

Anotace rozhodnutí Evropského soudu pro lidská práva

Rozsudek ze dne 25. května 2021 ve věcech č. 35252/08 – *Centrum för rättvisa proti Švédsku*

Velký senát Soudu patnácti hlasy proti dvěma rozhodl, že švédská právní úprava signálového zpravodajství, tedy hromadného sledování elektronické komunikace a souvisejících komunikačních dat zpravodajskými službami, neobsahuje dostatečné záruky proti zneužití, a je proto v rozporu s článkem 8 Úmluvy.

I. Skutkové okolnosti

Stěžovatelka je nadací, jejímž předmětem činnosti je zastupování jednotlivců v řízeních týkajících se lidských práv. Věnuje se též vzdělávacím a výzkumným projektům. Skutečnost, že při své činnosti často kritizuje vládní instituce, s sebou dle jejího názoru nese riziko, že její komunikace byla či bude zachycována a analyzována v rámci tzv. signálového zpravodajství. Jelikož stěžovatelka byla přesvědčena, že nemá k dispozici žádný prostředek nápravy tohoto tvrzeného porušení svých práv, nezhájila na vnitrostátní úrovni žádné řízení.

Signálové zpravodajství zahrnuje zachycování, zpracovávání, analyzování a kompilování informací získaných z elektronických signálů. Ty mohou být převedeny do textu, obrázku či zvuku. Takto získané informace se mohou týkat jak obsahu komunikace, tak souvisejících komunikačních dat. Informace mohou být získávány z rádiového a satelitního spojení nebo z kabelů. Velká většina komunikačního toku je přenášena kabely. Příslušná vnitrostátní úprava nerozlišuje mezi obsahem komunikace a souvisejícími komunikačními daty, ani mezi způsoby přenosu komunikace.

II. Odůvodnění rozhodnutí Soudu

K NAMÍTANÉMU PORUŠENÍ ČLÁNKU 8 ÚMLUVY

Stěžovatelka namítala, že švédská právní úprava a praxe signálového zpravodajství, tedy hromadného sledování elektronické komunikace a souvisejících komunikačních dat zpravodajskými službami, porušuje její právo na respektování soukromého života a korespondence chráněné článkem 8 Úmluvy.

Dne 19. června 2018 vydal senát třetí sekce Soudu rozsudek, v němž shledal, že k namítanému porušení článku 8 Úmluvy nedošlo. Dne 4. února 2019 panel pěti soudců vyhověl žádosti stěžovatelky o postoupení věci velkému senátu.

a) K postavení stěžovatelky jakožto možné oběti porušení Úmluvy

Soud úvodem shledal, že jelikož zachycována mohla být komunikace každého jednotlivce a vnitrostátní právo neposkytuje žádný prostředek, v němž by mohla být stěžovatelčina námitka přezkoumána v plné šíři, je namíste stěžovatelku považovat za možnou oběť porušení Úmluvy z důvodu samotné existence příslušné právní úpravy signálového zpravodajství a přezkoumat tuto úpravu *in abstracto*.

b) 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 v daný okamžik 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 přečíst 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.

c) 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 uzpůsobit. V situacích, kdy je veřejná moc uplatňována výkonou 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*, č. 54934/00, rozhodnutí ze dne 29. června 2006, § 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 využíváno hlavně 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 výkonné 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 výkonné 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 ve vnitrostátním právu a sleduje legitimní cíl ochrany národní bezpečnosti.

Ohledně dostupnosti zákona Soud poznamenal, že příslušná pravidla jsou obsažena v pěti různých zákonech a čtyřech nařízeních. Všechny tyto právní předpisy byly řádně publikovány, a jsou tedy dostupné.

Jelikož tyto právní předpisy nijak nerozlišují mezi obsahem komunikace a souvisejícími komunikačními daty, a pro obojí se tak uplatní stejná pravidla a postupy, Soud zkoumal, zda byla dosažena míra naplnění výše uvedených osmi záruk proti svévoli nutná pro splnění podmínky předvídatelnosti a nezbytnosti v demokratické společnosti, pro obojí dohromady.

2.1. *Důvody, pro které může být sledování povoleno*

Vnitrostátní právo stanoví, že signálové zpravodajství může být použito jen za účelem sledování externích vojenských hrozeb, zapojení Švédska do mezinárodních mírových a humanitárních misí, strategických okolností týkajících se mezinárodního terorismu a další závažné přeshraniční trestné činnosti, která může ohrozit klíčové národní zájmy, šíření zbraní hromadného ničení a dalšího vojenského materiálu, závažných hrozeb pro společenskou infrastrukturu, zahraničních konfliktů ovlivňujících mezinárodní bezpečnost, a pro sledování zahraničních zpravodajských operací proti švédským zájmům a jednání cizích mocností, jež mají zásadní význam pro švédskou zahraniční, bezpečnostní a obrannou politiku. Všechny tyto pojmy blíže vysvětlují důvodové zprávy k příslušným zákonům.

Dle Soudu je míra podrobnosti vymezení oblastí, v nichž může být hromadné sledování použito, dostatečná, a to i s přihlédnutím k tomu, že sledování cílí na odhalení dosud neznámých zahraničních hrozeb, jejichž povaha může být různorodá a v čase se vyvíjet.

Ohledně „závažné přeshraniční trestné činnosti“ Soud dodal, že výsledky na ni zacíleného sledování nemohou být použity v trestním řízení. Orgány policie mají přístup jen k analytickým výsledkům sledování.

Dle Soudu jsou tedy důvody, kdy lze ke sledování přistoupit, jasně vymezeny. Je tím tak umožněna nezbytná kontrola povolení a provádění sledování, stejně jako jeho následný přezkum.

2.2. *Okolnosti, za nichž může být sledována komunikace jednotlivce*

Okolnosti, za nichž může být signálovým zpravodajstvím komunikace zachycena, jsou velmi široké. Hromadné sledování totiž 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.

Příslušné předpisy stanoví, že může být zachycována jen přeshraniční komunikace. V praxi však v úvodní fázi zachycení není vždy možné rozlišit, zda se jedná o vnitrostátní či přeshraniční komunikaci. Nadto, příslušná zpravodajská služba může v rámci rozvojové činnosti zachycovat i vnitrostátní komunikaci. To je však možné jen za účelem analyzování systémů a cest, kterými jsou informace přenášeny, aby bylo možné lépe vybrat nosiče, které budou sledovány. Dle Soudu je nezbytné, aby příslušné orgány takto mohly reagovat na vývoj technologií a způsobů komunikace. Zásah do individuálních práv způsobený touto činností je minimální, jelikož data nejsou používána pro získávání zpravodajských informací. Povolení k této rozvojové činnosti navíc může dát jen Soud pro zahraniční zpravodajství a je monitorována nezávislým Inspektorátem.

Soud tak akceptoval, že příslušné předpisy dostatečně jasně vymezují okolnosti, kdy může být komunikace signálovým zpravodajstvím zachycena.

2.3. Proces povolení sledování

Hromadné sledování podléhá přechozímu schválení Soudem pro zahraniční zpravodajství. Pouze v případě, kdy by řízení mohlo způsobit zdržení či jiné obtíže zásadního charakteru, může povolení vydat příslušná zpravodajská služba sama. Tím je zároveň zahájeno řízení před zmíněným soudem, který musí rozhodnout urychleně.

Soud je nezávislý na výkonné moci. Jeho předseda a místopředseda jsou soudci. Ostatní členové jsou sice jmenováni vládou, avšak na pevně stanovené čtyřleté funkční období. Jeho rozhodnutí jsou závazná.

Je pravdou, že jeho jednání jsou neveřejná a jeho rozhodnutí podléhají utajení. Řízení se však účastní „zástupce pro ochranu soukromí“. Je jím soudce, bývalý soudce či advokát. Je nezávislý a v řízení hájí veřejný zájem. Toto uspořádání dle Soudu s ohledem na potřebu utajení zpravodajských operací, zejména v jejich úvodu, poskytuje dostatečnou záruku proti zneužití.

V žádosti o povolení musí zpravodajská služba specifikovat, proč je sledování potřebné, nosiče, na nichž bude probíhat a filtry, které budou používány, případně alespoň kategorie filtrů. Filtry musí být formulovány tak, aby vedly k co nejmenším zásahům do soukromí. To dle Soudu implikuje, že dochází k posouzení nezbytnosti a přiměřenosti. Jde tak o důležitou záruku proti zneužití.

U silných filtrů, které jsou zacíleny na konkrétního jednotlivce, soud ověřuje, zda je splněna zákonem stanovená podmínka „výjimečného významu“ pro zpravodajskou činnost. To dle Soudu představuje relevantní zesílenou ochranu proti zneužití sledování jednotlivců.

Soud poznamenal, že výše popsany režim povolování má své vnitřně dané meze. Pro soud může být těžké posoudit přiměřenost sledování, pakliže jsou mu předloženy jen kategorie filtrů nebo je množství filtrů v řádu tisíců a jsou vyjádřeny technickou kombinací číslic a písmen. Dle Soudu je nicméně i tak režim povolení nezávislý, dostatečně podrobný a poskytuje významnou záruku proti svévolnému či zjevně nepřiměřenému hromadnému sledování. Stanovuje též rámec, v němž se konkrétní operace musí pohybovat, a jehož dodržování je průběžně i následně sledováno.

2.4. Proces výběru, analyzování a použití zachyceného materiálu

Soud uvedl, že ať je zachycování prováděno automatizovaně, jako je tomu u velké většiny případů, či manuálně v případě odposlechů vojenských rádiových vln, uplatní se stejné záruky. Pakliže je zachycena vnitrostátní komunikace, je okamžitě smazána. To dle Soudu představuje významné omezení uvažení zpravodajských služeb a záruku proti zneužití.

Všechna vyhledávání, která provede analytik, musí být zaznamenána. Pokud se vyhledávání týká dat obsahujících osobní údaje, záznam musí obsahovat použité filtry, čas vyhledávání, jméno analytika a odůvodnění vyhledávání. Skutečnost, že je tato povinnost vést záznamy zakotvena pouze ve vnitřních instrukcích zpravodajských služeb, je podle Soudu nepochybně nedostatkem. Na druhou stranu, nic nenásvědčuje tomu, že by v praxi záznamy nebyly vedeny nebo že by si zpravodajské služby mohly tuto povinnost samy zrušit.

Nadto, na danou oblast se uplatní i příslušná obecná úprava ochrany osobních údajů. Korespondence právnických osob, jako je i stěžovatelka, pakliže obsahuje osobní údaje fyzických osob, požívá též této ochrany. Soud dodal, že mnoho požadavků a záruk ochrany osobních údajů má však význam jen pro fyzické osoby – týkají se totiž rasy, etnicity, politických či náboženských názorů, zdraví nebo sexuálního života.

Dle Soudu obsahuje s ohledem na výše uvedené právní úprava výběru, analyzování a používání zachycených dat dostatečné záruky proti zneužití, které by mohlo ovlivnit práva chráněná článkem 8 Úmluvy.

2.5. *Proces předávání dat třetím subjektům*

Soud konstatoval, že předávání dat na vnitrostátní úrovni je jasně definováno výčtem institucí, které mohou mít k datům přístup. Tento seznam obsahující zpravodajské služby, policejní orgány a armádní složky se nezdá vytvářet riziko zneužití.

Ohledně výměny informací se složkami třetích států stěžovatelka brojila pouze proti předávání informací těmto složkám, nikoli i proti přijímání informací od nich. Soud konstatoval, že je pochopitelné, že právní předpisy nemohou obsahovat detailní a vyčerpávající seznam situací, kdy mohou být informace předány. Musí však obsahovat záruky omezující riziko zneužití a nepřiměřené zásahy do práv chráněných článkem 8 Úmluvy.

V přezkoumávané věci je určitým omezením postupu zpravodajských služeb, že na zachycení předávaných informací se uplatní všechny záruky vztahující se na signálové zpravodajství. Podstatným nedostatkem dle Soudu však je, že vnitrostátní právní úprava neukládá zpravodajským složkám, aby před předáním zvážily nezbytnost a přiměřenost zásahu do práva na respektování soukromí, ke kterému může předáním dojít. Stejně tak právní předpisy nevyžadují, aby zpravodajské služby zkoumaly a ověřily, zda zahraniční příjemce informací datům poskytne akceptovatelnou úroveň ochrany. Žalovaná vláda nedoložila, že by existovaly nepřekonatelné překážky, aby toto posouzení přiměřenosti předání a zkoumání ochrany dat u příjemce byly provedeny. Ostatně, ve Spojeném království tento přezkum funguje (*Big Brother Watch a ostatní proti Spojenému království*, č. 58170/13 a další, rozsudek velkého senátu ze dne 25. května 2021, § 96).

Předávání dat sice podléhá dohledu Inspektorátu. Ten však kontroluje zákonnost hromadného sledování a zákon pro předávání podmínku přiměřenosti nestanoví. Nezávislý dohled tedy neposkytuje záruku, která by vyvážila zmíněný nedostatek právní úpravy. V celkovém posouzení souladu s článkem 8 Úmluvy k němu tedy musí být přihlédnuto.

2.6. *Délka sledování, uchovávání dat a jejich ničení*

Právní předpisy délku povolení omezují na šest měsíců. Může být prodloužena o dalších až šest měsíců, avšak jen po novém úplném přezkumu Soudem pro zahraniční zpravodajství.

Právní předpisy na druhou stranu neobsahují povinnost průběžně zkoumat nezbytnost pokračování sledování a v případě, že již nutné není, sledování ukončit. Dle Soudu by výslovné zakotvení této povinnosti poskytlo větší záruky, než současný stav. Ten však i tak podle Soudu poskytuje dvě záruky, které jsou dostatečné. V první řadě, zpravodajské služby mohou směrnici, která byla základem jejich žádosti o povolení, odvolat, což vede k ukončení operace. V druhé řadě, průběžný dohled Inspektorátu, který má přístup ke všem interním informacím zpravodajských služeb, zajišťuje ochranu před nepřiměřeně dlouhým sledováním.

Co se týká povinnosti data zničit, zákon ji ukládá v případech, kdy se data týkají určité fyzické osoby, avšak nemají zpravodajský význam, spadají pod ochranu novinářského zdroje, jsou důvěrnými informacemi mezi podezřelým a obhájcem či jde o údaje vztahující se k náboženskému vyznání. Chybí však obecné pravidlo pro výmaz dat, která nespádají do výše uvedených kategorií a neobsahují osobní údaje. Dle Soudu musí právní předpisy v minimální rovině obsahovat pravidlo zničení dat, která pozbyla relevance pro účely sledované signálovým zpravodajstvím. Jelikož však v praxi půjde o málo četné

případy, jde dle Soudu jen o procesní nedostatek. Byť musí být napraven, jako celek jsou podle Soudu vnitrostátním právem okolnosti, kdy musí být zachycený materiál zničen, upraveny jasně.

2.7. Dohled

Dohled nad signálovým zpravodajstvím vykonává Inspektorát zahraničního zpravodajství. Další kontrolu vykonává též úřad na ochranu osobních údajů.

Inspektorátu předsedají současní či bývalí soudci. Dalšími členy jsou osoby jmenované na nejméně čtyřleté funkční období vládou, vybrané z kandidátů navržených parlamentními stranami. Inspektorát je tak dle Soudu nezávislý.

Inspektorát povoluje zpravodajským službám přístup ke komunikačním nosičům, přičemž ověřuje, zda je požadovaný přístup v souladu s povolením vydaným Soudem pro zahraniční zpravodajství. Inspektorát též kontroluje zachycování, analyzování, použití dat, včetně předání třetím státům či mezinárodním organizacím, i jejich výmaz. Jeho rozhodnutí, že sledování musí být ukončeno či data vymazána, jsou závazná. Doporučení na změnu praxe sice nikoli, ale zpravodajské služby k nim v praxi náležitě přihlížejí a v minulosti vedly ke změnám. Inspektorát za dobu 8 let vykonal 102 kontrol zaměřených mj. na detailní přezkum použitých filtrů, výmaz dat či zacházení se zprávami vypracovanými na základě zachycených dat. Výsledky kontrol měly odraz v praxi. Inspektorát dále zveřejňuje roční zprávy o své činnosti.

Soud proto shledal, že dohled Inspektorátu, v kombinaci s režimem povolování sledování Soudem pro zahraniční zpravodajství, spolu tvoří funkční záruku proti zneužití v rozhodujících fázích sledování, tedy před a během zachycování, analyzování, použití a zničení informací získaných sledováním.

2.8. Následný přezkum

Dle příslušných právních předpisů sice existuje teoretická možnost oznámit jednotlivci *ex post*, že jeho komunikace byla sledována, v praxi se tak ale nikdy nestalo. Navíc to v mnohých případech ani nebude možné. Absence notifikačního mechanismu nicméně může být vyvážena účinným prostředkem nápravy, který je k dispozici každému, kdo má podezření, že jeho komunikace byla zachycena a analyzována.

V projednávané věci taková možnost existuje – každý se může obrátit na Inspektorát zahraničního zpravodajství, aniž by musel prokázat, že mohl být signálovým zpravodajstvím dotčen. Inspektorát je sice nezávislým orgánem, avšak do kontroly hromadného sledování je zapojen i jinak. Povoluje přístup ke komunikačním nosičům, monitoruje použití silných filtrů, analýzu komunikace a použití a výmaz dat. Následný přezkum na základě žádosti jednotlivce tak může vést k situaci, kdy bude posuzovat svou vlastní činnost. Toto uspořádání dle Soudu neposkytuje dostatečné záruky objektivity a důkladnosti. Nemůže být vyloučeno, že dvojí role Inspektorátu vyvolá konflikt zájmů a pokušení přehlédnout opomenutí či porušení ve snaze vyhnout se kritice či jiným důsledkům. Ani kontrola činnosti Inspektorátu ze strany nejvyššího kontrolního úřadu v této souvislosti není dostatečná.

Nadto, Inspektorát nevydává žádná odůvodněná rozhodnutí, která by byla přístupná žadatelům nebo alespoň advokátům majícím příslušnou bezpečnostní prověrku. Jednotlivec se tak vůbec nedozví, jaký byl rozsah a výsledek přezkumu. Toto uspořádání neposkytuje veřejnosti záruku, že zneužití, pakliže nastanou, budou odhalena a napravena.

Jednotlivec se sice může obrátit i na parlamentního ombudsmana či ministra spravedlnosti, avšak tyto prostředky nápravy neposkytují právní kontradiktorní řízení před nezávislým orgánem ústící ve vydání odůvodněného a závazného rozhodnutí. Britský systém přitom ukazuje, že takový prostředek nápravy, který slaďuje legitimní bezpečnostní zájmy a potřebu zajistit spolehlivou následnou kontrolu hromadného sledování, v praxi možný je (*Big Brother Watch a ostatní proti Spojenému království*, cit. výše, § 413–415).

Soud proto shrnul, že dvojí role Inspektorátu a nevydávání odůvodněného rozhodnutí jsou prvky, které nejsou v souladu s požadavky účinného následného přezkumu. Jde o nedostatky, které musejí být vzaty v potaz při celkovém posouzení souladu s článkem 8 Úmluvy.

2.9. Závěr

Soud uvedl, že nemá pochyb o tom, že hromadné sledování je pro identifikaci hrozeb pro národní bezpečnost pro státy životně důležité. Uznala to ostatně i Benátská komise. Zdá se, že neexistuje alternativa, která by ho mohla nahradit.

Soud dále připomněl, že jeho úlohou není vymezit ideální model signálového zpravodajství, ale ověřit soulad právního a praktického uspořádání, které se stát od státu koncepčně i funkčně liší, s článkem 8 Úmluvy.

Přezkoumávané švédské uspořádání jasně definuje důvody, pro něž může být sledování použito, i okolnosti, kdy jeho pomocí může být komunikace zachycena a analyzována. Délka sledování je upravena a kontrolována. Proces výběru, analyzování a použití zachyceného materiálu je obklopen adekvátními zárukami proti zneužití. Stejná pravidla se vztahují jak na obsah komunikace, tak na související komunikační data. Soud dále vyzdvihl nezávislost procesu povolení sledování Soudem pro zahraniční zpravodajství a dohled Inspektorátu zahraničního zpravodajství.

Soud nicméně identifikoval tři nedostatky: absence jasných pravidel pro výmaz dat neobsahujících osobní údaje, absence pravidla, že při předání dat třetím státům musí být zvážen jeho dopad do soukromí jednotlivců, a absence účinného následného přezkumu.

První nedostatek není dle Soudu zásadní, jelikož vnitrostátní právo upravuje řadu situací, kdy je třeba data zničit, a mezera v úpravě se týká jen dat, která neobsahují osobní údaje.

Druhý nedostatek však podle Soudu může vést k velmi citelným negativním dopadům do práv jednotlivců. Mohou tak být předána soukromá data, která mají velmi nízkou zpravodajskou hodnotu. Nadto, příslušné orgány nemusí ověřovat, jakou ochranu datům třetí strany zajišťují.

Třetí nedostatek, dvojí role Inspektorátu a nevydávání odůvodněných rozhodnutí, oslabuje následný přezkum natolik, že vytváří riziko, že dodržování práv jednotlivců nebude zajištěno.

Soud tak uzavřel, že hlavní rysy švédského režimu signálového zpravodajství naplňují požadavky, které článek 8 Úmluvy klade na kvalitu zákona. Druhý a třetí výše zmíněné shledané nedostatky však nejsou dostatečně vyváženy ostatními zárukami. Hromadné sledování s sebou přitom nese ohromný potenciál případného zneužití. Signálové zpravodajství ve Švédsku, hodnoceno ve svém celku, tak neobsahuje dostatečné záruky od počátku do konce procesu sledování. Došlo proto k porušení článku 8 Úmluvy.

III. Oddělená stanoviska

Soudci Lemmens, Vehabović a Bošnjak k rozsudku připojili souhlasné stanovisko, v němž odkázali na své oddělené stanovisko ve věci *Big Brother Watch a ostatní proti Spojenému království* (cit. výše).

Soudce Pinto de Albuquerque k rozsudku též připojil souhlasné stanovisko. Souhlasil se závěrem o porušení článku 8 Úmluvy, avšak dle jeho názoru většina zkreslila či zlehčila švédskou právní úpravu a praxi sledování. Neztotožnil se též s metodologií přezkumu, kterou většina zvolila. Systém záruk, který Soud v rozsudku rozvinul, označil za defektní. Vnitrostátní úpravu a praxi pak podrobil kritice zejména v aspektu nedostatečného dohledu a přezkumu.