSA with potentially less resistance from the US and the platforms.

It is crucial that age verification in the EU be carried out using eID rather than tools created by the platforms themselves—limiting the information they receive to only whether the user is entitled to use the service. This choice will determine whether the protection of minors comes at the cost of privacy and a further strengthening of big tech's position, or is based on trusted public digital infrastructure. Such a solution would also be consistent with the EU's efforts to build digital sovereignty and reduce dependence on external providers. Moreover, the bans should provide for exceptions—restricting access to social media must not simultaneously deprive children of access to messaging services and safe forms of contact with one another. For Poland, the priority remains the full implementation of the DSA, which already regulates children's online safety, and—once the EU tool becomes available—basing national restrictions on access to social media on age verification using eID.