# Efektivita Age Control legislatívy v EÚ

*Empirická analýza: dokáže reálne znížiť zneužívanie detí?*

17. apríl 2026 · blog.opportunist.global

Politická premisa za EÚ legislatívou v oblasti Age Control (AC) — overovanie veku, Chat Control/CSAR, veková brána pre sociálne siete — je emocionálne jednoduchá: chránime deti pred zneužívaním. Táto premisa si vyžaduje empirické overenie. Analýza sa pozerá na tri otázky: **kto a kde deti reálne zneužíva**, **čo z toho Age Control postihne**, a **ako ľahko sa AC obchádza v praxi**.

## Kontext: čo EÚ robí v apríli 2026

Situácia je trojvrstvová. **Chat Control 1.0** zomrel 3. apríla 2026, keď Európsky parlament odmietol jeho predĺženie hlasovaním 311:228. **Chat Control 2.0 (CSAR)** je v trilógovom rokovaní s cieľovým termínom leto 2026 — návrh by povinne zavádzal skenovanie obsahu vrátane end-to-end šifrovaných služieb. **Veková verifikačná aplikácia EÚ** bola 15. apríla 2026 oznámená ako „technicky pripravená"; používateľ nahrá pas alebo OP a platforma dostane iba potvrdenie „áno/nie" k vekovej hranici.

Pilotné krajiny: Francúzsko, Španielsko, Taliansko, Grécko, Dánsko, Írsko, Cyprus. Oficiálne je aplikácia dobrovoľná, ale pod DSA musia platformy preukázať „ekvivalentnú účinnosť" alebo čelia pokutám až 6 % globálneho obratu — de facto povinnosť. Rétorický rámec von der Leyenovej: „niet viac výhovoriek", „nulová tolerancia". Celá legitimita stojí na tom, že AC pomôže deťom. Poďme sa pozrieť na dáta.

## Kto v skutočnosti zneužíva deti

Toto je najdôležitejšia časť, pretože úplne rozmieňa premisu legislatívy. Dáta sú dlhodobo konzistentné naprieč krajinami a štúdiami:

**93 %** mladistvých obetí pozná páchateľa — 59 % sú známi, 34 % rodinní príslušníci, **iba 7 % cudzí ľudia** (DOJ/RAINN). V potvrdených prípadoch cez americkú CPS **76 % detí** bolo zneužitých rodičom alebo zákonným opatrovníkom. V Holandsku iba 7 % páchateľov boli cudzinci obete. Austrálske štúdie dospievajú k podobným číslam.

Rizikový profil je tiež známy: deti v jednorodičovských domácnostiach s nepríbuzným dospelým majú **20-násobne vyššie riziko**, deti so zdravotným postihnutím 3-násobne vyššie. Incest a zneužívanie nevlastným otcom je dominantný vzorec vnútrorodinného zneužívania.

Online rozmer existuje, ale je to prevažne *nadstavba* na offline vzťahoch — groomer je typicky dospelý, ktorého dieťa pozná cez rodinu, komunitu, šport, náboženstvo, školu. Úplne cudzí predátor z internetu je štatisticky okrajový jav.

***Záver: AC legislatíva je vo svojej konštrukcii navrhnutá proti tej minoritnej časti problému, ktorá generuje najmenej obetí. Otčim, tréner, kňaz, strýko na Vianociach — títo ľudia nemajú ako byť „zastavení“ verifikáciou veku na Instagrame.***

## Online vektory: čo AC rieši a čo nerieši

Online zneužívanie má štyri odlišné fenomény, ktoré sa v politickom diskurze miešajú dokopy:

**1. Distribúcia CSAM.** Podľa IWF je 62 % medzinárodne identifikovaného CSAM hosťovaných na serveroch v EÚ. Ale kľúčový detail: tento materiál prakticky nie je na mainstream platformách, ktoré AC postihne. Cirkuluje na darknete, cez P2P, Tor hidden services, špecifické šifrované kanály. Verifikácia veku na Instagrame neovplyvní nikoho, kto obchoduje s CSAM na hidden service.

**2. Grooming maloletých cez platformy.** Tu AC zdanlivo dáva zmysel, no logika zlyháva: AC overí vek používateľa pri vytváraní účtu. Dospelý predátor si vytvorí účet legálne (18+). Maloletý tiež (13+ alebo 16+). AC nezabráni tomu, aby si dospelí a deti posielali správy. Skutočné riešenie — „security by design“ podľa Breyera: predvolené súkromné profily pre maloletých, obmedzené kontaktovanie neznámymi, varovania pri zdieľaní kontaktov, nahých fotiek — nič z toho nevyžaduje celoplošné overovanie veku.

**3. Sextortion a self-generated obsah.** Rastúci problém, kde teenager pošle intímny obsah komusi, kto ho potom vydiera. AC tu nerieši nič — všetci aktéri môžu byť legálne verifikovaní.

**4. Vystavenie pornu.** Jediný prípad, kde AC *teoreticky* funguje. Empirický dôkaz z UK a Austrálie to ale rozbíja — viď nasledujúcu sekciu.

## Obchádzanie: čo sa stalo v praxi

Empirické dáta z krajín, ktoré AC zaviedli skôr, sú zničujúce:

Po zavedení britského **Online Safety Act** v lete 2025 vzrástlo používanie VPN **o 6 430 %**, registrácie VPN o 1 000 %. V **Austrálii** po 9. marci 2026 boli tri VPN aplikácie v top 15 bezplatných sťahovaní App Store v jediný deň. **Pornhub** odišiel z Austrálie, Francúzska, Louisiany a Texasu namiesto implementácie overovania — skončí iba s blokovacou obrazovkou.

Samotná Komisia to implicitne priznáva: dokumenty k novej EÚ aplikácii uvádzajú, že technicky zdatní neplnoletí môžu obísť obmedzenia cez VPN, ale EÚ to „považuje za obmedzenie akéhokoľvek verifikačného systému a nie za fatálnu chybu“. Preklad: vieme, že to nefunguje, ale aj tak to robíme.

Prieskumy: **41 %** používateľov internetu bolo požiadaných o overenie veku a **viac než polovica** sa pokúsila proces obísť. To nie je marginálny odpor — to je dominantné správanie.

Platformy reagujú cez detekciu VPN, GPS korelácie, deep packet inspection, blacklisty IP rozsahov. Ale obfuskované VPN (WireGuard cez port 443, shadowsocks, Mullvad s obfuskáciou, I2P) ostávajú prakticky nedetekovateľné. Rovnako triviálne metódy: zdieľaný účet rodiča, falošný OP, kúpený verifikovaný účet (už funkčný trh), hotspot z cudzej SIM.

> ***Bariéra obídenia je nižšia než bariéra implementácie. Dospelí musia obetovať súkromie a nahrať štátne doklady; deti si stiahnu bezplatný VPN.***

## Efektivita: čo hovoria dáta o znížení zneužívania

**Neexistuje empirický dôkaz**, že AC legislatíva v ktorejkoľvek jurisdikcii viedla k poklesu zneužívania detí. Žiadna seriózna štúdia. Zavádzajúce metriky (počet reportov cez NCMEC, počet odstránených obrázkov) merajú *činnosť systému*, nie *ochranu detí*. Rozdiel medzi aktivitou a efektom je tu celý argument.

Hodnotenie Európskeho parlamentu k pôvodnému CSAR návrhu bolo drvivé: v súčasnosti neexistujú technologické riešenia, ktoré dokážu detegovať CSAM bez vysokej chybovosti, a regulácia by podkopala end-to-end šifrovanie a bezpečnosť digitálnej komunikácie. Právna služba Rady EÚ sama varovala, že by to porušilo Články 7 a 8 Charty základných práv.

## Vedľajšie škody

Toto sú empirické, nie ideologické náklady AC:

**Budovanie infraštruktúry masového sledovania.** Aj keď je aktuálna aplikácia „privacy-preserving“ (zero-knowledge proofs, open source), vytvára centralizovanú identitnú vrstvu naviazanú na štátne doklady. Raz postavená infraštruktúra sa použije aj na iné účely — toto je štandardný vzorec (COVID passporty, ktoré von der Leyenová sama uviedla ako inšpiráciu).

**Vytláčanie platforiem z EÚ.** Signal avizoval odchod. Pornhub už odišiel z viacerých jurisdikcií. Menšie projekty, decentralizované služby a privacy-first operácie nemajú kapacitu na kompliance — prežijú iba mega-korporácie. AC je nepriama daň v prospech Meta, Google, Microsoft.

**Presun detí do horších prostredí.** Keď sú maloletí vytlačení z mainstream platforiem, idú na menej moderované miesta — Discord servery bez moderácie, Telegram, náhodné fóra. Skutočné grooming priestory sú často menšie a menej viditeľné, nie tie veľké.

**Falošný pocit bezpečia.** Rodičia, ktorí dôverujú, že „veková verifikácia chráni“, sú menej ostražití pri tom, čo dieťa reálne robí a s kým komunikuje. AC môže *zhoršiť* situáciu posunutím pozornosti od reálnej prevencie.

**Normalizácia štátnej identity pre online prístup.** V konečnom dôsledku AC smeruje k modelu, kde je anonymný prístup na internet technicky nemožný. Toto je civilizačný posun, nie technická úprava.

## Syntéza

Efektivita Age Control legislatívy pri znižovaní zneužívania detí je podľa dostupných dát blízka nule, možno marginálne pozitívna pri vystavení pornu u najmenej motivovaných detí. Zároveň:

• **Rieši nesprávny problém.** 93 % zneužívania prebieha offline, mimo dosahu akýchkoľvek digitálnych kontrol.

• **Rieši nesprávnu menšinu problému online.** CSAM necirkuluje na platformách, ktoré AC postihne.

• **Je triviálne obídateľná.** Empirické dáta z UK (+6 430 % VPN) a Austrálie to dokazujú v reálnom čase.

• **Vytvára infraštruktúru** s trvalými nákladmi na súkromie a architektonickú slobodu internetu.

• **Je politicky lacná.** Poskytuje silnú emocionálnu rétoriku („chránime deti“) bez nákladov, aké by mali skutočné opatrenia — zdroje pre sociálnu prácu, investigatívna polícia na darknete, vzdelávanie rodičov, legislatíva proti vnútrorodinnému zneužívaniu.

Skutočné zníženie zneužívania detí by vyžadovalo: viac zdrojov na CPS a pedopsychológov, lepšie detekčné protokoly v školách a zdravotníctve, programy pre rizikové rodiny (jednorodičovské domácnosti s nevlastnými partnermi), investigatívne kapacity cielene na darknetové siete distribúcie CSAM, „security by design“ prístup pre online platformy, a osvetu detí o hraniciach a komunikácii s dospelými.

Nič z toho nie je v aktuálnom AC balíčku prioritou. To samo osebe je najsilnejším argumentom, že deklarovaný cieľ a skutočný cieľ sa rozchádzajú.

## Zdroje a poznámky

Štatistické dáta o zneužívaní: U.S. DOJ / Bureau of Justice Statistics; RAINN (Rape, Abuse & Incest National Network); National Children's Alliance; holandské a austrálske národné štúdie. Dáta o VPN obchádzaní: ACS Information Age, TechRadar, Medianama, NordVPN/Proton reporty marec 2026. Štatút legislatívy EÚ: Wikipedia Chat Control entry, EDRi, Patrick Breyer MEP posts, European Commission press, EDPS.

*Táto analýza je deskriptívna a opiera sa o verejne dostupné dáta k aprílu 2026. Neobsahuje právne odporúčania.*