European Parliament

Virtual private networks and the protection of children online

There has been a significant surge in the number of virtual private networks (VPNs) used to bypass online age verification methods in countries where these have been put in place by law. Protection of children online is high on the political agenda, and new legislative frameworks are being implemented that require a minimum age to access certain online products and services. The European Union's Digital Services Act has introduced recommended guidelines for age assurance, which apply to online intermediaries and social media platforms. Some argue that access to VPN services should be restricted to users above a digital age of majority.

The rise of VPNs to bypass age verification

A virtual private network (VPN) is a digital technology designed to establish a secure and encrypted connection between a user's device and the internet. By hiding the user's Internet Protocol (IP) address and routing data through remote servers, VPNs can protect online communications from interception and surveillance. Initially designed for business purposes in the mid-1990s, VPNs have since evolved into tools widely used by individuals, institutions, and organisations.

In the corporate world, VPNs are essential for secure remote work, allowing employees to access company systems without compromising sensitive information. For individual users, VPNs prevent tracking by internet service providers, advertisers and potential cybercriminals. They are also used to access educational or entertainment content that may be restricted in certain countries, including authoritarian regimes, supporting freedom of information and digital inclusivity, as censorship becomes more difficult to enforce through VPN use.

Bypassing geographical restrictions on online content is among the main uses of VPNs. In the context of child protection, VPNs are relevant insofar as they allow users to bypass national requirements on online age verification methods on platforms and websites that provide pornographic content and other forms of content deemed harmful to children. As a result, their use has soared since mandatory age verification rules came into force in some states in the United States (US) and in the United Kingdom (UK).

In the UK, the Online Safety Act introduced duties on internet services to prevent children from accessing harmful and age-inappropriate content and required providers to offer parents and children clear and accessible reporting mechanisms. Since the related legislation came into force in 2025, half of the top 10 free apps in app-download charts in UK app stores have reportedly been VPN services. One app developer reported a 1 800 % spike in downloads in the first month after the legislation started to apply.

A loophole that needs closing

Some argue that this is a loophole in the legislation that needs closing and call for age verification to be required for VPNs as well. In response, some VPN providers argue that they do not share information with third parties and state that their services are not intended for use by children in the first place. The Children's Commissioner for England has called for VPNs to be restricted to adult use only.

While privacy advocates argue that imposing age-verification requirements on VPNs would pose significant risks to anonymity and data protection, child-safety campaigners claim that their widespread use by minors requires a regulatory response. Pornhub and other large pornography platforms have reportedly lost web traffic following the enforcement of age-verification rules in the UK, while VPN apps have reached the top of download rankings.

In France, Pornhub has blocked access to its websites after age-verification rules came into force, also driving a surge in VPN use. However, concerns remain that smaller, less-compliant rival sites may be gaining users and undermining child-safety goals, or that social media sites are escaping scrutiny as gateways to pornographic content for children, even though they remain a primary source of both pornography for

Author: Mar Negreiro, Members' Research Service
PE 782.618 – January 2026

children and for online grooming. A central argument for including mandatory age-verification methods in online services is the risk of online grooming of children by adult predators who pose as young users.

Age verification remains a technical challenge

Despite many online platforms having set a minimum age of 13 years for access to their services, use by younger children remains widespread, as verifying a user's real age continues to be technically and operationally challenging. Current age assurance measures – including verification, estimation and self-declaration – are relatively easy for minors to bypass.

In a UK study, over half of children aged 3 to 12 (55 %) were reported to use at least one social media app or website. Moreover, children as young as eight were reported to have accessed pornography online. Another study found that 94 % of Danish children have social media accounts before turning 13, despite this being the minimum age set by many social media platforms.

France started enforcing one of Europe's first age verification laws in January 2025, requiring all pornographic streaming sites to implement age-verification measures. However, there are multiple possible technical approaches to address the issue, including biometrics for direct checks, ID verification and database or digital checks for age confirmation, often combining methods such as liveness detection. Since April 2025, a key requirement in France is that at least one method must be 'double-blind', meaning that the adult platform receives no information about the user other than confirmation of eligibility, while the age-verification provider has no knowledge of which websites the user visits. Another approach is liveness detection, which provides an additional layer to distinguish a live human user from a photo, video or mask, helping to ensure that models are not applied to highly accurate age estimates of synthetic profiles.

There is also the approach of on-device age verification, adopted recently in California, which mandates that parents or users declare age during the device's initial setup and encodes that information into an encrypted signal that communicates an age bracket to apps and online services. This represents a broader, more automated method in which developers must request an age signal when applications are downloaded and launched.

Age verification in the EU: Towards a digital age of majority

In the EU, there is currently a fragmented approach to age assurance – encompassing verification, estimation and self-declaration – which risks fragmentation of the internal market and may result in uneven levels of protection for minors across the EU.

Some EU countries have agreed on (e.g. Denmark) or are considering (e.g. France) bans on social media use for under 15- or 16-year-olds and have called for the establishment of a pan-European digital age of majority. At the EU level, recommended guidelines for age assurance are set out under Article 28 of the Digital Services Act (DSA), which applies to online intermediaries and social media platforms. As the EU reviews cybersecurity and privacy legislation, VPN services may also come under stricter regulatory scrutiny. For instance, it is likely that the revised Cybersecurity Act will introduce child-safety criteria, potentially including measures to prevent the misuse of VPNs to bypass legal protections.

On 10 October 2025, most EU countries, along with Norway and Iceland, signed the Jutland Declaration on protecting minors online. The ministerial declaration supports the possible introduction of a digital age of majority for access to social media while also calling for the participation of young people themselves in the design and evaluation of such measures.

On the same date, the Commission announced that it had initiated its first investigative actions under the DSA concerning safeguards for minors on Snapchat, YouTube, Apple App Store and Google Play, requesting information on their age-verification systems.

On 26 November 2025, the European Parliament adopted a resolution supporting the use of age-verification methods and calling for a European digital age limit of 16 for social media use. In parallel, Parliament's Committee on Culture and Education (CULT) is preparing a related own-initiative report on the impact of social media on young people.