

Anotace rozhodnutí Evropského soudu pro lidská práva

Rozsudek ze dne 13. února 2024 ve věci č. 33696/19 – *Podchasov proti Rusku*

Senát třetí sekce Soudu jednomyslně shledal porušení práva stěžovatele na respektování soukromého života a korespondence podle článku 8 Úmluvy, když právní úprava stanovila vybraným subjektům širokou povinnost uchovávat obsah internetové komunikace uživatelů služeb a související údaje a zpřístupnit je na vyžádání úřadům, včetně případného dešifrování, aniž by obsahovala přiměřené a dostatečné záruky proti zneužití, resp. povinnost dešifrovat „end-to-end“ komunikaci byla nepřiměřená.

I. Skutkové okolnosti

Stěžovatel je uživatelem aplikace Telegram od stejnojmenné společnosti, jejímž prostřednictvím si osoby posílají zprávy. V roce 2017 úřady zařadily společnost do rejstříku subjektů šířících informace na internetu. Tím jí podle předpisů vznikla povinnost uchovávat obsah komunikace uživatelů po dobu šesti měsíců a související komunikační údaje po dobu jednoho roku a v určitých situacích vše předávat orgánům činným v trestním řízení nebo zpravodajským službám spolu s informacemi usnadňujícími dešifrování zpráv. Federální bezpečnostní služba vzápětí přikázala společnosti poskytnout jí informace k dešifrování komunikace několika uživatelů podezřelých z činností souvisejících s terorismem; mimo jiné i údaje týkající se šifrovacích klíčů, které jsou potřebné pro dešifrování komunikace. Společnost to odmítla. Daní uživatelé měli totiž v aplikaci zapnutou funkci „tajného chatu“ a používali šifrování „end-to-end“; poskytnutí informací by oslabilo šifrovací mechanismus pro všechny uživatele. Za odmítnutí příkazu byla společnosti uložena pokuta. Stěžovatel a další uživatelé aplikace neúspěšně napadli příkaz před vnitrostátními soudy.

II. Odůvodnění rozhodnutí Soudu

K TVRZENÉMU PORUŠENÍ ČLÁNKU 8 ÚMLUVY

Stěžovatel namítal, že předpisy stanovená povinnost uchovávat internetovou komunikaci a související komunikační údaje a zpřístupnit je na vyžádání úřadům, včetně případného poskytnutí informací k dešifrování zpráv, byla v rozporu s právem na respektování soukromého života a korespondence.

1. K existenci zásahu a jeho rozsahu

Soud připomněl, že již uchovávání údajů ze soukromého života osoby je zásahem ve smyslu článku 8 Úmluvy. Jejich následné použití nemá na tento závěr vliv. Nicméně při určení, zda informace uchovávané úřady zahrnují některý z aspektů soukromého života, Soud přihlíží ke kontextu, v němž byly informace zaznamenány a uchovávány, povaze záznamů, způsobu, jakým jsou používány a zpracovávány, a výsledkům, které mohou být získány (*S. a Harper proti Spojenému království*, č. 30562/04 a 30566/04, rozsudek velkého senátu ze dne 4. prosince 2008, § 67).

Podle Soudu uchovávání obsahu komunikace a souvisejících údajů Telegramem zasáhlo do práva stěžovatele na respektování soukromého života a korespondence (*Ekimdzhev a další proti Bulharsku*, č. 70078/12, rozsudek ze dne 11. ledna 2022, § 372–373). Není relevantní, zda úřady měly či neměly ke komunikaci a údajům přístup; uchovávání, byť provázené soukromým subjektem, vyžadoval zákon, zásah tedy byl přičitatelný státu. Dále Soud posuzoval, zda je stěžovatel obětí zásahu do práv podle článku 8 Úmluvy jen kvůli existenci předpisů, které úřadům umožňují přístup k informacím, byť neexistoval důkaz, že k tomu u něj došlo. Protože osoby nemohou s jistotou vědět, zda k jejich datům v Telegramu měly úřady přístup, Soud využil stejná kritéria jako u utajeného sledování osob (tamtéž, § 375–376). V tomto ohledu dříve shledal, že kvůli tajné povaze sledování, širokým možnostem využití, dopadajícím na všechny uživatele komunikačních sítí, a neexistenci účinných prostředků nápravy může

již samotná právní úprava zasahovat do soukromého života osoby (*Roman Zakharov proti Rusku*, č. 47143/06, rozsudek velkého senátu ze dne 4. prosince 2015, § 170–79). U stěžovatele se přístup k uchovávané komunikaci a souvisejícím údajům řídil stejným právním režimem. Už samotná existence právní úpravy proto představovala zásah do výkonu práv stěžovatele podle článku 8 Úmluvy (srov. *Ekimdzhiyev a další proti Bulharsku*, cit. výše, § 383–84). Stran povinnosti Telegramu dešifrovat komunikaci se Soud zaměřil jen na komunikaci prostřednictvím tajných chatů za využití šifrování „end-to-end“. Z dostupných podkladů, včetně vyjádření Telegramu na vnitrostátní úrovni, přitom vyplynulo, že není technicky možné poskytnout úřadům šifrovací klíče spojené s konkrétními uživateli aplikace. Musela by se oslabit šifrovací technologie, což nelze omezit na konkrétní osoby, ale postihlo by to všechny uživatele bez rozdílu. Soud měl tedy za to, že stěžovatel mohl být i tomto ohledu dotčen.

Podle Soudu proto povinnost Telegramu nepřetržitě uchovávat internetovou komunikaci stěžovatele a související údaje a umožnit na vyžádání úřadům přístup k těmto informacím, včetně usnadnění dešifrování, představovala zásah do práv stěžovatele podle článku 8 Úmluvy. Jelikož byly informace uchovávány za účelem umožnit úřadům provádět cílený utajený dohled nad internetovou komunikací, Soud zdůraznil, že uchovávání informací a tajné sledování byly v dané věci úzce propojeny.

2. K oprávněnosti zásahu

Soud opět posuzoval situaci nejen optikou uchovávání osobních údajů stěžovatele, ale zohlednil i judikaturu k tajnému sledování. Připomněl, že zákon musí poskytovat účinné záruky proti riziku zneužití a zásah do práv musí být podle čl. 8 odst. 2 Úmluvy v souladu se zákonem, sledovat legitimní cíl a být nezbytný v demokratické společnosti (tamtéž, § 291–93 a 395). Shledal, že uchovávání komunikace a souvisejících údajů mělo základ v příslušném zákoně. Zdůraznil také, že technologie značně zvýšily objem komunikace přes internet, čímž narostly i hrozby pro státy a jejich občany, včetně terorismu, obchodu s drogami či s lidmi a sexuálního vykořisťování dětí. Původci mnohých z nich jsou mezinárodní sítě aktérů s přístupem k sofistikovaným technologiím umožňujícím jim nepozorovaně komunikovat. Právní úprava tak sledovala i legitimní cíle ochrany národní bezpečnosti, předcházení nepokojům a trestné činnosti a ochrany práv a svobod druhých. Zbývalo proto posoudit, zda vnitrostátní právo obsahovalo i přiměřené a účinné záruky, aby splňovalo požadavky na kvalitu zákona a nezbytnosti.

i) K uchovávání internetové komunikace a souvisejících komunikačních údajů

V dané věci právní úprava vyžadovala nepřetržitě automatické uchovávání obsahu veškeré internetové komunikace po dobu šesti měsíců a souvisejících údajů po dobu jednoho roku. Dopadala na internetové služby sloužící k přenosu hlasové, textové, vizuální, zvukové, obrazové nebo jiné elektronické komunikace. Týkala se všech uživatelů internetové komunikace, byť u nich neexistovalo důvodné podezření z účasti na trestné činnosti nebo činnosti ohrožující národní bezpečnost, ani jiný důvod se domnívat, že uchovávání může přispět k boji proti závažné trestné činnosti nebo k ochraně národní bezpečnosti. Vztahovala se tedy na obsah veškeré komunikace a související údaje bez vymezení rozsahu opatření co do územní nebo časové působnosti nebo kategorií osob, u nichž mohou být osobní údaje uchovávány. Zásah tak zde byl mimořádně rozsáhlý a závažný (srov. tamtéž, § 394). Tím spíše musí předpisy poskytovat přiměřené a dostatečné záruky proti zneužití v souvislosti s možným přístupem úřadů.

ii) K možnému přístupu úřadů k uchovávaným informacím pro účely cíleného utajeného sledování

Soud zdůraznil, že umožnění přístupu v konkrétních případech musí doprovázet stejné záruky jako u tajného sledování osob (tamtéž, § 395). Podle předpisů ale úřady neměly povinnost předložit poskytovateli zapsanému v rejstříku soudní povolení před získáním přístupu ke komunikaci osoby. Poskytovatelé museli již po vydání příkazu úřady instalovat zařízení umožňující úřadům přímý přístup k uloženým datům. Úřady tak získaly vzdálený přístup ke všem internetovým komunikacím a souvisejícím údajům. Požadavek předložit soudní povolení ještě před získáním přístupu ke komunikaci osoby je přitom pro Soud důležitou zárukou proti zneužití. Zajišťuje, že ve všech případech utajeného sledování je získáno řádné povolení. Zde to ale právní režim umožňoval úřadům obcházet. Měly tak přímý přístup k internetové komunikaci každého občana a souvisejícím údajům bez předložení

soudního povolení. Systém zde tedy byl obzvláště náchylný ke zneužití. Potřeba záruk proti svévoli a zneužití byla proto mimořádně velká (*Roman Zakharov proti Rusku*, cit. výše, § 269–70).

Nadto vláda potvrdila, že se přístup k internetové komunikaci a souvisejícím údajům řídil stejným právním režimem jako odposlechy mobilní telefonní komunikace. Zde Soud už dříve shledal, že právní úprava nesplňovala požadavek na „kvalitu zákona“, když neposkytovala přiměřené a účinné záruky proti svévoli a riziku zneužití, resp. neumožňovala udržet zásahy na úrovni nezbytné v demokratické společnosti. Zároveň okolnosti, za kterých úřady mohly použít opatření utajeného sledování za účelem odhalování, prevence a vyšetřování trestných činů nebo ochrany národní, vojenské, hospodářské nebo ekologické bezpečnosti, nebyly vymezeny dostatečně jasně. Ve výsledku tak povolovací režimy nemohly zajistit přijetí opatření pouze, je-li to v demokratické společnosti nezbytné. Dohled nesplňoval požadavky na nezávislost a na pravomoci, které by byly dostatečné pro provádění účinné a průběžné kontroly, veřejné kontroly a účinnosti v praxi. Možnost domáhat se účinné nápravy byla dále oslabena tím, že utajený dohled nebyl osobě nikdy oznámen, ani nebyl zajištěn odpovídající přístup k dokumentům týkajícím se dohledu (tamtéž, § 243–305).

Soud proto konstatoval, že vnitrostátní právo neposkytovalo přiměřené a dostatečné záruky proti zneužití stran umožnění přístupu úřadů k internetové komunikaci a souvisejícím údajům osob.

iii) K požadavku na dešifrování komunikace

Dále se Soud zabýval povinností Telegramu poskytnout úřadům informace nezbytné k dešifrování komunikace. Z odborných podkladů vyplynulo, že šifrování poskytuje silné technické záruky proti neoprávněnému přístupu k obsahu komunikace. Proto je široce využíváno jako prostředek ochrany práva na respektování soukromého života a korespondence online. Technická řešení pro zabezpečení a ochranu soukromí komunikace, včetně šifrování, také přispívají k zajištění výkonu dalších práv, jako je svoboda projevu. Nadto šifrování pomáhá osobám bránit se proti zneužívání informačních technologií, jako jsou hackerské útoky, krádeže identity a osobních údajů, podvody a neoprávněné zveřejňování důvěrných informací. Uvedené proto musel Soud zohlednit při posuzování opatření oslabující šifrování.

Soud měl za to, že umožnění dešifrování komunikace chráněné šifrováním „end-to-end“, jako je komunikace prostřednictvím „tajných chatů“ Telegramu, by znamenalo oslabení šifrování pro všechny uživatele. Toto opatření údajně nelze omezit na konkrétní osoby, a postihlo by tedy všechny bez rozdílu, včetně osob, které nepředstavují hrozbu. Oslabení by také zřejmě umožnilo provádět běžný, všeobecný a neselektovaný dohled nad osobní elektronickou komunikací. Využít by toho mohly i zločinecké sítě a vážně ohrozit bezpečnost elektronické komunikace všech uživatelů. Soud neopomněl, že šifrování mohou používat i zločinci, což může komplikovat vyšetřování trestných činů (*Yüksel Yalçinkaya proti Turecku*, č. 15669/20, rozsudek velkého senátu ze dne 26. září 2023, § 312). Na druhou stranu podle Europolu, Agentury EU pro kybernetickou bezpečnost a Úřadu vysokého komisaře OSN pro lidská práva existují alternativní řešení dešifrování bez oslabení ochranných mechanismů, a to jak prostředky práva, tak i prostřednictvím neustálého technického vývoje.

Podle Soudu tedy povinnost dotčených provozovatelů dešifrovat „end-to-end“ komunikaci vedla k oslabení šifrovacího mechanismu pro všechny uživatele, a nebyla proto přiměřená sledovaným legitimním cílům.

iv) Závěr

Vzhledem k výše uvedenému Soud konstatoval, že předpisy uloženou povinnost uchovávat veškerou internetovou komunikaci všech uživatelů, přímý přístup úřadů k uchovávaným datům bez odpovídajících záruk proti zneužití a požadavek na dešifrování „end-to-end“ komunikace, nelze považovat za nezbytné v demokratické společnosti. V rozsahu, v němž právní úprava umožňuje úřadům všeobecný přístup k obsahu elektronických komunikací bez dostatečných záruk, narušuje samotnou podstatu práva na respektování soukromého života. Stát zde překročil jakýkoli přijatelný prostor pro uvážení.

Soud proto rozhodl, že došlo k porušení článku 8 Úmluvy.

III. Oddělené stanovisko

Soudce Serghides se v částečně nesouhlasném stanovisku ohradil proti závěru, že nebylo nutné zkoumat stížnost ve vztahu k článku 13 Úmluvy a že konstatování porušení Úmluvy představuje dostatečné spravedlivé zadostiučinění za případnou nemajetkovou újmu utrpěnou stěžovatelem. Měl za to, že stěžovateli měla být přiznána peněžitá náhrada; zároveň Soud nemůže stěžovateli poskytnout účinnou ochranu, pokud se stížností nezabýval z hlediska článku 13 Úmluvy.