

Anotace rozhodnutí Evropského soudu pro lidská práva

Rozsudek ze dne 25. května 2021 ve věcech č. 58170/13, 62322/14 a 24960/15 – *Big Brother Watch a ostatní proti Spojenému království*

Velký senát Soudu jednomyslně rozhodl, že britská právní úprava hromadného sledování elektronické komunikace a souvisejících komunikačních dat zpravodajskými službami stejně jako úprava získávání komunikačních dat od poskytovatelů komunikačních služeb neobsahují dostatečné záruky proti zneužití, a je proto v rozporu s články 8 a 10 Úmluvy. Dvanácti hlasy proti pěti dále rozhodl, že úprava přijímání zpravodajských informací od zpravodajských služeb třetích států požadavkům článků 8 a 10 Úmluvy vyhovuje.

I. Skutkové okolnosti

Stěžovateli je celkem 16 nevládních organizací a novinářů, kteří brojili proti programům sledování elektronické komunikace provozovaným vládou Spojeného království. V návaznosti na odhalení zveřejněná Edwardem Snowdenem měli za to, že s ohledem na povahu jejich činnosti je pravděpodobné, že jejich komunikace byla zachycena britskými zpravodajskými službami, byla těmito službám předána třetími státy či byla zpravodajskými službami získána od poskytovatelů komunikačních služeb.

Na vnitrostátní úrovni se část stěžovatelů obrátila na příslušný specializovaný soud, Soud vyšetřovacích složek (*Investigatory Powers Tribunal, IPT*). V řízení před ním stěžovatelé namítali porušení článků 8, 10 a 14 Úmluvy ze dvou důvodů. *Zprv* tvrdili, že britské zpravodajské služby, případně i další orgány, obdržely jejich zachycenou komunikaci a komunikační data od orgánů Spojených států amerických, které tyto údaje získaly v rámci programů PRISM a Upstream. *Zadruhé* stěžovatelé namítali, že britské zpravodajské služby, případně i další orgány, zachycují, kontrolují a uchovávají jejich komunikaci a komunikační data získané na základě programu TEMPORA.

IPT po pěti dnech veřejného a jednom dni uzavřeného jednání rozhodl, že režim výměny dat se zpravodajskými službami třetích států neporušuje Úmluvu. Výměna podléhá stejným zárukám, jaké se uplatní v případech získávání dat samotnými britskými zpravodajskými službami podle zákona o regulaci vyšetřovacích složek. Ačkoli jsou bližší pravidla stanovena vnitřní instrukcí zpravodajské služby, dle IPT v této oblasti postačí, pokud je veřejně známo, že adekvátní pravidla existují a jaký je jejich rámcový obsah, a na jejich dodržování je náležitě dohlíženo. To je dle IPT splněno. Existence a obsah pravidel byly v řízení prokázány. Na jejich dodržování dohlíží parlamentní komise a nezávislý komisař. Co se týká vlastního získávání a nakládání s daty samotnými britskými zpravodajskými složkami, IPT shledal, že záruky, které obsahuje zákon o regulaci vyšetřovacích složek, jsou dostatečné a v souladu s kritérii, která Soud stanovil ve věci *Weber a Saravia proti Německu* (č. 54934/00, rozhodnutí ze dne 29. června 2006). I v tomto ohledu proto k porušení Úmluvy nedošlo.

II. Odůvodnění rozhodnutí Soudu

Stěžovatelé namítali, že tři větve britského režimu hromadného zachycování elektronické komunikace jsou v rozporu s články 8 a 10 Úmluvy: hromadné zachycování komunikace podle čl. 8 odst. 4 zákona o regulaci vyšetřovacích složek, získávání informací od zpravodajských služeb třetích států a získávání komunikačních dat od poskytovatelů komunikačních služeb. Do řízení se jako vedlejší účastníci zapojily vlády Francie, Nizozemska a Norska, stejně jako zvláštní zpravodaj OSN ke svobodě projevu a sedm nevládních organizací.

Dne 13. září 2019 vydal senát první sekce Soudu rozsudek, v němž shledal, že hromadné sledování podle čl. 8 odst. 4 zákona o regulaci vyšetřovacích složek porušuje články 8 a 10 Úmluvy a že režim

výměny dat se zpravodajskými službami třetích států v rozporu s Úmluvou není. Dne 4. února 2019 panel pěti soudců vyhověl žádosti stěžovatelů o postoupení věci velkému senátu.

A. K HROMADNÉMU ZACHYCOVÁNÍ ELEKTRONICKÉ KOMUNIKACE

A.1. K NAMÍTANÉMU PORUŠENÍ ČLÁNKU 8 ÚMLUVY

Stěžovatelé v první řadě namítali, že režim hromadného zachycování elektronické komunikace je v rozporu s článkem 8 Úmluvy chránícím právo na respektování soukromého života.

a) Úvodní poznámky a existence zásahu do práv

Soud vymezil, že projednávaná věc se týká hromadného zachycování přeshraniční komunikace zpravodajskými službami. V současnosti nabývá velká většina komunikace elektronickou formu a je přenášena globálními telekomunikačními sítěmi za použití momentálně nejlevnějších a nejrychlejších cest, kdy hranice států při určení cesty nehrají žádnou roli. Hromadné zachycování je převážně používáno pro zpravodajské získávání zahraničních informací a identifikaci nových hrozeb, zejména v oblasti terorismu, obchodu s drogami, obchodu s lidmi či kybernetických útoků.

Dle Soudu je hromadné sledování postupným procesem, který lze rozdělit na čtyři základní etapy. První je zachycení a uložení komunikace a s ní souvisejících dat, druhou filtrování zachycených dat, třetí analýza vybraných dat zpravodajcem a čtvrtou uložení dat a zpracování a použití z nich získaných informací, včetně jejich sdílení s třetími subjekty.

První etapa se dotýká velkého množství osob. Sama o sobě nepředstavuje nijak významný zásah do práv, avšak i samotné uložení dat, i když je možné je přechytit jen za pomoci zvláštní technologie, představuje zásah do práv chráněných článkem 8 Úmluvy. Každá další fáze hromadného sledování s sebou nese závažnější zásah do práv, a roste tak i potřeba adekvátních záruk proti zneužití.

b) K odůvodnění zásahu

1. Stávající a nové obecné zásady

Soud úvodem připomněl, že tajné sledování musí být v souladu se zásadou právního státu, která je výslovně zmíněna v preambuli Úmluvy a obsažena v předmětu a cíli článku 8. Zákon, na jehož základě sledování probíhá, tedy musí být dostupný a předvídatelný.

V kontextu tajného sledování předvídatelnost nemůže znamenat, že jednotlivec musí být schopen předvídat, kdy ho příslušné orgány mohou sledovat, aby mohl své jednání dle toho upravit. V situacích, kdy je veřejná moc vykonávána výkonnou mocí utajeně, je však riziko svévole zjevné. Je proto zásadní, aby pravidla pro použití tajného sledování byla jasná a podrobná. Zákon musí jednotlivci poskytnout adekvátní vodítka, za jakých okolností a podmínek mohou orgány veřejné moci tajného sledování využít. Musí vymezovat rozsah uvážení svěřeného příslušnému orgánu a způsob jeho výkonu s dostatečnou přesností.

Jsou-li před Soudem napadeny právní předpisy umožňující tajné sledování, je otázka zákonnosti úzce spjata s nezbytností, a Soud je proto posuzuje společně. Vnitrostátní právo musí zaručit, že tajné sledování je použito pouze tehdy, pokud je to nezbytné v demokratické společnosti. Musí proto obsahovat adekvátní a účinné záruky proti zneužití.

Pro případy sledování pro účely trestního řízení Soud rozvinul následujících šest minimálních požadavků, které musí vnitrostátní právo zakotvovat: (i) povaha trestných činů, které mohou sledování odůvodnit, (ii) vymezení kategorií osob, které mohou být sledovány, (iii) omezení délky sledování, (iv) pravidla pro zkoumání, použití a uchovávání získaných dat, (v) pravidla pro předávání dat třetím subjektům a (vi) okolnosti, za nichž musí být data vymazána či zničena (např. *Roman Zakharov proti Rusku*, č. 47143/06, rozsudek velkého senátu ze dne 4. prosince 2015, § 236).

V posledně uvedeném rozsudku Soud nadto přihlédl k úpravě dohledu nad výkonem sledování, oznamování sledování dotčeným osobám a prostředkům nápravy (tamtéž, § 238). Při tajném sledování vyvstává otázka dohledu ve třech fázích: při jeho nařízení, během jeho provádění a po jeho skončení.

V prvních dvou fázích se sledování z logiky věci odehrává bez vědomí dotčené osoby, proto i dohled probíhá bez její účasti. Je proto žádoucí svěřit dohled soudci (tamtéž, § 233).

Při rozhodování, jak nejlépe dosáhnout legitimního cíle ochrany národní bezpečnosti, státy požívají širokého prostoru pro uvážení (*Weber a Savaria proti Německu*, cit. výše, § 106). Tajné sledování však pod pláštěm ochrany bezpečnosti a demokracie může tyto hodnoty podkopat či zničit. Soud proto musí ověřit, zda jsou k dispozici adekvátní a účinné záruky, že zásahy do práv způsobené tajným sledováním budou omezeny na to, co je nezbytné v demokratické společnosti (*Roman Zakharov proti Rusku*, cit. výše, § 232).

Soud dále potvrdil, že rozhodnutí přistoupit k hromadnému zachycování komunikace za účelem identifikace hrozeb pro národní bezpečnost či zásadní národní zájmy spadá do prostoru pro uvážení států. Prostor pro uvážení států je však již užší během samotného hromadného sledování. Výše zmíněných šest zásad pro cílené sledování pro účely trestního řízení je podle Soudu základem i pro hromadné sledování, avšak musí mu být uzpůsobeno. Jedná se totiž o sledování jiné povahy a rozsahu.

Hromadné sledování je obvykle zaměřeno na přeshraniční komunikaci a na osoby, které nemohou být sledovány pomocí jiných prostředků. Byť hromadné sledování může sloužit také pro vyšetřování určité závažné trestné činnosti, je hlavně využíváno pro získávání zahraničních zpravodajských informací, pro včasné odhalení kybernetických útoků, kontrašpionáž a boj proti terorismu. Ačkoli hromadné sledování není nutně zaměřeno na konkrétní osoby, může tomu tak být. Nejsou jím však sledována konkrétní komunikační zařízení, ale na jednotlivce je cíleno použitím silných filtrů, např. emailovou adresou.

U prvních dvou záruk platných pro cílené sledování (povaha trestné činnosti a kategorie sledovaných osob) je zřejmé, že se pro hromadné sledování neuplatní. Totéž platí pro požadavek „rozumného podezření“, protože účelem hromadného sledování je především prevence, nikoli vyšetřování konkrétního trestného činu. Vnitrostátní právo nicméně musí obsahovat podrobná pravidla, kdy příslušné orgány mohou tajného sledování využít. Zejména musí vymezit důvody, pro něž může být použito, a okolnosti, kdy lze sledovat komunikaci určitého jednotlivce. Zbývající čtyři záruky jsou pro hromadné sledování relevantní ve stejné míře jako pro cílené sledování.

Aby bylo minimalizováno riziko zneužití hromadného sledování, musí celý proces podléhat zárukám od počátku až do konce. V každé fázi sledování tak musí být zhodnocena nezbytnost a přiměřenost předmětných opatření. Tajné sledování musí na počátku, kdy je vymezen jeho cíl a rozsah, podléhat nezávislému povolení, na jeho průběh musí být dohlíženo a musí podléhat následnému nezávislému přezkumu.

Co se týká úvodní fáze povolení, soud představuje důležitou záruku, avšak nikoli nezbytnou. Povolení nicméně musí vydat orgán, který je nezávislý na výkoné moci. Tento orgán musí být informován o účelu sledování a o nosičích či komunikačních cestách, které budou sledovány.

Soud připustil, že požadavek, aby povolení obsahovalo všechny filtry, které budou použity pro výběr komunikace, jež bude dále analyzována, by byl v praxi neuskutečnitelný. Bývá používáno velké množství filtrů, které jsou mnohdy vyjádřeny kombinací čísel a znaků, a je u nich potřeba určité flexibility. Povolení však musí identifikovat druhy a kategorie filtrů, které mohou být použity.

Použití silných filtrů spojených s identifikovatelnými osobami však musí podléhat zesíleným zárukám. Jejich použití musí být podrobně zdůvodněno, zaznamenáno a musí podléhat předchozímu vnitřnímu schválení, zda je jejich použití nezbytné a přiměřené.

Každý dílčí aspekt hromadného sledování – úvodní povolení a každé další prodloužení, určení komunikačních nosičů, výběr a použití filtrů a vyhledávacích algoritmů, použití, uchovávání, předávání a výmaz zachycených dat – musí podléhat dohledu nezávislého orgánu. Dohled musí být natolik silný, aby umožnil udržení sledování jen v takovém rozsahu, který je nezbytný v demokratické společnosti. Aby byl dohled možný, zpravodajské služby musí vést podrobné záznamy o všech fázích sledování.

Každý, kdo se domnívá, že jeho komunikace byla zachycena, musí mít k dispozici účinný prostředek nápravy. Jednotlivci nemusí být oznámeno, že byl sledován, pakliže má možnost domáhat se ochrany,

i pokud má jen podezření na sledování. Oznámení v případě hromadného sledování ostatně v praxi nebude mnohdy realizovatelné. O prostředku nápravy nemusí nutně rozhodovat soud. Musí se však jednat o orgán nezávislý na výkoné moci, který zajistí spravedlivé řízení v nejvyšší možné míře respektující zásadu kontradiktornosti. Rozhodnutí tohoto orgánu musí být odůvodněno a musí být závazné, rozhodne-li o ukončení sledování či zničení zachycených dat.

Soud shrnul, že soulad režimu hromadného sledování s Úmluvou podrobí globálnímu posouzení jeho fungování. V první řadě se zaměří na existenci dostatečných záruk proti zneužití v právních předpisech pokrývajících všechny fáze sledování od samotného počátku až do jeho konce. Přihlédne však i k fungování režimu v praxi a případným důkazům o jeho zneužití.

Při společném přezkumu zákonnosti a přiměřenosti tajného sledování Soud přezkoumá, zda vnitrostátní právní řád dostatečně jasně definuje: (i) důvody, pro něž může být hromadné sledování povoleno, (ii) okolnosti, za nichž může být zachycena komunikace určitého jednotlivce, (iii) proces udělení povolení sledování, (iv) proces výběru, zkoumání a použití zachycených dat, (v) opatření při předání dat třetím subjektům, (vi) omezení délky sledování, uchovávání dat a okolností, za nichž musí být data zničena, (vii) proces a způsob dohledu nezávislého orgánu a pravomoci pro řešení zjištěných porušení a (viii) proces následného nezávislého přezkumu a pravomoci pro řešení zjištěných porušení.

Tyto záruky se vztahují nejen na komunikaci a její obsah, ale i na související komunikační data. Z nich lze v dnešní době sestavit o jednotlivci intimní obrázek např. skrze údaje z účtů na sociálních sítích, sledování polohy odesílatele a příjemce zpráv či sledování procházení internetu. Jejich sledování tak může představovat závažnější zásah než sledování obsahu komunikace. S obsahem komunikace a souvisejícími komunikačními daty však může v praxi být zpravodajskými službami zacházeno odlišně. Příslušná ustanovení vnitrostátního práva proto nemusí být nutně identická.

Co se týká předávání dat získaných hromadným sledováním třetím státům či mezinárodními organizacím, Soud uvedl, že takto lze nakládat jen s daty, které byly získány a uchovávány v souladu s Úmluvou. Nadto, okolnosti, kdy k předání dat může dojít, musí být ve vnitrostátním právu jasně vymezeny. Dále, předávající stát se musí ujistit, že ve státě, kam jsou data předávána, existují záruky proti zneužití a nepřiměřeným zásahům. To nicméně neznamená, že tento třetí stát musí poskytovat srovnatelnou úroveň ochrany. Zatřetí, jde-li o data vyžadující zvláštní důvěrnost, například důvěrný materiál novinářů, jsou třeba zesílené záruky. Konečně, předání dat musí podléhat nezávislé kontrole.

2. Použití těchto zásad na okolnosti projednávané věci

Soud úvodem konstatoval, že namítané hromadné sledování má základ v hlavě I. zákona o regulaci vyšetřovacích složek a sleduje legitimní cíle ochrany národní bezpečnosti, předcházení nepokojům a trestné činnosti a ochrany práv a svobod jiných.

Ohledně dostupnosti zákona Soud poznamenal, že zákonná ustanovení jsou komplexní a nejsou příliš jasná. Podrobnější pravidla jsou nicméně obsažena v Praktickém kodexu, který byl schválen oběma komorami parlamentu a publikován v tištěné podobě i online. Přihlížet k němu musí jak osoby, které sledování provádějí, tak soudy. Dle Soudu je tedy příslušné vnitrostátní právo dostatečně dostupné.

Otázku, zda tyto předpisy obsahují v dostatečné míře výše uvedených osm záruk proti svévoli, aby byla splněna podmínka předvídatelnosti a nezbytnosti v demokratické společnosti, Soud zkoumal primárně na oblasti sledování obsahu komunikace. V druhé části se zaměřil na specifika zachycování souvisejících komunikačních dat.

2.1. Sledování obsahu komunikace

2.1.1. Důvody, pro které může být sledování povoleno

Příslušný zákon hromadné sledování umožňuje pro zajištění národní bezpečnosti, předcházení závažné trestné činnosti a na ochranu ekonomických zájmů Spojeného království, pokud jsou tyto zájmy relevantní i z hlediska národní bezpečnosti. Pojem národní bezpečnosti byl praxí omezen na aktivity ohrožující bezpečnost či blahobyt státu nebo usilující o svržení parlamentní demokracie. Pojem

závažné trestné činnosti byl blíže specifikován samotným zákonem skrze odkaz na minimální trestní sazby, použití násilí či výši způsobené škody. Materiál získaný sledováním nadto může být použit pro odhalení a předejití trestné činnosti, avšak nesmí být použit v trestním řízení.

Soud poznamenal, že čím širší jsou důvody, pro něž lze sledování povolit, tím větší je riziko zneužití. Avšak i když jsou důvody sledování definovány relativně široce, jako je tomu ve Spojeném království, nemusí to samo o sobě znamenat porušení článku 8 Úmluvy. Soulad s článkem 8 bude zajištěn, pakliže ostatní záruky, posouzené v jejich celku, budou dostatečné, aby tuto slabou stránku kompenzovaly. Soud se proto zaměřil na další záruky.

2.1.2. Okolnosti, za nichž může být sledována komunikace jednotlivce

Z příslušných ustanovení zákona a kodexu vyplývá, že hromadné sledování není zaměřeno na jednotlivce či určité komunikační zařízení, ale na nosiče (*bearers*; nosiče se nacházejí na podmořských optických kabelech, jimiž je elektronická komunikace přenášena; internet spojuje cca 100 000 těchto nosičů). Na nosičích je zachycována veškerá komunikace, která jimi proudí.

Nosiče nejsou vybírány náhodně, ale zpravodajské služby jsou dle zákona povinny se zaměřit jen na ty, přes něž je podle jejich znalostí nejvíce pravděpodobné, že proudí přeshraniční komunikace. Zachycena nicméně může být i vnitřní komunikace, která je mnohdy dopravována kabely ležícími mimo britské území. Nadto, do zákonného vymezení externí komunikace spadají i cloudová úložiště, procházení internetu a aktivity na sociálních sítích.

Soud konstatoval, že omezení na přeshraniční komunikaci do určité, byť omezené, míry zužuje kategorii osob, které mohou být sledovány. To je dle Soudu relevantní aspekt, jelikož pro interní komunikaci státy mohou využít méně invazivní prostředky. Navíc, jelikož původce ani příjemce komunikace nemohou nijak ovlivnit, skrze jaké nosiče bude zpráva doručena, další omezení výběru nosičů, které mohou být sledovány, by předvídatelnost zákona nezvýšila. Vymezení okolností, za nichž může být sledována komunikace jednotlivce, je tedy podle Soudu dostatečně předvídatelné ve smyslu článku 8 Úmluvy.

2.1.3. Proces povolení sledování

Žádost o povolení sledování musí být zkontrolována alespoň dvěma pracovníky zpravodajské služby, která ji podává. Následně ji posuzuje a schvaluje příslušný ministr. Soud konstatoval, že toto nastavení procesu schválení nevyhovuje jednomu ze základních požadavků, aby hromadné sledování bylo schváleno orgánem, který je nezávislý na výkoné moci.

Co se týká rozsahu posouzení žádosti, Soud shledal, že zpravodajská služba je povinna uvést podrobné informace o účelu sledování a zdůvodnit, proč je sledování nezbytné k jeho dosažení a není k dispozici jiná, méně invazivní metoda. Žádost nemusí obsahovat výčet nosičů, ale musí specifikovat typy nosičů, na nichž bude sledování probíhat. Žádost nicméně neobsahuje žádné vymezení filtrů, které budou používány pro výběr komunikace, jejíž obsah bude analyzován zpravodajcem. I když je následně v průběhu sledování výběr filtrů kontrolován nezávislým komisařem, v okamžiku povolení sledování žádné nezávislé posouzení přiměřenosti zamýšlených filtrů neprobíhá.

Soud proto shrnul, že vedle nedostatku nezávislosti proces povolení hromadného sledování z pohledu článku 8 Úmluvy vykazuje deficit v podobě absence posouzení přiměřenosti filtrů, které mají být používány, a absence zvýšených záruk při použití silných filtrů zaměřených na identifikovatelné jednotlivce, které dle Soudu musí podléhat přechozímu internímu i nezávislému externímu schválení.

2.1.4. Proces výběru, analyzování a použití zachyceného materiálu

Analyzována zpravodajcem může být jen komunikace, která byla vybrána na základě filtrů a vyhledávacích algoritmů. Ty se nesmějí vztahovat k osobě, o níž je známo, že pobývá na území Spojeného království, ledaže by to schválil příslušný ministr. Před otevřením konkrétní komunikace zpravodajec musí písemně odůvodnit, proč je to nezbytné a proč daná informace nemůže být získána jinými prostředky. Zpravodajci procházejí pravidelným povinným školením ohledně příslušné právní

úpravy a požadavku přiměřenosti a nezbytnosti. Zachycený materiál musí být skladován bezpečným způsobem a přístup k němu mohou mít jen osoby s příslušnou bezpečnostní проверkou a jen v rozsahu, který je pro jejich potřeby nezbytný.

Soud shrnul, že příslušné záruky jsou z pohledu článku 8 Úmluvy dostatečné, s výjimkou stejných nedostatků, které byly identifikovány výše, týkajících se schvalování jednoduchých i silných filtrů.

2.1.5. Proces předávání dat třetím subjektům

Soud zopakoval, že příslušné předpisy omezují přístup k zachyceným datům, jak co se týká okruhu osob, tak co do rozsahu přístupu. Příslušné osoby musejí mít bezpečnostní проверku a data jsou jim zpřístupněna jen v nezbytné míře.

Ohledně předání dat mimo území Spojeného království Soud shledal, že jsou nastavena pravidla zaručující, že příjemci dat s nimi budou zacházet tak, že nedojde k nepřiměřenému zásahu do práv. Orgány třetích států mohou s daty zacházet jen v nezbytném rozsahu a nesmějí je předat dalším subjektům, ledaže je tak výslovně dohodnuto se zpravodajskou službou, která je jejich původcem. Data musí být zničena, jakmile již nejsou potřeba. Jsou-li předávána data důvěrné povahy, musí tak být označena.

Dle Soudu jsou záruky nastaveny tak, že data budou třetími subjekty bezpečně uložena a nebudou dále šířena. Soud dodal, že velmi důležité také je, že na proces předávání dohlíží nezávislý komisař a přezkoumává ho i IPT.

2.1.6. Délka sledování, uchovávání dat a jejich ničení

Zákon omezuje platnost povolení ke sledování na šest měsíců a v případě sledování za účelem předejití závažné trestné činnosti jen na tři měsíce. Platnost povolení může být prodloužena o stejnou dobu. Žádost o prodloužení musí obsahovat stejné informace jako úvodní žádost. Nadto musí obsahovat vyhodnocení dosavadního sledování a zdůvodnění, proč je jeho pokračování nezbytné. Příslušný ministr je vedle toho povinen nezbytnost sledování průběžně vyhodnocovat, a pakliže již sledování není nutné, povolení zrušit.

Dobu uchovávání zachycených dat zákon omezuje nejdéle na dva roky. Pro jednotlivé kategorie dat však zpravodajská služba po dohodě s nezávislým komisařem dle jejich povahy stanovuje individuální lhůty uchovávání, které v praxi dosahují délky jen několika měsíců. Po jejich uplynutí jsou data automaticky mazána.

Tyto záruky Soud vyhodnotil jako dostatečné z pohledu článku 8 Úmluvy. Dodal však, že by bylo žádoucí, aby kratší lhůty, které jsou uplatňovány v praxi, byly promítnuty do právní úpravy.

2.1.7. Dohled

Zákon dohled nad prováděním hromadného sledování svěřuje komisaři, který je nezávislý jak na výkonné, tak na zákonodárné moci. Komisař musí být soudcem některého ze soudů na vrcholu soudní soustavy. Komisař předkládá každého půl roku zprávu o své činnosti předsedovi vlády a jednou ročně oběma komorám parlamentu. Zprávy jsou publikovány, od roku 2013 v plném znění. Po každé inspekci zašle komisař zprávu i řediteli příslušné zpravodajské služby. Zpráva může obsahovat doporučení, na které je ředitel povinen do dvou měsíců reagovat.

Rozsah kontrol komisaře pokrývá všechny fáze sledování, jejich přiměřenost, výběr nosičů i filtrů, používání filtrů i nakládání se zachyceným materiálem, včetně jeho předávání třetím subjektům. Za rok 2016 takto komisař zkontroloval 970 povolení, což tvořilo přibližně jednu třetinu povolení vydaných v daném roce.

Soud shledal, že komisař vykonává z pohledu článku 8 Úmluvy dostatečný, nezávislý a účinný dohled.

2.1.8. Následný přezkum

Zákon zřídil IPT, specializovaný soud, který je příslušný k rozhodování o žalobách proti konkrétnímu sledování, tak k posouzení zákonnosti a souladu režimu hromadného sledování jako takového

s Úmluvou. Na IPT se může obrátit každý, kdo má podezření, že jeho komunikace mohla být sledována. Má pravomoc přezkoumat nejen sledování jako takové, ale i předávání dat třetím subjektům. Předsedou IPT je soudce nejvyššího soudu. Členy mohou být jen soudci vrcholných soudců či právníci s vymezenou alespoň desetiletou zkušeností. IPT má přístup ke všem dokumentům zpravodajských složek, včetně těch podléhajících utajení. Pokud koná uzavřené jednání, žalobci jsou při něm zastoupeni poradcem soudu. IPT zveřejňuje svá rozhodnutí na internetových stránkách.

Soud shrnul, že IPT poskytuje robustní soudní prostředek nápravy.

2.2. Související komunikační data

Soud konstatoval, že shora zjištěné nedostatky se ve stejné míře vztahují i k zachycování souvisejících komunikačních dat. Ve stejné míře se na ně vztahují i záruky, které Soud výše vyhodnotil jako účinné.

V obou režimech nicméně existují dva rozdíly. Zatímco použití silného filtru vztahujícího se k osobě nacházející se na území Spojeného království je ve vztahu k obsahu komunikace možné jen s předchozím souhlasem příslušného ministra, u použití takového filtru ve vztahu k souvisejícím komunikačním datům souhlas ministra potřebný není. Obdobně, zatímco komunikace, která neodpovídá silnému filtru či komplexnímu vyhledávacímu algoritmu, musí být bezodkladně smazána, tato související komunikační data mohou být uchovávána po dobu až několika měsíců.

Ve vztahu k prvnímu rozdílu Soud akceptoval, že v praxi je potřeba provést filtrování souvisejících komunikačních dat ve vztahu k osobám, které se nacházejí na území Spojeného království, v řádu tisíců týdně, přičemž identita těchto osob mnohdy není známa. Soud proto absenci souhlasu ministra nepovažoval za rozhodující. Klíčovým nedostatkem je dle Soudu již konstatovaná absence předchozího interního a nezávislého schválení silných filtrů a vyhledávacích algoritmů.

Co se týká délky uchovávání, Soud přijal, že relevance souvisejících komunikačních dat se může vyjasnit až po uplynutí určité doby. Určitá doba uchovávání dat, které se zprvu zdají jako nevýznamná, je tedy potřebná. Soud však konstatoval, že právní předpisy nijak ohledně dob uchovávání nerozlišují mezi obsahem komunikace a souvisejícími komunikačními daty. Delší lhůty uchovávání posledně zmíněných je tedy nepředvídatelné. Článek 8 Úmluvy vyžaduje, aby tyto lhůty byly zakotveny v právních předpisech.

2.3. Závěr

Soud akceptoval, že hromadné sledování je pro smluvní státy Úmluvy životně důležité k identifikování hrozeb pro jejich národní bezpečnost. Uznala to ostatně i Benátská komise. Hromadné sledování však v sobě nese ohromný potenciál k zneužití zasahujícího do práv jednotlivců na respektování soukromého života.

Ačkoli režim hromadného sledování podle čl. 8 odst. 4 zákona o regulaci vyšetřovacích složek obsahuje řadu záruk, neobsahuje dostatečné a účinné záruky od počátku do konce sledování. Hromadné sledování zejména není povolováno nezávislým orgánem. Žádost o povolení sledování nemusí obsahovat kategorie filtrů. Použití silných filtrů nepodléhá předchozímu internímu schválení.

Tyto nedostatky se vztahují ke sledování jak obsahu komunikace, tak souvisejících komunikačních dat.

Dohled nezávislého komisaře a přezkum IPT jsou důležitými zárukami, avšak nejsou dostatečné k vyvážení zjištěných nedostatků.

Právní úprava hromadného sledování tak nedosahuje potřebné kvality, aby bylo zajištěno, že zásah do práv způsobený sledováním zůstane v mezích, které jsou v demokratické společnosti nezbytné. Došlo proto k porušení článku 8 Úmluvy.

A.2. K NAMÍTANÉMU PORUŠENÍ ČLÁNKU 10 ÚMLUVY

Stěžovatelé, kteří byli novináři, dále namítali, že britský režim hromadného zachycování elektronické komunikace neposkytuje dostatečnou ochranu jejich privilegované komunikaci, čímž dochází k porušení článku 10 Úmluvy.

a) Stávající a nové obecné zásady

Soud připomněl, že ochrana novinářského zdroje je jedním ze základních kamenů svobody tisku. Příkaz odhalit zdroj může mít škodlivý dopad nejen na zdroj, jehož identita by byla odhalena, ale i na dotčené médium, jehož reputace bude ohrožena, a na veřejnost jako takovou, v jejímž zájmu je mít možnost dostávat informace z anonymních zdrojů. Zásah do ochrany novinářského zdroje je proto v souladu s článkem 10 Úmluvy jen tehdy, pokud je odůvodněn prvořadým veřejným zájmem (*Sanoma Uitgevers B. V. proti Nizozemsku*, č. 38224/03, rozsudek velkého senátu ze dne 14. září 2010, § 51). K posouzení, zda tu takový veřejný zájem je, musí dojít před odhalením zdroje, a musí ho vykonat soudce či jiný nezávislý a nestranný orgán (tamtéž, § 92).

Ve vztahu k hromadnému sledování Soud rozvinul, že jsou-li použity silné filtry spojené s novinářem či v souvislosti s použitím silných filtrů je vysoce pravděpodobné, že bude analyzován novinářský materiál, jedná se o zásah, který je srovnatelný se zásahem způsobeným domovní prohlídkou v bydlíšti či na pracovišti novináře. V těchto případech může být shromážděno velké množství důvěrného novinářského materiálu, což může ochranu novinářského zdroje ohrozit dokonce více než prostý příkaz k odhalení zdroje určité informace. Proto předtím, než zpravodajské služby použijí silné filtry spojené s novinářem či s velkou pravděpodobností vedoucí k zachycení důvěrného novinářského materiálu, musí být tento postup posouzen soudcem či jiným nezávislým a nestranným orgánem, zda je odůvodněn prvořadým veřejným zájmem a zda není možné sledovaného cíle dosáhnout méně invazivními prostředky.

I když nejsou použity výše vymezené silné filtry, stále je možné, že důvěrný novinářský materiál bude zachycen a analyzován. Tyto situace jsou nicméně odlišné od výše popsanych a míra narušení novinářského zdroje nebude na počátku předvídatelná. Soudce by proto předem nemohl posoudit, zda je dané sledování odůvodněné naléhavým veřejným zájmem. Přesto však, pokud vyjde najevo, že obsah komunikace či související komunikační data obsahují důvěrný žurnalistický materiál, jejich uchovávání a analyzování musí být povoleno soudcem či jiným nezávislým a nestranným orgánem, který posoudí, zda je takový postup odůvodněn naléhavým veřejným zájmem.

a) Použití těchto zásad na okolnosti projednávané věci

Soud úvodem akceptoval, že hromadné sledování v případě stěžovatelů, kteří se věnují novinářské činnosti, zasahuje i do jejich práv chráněných článkem 10 Úmluvy. Dále připomněl, že příslušná právní úprava i v této souvislosti vykazuje stejné nedostatky, které identifikoval na poli článku 8 Úmluvy.

Nadto, právní úprava toliko vyžadovala, aby příslušný ministr při vydání povolení k zacílenému sledování „náležitě přihlédl“ k možnosti, že bude zachycena i komunikace obsahující důvěrný novinářský materiál. Dále jen vyžadovala, aby nezbytnost a přiměřenost sledování důvěrného novinářského materiálu byly jasně zdokumentovány.

Soud uznal, že pravidla pro uchovávání, předávání a výmaz důvěrných novinářských materiálů poskytovala dostatečné záruky. Ty však dle Soudu nemohou vyvážit nedostatky zjištěné na poli článku 8 Úmluvy, absenci předchozího nezávislého povolení silných filtrů, které s velkou pravděpodobností mohou vést k zachycení důvěrného novinářského materiálu, a absenci nezávislého schválení uchovávání a analyzování novinářského materiálu, který byl zachycen bez přímého úmyslu. Došlo proto i k porušení článku 10 Úmluvy.

B. K ZÍSKÁVÁNÍ INFORMACÍ OD ZPRAVODAJSKÝCH SLUŽEB TŘETÍCH STÁTŮ

B.1. K NAMÍTANÉMU PORUŠENÍ ČLÁNKU 8 ÚMLUVY

Stěžovatelé dále spatřovali porušení článku 8 Úmluvy v přijímání dat od zpravodajských služeb třetích států, zejména od služeb Spojených států amerických získaných v rámci programů PRISM a Upstream.

Soud úvodem akceptoval, že existovala možnost, že komunikace stěžovatelů byla v rámci programu Upstream zachycena a byla vyžádána britskými zpravodajskými službami. Stěžovatelé tedy musí být považováni za oběti možného porušení článku 8 Úmluvy.

a) Obecné zásady

Soud konstatoval, že v souvislosti s přijetím materiálu od zpravodajských služeb třetích států může dojít k zásahu do práv chráněných článkem 8 Úmluvy, a to úvodní žádostí o takový materiál a poté jeho přijetím a následným uchováváním, analyzováním a použitím. Opačný závěr by znamenal, že stát by se mohl vyhnout odpovědnosti na základě Úmluvy tím, že by sledováním pověřil zpravodajskou službu třetího státu, vyžádal si od ní materiál či domluvil přímý přístup do jejích informačních systémů.

Žádost o sledování, přijetí materiálu a jeho následné zacházení s ním proto musí být upraveno zákonem, který bude poskytovat adekvátní záruky proti zneužití. Soud uvedl, že tyto záruky musí být stejné jako u případů vlastního sledování vnitrostátní zpravodajskou službou. Jelikož nemusí být vždy jednoznačné, zda předávaný materiál skutečně byl získán sledováním, záruky se musí uplatnit na veškerý materiál, který je přijímán od cizí zpravodajské služby, který sledováním mohl být získán. Žádosti o sledování či materiály a následné zacházení s předanými daty musí podléhat nezávislému dohledu. Jednotlivec musí též mít k dispozici následný nezávislý přezkum.

b) Použití těchto zásad na okolnosti projednávané věci

Obdobně jako u samotného sledování Soud shledal, že sdílení zpravodajských dat má základ v zákoně o regulaci vyšetřovacích složek a praktickém kodexu a sleduje legitimní cíle ochrany národní bezpečnosti, předcházení nepokojům a trestné činnosti a ochrany práv a svobod jiných. Soud tak dále přistoupil ke společnému posouzení předvídatelnosti příslušných právních předpisů a nezbytnosti v demokratické společnosti.

Právní předpisy stanovily, že o zachycenou komunikaci a související komunikační data mohou zpravodajské služby své zahraniční protějšky požádat, jen bylo-li v dané věci vydáno vnitrostátní povolení k hromadnému sledování, určitou komunikaci není možné si opatřit vlastním sledováním, a je proto nezbytné si vyžádat pomoc třetí strany, přičemž je přiměřené a nezbytné si tuto komunikaci opatřit. Za výjimečných okolností, např. kdy technicky není možné si danou komunikaci opatřit na základě vnitrostátního povolení ke sledování, lze o pomoc zpravodajské služby třetích států požádat i bez vydání tohoto povolení. Soud poznamenal, že v praxi se tak zatím nikdy nestalo. Dle Soudu tato právní úprava dává jednotlivci dostatečná vodítka, kdy mohou být vyžádány zpravodajské materiály od třetích států. Soud shrnul, že jelikož se žádosti adresované třetím státům mohou týkat jen záležitostí, kde již bylo příslušným ministrem vydáno vnitrostátní povolení, není třeba se procesem povolení dále zvlášť zabývat.

Co se týká analyzování, použití, uchovávání, dalšího sdílení a výmazu zpravodajských dat obdržených ze zahraničí, Soud konstatoval, že vnitrostátní předpisy na ně vztahují stejné záruky jako na data opatřená vnitrostátními zpravodajskými službami. Dle Soudu skutečnost, že zákon tyto záruky vztahuje jen na materiál, u něhož je zřejmé, že by získán sledováním, a nikoli i na ten, který tak mohl být získán, není z pohledu článku 8 Úmluvy zásadní. Příslušné záruky proto Soud považoval za dostatečné.

Nadto, další ochranu poskytuje dohled nezávislého komisaře a každý se může obrátit na IPT, který vykonává následnou kontrolu.

Soud proto učinil závěr, že příslušné právo obsahuje dostatečné záruky proti tomu, aby zpravodajské služby využívaly žádosti o asistenci zpravodajských služeb třetích států k obcházení zákona či závazků vyplývajících z Úmluvy. Stejně tak obsahuje dostatečné záruky ohledně následného zacházení se zpravodajských materiálem pocházejícím ze zahraničí. K porušení článku 8 Úmluvy proto nedošlo.

B.2. K NAMÍTANÉMU PORUŠENÍ ČLÁNKU 10 ÚMLUVY

Stěžovatelé, kteří byli novináři, dále namítali, že získávání informací od zpravodajských služeb Spojených států amerických porušilo i jejich práva chráněná článkem 10 Úmluvy.

Soud shledal, že tato námitka nevyvolává žádné další otázky, než které byly řešeny na poli článku 8, a proto nedošlo ani k porušení článku 10 Úmluvy.

C. K ZÍSKÁVÁNÍ KOMUNIKAČNÍCH DAT OD POSKYTOVATELŮ KOMUNIKAČNÍCH SLUŽEB

Stěžovatelé konečně namítali, že režim získávání dat od poskytovatelů komunikačních služeb porušuje jejich práva chráněná články 8 a 10 Úmluvy.

Soud konstatoval, že britská vláda nijak nebrojila proti závěrům senátu Soudu. Ten ve svém rozsudku shledal, že jelikož byl příslušný zákon v rozporu s unijním právem, které mělo v dané oblasti aplikační přednost, nebylo sledování provedené na jeho základě v souladu se zákonem ve smyslu článku 8 Úmluvy. Rozpor s unijním právem spočíval v tom, že britské právo umožňovalo přístup ke komunikačním datům nikoli pouze v souvislosti s bojem proti závažné trestné činnosti, ale u jakékoli trestné činnosti, a že tento přístup mohl být realizován i bez předchozího přezkumu soudem či jiným nezávislým a nestranným orgánem. Ve vztahu k článku 10 Úmluvy senát Soudu shledal porušení, vedle absence omezení přístupu na případy boje proti závažné trestné činnosti, také v absenci soudního schválení přístupu ke komunikačním datům novináře vyjma případů, kdy jde přímo o žádost o odhalení zdroje.

S ohledem na výše řečené velký senát plně odkázal na závěry senátu a vyslovil porušení článků 8 i 10 Úmluvy.

III. Oddělená stanoviska

Soudci Lemmens, Vehabović a Bošnjak k rozsudku připojili souhlasné stanovisko, v němž zdůraznili význam soukromí jednotlivce a popsali šíři škodlivých následků, které sledování má. Považovali za nutné tak učinit pro vyvážení rozsudku, který zdůrazňuje jen význam hromadného sledování pro ochranu společnosti. Dále poukázali na to, že jednotlivá kritéria, která Soud vymezil, neposkytují dostatečnou ochranu. Soud totiž stanovil, že tyto záruky mají ve vnitrostátním právu být zakotveny, avšak neurčil minimální míru jejich ochrany. Nadto, absence či nedostatečnost určité záruky může být dle Soudu napravena kumulativním posouzením všech záruk. Určení jasné minimální úrovně každé ze záruk by dle soudců poskytlo větší ochranu.

Soudce Pinto de Albuquerque nesouhlasil se závěrem většiny o neporušení článků 8 a 10 v aspektu získávání informací od zahraničních zpravodajských služeb. Nabídl dále rozsáhlé alternativní odůvodnění závěrů o porušení článků 8 a 10 Úmluvy stanovující hromadnému sledování přísnější pravidla.

Soudci Lemmens, Vehabović, Ranzoni a Bošnjak též nesouhlasili se závěrem většiny o neporušení článků 8 a 10 v aspektu získávání informací od zahraničních zpravodajských služeb. Poukázali zejména na to, že nedostatek týkající se nedostatku nezávislého povolení hromadného sledování vnitrostátními zpravodajskými službami je stejně relevantní i pro přijímání zpravodajských informací od zahraničních služeb.