28. 8. 2026

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Chat Control: dvě odlišné regulace pod stejným názvem

Debata o tzv. Chat Control patří v posledních letech mezi nejkontroverznější legislativní projekty Evropské unie. Ve veřejném prostoru se přitom často hovoří o „Chat Control“ jako o jediném návrhu, přestože se pod tímto označením skrývají dva zcela odlišné právní režimy. Zatímco tzv. Chat Control 1 představuje dočasnou výjimku umožňující dobrovolné skenování komunikace, Chat Control 2 má být trvalou právní úpravou, která zásadním způsobem mění přístup Evropské unie k odhalování materiálů zobrazujících sexuální zneužívání dětí (Child Sexual Abuse Material – CSAM).

Rozdíl mezi oběma režimy přitom nespočívá pouze v jejich časové působnosti ani nejde jen o technickou otázku odhalování nelegálního obsahu. Návrh otevírá širší spor o to, jak daleko může stát zasahovat do soukromé elektronické komunikace.

Chat Control 1

První generaci tzv. Chat Control představuje nařízení (EU) 2021/1232. Nařízení tehdy vytvořilo dočasnou výjimku ze směrnice 2002/58/ES o soukromí a elektronických komunikacích (ePrivacy), která poskytovatelům komunikačních služeb umožnila pokračovat v dobrovolném odhalování známých i nových materiálů CSAM a případů online groomingu. Nešlo však o povinnost. Každý poskytovatel se mohl sám rozhodnout, zda takové technologie využije.

Právě dobrovolnost je jeden z hlavních znaků Chat Control 1. Evropská unie tímto předpisem neuložila platformám povinnost monitorovat komunikaci svých uživatelů, ale pouze odstranila právní překážku, která dobrovolné skenování znemožňovala.

Stejně významné je, že se tato úprava v praxi netýkala běžné end-to-end šifrované komunikace. Dobrovolné skenování využívaly především služby pracující s nešifrovaným obsahem. Debata o prolomení end-to-end šifrování tak v této fázi ještě nestála v centru legislativního sporu.

Přestože mělo jít pouze o přechodné řešení, jeho účinnost byla opakovaně prodloužena. Po posledním prodloužení z července 2026 zůstává nařízení účinné až do 3. dubna 2028. Evropská unie tak i nadále zachovává režim dobrovolného skenování, než bude nalezena shoda na trvalé právní úpravě.

Chat Control 2

První nařízení se mnohým jevilo jako nedostatečné, a proto byl představen návrh nařízení o prevenci a potírání sexuálního zneužívání dětí (CSAR), označovaný jako Chat Control 2.

Evropská komise jej představila již v květnu 2022 s cílem vytvořit jednotnou evropskou úpravu nahrazující dočasné řešení z roku 2021. Návrh vychází z přesvědčení, že dobrovolný systém hlášení již nepostačuje k efektivnímu odhalování trestné činnosti a že mezi jednotlivými poskytovateli existují značné rozdíly v úrovni ochrany, kdy pachatelé šíření materiálů zobrazujících sexuální zneužívání dětí přecházejí k jiným poskytovatelům s nižší úrovní kontroly.

Chat Control 2 přitom chce vytvořit komplexní regulatorní rámec zahrnující povinné hodnocení rizik jednotlivých služeb, přijímání preventivních opatření, vznik nového Evropského centra pro boj proti sexuálnímu zneužívání dětí a možnost ukládat poskytovatelům tzv. detekční příkazy. Právě detekční příkazy představují nejdiskutovanější část celého návrhu.

Detekční příkazy

Podle původního návrhu Evropské komise by mohl příslušný vnitrostátní orgán po splnění zákonných podmínek požádat soud nebo jiný nezávislý orgán o vydání detekčního příkazu. Ten by konkrétnímu poskytovateli uložil povinnost vyhledávat materiály CSAM nebo případy online groomingu.

Návrh současně rozlišuje několik různých technologií detekce. Zatímco známé nelegální materiály mají být identifikovány prostřednictvím hash-matching databází, u nového obsahu nebo komunikace nasvědčující groomingu se počítá s využitím nástrojů umělé inteligence a rozpoznávání vzorů chování.

Právě zde začíná jedna z největších právních polemik. Technologie „hashování“ je obecně považována za relativně přesnou při identifikaci již známých materiálů. Naproti tomu detekce nového obsahu nebo samotné komunikace mezi uživateli pracuje s pravděpodobnostními modely, jejichž výsledkem mohou být falešně pozitivní označení zcela legální komunikace.

Proto se stále intenzivněji diskutuje nejen otázka technologické spolehlivosti, ale také proporcionality takových zásahů do základních práv.

Spor end-to-end šifrování

Zásadní rozdíl mezi oběma režimy spočívá v jejich vztahu k end-to-end šifrování. Chat Control 1 ponechal šifrovanou komunikaci fakticky mimo svůj praktický dosah. Naproti tomu Chat Control 2 otevírá otázku, zda lze efektivně odhalovat nelegální obsah i v prostředí plně šifrovaných poskytovatelů komunikačních služeb.

Technickým řešením bývá nejčastěji označováno tzv. client-side scanning, tedy kontrola obsahu přímo v zařízení uživatele ještě před jeho zašifrováním. Z pohledu zastánců představuje kompromis umožňující zachovat samotné šifrování přenosu dat.

Kritici však upozorňují, že se tím mění samotná podstata end-to-end šifrování. Přestože komunikace zůstává během přenosu šifrována, dochází k její automatizované kontrole ještě před samotným zašifrováním. Podle organizací zabývajících se ochranou digitálních práv tak vzniká trvalá kontrolní vrstva, kterou lze v budoucnu rozšiřovat i pro jiné účely. Přestože návrh CSAR počítá s působností i vůči poskytovatelům působícím na evropském trhu bez ohledu na jejich sídlo, v praxi může vznikat problém s vymahatelností těchto povinností, zejména pokud se data nacházejí mimo území EU.

Debata se proto již dávno netýká pouze ochrany dětí, ale obecně hranic digitálního soukromí a důvěry v šifrovanou komunikaci.

Závěr

Chat Control 1 zůstává po posledním prodloužení účinný až do dubna 2028 a dává prostor k jednání o Chat Control 2. Jednání mezi Evropským parlamentem, Radou a Komisí dosud nepřinesla konečný kompromis. Klíčovými spornými otázkami zůstávají zejména rozsah detekčních příkazů, možnost zásahů do end-to-end šifrované komunikace a samotná hranice mezi cíleným vyšetřováním

konkrétních podezřelých osob a plošným monitorováním běžných uživatelů.

Veřejná debata přitom často oba režimy směšuje pod společným označením „Chat Control“, ačkoli jejich dopady jsou z právního hlediska výrazně odlišné. Zatímco Chat Control 1 umožňuje poskytovatelům především dobrovolné odhalování materiálů souvisejících se sexuálním zneužíváním dětí, Chat Control 2 počítá s podstatně širšími regulatorními nástroji typu detekční příkazy, hash-matching a client-side scanning. Není proto rozhodující, že Chat Control 2 dosud nebyl přijat. Právě tento návrh může představovat skutečný zlom v dosavadním pojetí soukromé elektronické komunikace a zaslouží si veškerou pozornost odborné i širší veřejnosti, neboť může zásadně ovlivnit budoucí podobu digitálního soukromí v Evropské unii.

JUDr. Martin Kartner,
advokát

Jakub Klaus

CERHA HEMPEL
Kališ & Partners

CERHA HEMPEL Kališ & Partners

Týn 639/1
110 00 Praha 1

Tel.: +420 221 111 711
e-mail: office@cerhahempel.cz

Další články:

- Chat Control: dvě odlišné regulace pod stejným názvem
- Evropské dotace srozumitelně: Díl druhý – Žadatel nebo příjemce?

- Cyber Resilience Act: od září 2026 budete muset hlásit incidenty i zranitelnosti. Jste na to připraveni?
- Přeshraniční provoz dronů v Evropské unii
- Od Google Shopping k DMA: nové rozhodnutí jako most pro soukromoprávní vymáhání?
- Urban waste water treatment directive – legislativa a její dopady
- Aktuální vývoj odpadového práva v České republice: od implementace evropských cílů k praktickým problémům aplikační praxe
- Kam až sahá pojem „soud“ podle Brusel I bis? Nad rozsudkem Městského soudu v Praze o vykonatelnosti rozhodnutí finančního arbitra v zahraničí
- Méně plastu, méně vzduchu, víc povinností. Co přináší nové obalové nařízení PPWR?
- Novinky z české a evropské regulace finančních institucí za měsíc červen 2026
- Evropské dotace srozumitelně: Díl první – Unijní a národní rámec