UNIVERZITA KARLOVA

Právnická fakulta

Ondřej Serdula

Ochrana soukromí a osobních údajů v právu Evropské unie s ohledem na problematiku data retention

Protection of Privacy and Personal Data in European Union Law with Regards to Data Retention

Disertační práce

Školitel: prof. JUDr. Richard Král, LL.M., Ph.D., DSc.

Studijní program: Teoretické právní vědy - Evropské právo

Datum vypracování práce (uzavření rukopisu): 20. dubna 2021

Prohlašuji, že jsem předkládanou disertační práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 554 261 znaků včetně mezer.

V Praze dne 20. dubna 2021.

Ondřej Serdula

Rád bych poděkoval svému školiteli, prof. JUDr. Richardu Královi, LL.M., Ph.D., DSc., za odborné vedení v průběhu mého doktorského studia a za cenné připomínky při psaní disertační práce. Za podporu a trpělivost v průběhu celého doktorského studia, zejména při dokončování této práce, děkuji své manželce a rodině.

OBSAH

ÚVOD

Skutečnost, že orgány státu, jejichž úkolem je boj proti závažné trestné činnosti a jiným bezpečnostním hrozbám, mohou v určitých případech skrytě nahlédnout do soukromí jednotlivců, není v dnešní době příliš kontroverzní, a to ani ve vyspělých západních demokraciích. Ostatně, ESLP již v roce 1978 konstatoval, že demokratické společnosti čelí vysoce sofistikovaným formám špionáže a terorismu, proti kterým musí být schopny účinně zasáhnout, což odůvodňuje mj. existenci právních předpisů opravňujících příslušné orgány ke skrytému sledování („*secret surveillance*“) korespondence a telekomunikace.[1] Hrozby, o kterých ESLP hovořil, přitom v mezidobí jistě nevymizely. Právě naopak, vzhledem k rozvoji mezinárodního terorismu a další závažné přeshraniční trestné činnosti jsou dnes významnější než kdy dříve. Lze si jen stěží představit, že by státy mohly těmto hrozbám úspěšně čelit bez toho, aniž by orgány státu mohly v určitých případech skrytě monitorovat komunikaci probíhající na dálku.

Nástup a rapidní rozvoj digitálních technologií však přinesl zásadní změny v tom, jaké nástroje mají příslušné orgány k dispozici. Počátky používání těchto nástrojů je často možné spojovat již s reakcí na teroristické útoky v New Yorku, Madridu a Londýně na počátku 21. století. Zásadní společenskou diskuzi v této souvislosti však vyvolaly především informace zveřejněné bývalým zaměstnancem CIA a externím spolupracovníkem NSA Edwardem Snowdenem v roce 2013. Tato odhalení, která podrobně vykreslila míru a intenzitu zásahů do soukromí osob ze strany příslušných orgánů USA, způsobila zásadní posun v politické i právní diskuzi o ochraně soukromí a osobních údajů a byla impulzem pro řadu legislativních změn v následujících letech.[2] Tato odhalení měla a nadále mají přímé dopady i na situaci v EU, přinejmenším co se týče možnosti předávání osobních údajů z EU do USA.[3] Někteří autoři proto Snowdenova odhalení označují za „*jednu z nejdůležitějších geopolitických událostí posledních několika let*“,[4] resp. hovoří o současnosti jako o „*post-snowden době*“.[5]

---

[1] Rozsudek ESLP ze dne 6. září 1978, *Klass a další proti Německu*, stížnost č. 5029/71, CE:ECHR:1978:0906JUD000502971, bod 48 (dále jen „*rozsudek Klass proti Německu*“).

[2] Srov. Fundamental Rights Agency. *Surveillance by intelligence services Fundamental rights safeguards and remedies in the EU*, 2017, s. 9.

[3] Srov. rozsudek Soudního dvora ze dne 6. října 2015, *Schrems*, C-362/14, EU:C:2015:650 (dále jen „*rozsudek Schrems*“) či rozsudek Soudního dvora ze dne 16. července 2020, *Facebook Ireland a Schrems*, C-311/18, EU:C:2020:559 (dále jen „*rozsudek Facebook Ireland a Schrems*“).

[4] DEEKS, Ashley. An International Legal Framework for Surveillance. *Virginia Journal of International Law*, 2014, s. 293.

[5] CLARK, Ian. The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, 2016, s. 1.

Odhalení Edwarda Snowdena sehrála jistě podstatnou roli v tom, že když dnes hovoříme o skrytém sledování ze strany orgánů státu, představíme si – spíše než agenty v dodávkách se zatemnělými skly, štěnice v zasedacích místnostech či skryté kamery v hotelových pokojích – počítačové algoritmy hledající v moři dat z každodenní komunikace potenciálně nebezpečná sdělení či osoby. Pro tyto přístupy ke sledování se v odborné literatuře zažily pojmy jako strategické („*strategic surveillance*“),[6] hromadné („*bulk surveillance*“)[7] či nejčastěji masové sledování („*mass surveillance*“).[8] Tyto nástroje jsou dnes příslušným orgánům schopny zajistit množství dat, o kterém by si i autoritativní režimy druhé poloviny 20. století mohly nechat jenom zdát. Pro ilustraci – pokud by např. veškerá data, která za svou existenci od roku 1950 do roku 1989 nashromáždila východoněmecká tajná služba Stasi, byla převedena do fyzické podoby, zaplnila by zhruba 48 tisíc kabinetních skříní o celkové ploše 0,02 čtverečního kilometru. Pokud by mělo být do stejných kabinetních skříní uloženo množství dat odpovídající kapacitě jediného datového centra NSA v Utahu, bylo by jich 42 trilionů a zabíraly by 17 milionů kilometrů čtverečních, tedy zhruba stejnou plochu jako Ruská federace.[9]

Ruku v ruce s kvantitou dostupných údajů jde však i kvalitativní posun v tom, jakým způsobem jsou tyto údaje analyzovány. I ta nejrozsáhlejší a nejvíce intrusivní opatření totiž nutně musí fungovat v režimu „*sbírat hromadně, analyzovat adresně*“.[10] Sesbírané údaje jsou tak nejprve filtrovány za pomoci počítačových algoritmů, které z nepřeberného množství dat vybírají jen jejich miniaturní zlomek pro další analýzu. Namísto obsahu komunikace se pak díky své snadné zpracovatelnosti do popředí zájmu příslušných orgánů dostávají metadata, často označována jako komunikační údaje („*communications data*“) či v evropském kontextu provozní a lokalizační údaje („*traffic and location data*“). Fungování těchto hromadných systémů skrytého sledování však nutně vede ke dvěma zásadním otázkám.

Zaprvé, v jakém z těchto kroků dochází ke sledování komunikace v pravém slova smyslu? Představuje sledování již uložení údajů? Nebo až jejich zpracování prostřednictvím

---

[6] Srov. např. rozhodnutí ESLP ze dne 29. června 2006, *Weber a Saravia proti Německu*, stížnost č. 54934/00, CE:ECHR:2006:0629DEC005493400, bod 4 (dále jen „*rozhodnutí Weber a Saravia proti Německu*“).

[7] Srov. např. MURRAY, Daragh. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, 2019, s. 31.

[8] Srov. např. NI LOIDEAIN, Nora. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, 2015, s. 1.

[9] Srov. BOSCO, Francesca et al. Profiling Technologies Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities. In: GUTWIRTH, Serje et al. *Reforming European Data Protection Law*, 2015, s. 9.

[10] BERNAL, Paul. Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 2016, s. 246.

počítačového algoritmu? Nebo snad dochází ke sledování v pravém slova smyslu až ve chvíli, kdy jsou poprvé spatřeny příslušnými osobami, které mají z jejich analýzy vyvodit důsledky? Dnes ve světle ustálené judikatury ESLP nelze pochybovat o tom, že již uchování údajů představuje určitých zásah do práva na soukromí.[11] Spatřovaná intenzita tohoto zásahu se však může podstatně lišit podle toho, jak odpovíme na výše uvedené otázky.

Zadruhé, jaká je intenzita zásahu do práv na soukromí a ochranu osobních údajů způsobeného zpracováním komunikačních metadat ve srovnání s obsahem komunikace? Jde o menší, stejný, či dokonce větší zásah? Opět, ačkoliv lze jen stěží tvrdit, že zpracování komunikačních metadat nepředstavuje zásah do těchto práv, intenzita tohoto zásahu je stále hojně debatována.

Tyto otázky si nutně musel klást i Soudní dvůr, když se ve věci *Digital Rights Ireland*[12] – mimochodem ve stejné době, kdy Edward Snowden zveřejnil detaily fungování sledovacích režimů v USA – zabýval souladem směrnice 2006/24[13] s čl. 7 a 8 Listiny. Směrnice 2006/24 představovala unijní právní rámec data retention[14], tj. povinného uchovávání komunikačních metadat poskytovateli telekomunikačních služeb za účelem případného pozdějšího adresného přístupu k těmto údajům ze strany orgánů členských států činných v oblasti trestního práva.[15] Tato směrnice byla typickým příkladem opatření založeného na principu „sbírat hromadně, analyzovat adresně“, ovšem s důležitým rozdílem oproti režimům hromadného sledování, kterých se týkala Snowdenova odhalení. Uchované údaje totiž dle pravidel směrnice nebyly hromadně automaticky analyzovány, ale zůstávaly toliko uloženy u samotných poskytovatelů služeb, přičemž příslušným orgánům mohly být zpřístupněny pouze v konkrétních případech.

I tak se z data retention stala značně kontroverzní otázka. To se projevilo mj. tak, že řada ústavních soudů členských států ještě předtím, než o platnosti směrnice 2006/24 rozhodl Soudní

---

[11] Srov. rozsudek ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, stížnosti č. 30562/04 a 30566/04, CE:ECHR:2008:1204JUD003056204 (dále jen „*rozsudek S. a Marper proti Spojenému království*“).
[12] Rozsudek Soudního dvora ze dne 8. dubna 2014, *Digital Rights Ireland a Seitlinger a další*, spojené věci C-293/12 a C-594/12, EU:C:2014:238 (dále jen „*rozsudek Digital Rights Ireland*“).
[13] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.
[14] Drtivá většina literatury zabývající se problematikou skrytého sledování a data retention je v anglickém jazyce. Kde je to možné, snaží se tato práce používat spíše české výrazy a odpovídající anglické pojmy uvádět v závorce a kurzívou při jejich prvním uvedení v textu. Výjimku z tohoto obecného pravidla však tvoří pojem data retention, kdy je v textu po vzoru většiny české odborné literatury a judikatury primárně uváděn anglický pojem, mj. z důvodu, že tento pojem nemá zcela odpovídající český ekvivalent. S ohledem na četnost použití tohoto pojmu a pro účely přehlednosti textu není tento pojem, na rozdíl od ostatních cizojazyčných pojmů, uváděn kurzívou.
[15] Zcela přesně se jedná o povinnost uchovávat provozní, lokalizační a související údaje s cílem zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů, uloženou poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

dvůr, shledala vnitrostátní právní předpisy provádějící tuto směrnici za protiústavní.[16] Soudní dvůr ve svém rozsudku shledal, že zásah do práv na soukromí a ochranu osobních údajů způsobený data retention je třeba považovat za zvlášť závažný, přičemž směrnice 2006/24 nestanovila dostatečné záruky v oblasti uchovávání údajů a přístupu k nim, aby tento zásah bylo možné považovat za souladný s čl. 7 a 8 Listiny. Ačkoliv byl rozsudek Soudního dvora z hlediska svých dopadů významný, nedá se říct, že byl ve světle předchozích závěrů ústavních soudů napříč Evropou zcela nepředvídatelný.

Mnohem překvapivější byl však následující rozsudek *Tele2 Sverige*, ve kterém Soudní dvůr posuzoval slučitelnost britské a švédské vnitrostátní úpravy data retention se směrnicí 2002/58[17] a čl. 7, 8 a 11 Listiny.[18] Soudní dvůr rozhodl, že plošné uchovávání komunikačních metadat je v rozporu s unijním právem *per se*, tedy bez ohledu na to, jaké záruky vnitrostátní právo stanoví v rovině uchovávání a přístupu. Členské státy, jež považovaly data retention nejen za nepostradatelný nástroj k zajištění bezpečnosti v moderním kontextu, ale především za nástroj šetrnější k právům osob než podobně účinné alternativy, byly tímto rozsudkem značně zaskočeny.[19] Není divu – závěry Soudního dvora se totiž rozcházely nejen s názory všech členských států, jež se řízení účastnily, ale také s názorem Komise i generálního advokáta.

Ve světle kategorických závěrů Soudního dvora bylo možné očekávat, že rozsudek *Tele2 Sverige* bude znamenat konec data retention v EU, k čemuž ale v žádném případě nedošlo. Mnoho členských států se i přes tento rozsudek odmítlo plošné data retention vzdát, což vedlo řadu vnitrostátních, především ústavních soudů k pokládání dalších předběžných otázek na toto téma. Některé z těchto věcí již byly v průběhu psaní této práce Soudním dvorem

[16] Pro stručnou a přehlednou analýzu rozhodnutí ústavních soudů členských států v oblasti data retention viz KOSTA, Eleni. The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection. *SCRIPTed-A Journal of Law, Technology and Society*, 2013, s. 339-363. Srov. také VAINIO, Niklas. Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States. *International Journal of Law and Information Technology*, 2015, s. 293-295. Pro podrobnější zpracování této problematiky viz ZUBIK, Marek et al. *European Constitutional Courts towards Data Retention Laws*, 2021.

[17] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

[18] Rozsudek Soudního dvora ze dne 21. prosince 2016, *Tele2 Sverige a Watson a další*, spojené věci C-203/15 a C-698/15, EU:C:2016:970 (dále jen „*rozsudek Tele2 Sverige*“).

[19] Srov. Council of the European union. *Retention of electronic communication data – next steps*, 2017, bod 3.

rozhodnuty,[20] jiná řízení doposud běží.[21] Zajímavostí těchto řízení je, že nejen všechny zapojené členské státy, ale i Komise a většina předkládajících soudů polemizovaly s názorem Soudního dvora ohledně nepřípustnosti plošné data retention a více či méně otevřeně jej vyzývaly k přehodnocení jeho striktního přístupu. Zatímco tedy přístup Soudního dvora k nedostatkům směrnice 2006/24 v zásadě odpovídal tehdejšímu pohledu drtivé většiny odborné veřejnosti a vrcholných soudů členských států, totéž se v žádném případě nedá říct o zákazu plošné data retention jako takovém.

Právě šíře propasti mezi názory Soudního dvora (a, nutno dodat, také nevládních organizací zabývajících se ochranou soukromí a osobních údajů) a ostatních subjektů zapojených do těchto řízení stála na počátku mého zájmu o bližší zkoumání této problematiky. Z jakých důvodů Komise, která většinou jednou vyslovené závěry Soudního dvora přijímá a prosazuje, nejenže v této souvislosti s „neposlušnými" státy nezahajuje řízení pro porušení povinnosti, ale naopak v souvisejících soudních řízeních navrhuje přehodnocení závěrů Soudního dvora? Na základě jakých argumentů Soudní dvůr, jehož primárním účelem nikdy nebyla ochrana základních práv,[22] požaduje v souvislosti s problematikou data retention takovou úroveň ochrany, kterou považují za excesivní i některé vnitrostátní ústavní soudy? Je v tomto ohledu přístup Soudního dvora odlišný od přístupu ESLP, tedy dalšího evropského soudu, který však má na rozdíl od Soudního dvora ochranu základních práv v hlavním popisu práce? Pokud mezi přístupem obou těchto soudů existují významnější rozdíly, jaké jsou důsledky těchto rozdílů pro subjekty údajů a pro členské státy?

Ačkoliv rozsudky Soudního dvora v této oblasti jsou často předmětem akademické diskuse v podobě časopiseckých článků či příspěvků ve sbornících, řada výše uvedených aspektů je v těchto publikacích řešena pouze dílčím způsobem nebo vůbec. Zároveň dle vědomí autora neexistuje česká ani zahraniční publikace, která by se problematikou data retention zabývala skutečně komplexně v celém jejím rozsahu, mj. s ohledem na judikaturu Soudního dvora a ESLP, která navíc v letech 2017-2020 prošla značným vývojem. Tato práce si proto klade za cíl tuto mezeru alespoň částečně zaplnit a odpovědět na co možná nejvíce otázek uvedených výše.

---

[20] Rozsudkek Soudního dvora ze dne 6. října 2020, *Privacy International*, EU:C:2020:790 (dále jen „*rozsudek Privacy International*") a rozsudek Soudního dvora ze dne 6. října 2020, *La Quadrature du Net a další*, spojené věci C-511/18, C-512/18 a C-520/18, EU:C:2020:791 (dále jen rozsudek „*La Quadrature du Net*").

[21] Srov. doposud běžící řízení před Soudním dvorem ve věci C-140/20 *Commissioner of the Garda Síochána a další*, ve věci C-793/19 *SpaceNet* a ve věci C-794/19 *Telekom Deutschland*.

[22] Srov. např. LENAERTS, Koen a GUTIÉREZ-FONS, José A. The constitutional allocation of powers and general principles of EU law. *Common Market Law Review*, 2010, s. 1629.

1 STRUKTURA A CÍLE PRÁCE

Hlavním cílem práce je analytické zpracování právního rámce ochrany soukromí a osobních údajů v EU ve vztahu k problematice data retention, a to nejenom s ohledem na příslušná pravidla primárního a sekundárního práva, ale zejména s ohledem na judikaturu Soudního dvora, která tato pravidla významným způsobem dotváří. V tomto ohledu si práce klade celkem tři dílčí cíle.

Prvním dílčím cílem je posouzení oprávněnosti kritiky, kterou členské státy ve značném počtu a dlouhodobě vznáší vůči judikatuře Soudního dvora v této oblasti. Tato kritika má dvě základní roviny. Ta první se týká působnosti unijních předpisů v této oblasti. Členské státy měly např. v minulosti za to, že je nepřípustné, aby se předpisy přijaté v rámci dřívějšího prvního pilíře vztahovaly také na problematiku přístupu příslušných orgánů k uchovávaným údajům.[23] Za zcela nepřípustné pak považují, aby se tyto předpisy dotýkaly dokonce problematiky zajišťování národní bezpečnosti, která dle čl. 4 odst. 2 SEU spadá do výlučné pravomoci členských států.[24] Druhá rovina kritiky se týká zákazu plošného uchovávání komunikačních metadat. Dle členských států je plošnost uchovávání základním předpokladem účinnosti data retention. Členské státy se domnívají, že zatímco odpovídající úroveň ochrany soukromí a osobních údajů lze zajistit pomocí přísných záruk v oblasti uchovávání údajů a přístupu k nim, bez možnosti plošného uchovávání těchto údajů není v moderním kontextu možné účinně bojovat proti závažným bezpečnostním hrozbám. Tyto členské státy, v tomto ohledu podporované taktéž Komisí, mají tedy za to, že vyloučením možnosti plošného uchovávání Soudní dvůr správně neprovedl vážení proti sobě stojících práv a zájmů, a jeho závěry je tudíž třeba přehodnotit.[25] Jistou váhu těmto argumentům navíc přidává fakt, že řada vnitrostátních soudů dospěla k podobným závěrům.[26]

---

[23] Srov. rozsudek *Tele2 Sverige*, body 65-66.
[24] Srov. rozsudek *Privacy International*, bod 32 či rozsudek *La Quadrature du Net*, body 89-90.
[25] Tyto názory zastávaly ve svých písemných vyjádřeních a případně na ústním jednání ve věcech *Privacy International*, *La Quadrature du Net* a *Ordre des barreaux francophones a germanophone* Česká republika, Belgie, Dánsko, Německo, Estonsko, Irsko, Španělsko, Francie, Kypr, Maďarsko, Nizozemsko, Polsko, Švédsko, Velká Británie a Komise.
[26] Srov. předkládací rozhodnutí v řízení před Soudním dvorem ve věci C-140/20 *Commissioner of the Garda Síochána a další*, body 5-8; ve věci C-793/19 *SpaceNet,* body 17-31; ve věci C-623/17 *Privacy International*, body 3-6 či ve věci C-511/18 *La Quadrature du Net a další*, bod 23. Všechna předkládací rozhodnutí jsou dostupná na http://curia.europa.eu/. Pro další polemiku se závěry Soudního dvora srov. také nález Ústavního soudu ČR ze dne 14. května 2019, Pl. ÚS 45/17, body 76-82. Srov. také např. WAHL, Thomas. CJEU: Data Retention Allowed in Exceptional Cases. *Eucrim*, 2020, s. 154.

Druhým dílčím cílem je srovnání judikatury Soudního dvora a ESLP k problematice data retention a posouzení, zda judikatura ESLP nevede z hlediska nalezení rovnováhy mezi ochranou soukromí a osobních údajů a bezpečnostními zájmy členských států k lepším výsledkům než judikatura Soudního dvora. Provedení takového posouzení je důležité, jelikož jedním z argumentů pro zmírnění striktního přístupu Soudního dvora je právě zajištění souladu s judikaturou ESLP v dané oblasti. V této souvislosti bývá uváděno, že je na data retention třeba nahlížet jako na nástroj k plnění pozitivních povinností vyplývajících z práva na bezpečnost ve smyslu čl. 5 Úmluvy.[27]

V případě, že by se ani přístup Soudního dvora, ani přístup ESLP nejevil jako ideální, je třetím dílčím cílem práce navržení takových požadavků na právní úpravy data retention, které by bylo možné považovat za vyvážené, a to jak z hlediska práv na soukromí a ochranu osobních údajů, tak z hlediska veřejného zájmu na potírání trestné činnosti a zajišťování národní bezpečnosti. Nelze totiž ignorovat, že požadavky Soudního dvora v této oblasti – zřejmě kvůli zásadnímu nesouhlasu s jeho závěry – rozhodně nebyly provedeny do praxe všemi členskými státy. Životnost problematických vnitrostátních právních úprav je pak posílena i tím, že se závěry Soudního dvora nesouhlasí ani Komise, která s dotčenými členskými státy nezahajuje řízení pro porušení povinnosti. Nalezení kompromisního řešení, které by do budoucna mohlo nabýt podoby např. nové společné unijní úpravy, se tak jeví jako nanejvýš žádoucí. Takové řešení by totiž v konečném důsledku mohlo vést k vyšší úrovni ochrany v členských státech, které provádění požadavků Soudního dvora do svých vnitrostátních právních řádů doposud vzdorují.

Práce je členěna do tří hlavních částí. První část se v prvé řadě zabývá historickým vývojem a základními konturami právní úpravy ochrany soukromí a osobních údajů v EU. Ačkoliv je jádrem této práce analýza judikatury Soudního dvora v oblasti data retention, není vhodné k této analýze přikročit, aniž by byly popsány a analyzovány relevantní právní předpisy týkající se ochrany soukromí a osobních údajů. Vzhledem k tomu, že Soudní dvůr přistupuje k data retention jako k „výjimce z pravidla“, měla by tato část práce čtenáři umožnit jasně pochopit ono pravidlo (tj. principy ochrany soukromí a osobních údajů v EU) předtím, než dojde ke zkoumání problematiky data retention jakožto výjimky z něj. První část práce by se dále měla věnovat i ochraně soukromí a osobních údajů s ohledem na jejich charakter základních práv, jelikož právě lidskoprávní argumentace tvoří jádro rozsudků Soudního dvora

[27] Srov. např. rozsudek *La Quadrature du Net*, body 125-126.

v této oblasti. V rámci této části práce budou použity převážně metody deskripce, analýzy a abstrakce.

Předmětem druhé části práce, v rámci které budou použity tytéž metody, je popis a analýza data retention jakožto účinného nástroje v boji proti bezpečnostním hrozbám na straně jedné, avšak i významného zásahu do práv na soukromí a ochranu osobních údajů na straně druhé. V této souvislosti se kapitola zabývá také historickým vývojem data retention v EU a jejím současným právním rámcem.

Předmětem třetí části práce je analýza a komparace judikatury Soudního dvora a ESLP k problematice data retention, a to především s ohledem na výše uvedené tři dílčí cíle práce. Tato část tvoří jádro práce a měl by v ní spočívat její hlavní přínos.

Na tomto místě je vhodné ještě stručně shrnout limity této práce, resp. vysvětlit a zdůvodnit, co obsahem této práce nebude. Tato práce si v prvé řadě neklade za cíl podrobně se věnovat každému z aspektů diskutovaných v její první a druhé části. Věnovat se vyčerpávajícím způsobem všem aspektům unijní úpravy ochrany soukromí a osobních údajů jde jistě nad možnosti této práce, což však nic nemění na tom, že je z výše uvedených důvodů vhodné tuto právní úpravu alespoň nastínit. V případě mnohých těchto aspektů si tak práce klade za cíl předložit především stručnou deskripci základních pravidel a zásad v oblasti ochrany soukromí a osobních údajů, případně doplněnou o hlubší analýzu v oblastech, které mají užší souvislost s jádrem této práce (tak tomu bude např. v případě problematiky působnosti příslušných unijních předpisů). Tato práce si dále neklade za cíl detailně se věnovat ryze technickým aspektům problematiky data retention, zejména co se týče konkrétních technických řešení uchovávání a předávání údajů.[28] V neposlední řadě se práce nezabývá českou vnitrostátní právní úpravou data retention a nesnaží se odpovědět na otázku, zda a do jaké míry je česká právní úprava v souladu s požadavky Soudního dvora.

Tato práce pojednává o stavu právní úpravy a judikatury k 20. dubnu 2021.

[28] Více technické aspekty data retention nicméně v minulosti dobře popsal Jirovský. Srov. JIROVSKÝ, Lukáš. *Data retention – ukládání provozních a lokalizačních údajů*, 2015. Srov. také STAMPFEL, Gerald. et al. *Data Retention: The EU Directive 2006/24/EC from a Technological Perspective*, 2008.

2 OCHRANA SOUKROMÍ A OSOBNÍCH ÚDAJŮ V EVROPSKÉ UNII

Dříve než se budeme zabývat problematikou data retention jakožto zásahu práv na soukromí a ochranu osobních údajů, je zcela nezbytné mít přesnější představu o tom, odkud se tato práva vzala a co znamenají. Z tohoto důvodu se tato kapitola nejprve stručně věnuje historickému vývoji práv na soukromí a ochranu osobních údajů, jakož i vzájemnému vztahu mezi nimi. V kapitole jsou následně popsány a analyzovány základní pravidla a principy ochrany soukromí a osobních údajů v Evropské unii, a to včetně související judikatury Soudního dvora. V neposlední řadě se kapitola zabývá lidskoprávní rovinou ochrany soukromí a osobních údajů, tedy čl. 8 Úmluvy a čl. 7 a 8 Listiny. Tato kapitola si v žádném případě neklade za cíl obsáhnout problematiku ochrany soukromí a osobních údajů v celé její šíři, ale právě toliko v míře nezbytné, s tím, že aspekty důležitější pro pochopení následujících částí práce jsou zkoumány podrobněji. Stejně tak se tato kapitola nezabývá přímo právní úpravou data retention ani související judikaturou, která je předmětem navazujících kapitol.

2.1 HISTORICKÉ KOŘENY OCHRANY SOUKROMÍ A OSOBNÍCH ÚDAJŮ V EVROPSKÉ UNII

2.1.1 Historické kořeny ochrany soukromí

Skutečnost, že soukromí jednotlivce má požívat určité právní ochrany, dnes většině lidí přijde zcela samozřejmá. Právo na soukromí je ostatně obsaženo ve většině mezinárodních katalogů základních práv i moderních ústav. Mezi základními právy často zaujímá poměrně významnou pozici, přičemž v odborné literatuře bývá dokonce označováno jako „*neoddělitelná součást lidskosti*“, „*jádro individuální svobody*“ či „*prvopočátek veškeré svobody*“.[29]

Je tedy vcelku překvapivé, že právo na soukromí představuje relativně mladý koncept, jehož vznik je nejčastěji spojován s esejí *Right to Privacy* amerických právníků Warrena a Brandeise, která vyšla v časopise *Harvard Law Review* v roce 1890. V této eseji, která byla reakcí na nové technologie (kompaktní fotoaparáty) a obchodní praktiky (senzacechtivost tisku) tehdejší doby, demonstrují Warren a Brandeis potřebu uznání práva na soukromí jako nového svébytného práva.[30] Warren a Brandeis totiž po rozboru tehdejších pravidel ochrany majetku, obydlí, duševního vlastnictví a dobrého jména v *common law* dospěli k závěru, že tyto právní instituty již samy o sobě nejsou z různých důvodů dostatečné pro zajištění odpovídající ochrany jednotlivce v nové době. Právo na soukromí následně definují jako „*právo být nechán*

[29] Srov. KASNECI, Dede. *Data Protection Law: Recent Developments*, 2010, s. 1.
[30] WARREN, Samuel D. a BRANDEIS, Luis. Right to Privacy. *Harvard Law Review*, 1890, s. 195.

na pokoji“,[31] jež podle nich vychází z širšího konceptu „*práva na osobnost*“.[32] Má se jednat o právo, kterého se jednotlivec může dovolávat „*vůči světu*“ a které vyplývá z *„obecných pravidel slušnosti a morálky*“.[33]

Ačkoliv je dotčený článek obecně považován za prvopočátek diskuse o právu na soukromí v právní literatuře, a to nejen v americkém kontextu, neznamená to, že by ochrana soukromí v určité podobě byla tehdejšímu právu zcela cizí. Ostatně, sami Warren a Brandeis v daném článku citují řadu tehdejších precedentů, v nichž lze náznaky tohoto institutu vypozorovat. Instituty sledující účel ochrany soukromí jednotlivce navíc již tehdy existovaly přinejmenším ve francouzském právu.[34] I co se týče zvoleného pojmosloví, odkazují Warren a Brandeis na amerického ústavního právníka Cooleyho, který zřejmě použil obrat „právo být nechán na pokoji“ jako první.[35]

To však nic nemění na stěžejním významu tohoto textu. Warrenovi a Brandeisovi se podařilo jednak identifikovat společné rysy v celé řadě zdánlivě různorodých právních problémů a poukázat na to, že všechny tyto právní otázky lze vlastně shrnout pod něco, co lze společně nazvat právě soukromím. Warren a Brandeis zároveň výstižně klasifikovali základní důvody pro možné omezení práva na soukromí. Ačkoliv tedy právo na soukromí v určité podobě existovalo i před Warrenem a Brandeisem, byli to oni, kdo toto právo jasně pojmenoval a popsal. Nutno dodat, že Warren a Brandeis právo na soukromí vymezili způsobem, který je velice podobný tomu, jak právo na soukromí – nebo alespoň jeho významnou část – chápeme dodnes, a to i v evropském prostředí. Není proto divu, že dotčený článek bývá považován dokonce za nejvlivnější právnický článek všech dob.[36]

Ačkoliv se právo na soukromí následně stalo předmětem horlivých akademických debat, do právní praxe tento koncept rozhodně nepronikl okamžitě. V této souvislosti lze poukázat na případ *Olmstead proti Spojeným státům* z roku 1923, ve kterém Nejvyšší soud USA dospěl k závěru, že použití soudem nepovolených odposlechů v soudním řízení není porušením práv vyplývajících ze čtvrtého a pátého dodatku americké ústavy, mj. proto, že nedošlo k prohledání či zabavení komunikace obžalovaných (tj. porušení listovního tajemství) či vstupu do jejich obydlí (tj. porušení domovní svobody). Vzhledem k výše uvedenému není divu, že Luis

[31] Ibidem, s. 193.
[32] Ibidem, s. 207.
[33] Ibidem, s. 213.
[34] Ibidem, s. 214.
[35] ŠIMÍČEK, Vojtěch. *Právo na soukromí*, 2011, s. 12.
[36] NIMMER, Melville B. The Right of Publicity. *Law and Contemporary Problems*, 1954, s. 203.

Brandeis, tehdy již soudce Nejvyššího soudu USA, v dané věci napsal významné disentní stanovisko. V něm Brandeis zdůraznil nutnost nerozlišovat v tomto ohledu mezi jednotlivými způsoby komunikace a poukázal na to, že odposlouchávání telefonních hovorů představuje mnohdy dokonce větší ohrožení soukromí než porušení listovního tajemství. Dotčené rozhodnutí Nejvyššího soudu USA bylo přesto překonáno až rozsudkem *Katz proti Spojeným státům* v roce 1967.[37]

Dalším zásadním okamžikem pro vývoj práva na soukromí byl, podobně jako u ostatních základních práv, konec druhé světové války. Právo na soukromí se dostalo do klíčových mezinárodních a regionálních instrumentů ochrany lidských práv. Všeobecná deklarace lidských práv a základních svobod z roku 1945 ve svém čl. 12 stanoví, že: „*nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům*." Dále můžeme právo na soukromí nalézt i v čl. 17 Mezinárodního paktu o občanských a politických právech[38] a samozřejmě i většině moderních ústav.[39] V evropském kontextu je z hlediska vymezení obsahu práva na soukromí klíčový především čl. 8 Úmluvy, zakotvující právo na respektování soukromého a rodinného života, jakož i související judikatura ESLP, která značně ovlivňuje nejen ústavní soudy členských států, ale také Soudní dvůr.[40] Právu na soukromí ve smyslu čl. 8 Úmluvy a související judikatuře ESLP se proto samostatně věnuje kapitola 2.4.1.

2.1.2 Historické kořeny ochrany osobních údajů

2.1.2.1 OECD a Rada Evropy

Ačkoliv většina současné literatury zabývající se vztahem práva na soukromí a práva na ochranu osobních údajů volá po důslednějším rozlišování obou práv,[41] nelze popřít, že obě

---

[37] SOLOVE, Daniel J. *Understanding Privacy*, 2008, s. 17.

[38] Úřad Vysokého komisaře OSN pro lidská práva pak publikoval několik zpráv týkajících se ochrany soukromí v moderním kontextu. Tyto zprávy jsou mj. značně kritické vůči metodám hromadného sledování komunikace. Srov. např. Office of the High Commissioner for Human Rights. *The right to privacy in the digital age: report*, 2018.

[39] Pro informace o tom, jak jsou práva na soukromí a ochranu osobních údajů zakotvena v ústavách jednotlivých členských států EU, viz RIJPMA, Jorrit J. *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, 2020, s. 109 a násl.

[40] Pokud je tedy v této práci používán zjednodušený pojem „právo na soukromí" či „právo na soukromý život", je tím myšleno právě právo na respektování soukromého života ve smyslu čl. 8 Úmluvy, resp. také čl. 7 Listiny. Srov. kapitola 2.4.

[41] Srov. např. LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015; MÁDR, Petr. *Právo na ochranu osobních údajů dle článku 8 Listiny základních práv Evropské unie*, 2016 či FILIPOVÁ, Paula. *The impact of the CJEU case law on the interpretation of the fundamental rights to privacy and data protection*, 2017.

tato práva mají společné kořeny. Diskuse o ochraně osobních údajů nebyla z počátku ničím jiným než diskusí o ochraně soukromí v éře počítačů, jež započala v Evropě i v USA na počátku sedmdesátých let minulého století. Stejně jako je diskuse o právu na soukromí spojena s nástupem a postupným rozšířením přenosných fotoaparátů a jejich využíváním ze strany tisku, je diskuse o problematice ochrany osobních údajů spojena s nástupem prvních počítačových sítí, zpočátku především ve veřejné správě. Mnozí si totiž právě tehdy začali uvědomovat rizika spojená s vytvářením prvních počítačových databází a jejich propojováním, a to včetně propojování napříč jednotlivými státy. Na vnitrostátní a záhy i na mezinárodní půdě se proto začalo diskutovat o potřebě chránit soukromí osob v souvislosti s automatizovaným zpracováním dat.

Jako první vnitrostátní zákon zabývající se problematikou ochrany osobních údajů je v odborné literatuře označován hesenský zákon o ochraně osobních údajů z roku 1970. V následujících letech byly zákony na ochranu osobních údajů přijímány ve Švýcarsku (1973), SRN (1977), Francii (1978) i dalších státech.[42] Obsah těchto předpisů se následně obtiskl do dokumentů přijatých na mezinárodní úrovni, konkrétně na půdě Rady Evropy a OECD.

Diskuse o ochraně osobních údajů na půdě OECD byla v roce 1980 zakončena přijetím Doporučení k ochraně soukromí a přeshraničním tokům osobních údajů.[43] Tato doporučení si kladla za cíl podpořit harmonizaci předpisů na ochranu osobních údajů v členských státech OECD, aby bylo možné zachovat volný pohyb údajů mezi státy. Byla výsledkem činnosti expertní skupiny a vycházela mj. právě ze společných rysů dosavadních vnitrostátních režimů. Přestože ve svém názvu hovoří dotčená doporučení jednoduše o ochraně soukromí, ve vysvětlujícím memorandu již najdeme, že se týkají „*ochrany soukromí v souvislosti se sběrem a použitím osobních údajů*“. Vysvětlující memorandum dále poukazuje na nutnost rozšířit obsah pojmu soukromí nad rámec typického „práva být nechán na pokoji“ a potřebu stanovit některé další povinnosti správců údajů směrem k veřejnosti, např. co se informací o činnostech zpracování a práv subjektů údajů týče. Doporučení již zároveň pracují s pojmy „osobní údaj“ a „správce údajů“, které v zásadě definují způsobem odpovídajícím jejich

[42] V roce 1980 existovaly zákony upravující problematiku ochrany osobních údajů i v Rakousku, Kanadě, Dánsku, Lucembursku, Norsku a USA. V Belgii, Španělsku, Nizozemí, Švýcarsku a na Islandu byl již v běhu zákonodárný proces vedoucí k přijetí těchto předpisů. Srov. např. LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 47 či GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, s. 55 a násl.

[43] OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Tato doporučení byla následně revidována v roce 2013.

širokému pojetí v dnešním právu EU. Jádro doporučení pak tvoří principy zpracování osobních údajů – mj. principy omezení sběru údajů, transparentnosti, bezpečnosti, odpovědnosti apod. Tyto principy dle vysvětlujícího memoranda odpovídají základním pilířům ochrany osobních údajů v jednotlivých státech a spočívají v limitování důvodů pro sběr osobních údajů, limitování jejich použití pouze ke specifikovaným účelům, vytvoření institutů k zajištění informovanosti subjektů údajů a stanovení odpovědných osob za dodržování těchto principů. Již doporučení OECD tedy obsahovala řadu právních principů a institutů charakteristických pro oblast ochrany osobních údajů a odlišujících ji od ochrany soukromí.[44] Ačkoliv se nejednalo o závazný instrument, obsahovala doporučení i výčet důvodů pro omezení výše uvedených principů (mj. národní bezpečnost a veřejný pořádek), s tím, že těchto výjimek by mělo být využíváno minimálně a pouze v případech, kdy se o tom veřejnost může dozvědět.

Paralelně s vývojem na půdě OECD probíhaly práce na mezinárodním nástroji pro ochranu osobních údajů i v Radě Evropy. Již v letech 1973 a 1974 přijal Výbor ministrů dvě rezoluce k problematice zpracování osobních údajů ve veřejném i soukromém sektoru, které se následně odrazily i ve vnitrostátních zákonech na ochranu osobních údajů přijímaných v dané době.[45] Za klíčový posun je však obecně považováno přijetí Úmluvy 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat v roce 1981 jakožto prvního závazného mezinárodního nástroje na ochranu osobních údajů.[46] Stejně jako v případě Doporučení OECD jsou pravidla obsažená v Úmluvě 108 již dosti podobná dnešním pravidlům na ochranu osobních údajů na půdě EU, včetně širokých definic pojmů jako „osobní údaj“, „automatické zpracování“ či „správce“. Stejně jako v případě Doporučení OECD tvoří jádro Úmluvy základní principy zpracování osobních údajů (kvalita údajů, bezpečnost údajů, práva subjektu údajů apod.). Úmluva 108 dále jasně zdůrazňuje lidskoprávní rovinu problematiky osobních údajů a klade důraz na volný pohyb údajů za podmínky dodržení základních práv, zejména práva na soukromí. Úmluva 108 tedy v zásadě zakazuje bránit pohybu osobních údajů mezi smluvními státy a obsahuje rozličné nástroje mezinárodní spolupráce (povinnost stanovit orgány odpovědné za mezinárodní spolupráci, konzultační výbor apod.), včetně povinnosti asistence subjektům údajů z ostatních smluvních států. Na rozdíl od Doporučení OECD

[44] Blíže k problematice rozdílů mezi právem na ochranu soukromí a právem na ochranu osobních údajů viz kapitola 2.4.3.
[45] Srov. GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, s. 84 a násl.
[46] Srov. také Protokol o změně Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat z roku 2018, který rozšiřuje a modernizuje některá pravidla obsažená v Úmluvě 108.

se Úmluva 108 vztahuje pouze na automatizované zpracování osobních údajů. Ačkoliv Úmluva 108 nebyla zamýšlená jako dokument s přímým účinkem, na jehož dodržování by měl dohlížet ESLP, tento soud její ustanovení a principy z ní vyplývající poměrně často zohledňuje při výkladu čl. 8 Úmluvy.[47]

S ohledem na téma této práce stojí za zmínku i širší působnost Úmluvy 108 ve srovnání s prvními unijními předpisy v této oblasti. Úmluva 108 se na rozdíl od směrnice 95/46[48] či směrnice 2002/58 vždy jasně vztahovala nejen na oblasti spadající do tzv. třetího pilíře unijního práva, tedy na činnost příslušných orgánů státu v oblasti trestního práva, ale také na oblast zajišťování národní bezpečnosti, tj. např. činnost zpravodajských služeb.[49] Úmluva 108 však samozřejmě umožňovala odchylky od svých pravidel za účelem zajištění bezpečnosti státu, veřejné bezpečnosti či potírání trestné činnosti, za podmínky, že takové odchylky budou stanoveny zákonem a nezbytné v demokratické společnosti.

V roce 1987 pak Výbor ministrů Rady Evropy přijal Doporučení R (87) 15, které se týkalo zpracování osobních údajů v rámci činnosti policie.[50] Cílem tohoto doporučení bylo v zásadě stanovit přípustné limity odchylek od pravidel Úmluvy 108 a čl. 8 Úmluvy při zpracování osobních údajů zejména policejními orgány. Přestože se jednalo o poměrně obecná doporučení ve formě *soft-law*, nebylo by správné význam těchto doporučení podceňovat, mj. proto, že obsahovala řadu principů, které byly převzaty do současné unijní úpravy této problematiky, tj. směrnice 2016/680[51]. Z jednotlivých doporučení lze v této souvislosti zmínit zejména to, aby i zpracování v této oblasti podléhala dohledu nezávislého dozorového úřadu, se kterým by mělo být konzultováno mj. nasazování nových technologií v oblasti automatického zpracování údajů.[52] Za hlavní nosný princip doporučení by bylo možné označit účelové omezení sběru údajů příslušnými orgány, a to mj. v tom smyslu, že by nemělo docházet

---

[47] HUSTINX, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,* 2013, s. 7.

[48] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[49] Srov. BLAS, Diana A. First Pillar and Third Pillar: Need for a Common Approach on Data Protection? In: GUTWIRTH, Serge et al. *Reinventing Data Protection?* 2009, s. 226. Jak však bude demonstrováno níže v kapitole 4.1.2, extenzivní výklad působnosti unijních pravidel na ochranu osobních údajů ze strany Soudního dvora v praxi nevylučuje, že se unijní pravidla významně dotknou i této oblasti.

[50] Council of Europe. *Council of Europe Committee of Ministers Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector*, 1987.

[51] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[52] Ibidem, body 1.1-1.3.

ke sběru údajů za jiným účelem než za účelem odvrácení reálného rizika či potírání konkrétní trestné činnosti. Jinými slovy, že by nemělo docházet k plošnému sběru údajů.[53] Tento přístup tedy koresponduje se základní myšlenkou judikatury Soudního dvora v oblasti data retention. Samo doporučení však uvádělo, že je možné se od tohoto principu odchýlit v případech stanovených zákonem. Dále bylo doporučeno omezit zpracování citlivých údajů pouze na to, co je absolutně nezbytné v konkrétních případech,[54] stanovení požadavků na zabezpečení údajů[55] a maximální dobu uložení údajů,[56] rozlišování mezi údaji na základě jejich spolehlivosti[57] apod. V neposlední řadě bylo doporučeno zakotvit práva subjektu údajů na přístup a opravu údajů, samozřejmě v rozsahu, aby nedošlo k ohrožení účelu zpracování.[58] Ačkoliv se doporučení netýkalo problematiky zajišťování národní bezpečnosti, nevylučovalo, že některé principy je možné na danou oblast převést.[59]

Z výše uvedeného tedy vyplývá, že ačkoliv původní diskuse o ochraně osobních údajů vycházela z konceptu soukromí jako „práva být nechán na pokoji" v éře počítačů, již z prvních dokumentů v této oblasti je zřejmý důraz na určité specifické zásady (zejména zásadu účelového omezení) a záruky (zejména dozor ze strany nezávislých orgánů), resp. možnosti subjektu údajů proaktivně kontrolovat a ovlivňovat zpracování svých osobních údajů (práva na přístup a opravu údajů). Zároveň je již z původních dokumentů zjevná potřeba přizpůsobit v určitých případech obecná pravidla specifickým požadavkům činnosti příslušných orgánů v oblasti trestního práva, za podmínky, že je takové omezení stanoveno zákonem a nezbytné v demokratické společnosti. S nejvolnějším režimem bylo od počátku počítáno pro oblast zajišťování národní bezpečnosti.

2.1.2.2 Evropská společenství

Vývoj právní úpravy ochrany osobních údajů na půdě Evropských společenství byl z počátku mnohem pomalejší. Ačkoliv je to dnes právě EU, kdo hraje v oblasti ochrany osobních údajů z globálního hlediska prim, v sedmdesátých a osmdesátých letech byl vývoj na půdě Společenství zastíněn právě vývojem na půdě Rady Evropy a OECD. První důležitější

---

[53] Srov. ibidem, bod 2.1 a Council of Europe. *Explanatory Memorandum to Council of Europe Committee of Ministers Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector*, 1987, bod 43.
[54] Council of Europe. *Council of Europe Committee of Ministers Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector*, 1987, bod 2.4.
[55] Ibidem, bod 8.
[56] Ibidem, bod 7.
[57] Ibidem, bod 3.2.
[58] Ibidem, bod 6.
[59] Ibidem, část „*Oblast působnosti a definice*".

dokument Komise v této oblasti nazvaný *Community Policy on Data Processing* byl vydán v roce 1973, avšak dominovaly v něm především soutěžní aspekty dané problematiky, což bylo reakcí na vstup velkých amerických IT společností (zejména IBM) na v tomto ohledu nerozvinutý evropský trh.[60] V dokumentu je nicméně stručně zmíněna i potřeba ochrany soukromí jednotlivce v souvislosti se zpracováním dat, a to v podobě doporučení započít se širší veřejnou debatou ohledně možné komunitární legislativy.[61] González Fuster si v této souvislosti všímá, že ve všech jazykových verzích tohoto sdělení, s výjimkou verze anglické, se již objevuje zmínka o ústavněprávním rozměru této problematiky.[62]

V dané oblasti začal být následně aktivnější spíše Evropský parlament, který v průběhu sedmdesátých let vyzval Komisi k předložení legislativy pro ochranu jednotlivců v souvislosti se zpracováním dat celkem třikrát, aniž bylo jeho volání vyslyšeno. Tuto zdráhavost Komise k větší aktivitě v oblasti ochrany osobních údajů Lynskey připisuje skutečnosti, že skutečná rizika pro jednotlivce byla v dané době spojena především s databankami veřejného sektoru, k jehož regulaci se Komise necítila oprávněna.[63] Ve zmíněných dokumentech Evropského parlamentu z let 1975[64], 1976[65] a 1979[66] jsou již zřetelné kontury budoucí unijní legislativy, včetně vzájemné souvislosti mezi potřebou chránit jednotlivce na straně jedné, a zajistit volný pohyb údajů na straně druhé. Krátce po těchto výzvách nicméně došlo k finalizaci prací na půdě OECD i Rady Evropy, čehož Komise využila a namísto započetí s přípravou vlastní legislativy vyzvala členské státy k rychlému přistoupení k Úmluvě 108, k pokračující nespokojenosti Evropského parlamentu.[67]

Do platného práva Společenství pronikla problematika ochrany osobních údajů, možná poněkud překvapivě, nejprve v rámci Úmluvy k provedení Schengenské dohody, konkrétně v souvislosti se zřízením schengenského informačního systému a potřebou chránit data v něm obsažená. Pravidla zaváděná za tímto účelem byla zjevně inspirována Úmluvou 108. Úmluva k provedení Schengenské dohody v této souvislosti pracuje již s pojmem osobních údajů

---

[60] Srov. Commission of the European Communities. *Community Policy on Data Processing*, 1973, s. 3.
[61] Ibidem, bod 20.
[62] GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, s. 112.
[63] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 16.
[64] European Parliament. *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1975.
[65] European Parliament. *Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing*, 1976.
[66] European Parliament, *Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing*, 1979.
[67] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 48.

a obsahuje pravidla pro účelové omezení nakládání s osobními údaji, pro opravu a výmaz chybných osobních údajů, jakož i právo na přístup k osobním údajům v mezích použitelných vnitrostátních předpisů. Novinkou předznamenávající budoucí vývoj je požadavek na nezávislou kontrolu ze strany příslušných vnitrostátních orgánů.

Na přelomu osmdesátých a devadesátých let začala i Komise vnímat problémy způsobené absencí obecné komunitární úpravy ochrany osobních údajů. Zaprvé, Doporučení OECD a Úmluva 108 neměly kýžené harmonizační dopady, což bylo dáno jejich zřejmými limity – v případě Doporučení OECD jejich nezávazností, v případě Úmluvy 108 její obtížnou vynutitelností a širokým prostorem pro diskreci členských států. Mezi pravidly členských států tak nadále existovaly značné rozdíly.[68] V některých členských státech dotčená problematika dokonce nebyla upravena, jelikož i přes výzvy Komise Úmluvu 108 v dané době ratifikovalo pouze sedm členských států.[69] Tyto nedostatky se v praxi začaly projevovat např. tím, že vnitrostátní orgány na ochranu osobních údajů znemožňovaly přesun osobních údajů v rámci skupiny společností z důvodů údajně nedostatečné úrovně ochrany v jiném členském státě.[70] Zadruhé, rapidní rozvoj technologií v průběhu osmdesátých let ukázal na obrovský potenciál volného pohybu údajů pro tehdejší ekonomiku Společenství, stejně jako čím dál větší rizika pro jednotlivce.[71]

V návaznosti na tyto nedostatky započala v závěru osmdesátých let Komise legislativní práci, na jejímž konci byl návrh směrnice o ochraně osob v souvislosti se zpracováním osobních údajů.[72] Daný návrh byl zákonodárci předkládán celkem dvakrát, mj. z důvodu následného přijetí Maastrichtské smlouvy, jež mělo značné dopady na legislativní proces v rámci EU. Druhá, značně přepracovaná verze směrnice již obsahovala změny v návaznosti na přechozí připomínky některých členských států a Evropského parlamentu. Osud směrnice v Radě byl nicméně i nadále po určitou dobu nejistý zejména kvůli nesouhlasnému postoji Irska, Spojeného království a Německa. Naopak státy jižní Evropy a státy Beneluxu byly směrnici nakloněny. Nakonec bylo v návaznosti na několik změkčení směrnice (např. v oblasti

---

[68] HUSTINX, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,* 2013, s. 9.
[69] European Commission. *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, 1990, body 2 a 3.
[70] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 49.
[71] European Commission. *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, 1990, bod 1.
[72] Součástí legislativního balíčku byl také návrh směrnice 97/66 a návrh na udělení mandátu k vyjednání možnosti Společenství přistoupit k Úmluvě 108.

zdravotnického výzkumu) dosaženo shody a směrnice byla přijata spolurozhodovací procedurou v říjnu 1995. V Radě byla směrnice schválena jednohlasně, ačkoliv Spojené království se hlasování zdrželo.[73]

Lze tedy shrnout, že počátky ochrany osobních údajů v rámci Společenství byly charakterizovány na jedné straně úsilím Evropského parlamentu, který dotčenou problematikou od počátku vnímal optikou potřebou ochrany základních práv jednotlivců, o přijetí společné komunitární legislativy, a na druhé straně zdráhavostí Komise přistoupit k takovému kroku vzhledem k tehdejším pravomocem Společenství. Prostor pro přijetí komunitární legislativy se následně otevřel až spolu s technologickým rozvojem, mj. kvůli tomu, že v určitých případech začala absence této legislativy skutečně bránit volnému pohybu údajů napříč členskými státy. Specifickou potřebu zavedení pravidel na ochranu osobních údajů do práva Společenství pak vyvolala potřeba výměny informací v rámci budování schengenského prostoru, přičemž pravidla přijatá za tímto účelem odrážela ty nejzákladnější principy ochrany osobních údajů, mj. účelové omezení, nezávislý dohled a práva subjektu údajů na přístup k údajům a výmaz údajů.

2.2 Ochrana osobních údajů v sekundárním právu EU

2.2.1 Směrnice 95/46

Směrnice 95/46 byla značně inspirována Úmluvou 108, což potvrzuje i bod 11 jejího odůvodnění, jež v souvislosti s Úmluvou 108 uvádí, že „*zásady ochrany lidských práv a svobod, zejména práva na soukromí, obsažené v této směrnici upřesňují a rozšiřují zásady obsažené v Úmluvě*“. Dále se v textu odrážely určité prvky tehdejší německé a v menší míře i francouzské vnitrostátní právní úpravy.[74]

Stejně jako Úmluva 108, i směrnice 95/46 sledovala dva hlavní cíle – zajištění vysoké úrovně ochrany základních práv jednotlivců (zejména jejich práva na soukromí) na straně jedné, a zajištění volného pohybu osobních údajů na straně druhé.[75] Oba cíle směrnice 95/46 se jasně odráží v jejím čl. 1, kdy první odstavec ukládá členským státům zajistit vysokou úroveň ochrany

---

[73] NUTILOVÁ, Helena. *Ochrana osobních údajů*, 2012, s. 61.
[74] GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, s. 126.
[75] Původní návrh Komise hovořil v souvislosti s cílem směrnice výhradně o právu na soukromí, ovšem na základě požadavku Hospodářského a sociálního výboru byla tato formulace zobecněna. Tento požadavek se později ukázal jako oprávněný, nejen vzhledem ke vzniku nového svébytného práva na ochranu osobních údajů, ale mj. s ohledem na provázanost pravidel směrnice a některých dalších základních práv a svobod – mj. práva na účinnou soudní ochranu či svobodu slova, jak ostatně bude vidět taktéž na judikatuře Soudního dvora týkající se data retention. O právu na ochranu osobních údajů jakožto svébytném základním právu však v daném období ještě nemohla být řeč.

základních práv fyzických osob v souvislosti se zpracováním osobních údajů, přičemž druhý odstavec členským státům následně zakazuje bránit volnému pohybu osobních údajů na vnitřním trhu z důvodu ochrany těchto práv. Bod 8 odůvodnění směrnice následně vyjasňoval vztah mezi oběma těmito cíli, když uváděl, že „*pro odstranění překážek toku osobních údajů musí být úroveň ochrany práv a svobod osob v souvislosti se zpracováním těchto údajů rovnocenná ve všech členských státech*". Takové vysvětlení, dle kterého nebyla ochrana základních práv ani tak cílem *sama o sobě*, jakož spíše prostředkem k dosažení skutečného cíle směrnice – volného pohybu osobních údajů na vnitřním trhu – pak plně korespondovalo s právním základem směrnice, kterým byl „tržně-harmonizační" ex čl. 100a SES. Tento přístup také korespondoval s tím, jak vztah mezi oběma cíli definovala Komise ve svém sdělení doprovázejícím první návrh směrnice[76] i v důvodové zprávě.[77] Odpovídaly jí taktéž výjimky z věcné působnosti směrnice. Ta se dle svého čl. 3 neměla vztahovat mj. na zpracování prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností či na zpracování prováděné pro výkon činností nespadajících do působnosti práva Společenství.

Takový přístup k lidskoprávní rovině směrnice 95/46 byl nicméně některými kritizován. Např. Gutwirth v této souvislosti v roce 2002 uvedl, že v případě směrnice 95/46 byly obavy týkající soukromí „*zcela podřízeny tržním prioritám*".[78] Dle Gutwirtha se Komise odklonila od toho, co od ní v sedmdesátých letech požadoval Evropský parlament, jehož volání po legislativě sledovalo primárně lidskoprávní cíle.[79] Vzhledem k právnímu základu směrnice 95/46 a absenci jakéhokoliv ustanovení primárního práva, jež by tehdejšímu Společenství umožňovalo regulovat problematiku ochrany základních práv samostatně, s Gutwirthovou kritikou nesouhlasím. Každopádně již první rozsudky Soudního dvora v této oblasti vnímanou „druhořadost" cíle ochrany základních práv a jeho závislost na cíli volného pohybu údajů značně relativizovaly, ne-li zcela popřely.[80] Jelikož tato problematika dodnes úzce souvisí

---

[76] European Commission. *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, 1990, bod 15.
[77] European Commission. *Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data – Explanatory memorandum*, 1990, s. 12.
[78] Srov. BIRNHACK, Michael D. The EU Data Protection Directive: An Engine of a Global Regime. *Computer Law & Security Report*, 2008, s. 6.
[79] Srov. ibidem.
[80] Srov. rozsudek Soudního dvora ze dne 23. května 2003 ve spojených věcech *Österreichischer Rundfunk a další*, C-465/00, C-138/01 a C-139/01, EU:C:2003:294 (dále jen „*rozsudek Österreichischer Rundfunk*") a rozsudek Soudního dvora ze dne 6. listopadu 2003 ve věci *Lindqvist*, C-101/01, EU:C:2003:596 (dále jen „*rozsudek Lindqvist*").

s otázkou působnosti unijních předpisů v oblasti ochrany osobních údajů, bude o ní podrobněji pojednáno níže.[81]

Co se týče struktury a vlastního obsahu směrnice, její jádro tvořily v prvé řadě definice základních pojmů jako osobní údaj, správce, zpracování, souhlas apod. Obsah těchto definic byl taktéž inspirovaný Úmluvou 108. Dále směrnice upravovala základní zásady zpracování údajů (zákonnost, korektnost, přiměřenost, přesnost, účelové omezení, bezpečnost údajů apod.) a taxativní výčet titulů pro zpracování (souhlas, zákonná povinnost, plnění smlouvy apod.). Dále směrnice obsahovala práva subjektů údajů (právo na přístup k údajům, na informace o zpracování, na výmaz apod.) a možné důvody pro omezení těchto práv (mj. veřejná či národní bezpečnost), a to včetně zvláštních omezení v některých specifických oblastech (žurnalistika, vědecký výzkum apod.). Na rozdíl od původního návrhu Komise a od právního režimu v USA se směrnice vztahovala společně na zpracování osobních údajů v soukromém i veřejném sektoru. Novinkou směrnice oproti Úmluvě 108 byla úprava podmínek pro předávání osobních údajů do třetích zemí a požadavek na zřízení nezávislých dozorových úřadů, byť je třeba uvést, že takový požadavek se, jak bylo uvedeno výše, objevil i dříve, např. v Doporučení R (87) 15.

Co se týče úrovně harmonizace zaváděné směrnicí 95/46, dle Soudního dvora směrnice zavádí harmonizaci, „*která je v zásadě úplná*“.[82] To znamená, že ačkoliv členské státy např. nemohly ukládat správcům povinnosti nad rámec směrnice 95/46,[83] sama směrnice obsahovala i řadu velmi obecných a pružných pravidel, u kterých členské státy zjevně disponovaly prostorem pro uvážení při jejich provádění do vnitrostátního práva.

Směrnice 95/46 dnes bývá považována z hlediska zvýšení úrovně ochrany nejen v EU, ale i ve světě, za výjimečně úspěšný nástroj. To se může jevit jako poměrně zvláštní vzhledem k tomu, v jaké míře pouze přebírala instituty obsažené v dříve přijatých instrumentech na mezinárodní úrovni. Musíme si však uvědomit, že na rozdíl od Doporučení OECD byla směrnice 95/46 právně závazná. Na rozdíl od Úmluvy 108 na její řádnou transpozici do vnitrostátního práva dohlížela Komise a za určitých podmínek byla směrnice dokonce přímo použitelná. Důležitou roli v tomto ohledu jistě hrály i nezávislé dozorové úřady a samozřejmě i Soudní dvůr, jehož judikatura od samého počátku hovořila jednoznačně ve prospěch vysoké úrovně ochrany osobních údajů. Zároveň díky široce pojaté místní působnosti směrnice, jakož

[81] Viz kapitola 2.2.2.3.
[82] Srov. rozsudek Soudního dvora ze dne 29. července 2019, *Fashion ID*, C-40/17, EU:C:2019:629, bod 54 (dále jen „*rozsudek Fashion ID*“).
[83] Srov. rozsudek Soudního dvora ze dne 19. října 2016, *Breyer*, C-582/14, EU:C:2016:779, bod 62 (dále jen „*rozsudek Breyer*“).

i požadavkům na předávání údajů do třetích zemí, se její dopad neomezil jen na území EU. Někteří autoři proto o směrnici 95/46 hovoří jako o „*nástroji regulatorní nadvlády*“[84] či „*nástroji právní globalizace*“.[85]

Nicméně v souvislosti s rapidním rozvojem informačních technologií začal i směrnici 95/46 pomalu docházet dech, a začaly tak zaznívat hlasy o potřebě její revize. K té došlo v roce 2016 přijetím GDPR[86], které převzalo drtivou většinu institutů ze směrnice 95/46. Ne nadarmo se proto z konstatování, že GDPR představuje „*evoluci, nikoliv revoluci v ochraně osobních údajů*“ stalo klišé konferencí a seminářů na dané téma. Z těchto důvodů budou základní instituty připomenuté výše blíže popsány až v následující kapitole týkající se GDPR, s tím, že přitom bude zohledněna i judikatura Soudního dvora ke směrnici 95/46, jejíž závěry jsou téměř bez výhrad platné i pro GDPR.

2.2.2 GDPR

Obecné nařízení o ochraně osobních údajů, známé i v českém prostředí spíše pod zkratkou GDPR, dnes představuje obecný unijní předpis v oblasti ochrany osobních údajů. Jedná se o poměrně rozsáhlý předpis obsahující širokou škálu právních institutů, zásad a pravidel, jejichž podrobná analýza by se zřejmě nevešla do disertační práce věnující se pouze GDPR, natož do disertační práce jako je tato, jejíž těžiště leží jinde. Na druhou stranu – třetí i čtvrtá kapitola pracují s řadou pojmů a konceptů, které jsou v současnosti vymezeny právě v GDPR. Z důvodu zachování ucelenosti výkladu jsou tedy základní pojmy a koncepty GDPR níže popsány alespoň stručně, s podrobnější analýzou tam, kde se to jeví účelné z pohledu následujících částí práce.

2.2.2.1 Okolnosti přijetí

Jak bylo uvedeno, směrnice 95/46 byla v dosahování vytyčených cílů nadmíru úspěšná. Technická neutralita pravidel obsažených ve směrnici spolu s velmi progresivní judikaturou Soudního dvora zapříčinila, že tato pravidla byla z velké části nadále aktuální a funkční i více než 20 let po jejich přijetí.[87] A nebylo to přitom ledajakých 20 let. Musíme si uvědomit, že v době, kdy byla směrnice přijata, používalo internet jen zhruba 1 % evropské populace.[88] Zákonodárce mohl jen stěží předjímat způsoby zpracování osobních údajů, které se dostavily

[84] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 41.
[85] KASNECI, Dede. *Data Protection Law: Recent Developments*, 2010, s. 97.
[86] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[87] Srov. ROBINSON, Neil et al. *Review of EU Data Protection Directive: Summary*, 2009, s. 2.
[88] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 4.

jako důsledek rozvoje internetu. Ačkoliv tedy směrnice 95/46 riziku ztráty relevantnosti v souvislosti nástupem nových technologií odolávala poměrně zdatně, po roce 2000 se čím dál tím častěji objevovaly hlasy volající po její revizi. V roce 2009 proto Komise spustila rozsáhlé konzultace se všemi zúčastněnými stranami (mj. zástupci dozorových úřadů, členských států a byznysu) o možné revizi unijního právního rámce ochrany osobních údajů.

Důvodů pro tuto revizi bylo několik. Tím prvním a nejčastěji zmiňovaným byl již uvedený technologický rozvoj – v průběhu let se extrémně změnilo jak množství zpracovávaných osobních údajů, tak možné způsoby jejich zpracování, což bylo logicky spojeno s vyšším rizikem pro jednotlivce. Bylo třeba reagovat na fenomény jako např. *cloud computing*, *big data*, či *internet of things*, a to nejen obecným posílením práv subjektu údajů, ale také zavedením některých specifických pravidel.[89] Bylo také třeba zohlednit stále globálnější povahu trhu s osobními údaji. Dalším cílem připravované revize byla větší harmonizace – ačkoliv směrnice 95/46 představovala „v zásadě úplnou harmonizaci", zejména podnikatelské subjekty si často stěžovaly na nejednotné uplatňování jejích pravidel napříč členskými státy.[90] Směrnice proto měla být nahrazena nařízením, jehož harmonizační účinky měly být intenzivnější. V neposlední řadě bylo třeba zohlednit právní vývoj v této oblasti, představovaný nejen progresivní judikaturou Soudního dvora, ale také změnami primárního práva. Lisabonská smlouva prostřednictvím nového článku 16 odst. 2 SFEU umožnila, aby se problematika ochrany osobních údajů konečně i formálně oddělila od „tržně-harmonizačního" právního základu. Jako žádoucí se proto jevilo co možná nejvíce sblížit pravidla pro ochranu osobních údajů ve všech oblastech pokrytých unijním právem. Určitým impulsem ke změnám mělo být i zakotvení samostatného práva na ochranu osobních údajů v Listině.[91]

Následná legislativní práce postupně vyústila hned v přijetí několika předpisů. Krom GDPR se jednalo i o směrnici 2016/680, jež stanovila pravidla pro ochranu osobních údajů při jejich zpracování orgány členských států za účelem boje proti trestné činnosti a nahradila rámcové rozhodnutí 2008/977/SVV[92], jež tuto problematiku předtím upravovalo v rámci

[89] Pro stručné shrnutí výzev, které s sebou tyto nové fenomény přinášejí, srov. např. European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law 2018 edition*, 2018, s. 347-371.
[90] Evropská komise. *Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) – důvodová zpráva*, 2012, s. 4.
[91] Srov. HUSTINX, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation,* 2013, s. 26-27.
[92] Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech.

tehdejšího třetího pilíře. S bojem proti trestné činnosti dále souvisela i směrnice 2016/681[93], jež upravovala problematiku předávání údajů cestujících v letecké dopravě (tzv. údaje PNR). Dále bylo přijato nařízení, které aktualizovalo pravidla zpracování osobních údajů unijními orgány tak, aby odpovídala pravidlům GDPR.[94] Obdobným způsobem byla aktualizována i pravidla pro ochranu osobních údajů při jejich zpracování Europolem[95] a unijním veřejným žalobcem.[96] V rámci této revize mělo dojít i k přijetí nařízení upravujícího problematiku ochrany soukromí v elektronických komunikacích, avšak toto nařízení doposud přijato nebylo.

2.2.2.2 Cíle, právní základ a struktura

Stejně jako směrnice 95/46, i GDPR sleduje dva cíle – chránit základní práva jednotlivců a zajistit volný pohyb osobních údajů. Zatímco však směrnice 95/46 hovořila v této souvislosti zejména o právu na soukromí, GDPR již naplno pracuje s právem na ochranu osobních údajů jakožto hlavním základním právem, které má být skrze GDPR chráněno. Explicitně jsou však zmiňována i další práva, k jejichž ochraně mohou pravidla GDPR sloužit – v této souvislosti jsou v bodě 4 odůvodnění zmiňována práva na ochranu soukromého a rodinného života, obydlí a komunikace, svoboda myšlení, svědomí a náboženského vyznání, svoboda projevu a informací, svoboda podnikání či právo na účinnou právní ochranu a spravedlivý proces.

V případě směrnice 95/46 bylo zpočátku poměrně sporné, do jaké míry je cíl ochrany základních práv svázán s problematikou volného pohybu osobních údajů. Tato otázka přitom nebyla pouze akademická a mohla mít dopad na výklad nejen celé řady pojmů obsažených ve směrnici 95/46, ale i na vymezení její věcné působnosti. V případě GDPR už se těmito otázkami není třeba zabývat. GDPR již nebylo přijato výhradně na „tržně-harmonizačním“ právním základě, ale na základě nového čl. 16 odst. 2 SFEU, který k přijetí pravidel pro ochranu osobních údajů zmocňoval výslovně a přímo. Zároveň dle judikatury Soudního dvora ani ochrana osobních údajů stanovená směrnicí 95/46 nebyla tímto způsobem omezena na případy, u nichž existuje spojitost s volným pohybem údajů. Právě naopak – ochrana osobních údajů

[93] Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

[94] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES.

[95] Nařízení Evropského parlamentu a Rady (EU) 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV.

[96] Nařízení Rady (EU) 2017/1939 ze dne 12. října 2017, kterým se provádí posílená spolupráce za účelem zřízení Úřadu evropského veřejného žalobce.

byla považována nejen za samostatný, ale základní cíl směrnice 95/46.[97] I GDPR tak musí být vykládáno zejména s ohledem na tento základní cíl, což dle Soudního dvora mj. znamená, že výjimky z ochrany osobních údajů mohou být činěny pouze v naprosto nezbytném rozsahu.[98]

Co se týče struktury GDPR, ta ve značné míře kopíruje strukturu směrnice 95/46 připomenutou výše. Po vymezení cílů, působnosti a základních pojmů následují základní zásady zpracování, právní tituly pro zpracování, práva subjektu údajů a povinnosti správců a zpracovatelů. Následně je řešena problematika předávání osobních údajů, činnost dozorových úřadů, některé specifické oblasti zpracování a v neposlední řadě otázky odpovědnosti za porušení GDPR.

Ačkoliv volba právní formy nařízení byla zdůvodňována potřebou zajištění větší úrovně harmonizace, než jaké bylo dosaženo v případě směrnice 95/46, GDPR se v mnoha ohledech jako nařízení spíše jen tváří, resp. je typickým příkladem stírání rozdílů mezi obsahem nařízení a směrnic, na který upozorňuje např. Whelanová.[99] Celá řada ustanovení nejenže umožňuje, ale v mnohých případech dokonce vyžaduje doplnění či konkretizaci prostřednictvím vnitrostátního práva.[100] Navíc v řadě případů, kde nařízení formálně stanoví možnost konkretizace, je taková konkretizace v praxi nezbytná. Ve vnitrostátním právu je tak např. možné stanovit jak povinnost, tak oprávnění ke zpracování osobních údajů (čl. 6 odst. 1 písm. c) a e) a čl. 6 odst. 2 GDPR), což v praxi bude třeba učinit v nespočtu případů. Ve vnitrostátním právu je dále např. možné blíže vymezit subjekty, které mají povinnost jmenovat pověřence pro ochranu osobních údajů (čl. 37 odst. 4 GDPR), stanovit minimální věk dítěte potřebný k udělení souhlasu (čl. 8 odst. 1 GDPR) apod. Velký prostor pro legislativní činnost členských států poskytují zejména čl. 85 až 91 GDPR, které vyžadují sladění pravidel GDPR a dalších významných práv a veřejných zájmů, jako je např. svoboda projevu, právo na informace, svoboda vyznání, svoboda vědeckého bádání apod. V některých případech jde o povinnost takové sladění provést (čl. 85 GDPR), v jiných případech o možnost (čl. 88 GDPR).

GDPR dále svěřuje členským státům řadu možností stanovit odchylky od jeho pravidel, a to i od těch zcela zásadních. V tomto ohledu je klíčový čl. 23 GDPR, jež umožňuje členským

---

[97] Srov. rozsudek Soudního dvora ze dne 14. února 2019, *Buivids*, C-345/17, EU:C:2019:122, bod 41.
[98] Srov. rozsudek Soudního dvora ze dne 11. prosince 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, bod 46.
[99] Srov. WHELANOVÁ, Markéta. Implementace přímo použitelných nařízení Evropské unie do českého právního řádu. *Správní právo*, 2019, s. 66.
[100] Co se týče obecně metod adaptace vnitrostátních právních řádů na unijní nařízení viz např. KRÁL, Richard. *Nařízení ES z pohledu jejich vnitrostátní aplikace a implementace*, 2006.

státům omezit práva a povinnosti vyplývající z GDPR, respektují podstatu základních práv a svobod a představují nezbytná a přiměřená opatření v demokratické společnosti. Hospodářské subjekty působící ve více členských státech tak proto nadále musí dbát i na vnitrostátní adaptační zákony. Na druhou stranu je třeba zmínit, že ke zmírnění zátěže spojené s působením ve více členských státech může poměrně značně přispět jak princip *one-stop shop* v oblasti dohledu, tak skutečnost, že základní pojmy jsou nyní vymezeny přímo v nařízení bez možnosti konkretizace či doplnění na vnitrostátní úrovni.

2.2.2.3 Působnost

Co se týče věcné působnosti GDPR, to se dle svého čl. 2 odst. 1 – stejně jako před ním směrnice 95/46 – vztahuje na „*zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny*." Pojem zcela či částečně automatizovaného zpracování osobních údajů nevyvolává větší interpretační problémy – bude se jednat o jakékoliv zpracování, v rámci kterého je alespoň část relevantních úkonů prováděna prostřednictvím počítače.[101] Pojem evidence je nově definován v čl. 4 odst. 6 GDPR jako „*jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska*". Obsahově odpovídá pojmu „rejstřík" ve směrnici 95/46. Zpravidla tedy půjde o různé kartotéky, archivy a adresáře, ve kterých jsou údaje uspořádány dle kritérií umožňujících jejich snadnější dohledání v budoucnu. Zatímco směrnice 95/46 v bodě 27 svého odůvodnění počítala s tím, že určující prvky rejstříku budou vymezeny členskými státy, GDPR jim již tento prostor nepřiznává.

K obsahu pojmu rejstřík se vcelku nedávno vyjádřil i Soudní dvůr ve věci *Jehovan Todistajat.*[102] Jednou z otázek překládajícího soudu v dané věci bylo, zda rejstřík ve smyslu směrnice 95/46 představuje i poznámkový blok obsahující jména a adresy osob navštívených členy náboženské skupiny při jejich zvěstovatelské činnosti. Obdobně jako v případě jiných pojmů v oblasti ochrany osobních údajů, i v tomto případě dospěl Soudní dvůr k potřebě širokého výkladu. Dle Soudního dvora není nezbytné, aby údaje byly zařazeny do specifické kartotéky či seznamu. Jádro toho, zda je určitý soubor údajů možné považovat za rejstřík, dle Soudního dvora spočívá v tom, zda tento soubor slouží jako referenční pomůcka, resp. zda je možné osobní údaje o jednotlivých osobách snadno dohledat z důvodu jejich organizace podle

[101] Samozřejmě jsou myšleny počítače v širším smyslu než ve smyslu osobního počítače.
[102] Rozsudek Soudního dvora ze dne 10. července 2018, *Jehovan Todistajat*, C-25/17, EU:C:2018:551.

určitého kritéria.[103] Je-li tomu tak, je dle Soudního dvora třeba soubor údajů považovat za rejstřík.

Na čl. 2 odst. 1 GDPR navazuje čl. 2 odst. 2 obsahující několik výjimek z takto široce vymezené působnosti. Dle tohoto ustanovení se GDPR nepoužije na zpracování osobních údajů:

a) při výkonu činností, které nespadají do oblasti působnosti práva Unie;
b) členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU;
c) fyzickou osobou v průběhu výlučně osobních či domácích činností;
d) příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

Především první výše uvedená výjimka může vyvolávat určité interpretační potíže, pokud není člověk důkladněji obeznámen se související judikaturou Soudního dvora. Na první pohled totiž jde o vyjádření poměrně logické zásady: pokud EU obecně nemá pravomoc regulovat určité činnosti, nemá pravomoc přijímat ani pravidla pro zpracování osobních údajů, ke kterému dochází v rámci výkonu těchto činností. Mohlo by se tedy zdát, že se GDPR uplatní pouze v oblastech jinak pokrytých primárním či sekundárním právem. Realita je však odlišná, jak Soudní dvůr potvrdil poměrně nedávno ve věci *Land Hessen*, když rozhodl, že se GDPR použije na zpracování osobních údajů petičním výborem parlamentu členského státu.[104] Tedy v rámci činnosti, kterou by jinak mohl unijní zákonodárce regulovat jen stěží. Abychom tento přístup Soudního dvora pochopili, je dobré se vrátit na začátek.

Otázka věcné působnosti směrnice 95/46 (konkrétně toho, do jaké míry je aplikovatelnost směrnice 95/46 závislá na existenci určitého „tržního prvku“), se totiž stala spornou hned v prvních dvou případech, ve kterých se Soudní dvůr výkladem směrnice zabýval. Věc *Österreichischer Rundfunk* se týkala problematiky předávání osobních údajů o platech zaměstnanců veřejnoprávního rozhlasu rakouskému účetnímu dvoru pro účely zpracování jeho výroční zprávy. Ve věci *Lindqvist* byla předmětem sporu pokuta, kterou ve Švédsku obdržela katechetka lokální farnosti, jež vytvořila internetové stránky obsahující informace o jejích kolezích, ovšem bez jejich souhlasu. Žalovaní ve věci *Österreichischer Rundfunk* i paní

[103] Srov. ibidem, body 58-59.
[104] Srov. rozsudek Soudního dvora ze dne 9. července 2020, *Land Hessen*, C-272/19, EU:C:2020:535 (dále jen „*rozsudek Land Hessen*“).

Lindqvist argumentovali tím, že jejich činnost nespadá do působnosti směrnice 95/46, přičemž se odvolávali mj. na čl. 3 odst. 2 první odrážku této směrnice. Dle tohoto ustanovení, které odpovídalo současnému čl. 2 odst. 2 písm. a) GDPR, se směrnice 95/46 nevztahovala na zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Společenství.[105] Členské státy v pohledu na použitelnost směrnice 95/46 v dotčených případech nebyly za jedno. Ani Komise si patrně nebyla zcela jista, jaký přístup v dané věci zvolit.[106]

Generální advokát Tizzano dospěl v obou případech k závěru, že se směrnice 95/46 nepoužije. Vycházel přitom nejen ze znění čl. 3 odst. 2 první odrážky směrnice 95/46, ale také z jejího cíle a právního základu. Ve věci *Lindqvist* poukázal na to, že paní Lindqvist zpracovávala osobní údaje v rámci své dobrovolnické činnosti, tedy v rámci nevýdělečné aktivity, která nebyla regulována žádnými komunitárními pravidly, přičemž v daném případě neexistovala ani jakákoliv spojitost se základními svobodami vnitřního trhu.[107] Stejně tak ve věci *Österreichischer Rundfunk* generální advokát uvedl, že auditní činnost rakouského účetního dvora sleduje účel zajištění řádného hospodaření s veřejnými prostředky, a je tedy regulována ústavním právem členských států, nikoliv komunitárním právem. Jakoukoliv spojitost se svobodami vnitřního trhu (např. v tom smyslu, že předmětné zpracování platových údajů může odradit potenciální zaměstnance z jiných členských států) generální advokát odmítl jako příliš nepřímou. Generální advokát v obou případech připomněl, že ačkoliv směrnice 95/46 má mj. zajistit ochranu základních práv v souvislosti se zpracováním osobních údajů, vzhledem k jejímu právnímu základu se nemůže jednat o cíl *sám o sobě*. Dotčené činnosti proto měly být dle generálního advokáta považovány za „*činnosti, které nespadají do oblasti*

---

[105] V této souvislosti je třeba upozornit na poněkud nepřesné české znění čl. 3 odst. 2 první odrážky směrnice 95/46, dle kterého se směrnice nepoužila na zpracování osobních údajů „*prováděné pro výkon činností, které nespadají do oblasti působnosti práva Společenství* ***a*** *jsou uvedeny v hlavě V a VI Smlouvy o Evropské unii, a v každém případě na zpracování, které se týká veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské stability státu, pokud jsou tato zpracování spojená s otázkami bezpečnosti státu) a činnosti státu v oblasti trestního práva*“. Tato formulace by mohla vést k závěru, že výčet činností nespadajících do působnosti směrnice v daném ustanovení je taxativní. Z jiných jazykových verzí je nicméně jasné, že se jedná o demonstrativní výčet, viz např. anglická verze daného ustanovení: „*in the course of an activity which falls outside the scope of Community law,* ***such as*** *those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*“.

[106] Srov. stanovisko generálního advokáta Tizzana ze dne 14. listopadu 2002 ve spojených věcech *Österreichischer Rundfunk a další*, C-465/00, C-138/01 a C-139/01, EU:C:2002:662, bod 36 (dále jen „*stanovisko GA ve věci Österreichischer Rundfunk*“).

[107] Srov. stanovisko generálního advokáta Tizzana ze dne 19. září 2002 ve věci *Lindqvist*, C-101/01, C:2002:513, body 33 a násl.

působnosti práva Společenství“ ve smyslu čl. 3 odst. 2 první odrážky směrnice 95/46. Pokud by totiž mohla směrnice 95/46 regulovat otázky ochrany osobních údajů v rámci činností zcela nesouvisejících s vnitřním trhem, byla by dle generálního advokáta neplatná z důvodu nedostatečného právního základu.[108]

Soudní dvůr se s názorem generálního advokáta neztotožnil, a to ani v jednom z výše uvedených případů. Soudní dvůr ve věci *Österreichischer Rundfunk* uvedl, že použitelnost směrnice 95/46 nemůže záviset na otázce, zda v situacích, které jsou předmětem původních řízení, existuje spojitost s výkonem základních svobod. V případě opačného výkladu by totiž hrozilo nebezpečí, že by se omezení působnosti této směrnice stala neurčitými a nahodilými, což by bylo v rozporu s jejím harmonizačním cílem. Dle Soudního dvora je naopak třeba vycházet z toho, že každý osobní údaj je způsobilý pohybovat se mezi členskými státy, a směrnice 95/46 tak v zásadě ukládala povinnost dodržovat pravidla na ochranu osobních údajů v souvislosti s jakýmkoli jejich zpracováním.[109] Ve věci *Lindqvist* Soudní dvůr navíc doplnil, že výjimka v čl. 3 odst. 2 první odrážce směrnice 95/46 se vztahovala pouze na činnosti, které jsou v tomto ustanovení takto výslovně uvedeny, a dále jen na ty činnosti, které lze zařadit do stejné kategorie. Dle Soudního dvora tak mělo jít zpravidla o činnosti států a státních orgánů, které nemají nic společného s činností jednotlivců.[110] Ani v jednom případě tedy Soudní dvůr nedospěl k závěru, že by se měla směrnice 95/46 neaplikovat z důvodu, že ke zpracování došlo v rámci činností, které nespadají do působnosti práva Společenství.

V této argumentaci Soudního dvora lze nalézt jisté problémy. Je pravdou, že již z tehdy platné judikatury vyplývalo, že použití ex čl. 100a SES jako právního základu nepředpokládá existenci skutečné vazby na volný pohyb mezi členskými státy v každé ze situací, na něž se vztahuje dotčený akt. Jinými slovy – použitelnost legislativy přijaté na základě ex čl. 100a SES nemůže záviset na existenci přeshraničního prvku v každém konkrétním vnitrostátním řízení, jako je tomu např. v případech, kdy se žalobce dovolává pouze základních svobod. Je si však třeba uvědomit, že Soudním dvorem citovaná judikatura se týkala sekundární legislativy upravující podmínky výroby, obchodní úpravy a prodeje tabákových výrobků.[111] U tohoto druhu legislativy bylo možné předpokládat, že všechny situace, na které dopadá, budou vykazovat určitý ekonomický prvek. Jinými slovy – tato legislativa ze své podstaty nebude

[108] Srov. stanovisko generálního advokáta ve věci *Österreichischer Rundfunk*, body 40-56.
[109] Srov. rozsudek *Österreichischer Rundfunk*, body 39-47.
[110] Srov. rozsudek *Lindqvist*, body 37-48.
[111] Srov. rozsudek *Österreichischer Rundfunk*, bod 41 a zde citovaná judikatura.

dopadat na činnosti zjevně mimo působnost práva Společenství, jako je dobrovolnická činnost paní Lindqvist či činnost parlamentního petičního výboru ve věci *Land Hessen*. Nemyslím si však, že bylo správné stejný přístup jednoduše přenést i na směrnici 95/46. V případě této směrnice totiž takový přístup vedl k tomu, že její použitelnost byla shledána právě i v případech činností, u nichž je byť jen potenciální souvislost nejen se základními svobodami vnitřního trhu, ale dokonce obchodem jako takovým, zcela vyloučena.

Kritizovat je možné i to, že Soudní dvůr k velmi úzkému výkladu výjimky z působnosti v čl. 3 odst. 2 první odrážce směrnice 95/46 přistoupil s odkazem na to, že je třeba v maximální míře zachovat její harmonizační účinky. Je si však třeba uvědomit, že dotčená výjimka měla zjevně odrážet nedostatek pravomoci Společenství regulovat činnosti v této výjimce zmíněné. Za takové situace by cíl směrnice neměl vést k restriktivnímu výkladu této výjimky. Právě naopak – cíl směrnice by měl být vykládán ve světle jejího právního základu, jak v daných věcech navrhoval generální advokát. A v situaci, kdy by cíl směrnice 95/46 zjevně překračoval její právní základ, mělo by to vést ke shledání její neplatnosti.

Soudní dvůr navíc ve své navazující judikatuře začal o ochraně základních práv hovořit *de facto* jako o svébytném, ne-li dokonce primárním cíli směrnice, aniž by se zabýval otázkou, zda takové pojetí odpovídá jejímu právnímu základu.[112] To je samozřejmě o něco méně problematické v dnešní době, kdy čl. 16 odst. 2 SFEU zmocňuje unijní orgány přímo k přijímání legislativy v oblasti ochrany osobních údajů, a GDPR tudíž již není založeno na právním základě týkajícím se výhradně vytváření podmínek pro fungování vnitřního trhu. Ovšem co se týče předpisů přijatých výhradně na „tržně-harmonizačním“ právním základu, mj. dodnes platné směrnice 2002/58, která tvoří současný unijní rámec pro vnitrostátní právní úpravy data retention, je takový přístup problematický.

Co se týče GDPR, lze se s ohledem na výše uvedené ptát, zda má dnešní čl. 2 odst. 2 písm. a) GDPR vůbec nějaký obsah. Nejistota ohledně obsahu tohoto ustanovení se naplno projevila např. při adaptaci českého právního řádu na GDPR. Český zákonodárce totiž za účelem zajištění právní jistoty raději prostřednictvím vnitrostátního práva *de facto* rozšířil působnost pravidel GDPR na veškerá zpracování osobních údajů s výjimkou těch, která jsou buď upravena jiným předpisem unijního práva (tj. např. zpracování příslušnými orgány v oblasti trestního práva upravená směrnicí 2016/680) či která do působnosti unijního práva slovy důvodové zprávy „*nespadají vůbec, a to ani potenciálně*“ (tj. zpracování za účelem

[112] Srov. např. rozsudek Soudního dvora ze dne 24. září 2019 ve věci *Google*, C-507/17, EU:C:2019:772, bod 54.

zajišťování obranných a bezpečnostních zájmů ČR).[113] Z výše uvedeného vyplývá, že zatímco v jiné oblasti unijního práva by takový přístup mohl být považován za příklad neodůvodněného „gold-platingu", v oblasti ochrany osobních údajů má v důsledku zmíněné judikatury Soudního dvora své opodstatnění.[114]

Další výjimkou z působnosti, která v minulosti budila určité interpretační potíže, je výjimka v čl. 2 odst. 2 písm. c) GDPR, dle které se GDPR nevztahuje na zpracování osobních údajů „*prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností*". Za výlučně domácí činnost nelze dle Soudního dvora považovat již zmíněnou činnost paní Lindqvist spočívající v nahrání osobních údajů o členech církve na webovou stránku, jelikož tím dochází k zpřístupnění těchto údajů neomezenému počtu osob prostřednictvím internetu. Dle Soudního dvora lze za domácí činnosti ve smyslu dotčené výjimky považovat pouze činnosti probíhající v rámci soukromého nebo rodinného života jednotlivců.[115]

Kritériu výlučně domácí činnosti by zdánlivě mohlo odpovídat zpracování osobních údajů, ke kterému docházelo ve věci *Ryneš*, která se týkala zpracování osobních údajů prostřednictvím kamery, kterou pan Ryneš instaloval na svůj dům za účelem ochrany svého majetku a života zdraví sebe a své rodiny.[116] V daném případě Soudní dvůr svůj závěr o nemožnosti aplikovat dotčenou výjimku nicméně založil na tom, že kamera snímala mj. i ulici a vchod do protějšího domu, nikoliv tedy výlučně domov pana Ryneše.[117] Ačkoliv tedy v daném případě nebyly záznamy přístupné nikomu jinému než panu Rynešovi a jeho rodině, přičemž i cíle zpracování se týkaly výhradně pana Ryneše a jeho rodiny, Soudní dvůr dospěl k závěru, že ve chvíli, kdy předmětná kamera snímá i osoby pohybující se na veřejném prostranství, jsou meze osobního a domácího zpracování překročeny.

Soudní dvůr také v této souvislosti uvedl, že je třeba pod dotčenou výjimku zařadit pouze činnosti podobné těm, které demonstrativně zmiňovala směrnice 95/46 v bodě 12 svého odůvodnění, tj. např. korespondence nebo vedení adresáře. Soudní dvůr doplnil, že tento druh činností je charakteristický tím, že se soukromí jiných osob týká pouze „*mimochodem*".[118]

---

[113] Srov. § 4 odst. 2 zákona č. 110/2019 o zpracování osobních údajů a odpovídající část důvodové zprávy k zákonu. V souladu s čl. 2 odst. 2 písm. b) GDPR zůstala stranou taktéž zpracování osobních údajů v rámci společné zahraniční a bezpečnostní politiky.
[114] K problematice gold-platingu srov. např. KRÁL, Richard. *Zbytečně zatěžující transpozice – neodůvodněný gold-plating směrnic EU v České republice*, 2015.
[115] Srov. rozsudek *Lindqvist*, bod 47.
[116] Srov. rozsudek Soudního dvora ze dne 11. prosince 2014 ve věci *Ryneš*, C-212/13, EU:C:2014:2428.
[117] Ibidem, bod 33.
[118] Ibidem, bod 32.

Bez bližšího odůvodnění však toto kritérium nepůsobí příliš důvěryhodně – zejména u vedení adresáře je orientace na údaje o jiných osobách poměrně zjevná. Na druhou stranu je pravdou, že takové vedení soukromého adresáře bude zřejmě ve většině případů svou intenzitou podstatně menším zásahem do soukromí těchto osob než jejich kamerové sledování.

Zbylé dvě výjimky z působnosti GDPR v jeho čl. 2 odst. 2 pak nevyvolávají větší interpretační potíže. Výjimka v čl. 2 odst. 2 písm. b) svým rozsahem odpovídá Hlavě V Smlouvy o EU, výjimka v čl. 2 odst. 2 písm. d) pak odpovídá věcné působnosti směrnice 2016/680, o níž bude řeč níže. Čl. 2 odst. 3 GDPR pak toliko vyjasňuje, že na zpracování osobních údajů orgány, institucemi a jinými subjekty Unie se vztahují jiné předpisy. Čl. 2 odst. 4 GDPR nakonec uvádí, že se pravidla GDPR nedotýkají uplatňování směrnice 2000/31/ES[119]. Toto ustanovení má za cíl zajistit, aby nebyla dotčena specifická pravidla odpovědnosti poskytovatelů zprostředkovatelských služeb uvedená v článcích 12 až 15 uvedené směrnice, a aby tak např. provozovatel zprostředkovatelské služby spočívající v prostém přenosu informací nebyl dle GDPR činěn odpovědným za protiprávní zpracování osobních údajů uživatelem této služby.[120]

Čl. 3 GDPR následně upravuje jeho místní působnost. Dle tohoto ustanovení se GDPR v prvé řadě použije na zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v Unii bez ohledu na to, zda zpracování probíhá v Unii či mimo ni. K tomu, co v daném kontextu znamená „v souvislosti s činnostmi provozovny" se Soudní dvůr již vyjádřil při výkladu směrnice 95/46, jelikož na témže principu byla postavena i její působnost.[121] Od téhož kritéria se odvíjelo dále i určení toho, jaké vnitrostátní implementační předpisy budou na určité zpracování použity. Dotčená problematika byla Soudním dvorem řešena ve věci *Google Spain*.[122] Společnost Google v tomto případě uváděla, že se španělské předpisy o ochraně osobních údajů nepoužijí, jelikož zpracování osobních údajů v daném řízení bylo prováděno výhradně společností Google Inc. na území USA, přičemž činnost její dceřiné

---

[119] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).

[120] Srov. NULÍČEK, Michal et al. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář*, 2017, s. 68.

[121] Česká verze směrnice 95/46 v této souvislosti obsahovala užší pojem „*v rámci činnosti provozovny*", který byl pak v GDPR zpřesněn. Ostatní jazykové verze však zůstaly beze změny, a dotčenou změnu tak lze spíše než za rozšíření působnosti GDPR oproti směrnici 95/46 považovat za zpřesnění překladu. Srov. NULÍČEK, Michal et al. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář*, 2017, s. 71.

[122] Rozsudek Soudního dvora ze dne 13. května 2014, *Google Spain a Google*, C-131/12, EU:C:2014:317 (dále jen „*rozsudek Google Spain*").

společnosti Google Spain se omezovala na poskytování podpory reklamní činnosti, která se liší od služeb vyhledávače. Soudní dvůr takovou argumentaci odmítl. V prvé řadě uvedl, že dotčené ustanovení nepředpokládá, že činnost zpracování bude provádět přímo provozovna v členském státě, nýbrž že toto zpracování bude prováděno v rámci činnosti této provozovny. Pojem „v rámci činnosti provozovny" pak dle Soudního dvora – s ohledem na cíl směrnice spočívající v zajištění účinné a úplné ochrany základních práv subjektů údajů – nelze vykládat restriktivně. Naopak, unijní zákonodárce dle Soudního dvora zamýšlel stanovením obzvláště široké územní působnosti zabránit tomu, aby docházelo k obcházení ochrany poskytované unijními předpisy. Soudní dvůr uvedl, že činnost prodeje reklamního prostoru je natolik úzce spojena s činností vyhledávače, že lze dospět k závěru, že ji lze považovat za činnost, k níž dochází v rámci činnosti španělské provozovny. Takto široký výklad pojmu konceptu činnosti provozovny pak Soudní dvůr potvrdil ve věci *Wirtschaftsakademie Schleswig-Holstein*[123] i přesto, že v daném případě se řešila pouze otázka, které vnitrostátní implementační předpisy (zda německé či irské) mají být použity a který dozorový orgán má být příslušný, a tudíž nebylo přítomno riziko obcházení unijní úrovně ochrany jako v případě *Google Spain.*

Na rozdíl od směrnice 95/46 se GDPR nově použije také na zpracování správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb subjektům údajů v Unii nebo s monitorováním jejich chování. Oproti směrnici 95/46 tak dochází k podstatnému rozšíření extrateritoriálních dopadů, které jsou nyní srovnatelné s těmi v oblasti hospodářské soutěže.[124] Tento přístup je logický mj. právě s ohledem na hospodářskou soutěž, jelikož vede k určitému narovnání podmínek mezi subjekty působícími na území Unie a subjekty, které na území Unie nemají ani provozovnu, avšak díky možnostem internetu mohou do soukromí unijních obyvatel zasahovat stejně intenzivně. Otázkou je, do jaké míry se bude dařit tato pravidla v praxi vynucovat. Např. v případě čínských společností budou možnosti reálného uplatnění extrateritoriality GDPR naprosto minimální, a dotčené ustanovení tak bude mít v těchto případech spíše symbolický charakter.

V neposlední řadě se GDPR použije i na zpracování správcem mimo Unii, pokud se na něj právo členského státu uplatňuje na základě mezinárodního práva veřejného,

---

[123] Rozsudek Soudního dvora ze dne 5. června 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388 (dále jen „*rozsudek Wirtschaftsakademie Schleswig-Holstein*").

[124] K tzv. doktríně účinků v oblasti hospodářské soutěže viz např. ZELGER, Bernadette. EU Competition law and extraterritorial jurisdiction – a critical analysis of the ECJ's judgement in Intel. *European Competition Journal*, 2020, s. 613-620.

tj. například na zpracování prováděné v rámci činnosti diplomatické mise či konzulárního zastoupení členského státu.

2.2.2.4 Základní koncepty a pojmy

Ústředním pojmem GDPR je z logických důvodů především pojem osobního údaje. I přes klíčový význam tohoto pojmu nicméně existovaly po delší dobu rozdíly v jeho výkladu napříč členskými státy, což vedlo pracovní skupinu WP29 k vydání stanoviska ke správnému výkladu tohoto pojmu.[125] V posledních letech se k obsahu tohoto pojmu také několikrát vyjádřil i Soudní dvůr EU, některé sporné otázky však doposud zůstávají nezodpovězené.

GDPR definuje osobní údaje jako „*veškeré informace o identifikované nebo identifikovatelné osobě*“. Tato definice je – zcela v souladu s úmyslem zákonodárce jasně vyjádřeným v legislativním procesu – značně široká. Tato šíře přitom vyplývá zejména ze dvou jejích zásadních prvků.

Zaprvé, dotčená definice výslovně zahrnuje *veškeré* informace o určité osobě. Druh či povaha informace není určující. Není tedy relevantní, zda má dotčený údaj povahu skutkového tvrzení či hodnotového soudu. Relevantní není ani to, zda se jedná o údaj pozitivního, negativního či dokonce zjevně urážlivého charakteru. V neposlední řadě nejde ani o to, zda je údaj pravdivý. Výše uvedené aspekty sice mohou být relevantní pro účely posouzení míry zásahu do soukromí dotčené osoby, který může zpracování takových údajů způsobit, ale nejsou relevantní pro určení, zda se o osobní údaje jedná. O ty totiž půjde ve všech výše uvedených případech. Zároveň je třeba upozornit, že z mnohých údajů, které na první pohled nejenže nejsou informace o „identifikované či identifikovatelné osobě“, ale vůbec nejsou „o osobě“, se přesto mohou osobní údaje stát. Např. cena domu, která je údajem o věci, se tak stává osobním údajem ve chvíli, kdy existuje rozumná možnost zjištění vlastníka tohoto domu.

Zadruhé, osoba nemusí být nutně identifikovaná, ale postačí její *identifikovatelnost*, tj. potenciál identifikace. Dle bodu 26 odůvodnění GDPR platí, že „*při určování, zda je fyzická osoba identifikovatelná, by se mělo přihlédnout ke všem prostředkům, jako je například výběr vyčleněním, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby.*“, přičemž „*ke stanovení toho, zda lze rozumně předpokládat použití prostředků k identifikaci fyzické osoby, by měly být vzaty v úvahu všechny objektivní faktory, jako jsou náklady a čas, které si identifikace vyžádá, s přihlédnutím*

[125] Pracovní skupina pro ochranu údajů zřízená podle čl. 29 směrnice 95/46. *Stanovisko č. 4/2007 k pojmu osobní údaje*, 2007.

k technologii dostupné v době zpracování i k technologickému rozvoji.“ Dotčený bod odůvodnění tedy potvrzuje přístup již dříve zastávaný v odborné literatuře, dle kterého je při posuzování identifikovatelnosti subjektu údajů třeba zvolit objektivní pohled, tedy nevycházet pouze z prostředků, které má k dispozici správce údajů, ale vzít v potaz také možnost identifikace třetími osobami.[126]

Otázkou identifikovatelnosti subjektu údajů se Soudní dvůr zabýval ve věci *Breyer*, ve které bylo sporné, zda osobní údaj představuje tzv. dynamická IP adresa, tj. dočasná IP adresa, jež je přidělována při každém internetovém připojení a nahrazována při dalších připojeních. V daném případě byl správcem údajů provozovatel webové stránky, který ovšem nebyl schopen identifikovat osobu používající počítač s dotčenou IP adresou, aniž by obdržel dodatečné informace od poskytovatele telekomunikačních služeb. Ten však dle příslušného vnitrostátního práva nebyl oprávněn tyto informace provozovateli webové stránky předat. Soudní dvůr uvedl, že dotčená dynamická IP adresa představuje osobní údaj, jelikož vnitrostátní právo umožňuje provozovateli webové stránky obrátit se v případě kybernetických útoků na policii, aby podnikla kroky nezbytné k získání těchto informací od poskytovatele internetového připojení a k zahájení trestního stíhání. Mám však za to, že výše uvedený rozsudek by neměl být interpretován tak, že vždy, kdy bude existovat možnost identifikace subjektu údajů třetí osobou, je třeba považovat určité údaje za osobní údaje. I v případě objektivního pojetí osobního údaje je tedy třeba brát v potaz toliko prostředky, které mohou být rozumně použity. V daném případě se o rozumně použitelné prostředky z mého pohledu jednalo z důvodu, že ke zpracování dynamických IP adres docházelo právě za účelem odhalení kybernetických útoků, a zapojení policie tedy bylo rozumně předvídatelné. Dle mého názoru by nicméně logika, dle které je osoba identifikovatelná vždy, kdy jí lze identifikovat při získání dodatečných údajů v rámci trestního řízení, neměla být přenášena na zpracování, u nichž zahájení takového trestního řízení (a tedy použití prostředků identifikace, které mají k dispozici orgány působící v oblasti trestního práva) nelze rozumně očekávat.

Předmětem rozhodovací činnosti Soudního dvora se krom již zmíněných IP adres stala řada kategorií údajů, u nichž byla jejich osobní povaha poměrně jasná. V této souvislosti lze zmínit např. jméno, datum, místo narození, rodinný stav, pohlaví, číslo dokladu, otisky prstů apod. Dále pak např. údaje o zdravotním stavu, o dosahovaných příjmech, o výši obdržené

[126] Srov. např. HARAŠTA, Jakub. a MÍŠEK Jakub. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie*, 2015, s. 29.

dotace, o účasti na určitém jednání, kamerové záznamy apod. U některých kategorií údajů je však toto posouzení poněkud komplikovanější.

V rozsudku *YS*[127] se Soudní dvůr zabýval otázkou, zda lze za osobní údaj považovat právní rozbor uvedený v protokolu přiloženém k návrhu rozhodnutí o azylové žádosti. Soudní dvůr dospěl k závěru, že ačkoliv dotčený rozbor může určité osobní údaje obsahovat (zejména v podobě jména, původu, vyznání a dalších údajů o žadateli), sám o sobě není osobním údajem. Soudní dvůr uvedl, že „*takový právní rozbor nepředstavuje informaci týkající se žadatele o povolení k pobytu, ale nanejvýš – v rozsahu, v němž se neomezuje na ryze abstraktní výklad práva – informaci týkající se posouzení a použití tohoto práva příslušným orgánem na situaci tohoto žadatele, jelikož tato situace je dokládána především osobními údaji, které se týkají jeho osoby, jimiž tento orgán disponuje*."

Tyto závěry Soudního dvora byly také podpořeny srovnáním cílů sledovaných směrnicí 95/46 a cíle, který v daném případě sledovali žadatelé. Soudní dvůr, stejně jako před ním generální advokátka, měl za to, že žadatelé požadavkem na přístup k dotčenému právnímu rozboru nesledovali ani tak cíle předpokládané směrnicí 95/46 (tj. neusilovali např. o případnou opravu nesprávných osobních údajů či nechtěli rozporovat oprávněnost zpracování), ale spíše cíle vlastní předpisům z jiných oblastí (typicky z oblasti správního přezkumu rozhodnutí, resp. přístupu ke správním dokumentům). Ačkoliv nelze se Soudním dvorem polemizovat o tom, že osobním údajem není abstraktní výklad práva, v případě aplikování tohoto rozboru na situaci žadatele je taková hranice už velmi tenká. Úvahy ohledně toho, zda žadatel vyhověl podmínkám vyplývajících z právních předpisů a proč, jsou totiž zjevně svázány s osobou žadatele, dle mého názoru natolik, že by měly spadnout do výše uvedené široké definice osobního údaje. Na druhou stranu nelze se Soudním dvorem polemizovat o tom, že cílem směrnice jistě nebylo vytvořit určitou alternativní cestu pro přístup ke správním spisům.

Z mého pohledu k opačným závěrům než ve věci *YS* dospěl Soudní dvůr ve vztahu k odpovědím na testové otázky a poznámkám zkoušejícího k těmto odpovědím. V případu *Nowak* Soudní dvůr uvedl, že obsah odpovědí odráží znalosti a schopnosti uchazeče, přičemž může mít vliv na jeho práva a zájmy, neboť může ovlivnit například jeho šanci na přístup k požadovanému povolání nebo zaměstnání.[128] Stejně tak korekturní poznámky mají dle Soudního dvora za cíl zdokumentovat hodnocení zkoušejícího týkající se výkonu zkoušeného

[127] Rozsudek Soudního dvora ze dne 17. července 2014, *YS a další*, C-141/12, EU:C:2014:2081 (dále jen *„rozsudek YS"*).
[128] Rozsudek Soudního dvora ze dne 20. prosince 2017, *Nowak*, C-434/16, EU:C:2017:994.

a mohou mít pro zkoušeného důsledky. Ačkoliv lze s hodnocením Soudního dvora souhlasit, nabízí se otázka, zda by veškeré tyto úvahy nemohly být v zásadě stejným způsobem aplikovány na právní rozbor, který byl předmětem sporu ve věci *YS.* Dle mého názoru rozhodně.

Opakem osobních údajů jsou údaje anonymní, tj. údaje, které se netýkají identifikované či identifikovatelné osoby. Anonymními údaji jsou i údaje anonymizované, tedy osobní údaje, které sice bylo možné v minulosti k určité osobě přiřadit, avšak na základě provedené operace anonymizace to již možné není. Anonymizované údaje nicméně není možné zaměňovat s údaji pseudonymizovanými, tj. údaji, které nemohou být přiřazeny konkrétnímu subjektu údajů bez prvotního použití dodatečných informací, jež jsou uchovávány odděleně. Pseudonymizované údaje je totiž kvůli nadále existující možnosti identifikace subjektu údajů třeba považovat za údaje osobní. Totéž platí pro osobní údaje šifrované, tj. osobní údaje převedené do podoby, která není čitelná bez znalosti speciální informace (šifrovacího klíče).[129]

Pro účely této práce je třeba uvést, že komunikační metadata budou zjevně spadat do široké definice osobního údaje uvedené v GDPR. Tato komunikační metadata, zjednodušeně řečeno, vypovídají o tom, „kdy, s kým, odkud a jak dlouho" určitá osoba komunikovala, a nelze tedy pochybovat o tom, že se jedná o údaje „o osobě", resp. o osobách odesílatele a adresáta sdělení. O identifikovatelnosti dotčených osob také nemůže být větších pochyb – možnost identifikovat dotčené osoby je ostatně samotnou podstatou data retention. Kvůli tomu také nemohou být uchovávaná komunikační metadata anonymizována. Na druhou stranu využívání nástrojů pseudonymizace a šifrování se jeví v kontextu data retention jako velmi vhodné, jelikož s ohledem na množství uchovávaných údajů a jejich citlivost je potřeba přijmout taková opatření, která v maximální míře snižují možnost neoprávněné identifikace subjektu údajů.

Fyzickou osobu, ke které se osobní údaje váží, nazývá GDPR subjektem údajů. Obsah tohoto pojmu je tedy logicky úzce svázán s pojmem osobního údaje. Subjektu údajů pak GDPR přiznává řadu práv, jako např. právo na informace o zpracování, právo na opravu údajů, právo na výmaz údajů, právo na námitku, právo obrátit se na dozorový úřad apod.

Dalším důležitým pojmem je pojem zpracování. Tím je dle čl. 4 odst. 2 GDPR jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí,

[129] Srov. NULÍČEK, Michal et al. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář*, 2017, s. 293.

použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení. Šíře dotčené definice neponechává příliš prostoru pro pochybnost, co je a co není zpracováním osobních údajů. Zpracováním údajů je v zásadě jakýkoliv úkon s údaji (včetně např. jejich vymazání). Určité pochybnosti tak může vyvolávat maximálně určení, co je třeba považovat za automatizované zpracování. Tato otázka je důležitá taktéž pro posouzení věcné působnosti GDPR a byla již rozebrána. V případě data retention bude zpracováním jak samotné uložení údajů, tak každá další operace s nimi, včetně jejich předání či jiného zpřístupnění příslušným orgánům státu. Je samozřejmé, že tyto úkony v současnosti probíhají prostřednictvím automatických prostředků.

Dalším klíčovým pojmem, se kterým GDPR pracuje, je bezpochyby pojem správce. Je to právě správce, kdo je v drtivé většině případů odpovědný za zajištění souladu s pravidly GDPR. Správcem je dle GDPR „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů*“. Opět se jedná o značně širokou definici, což je způsobeno především dvěma aspekty.

Zaprvé tím, že správcem může být skutečně jakýkoliv subjekt bez ohledu na jeho právní formu. Zadruhé tím, že sám správce vůbec nemusí zpracování osobních údajů provádět. Postačí, pokud se jen podílí na určení účelu a prostředků takového zpracování. Judikatura Soudního dvora s ohledem na tyto aspekty a cíl zajištění vysoké úrovně ochrany osobních údajů potřebu širokého výkladu pojmu správce dlouhodobě potvrzuje.[130] Oprávnění správce určovat účel a prostředky zpracování sice může explicitně či alespoň implicitně vyplývat z určitého formálního pramene (zákona, interního předpisu, smlouvy), ovšem není to podmínkou. Je tudíž třeba vždy vycházet především z reálného stavu věcí. Z definice správce uvedené výše je také zřejmé, že v souvislosti s jedním zpracováním může být spojeno vícero subjektů v pozici správce – abychom však mohli hovořit o společném správcovství, je nezbytné, aby se opravdu jednalo o totéž zpracování.

Soudní dvůr tak v rozsudku *Google Spain* rozhodl, že provozovatele internetového vyhledávače je třeba považovat za správce, přestože nedisponuje možností ovlivnit zpracování osobních údajů na samotných webových stránkách v seznamu výsledků vyhledávání. Soudní dvůr nicméně vcelku logicky považoval činnost vyhledávače za samostatné zpracování osobních údajů a provozovatele vyhledávače za správce těchto údajů. Skutečnost, že dotčené

[130] Srov. např. rozsudek *Google Spain*, bod 34.

údaje jsou přístupné veřejnosti i bez činnosti vyhledávače a že sám vyhledávač nemůže jejich zveřejnění na dotčené stránce ovlivnit, v tomto ohledu nehraje roli.[131] Stejně tak Soudní dvůr ve věci *Fashion ID* dovodil, že za správce osobních údajů je třeba považovat provozovatele webové stránky, který na svou stránku umístí sociální modul společnosti Facebook, který umožňuje společnosti Facebook sbírat data o návštěvnících této webové stránky. Obdobně jako v předchozím případě, i zde provozovatel webové stránky vlastní činností umožňuje společnosti Facebook sbírat osobní údaje, které by jinak sbírat nemohla, což z něj činí správce společně s touto společností. Výše uvedené platí i přesto, že provozovatel webové stránky nemusí mít k takto sbíraným údajům přístup a že nemůže ovlivnit žádný z aspektů následného zpracování dotčených údajů společností Facebook.[132] Odpovědnost provozovatele webové stránky nicméně musí být omezena na operace nebo soubor operací zpracování osobních údajů, u nichž skutečně určuje účely a prostředky, a sice sběr a přenos dotčených údajů.

Ještě dále zašel v tomto ohledu Soudní dvůr v případu *Wirtschaftsakademie Schleswig-Holstein*, když na základě podobných úvah jako ve výše uvedených případech dospěl k závěru, že za společného správce je třeba považovat i pouhého zakladatele tzv. „fanouškovské stránky“[133] na sociální síti Facebook – tedy osobu, která se na zpracování osobních údajů podílí pouze využitím určité funkcionality, kterou tato sociální síť nabízí.[134] Dle Soudního dvora „*správce fanouškovské stránky umístěné na Facebooku vytvořením takové stránky umožňuje Facebooku, aby umisťoval soubory cookies na počítači nebo jakémkoli jiném zařízení osoby, která jeho fanouškovskou stránku navštívila*“. Je sice pravdou, že Soudní dvůr k těmto závěrům dospěl i ve světle toho, že povaha dotčené fanouškovské stránky byla komerční a sloužila propagaci určité vzdělávací instituce. Díky tomu mohl správce fanouškovské stránky využít řadu funkcionalit komerčního charakteru, které mu Facebook nabízel. Nicméně ne všechny fanouškovské stránky mají nutně komerční povahu (může se jednat např. o stránky, které jsou založeny za účelem diskuse o věcech určitého společného zájmu apod.). Soudní dvůr však také uvedl, že z existence společného „správcovství“ společnosti Facebook a správce fanouškovské

[131] Srov. rozsudek *Google Spain*, body 21-41.
[132] Soudní dvůr v dané souvislosti mj. zdůraznil, že zpracování osobních údajů společností Facebook bylo pro provozovatele stránky prospěšné, jelikož mu umožňovalo lépe zacílit propagaci svých služeb na dotčené sociální síti.
[133] Fanouškovské stránky jsou uživatelskými účty, které mohou jednotlivci nebo podniky vytvořit na Facebooku. Za tímto účelem může autor fanouškovské stránky poté, co se zaregistruje u Facebooku, využít platformu provozovanou Facebookem k tomu, aby se prezentoval uživatelům této sociální sítě a osobám, které tuto stránku navštíví, a šířil na mediálním trhu sdělení všeho druhu.
[134] Srov. rozsudek *Wirtschaftsakademie Schleswig-Holstein*, body 25-44.

stránky nelze nezbytně dovozovat, že by oba měli nést stejný podíl odpovědnosti. Takový závěr by byl zjevně nepřiměřený. Lze také očekávat, že zatímco v praxi bude v těchto případech společnosti Facebook udělena dostatečně odstrašující finanční sankce, správci fanouškovské stránky bude toliko uloženo profil či fanouškovskou stránku zrušit.

Nabízí se otázka, zda se na základě výše uvedené logiky může na zpracování osobních údajů společností Facebook podílet i běžný uživatel vytvořením soukromého profilu. Mám za to, že obecně nikoliv, jelikož bod 18 odůvodnění GDPR uvádí, že užívání sociálních sítí v rámci činnosti čistě osobní povahy by nemělo spadat do působnosti GDPR. S ohledem na závěry Soudního dvora ve věci *Lindqvist* a potřebu vykládat dotčenou výjimku restriktivně se však domnívám, že pod ni nebude spadat každý profil, který je formálně soukromý. Např. i formálně soukromé profily politiků či celebrit by např. s ohledem na počet sledujících nemusely pod dotčenou výjimku spadat, a zřejmě by se tak v jejich případě uplatnil stejný přístup jako v případě fanouškovských stránek.

Dalším klíčovým pojmem, úzce souvisejícím s pojmem správce, je pojem zpracovatele. Na rozdíl od předchozích pojmů nemá tento pojem původ v Úmluvě 108, ale jedná se o koncept zavedený směrnicí 95/46, jehož cílem bylo zajistit vysokou úroveň ochrany osobních údajů v případech, kdy správce zpracování deleguje na určitou třetí osobu. Význam tohoto institutu samozřejmě rostl s rozvojem informačních technologií, kdy docházelo ke štěpení jednotlivých úkolů v rámci zpracování osobních údajů a kdy se ze zpracování osobních údajů pro jiné osoby stala běžná služba. Dle GDPR je zpracovatelem fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce. Hranice mezi správcem a zpracovatelem může být v mnoha případech značně tenká a nebude vždy lehké odlišit, kdy se jedná o zpracovatele zpracovávajícího osobní údaje pro správce, a kdy jde o poskytovatele služby, který zpracovává údaje pro účely poskytnutí této služby, a tudíž „pro sebe“. Typické bude takové dilema např. u služeb mzdových účetních apod. Opět platí, že je třeba vycházet nejen ze smluvních ujednání (která mohou být nápomocná, nikoliv však určující sama o sobě), ale především z fakticity daného smluvního vztahu. V hraničních případech se pak jeví jako užitečné přihlížet především k tomu, do jaké míry objednatel určuje prostředky dotčeného zpracování. Čím větší volnost na straně poskytovatele služby, tím větší šance, že se bude jednat o samostatného správce, nikoliv pouze zpracovatele. Novinkou zaváděnou GDPR je povinnost uzavření tzv. zpracovatelské smlouvy mezi správcem a zpracovatelem, jejíž minimální obsahové náležitosti stanoví čl. 28 odst. 3 GDPR.

Vzhledem k uvedenému výkladu by bylo možné uvažovat o tom, že jelikož v případě data retention uchovávají poskytovatelé telekomunikačních služeb údaje výhradně pro účely jejich zpřístupnění příslušným orgánům státu, plní vůči těmto orgánům toliko funkci zpracovatele údajů. Takový přístup by ale nebyl správný. Sama skutečnost, že k určitému zpracování dochází na základě zákonné povinnosti, totiž ještě neznamená, že subjekt provádějící toto zpracování není správcem. Právě naopak, za správce je vždy třeba považovat přinejmenším osobu, které je tato povinnost uložena. To platí i v případech, kdy tato osoba reálně nemá na výběr, zda dané zpracování provede.

2.2.2.5 Zásady zpracování osobních údajů

Klíčové povinnosti správce, jejichž dodržení je podmínkou legality každého zpracování, se nachází v čl. 3 (nadepsaném „*Zásady zpracování osobních údajů*“) a čl. 4 (nadepsaném „*Zákonnost zpracování*“) GDPR. Obecné zásady každého zpracování dle GDPR lze s jistou mírou zjednodušení shrnout následovně:

- údaje musí být zpracovávány korektně (zásada korektnosti) a zákonným způsobem (zásada zákonnosti);
- subjekt údajů by měl být o důležitých aspektech zpracování informován (zásada transparentnosti);
- údaje musí být zpracovávány za legitimním, výslovně vyjádřeným účelem, přičemž následné zpracování za odlišným účelem je možné pouze tehdy, je-li nový účel slučitelný s prvotním (zásada účelového omezení);
- údaje musí být zpracovávány v míře odpovídající tomuto účelu, a jen po dobu nezbytnou k dosažení tohoto účelu (zásada minimalizace údajů), přičemž následně by měly být vymazány či anonymizovány (zásada omezení uložení);
- musí být přijata veškerá rozumná opatření, aby zpracovávané údaje byly přesné a aktualizované (zásada přesnosti);
- v průběhu zpracování musí být dbáno na to, aby byla zajištěna bezpečnost údajů, tj. jejich integrita a důvěrnost (zásada integrity a důvěrnosti);
- dodržení výše uvedených zásad navíc musí být doložitelné ze strany správce (zásada odpovědnosti).

Aniž by bylo na místě probírat obsah veškerých výše uvedených zásad detailněji, nelze ignorovat poměrně zjevné napětí mezi celou řadou výše uvedených zásad (účelové omezení, minimalizace údajů, uchovávání po nezbytnou dobu či povinnost zajistit přesnost údajů) a plošným uchováváním komunikačních metadat o všech uživatelích prostředků elektronické

komunikace. Samozřejmě, tyto zásady nejsou absolutní a mohou být dle čl. 23 GDPR omezeny, sleduje-li takové opatření legitimní cíl a je-li v souladu se zásadou proporcionality. Již z letmého pohledu na „běžný režim“ výše je nicméně zřejmé, proč je data retention tolik kontroverzní otázkou.

Údaje musí být dále zpracovávány na základě jednoho z titulů pro zpracování obsažených v čl. 4 GDPR. Mezi tyto tituly patří:

- svobodný, konkrétní, informovaný a jednoznačný souhlas subjektu údajů, udělený prohlášením či jiným zjevným potvrzením, který může být kdykoliv odvolán;
- nezbytnost zpracování pro splnění či uzavření smlouvy, jejíž stranou je subjekt údajů
- nezbytnost zpracování pro splnění právní povinnosti, které podléhá správce;
- nezbytnost zpracování pro zachování životně důležitých zájmů subjektu údajů;
- nezbytnost zpracování pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci;
- nezbytnost zpracování pro uskutečnění oprávněných zájmů správce nebo třetí osoby, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů.

Co se týče data retention, v případě uchovávání údajů a jejich předávání příslušným orgánům poskytovateli služeb bude právním titulem povinnost uložená vnitrostátním právem. Právním titulem pro přístup k údajům ze strany příslušných orgánů a jejich následné zpracování bude plnění úkolu ve veřejném zájmu, které jako titul pro zpracování stanovuje směrnice 2016/680. Problematika existence titulu pro zpracování tak v případě data retention nevyvolává otázky. Značné množství provozních a lokalizačních údajů si nicméně budou uchovávat taktéž poskytovatelé služeb na základě jiných právních titulů. Zpravidla půjde o nezbytnost pro splnění smlouvy (např. kvůli následnému vyúčtování služby) či oprávněný zájem (např. vymáhání občanskoprávního nároku). V této souvislosti je vhodné upozornit na to, že za oprávněný zájem lze dle bodu 47 odůvodnění GDPR považovat i přímý marketing.

Judikatura Soudního dvora k problematice titulů pro zpracování se týká spíše dílčích praktických problémů. Z této judikatury např. vyplývá, že souhlas musí být proveden pouze aktivním jednáním subjektu údajů, např. zaškrtnutím políčka na webové stránce, které nemůže být zaškrtnuto již předem.[135] Několik rozsudků se dále zabývalo titulem spočívajícím v uskutečnění oprávněných zájmů správce nebo třetí osoby. Soudní dvůr např. rozhodl,

[135] Srov. rozsudek Soudního dvora ze dne 11. listopadu 2020, *Orange Romania*, C-61/19, EU:C:2020:90.

že za oprávněný zájem je možné považovat podání žaloby na náhradu škody,[136] ochranu webových stránek před kybernetickými útoky,[137] či ochranu osob a majetku prostřednictvím bezpečnostních kamer.[138]

Čl. 9 GDPR dále obsahuje specifická pravidla pro zpracování zvláštních kategorií údajů, často nazývaných také „citlivé údaje", byť GDPR tento pojem nepoužívá.[139] Jde o údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém přesvědčení, odborové příslušnosti, zdraví a sexuálním životě. Tyto údaje je možné zpracovávat pouze na základě výslovného souhlasu subjektu údajů; v případech, kdy tyto údaje zjevně zveřejní sám subjekt nebo dále v jiných, přísně vymezených situacích a za dodržení dalších opatření (půjde např. o zpracování v oblasti pracovního práva, zdravotnictví či za účelem jiného dostatečně významného veřejného zájmu). Specifická pravidla obsahuje GDPR i pro zpracování údajů týkajících se protiprávního jednání či rozsudků v trestních věcech.

Pro účely této práce je třeba uvést, že i komunikační metadata mohou mít v některých případech povahu citlivých údajů. I tyto údaje mohou totiž leccos odhalit např. o náboženském přesvědčení (bude-li z nich např. vyplývat, že se mobilní zařízení vlastněné subjektem údajů každou neděli nachází v místě kostela) či zdravotním stavu (bude-li např. subjekt údajů pravidelně dostávat e-maily z lékařského zařízení zabývajícího se léčbou rakoviny). Povaha plošného uchovávání navíc reálně neumožňuje, aby byly z uchovávaných provozních a lokalizačních údajů vyřazeny citlivé údaje, jelikož jejich citlivost může být odhalena až v rámci následného zpracování. Zároveň však data retention sleduje dostatečně významné cíle veřejného zájmu a příslušné právní úpravy často stanovují přísné dodatečné záruky. Data retention zároveň výslovně umožňuje čl. 15 odst. 1 směrnice 2002/58, která má vůči GDPR povahu *lex specialis*.[140]

2.2.2.6 Práva subjektu údajů

GDPR dále obsahuje řadu práv subjektu údajů. Mezi tyto práva patří:

- právo na informace o zpracování, mj. o identitě správce, účelu zpracování a dalších právech subjektu údajů;
- právo na přístup k údajům;

[136] Srov. rozsudek Soudního dvora ze dne 4. května 2017, *Rīgas satiksme*, C-13/16, EU:C:2017:336.
[137] Srov. rozsudek *Breyer*, body 50-64.
[138] Srov. rozsudek věci *Ryneš*, bod 34.
[139] Pro zjednodušení pracuje s pojmem citlivé údaje i tato práce.
[140] Viz kapitola 2.3.2.

- právo na opravu, výmaz či blokování údajů, jejichž zpracování není v souladu s GDPR, zejména z důvodů jejich neúplné nebo nepřesné povahy;
- právo na přenositelnost některých údajů;
- právo vznést námitku proti některým zpracováním osobních údajů;
- právo nebýt předmětem rozhodnutí přijatého výhradně na základě automatizovaného zpracování údajů určeného k hodnocení určitých rysů jeho osobnosti, například pracovního výkonu, důvěryhodnosti, spolehlivosti, chování atd.

V souvislosti s výše uvedenými právy a povinnostmi je zcela zásadní i čl. 23 GDPR, jež umožňuje členským státům prostřednictvím vnitrostátního práva omezit rozsah těchto povinností a práv, je-li to nezbytné pro zajištění některého z legitimních cílů obsažených v tomto ustanovení, za podmínky, že takové omezení respektuje podstatu základních práv a svobod a představuje nezbytné a přiměřené opatření v demokratické společnosti. Okruh těchto legitimních cílů je široký, zahrnující samozřejmě taktéž problematiku potírání trestné činnosti a zajišťování národní bezpečnosti, tedy cíle sledované právními úpravami data retention.

Judikatura zabývající se podrobněji právy subjektu údajů je ve srovnání s judikaturou týkající výkladu působnosti příslušných předpisů či výkladu základních pojmů poměrně vzácná. Výjimku v tomto ohledu tvoří „právo být zapomenut“, dovozené Soudním dvorem v rozsudku *Google Spain* a nyní blíže upravené v čl. 17 GDPR jako „právo na výmaz“. Předmětem sporu ve věci *Google Spain* bylo, zda má subjekt údajů právo na to, aby internetový vyhledávač jakožto správce údajů odstranil z výsledků vyhledávání odkaz na webové stránky obsahující osobní údaje zjednodušeně řečeno z důvodu, že si subjekt údajů přeje, aby uvedené informace byly po určité době „zapomenuty“. Soudní dvůr dospěl k závěru, že subjekt údajů toto tzv. „právo být zapomenut“ má. Dle Soudního dvora i zpracování přesných údajů, které bylo původně v souladu se zákonem, se časem může stát neslučitelným se směrnicí 95/46 (tedy dnes GDPR), jestliže uvedené údaje již nejsou nezbytné pro účely, pro které byly shromažďovány nebo zpracovány. To platí zejména v případě, že se zdají nepřiměřenými či nepodstatnými s ohledem na uvedené účely a uplynulý čas. V takových případech má subjekt údajů právo, aby bylo zpracování jeho údajů ukončeno (v praxi půjde odstranění článku z webu či o odstranění odkazu z výsledků vyhledávání).[141] Přestože v teoretické rovině nelze závěrům Soudního dvora mnoho vytknout, z praktického hlediska se naplňování požadavků rozsudku – zejména v případě zmíněných internetových vyhledávačů – jeví jako poněkud problematické,

[141] Srov. rozsudek *Google Spain*, body 89-99.

obzvlášť vzhledem k upřesnění požadavků na tyto vyhledávače v rozsudku *GC*.[142] Z tohoto rozsudku vyplývá, že internetový vyhledávač má navíc povinnost před odstraněním odkazu posoudit, zda v daném případě není uvedení odkazu na předmětnou internetovou stránku v seznamu výsledků nezbytné za účelem výkonu práva uživatelů internetu na svobodu informací chráněného článkem 11 Listiny.[143]

Internetový vyhledávač se tedy nemůže rozhodnout sporné zpracování prostě ukončit, aby vyloučil jakékoliv případné porušení GDPR, nýbrž musí také posoudit, zda nad právy subjektu nepřeváží právo třetích osob na informace. Takové posouzení je samozřejmě zcela závislé na posouzení konkrétních okolností každého zpracování, přičemž je velmi obtížné si představit, jak taková posouzení mají provádět právě provozovatelé internetových vyhledávačů či sociálních sítí, kteří provádí miliardy automatických zpracování denně. Povinnost zajistit, že daným zpracováním nedochází k porušení GDPR, je s ohledem na to, že je třeba provozovatele vyhledávače považovat za správce údajů, zcela logická. Ovšem klást na něj v této souvislosti břemeno vážení protichůdných práv a zájmů subjektu údajů a „původního správce", tj. osoby, která na internet sporný obsah umístila, považuji za poměrně nešťastné a v praxi velmi obtížně proveditelné.

Stávající judikatura Soudního dvora ani čl. 17 odst. 1 písm. a) GDPR přitom blíže neupravuje konkrétní postup správce údajů v takových případech, např. co se týče důkazního břemene. Postačí v této souvislosti tvrzení subjektu údajů? Je potřeba umožnit vyjádření např. také původnímu správci? Do jaké míry musí provozovatel ověřovat správnost těchto tvrzení? Tyto otázky jsou v současné době předmětem sporu před Soudním dvorem ve věci *Google.*[144] Nelze než doufat, že Soudní dvůr zaujme alespoň trochu praktický přístup, a nebude vyžadovat, aby provozovatel internetového vyhledávače k věci přistupoval s pečlivostí srovnatelnou s vnitrostátním soudem, zejména co se týče ověřování skutkových tvrzení.

Jedním z případů, kdy se subjekt údajů svého práva být zapomenut dovolával neúspěšně, byl případ *Manni*, ve kterém se dřívější jednatel zkrachovalé společnosti domáhal, aby po určité době od likvidace společnosti z obchodního rejstříku odstraněny jeho osobní údaje. Byť Soudní dvůr právo nevyloučil, že v některých specifických případech subjekt údajů právo na výmaz údajů z obchodního rejstříku mít může, zcela rozumně konstatoval, že v zásadě

[142] Srov. rozsudek Soudního dvora ze dne 24. září 2019, *GC a další*, C-136/17, EU:C:2019:773.
[143] Ibidem, bod 68.
[144] Srov. řízení před Soudním dvorem ve věci C-460/20 *Google.* Předkládací rozhodnutí v této věci je dostupné na https://curia.europa.eu/.

bude nad zájmy subjektu údajů převažovat nezbytnost chránit zájmy třetích osob a potřeba zajistit právní jistotu.[145]

2.2.2.7 Povinnosti správce a zpracovatele

Ustanovení týkající se povinností správce a zpracovatele jsou oproti směrnici 95/46 v GDPR rozsáhlejší i detailnější. Základním stavebním kamenem je v tomto ohledu zásada záměrné a standardní ochrany osobních údajů (tzv. „*data protection by design and default*“, často také „*privacy by design*“), ze které zjednodušeně řečeno vyplývá obecná povinnost správce veškerá zpracování údajů od počátku plánovat a realizovat tak, aby bylo zpracováváno jen nezbytné množství osobních údajů, po nezbytnou dobu a aby tyto údaje nebyly zpřístupňovány neoprávněným osobám. Ruku v ruce s touto zásadou jdou i konkrétnější požadavky na zabezpečení údajů. Tato opatření mohou spočívat např. v pseudonymizaci, šifrování či pravidelném testování, posuzování a hodnocení účinnosti zavedených opatření, jakož i v oznamování porušení zabezpečení dozorovému úřadu či subjektu údajů. Obecně se může jednat o opatření jak technické (např. šifrování), tak organizační povahy (omezení přístupu zaměstnanců k údajům, školení zaměstnanců apod.). Společným jmenovatelem povinností správce a zpracovatele v GDPR je přístup založený na riziku, což mj. znamená, že se rozsah a povaha opatření, které správce musí přijmout, zpravidla odvíjí od rozsahu a povahy daného zpracování a souvisejících rizik.[146]

Účinným nástrojem zvýšení úrovně ochrany mohou být záznamy o činnostech zpracování, které čl. 30 GDPR ukládá vést organizacím s více než 250 zaměstnanci či provádějícím určitá z pohledu GDPR rizikovější zpracování. Lze očekávat, že povinnost zamyslet se nad každým prováděným zpracováním údajů a zaznamenat jeho základní charakteristiky bude mít pozitivní dopady zejména v případě správců, kteří až do přijetí GDPR nevěnovali otázce zpracování údajů jakoukoliv pozornost, a často povede k odstranění těch nejvážnějších excesů v této oblasti bez toho, aby byl třeba zásah dozorového úřadu.

Logickou nástavbou povinnosti záznamů o činnostech o zpracování je čl. 35 GDPR, který ukládá povinnost provádět posouzení vlivů zpracování na ochranu osobních údajů v případech, kdy je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Jelikož

---

[145] Srov. rozsudek Soudního dvora ze dne 9. března 2017, *Manni*, C-398/15, EU:C:2017:197.

[146] Povinnosti zabezpečení osobních údajů samozřejmě mohou vyplývat také z předpisů v oblasti kybernetické bezpečnosti, které se na některé správce mohou vztahovat. Tak tomu bude např. právě v případě poskytovatelů služeb elektronických komunikací, kterých se týká povinnost uchovávání provozních a lokalizačních údajů.

však určení takových zpracování nemusí vždy být na první pohled zřejmé, lze ocenit, že dozorovým úřadům byla uložena povinnost zveřejnit alespoň seznamy těch zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné. Nařízení také ukládá povinnost konzultovat s dozorovým úřadem situace, kdy z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko, které správce nezmírnil. Je však otázka, zda k takovým konzultacím bude reálně docházet, jelikož pravděpodobně povedou k tomu, že dozorový úřad neumožní takové zpracování provést.

Poslední novou významnou povinností, o které je vhodné se na tomto místě stručně zmínit, je povinnost jmenovat pověřence pro ochranu osobních údajů dle čl. 37-39 GDPR, tedy osobu, která bude v rámci organizace nezávisle dohlížet na dodržování nařízení a radit správci ohledně různých aspektů spojených s ochranou osobních údajů. Povinnost jmenovat pověřence GDPR ukládá veškerým orgánům veřejné moci a veřejným subjektům (bez ohledu na to, jaké údaje zpracovávají), jakož i dalším organizacím, které systematicky a ve velkém rozsahu monitorují fyzické osoby nebo které ve velkém rozsahu zpracovávají citlivé údaje. GDPR dále upravuje kvalifikační předpoklady pověřence, jeho postavení v rámci organizace a jeho hlavní úkoly, mezi které krom monitoringu souladu s nařízením a souvisejících konzultací patří také spolupráce s dozorovým úřadem a působení jako kontaktní místo pro subjekty údajů. Z hlediska ochrany osobních údajů by měl mít institut pověřence pozitivní dopady, už jen kvůli tomu, že organizaci donutí vyčlenit zaměstnance, který se bude dotčenou problematikou podrobněji zabývat. V případě, že by takový zaměstnanec ve firmě neexistoval, nevylučuje GDPR, aby byly služby pověřence zajišťovány externě.

Nové instituty zaváděné GDPR v oblasti povinností správce a zpracovatele je třeba hodnotit kladně. Platí však, že rozsah, ve kterém je plnění těchto povinností vyžadováno a vynucováno, by se měl v prvé řadě odvíjet od povahy daného zpracování a souvisejících rizik, stejně jako od technických a ekonomických možností správce. Jelikož takový přístup GDPR předpokládá, bude především na dozorových úřadech, jak se k této otázce postaví. Ty by přitom měly být velice transparentní a konkrétní ohledně toho, v případě jakých zpracování budou vyžadovat plnění jakých povinností. V opačném případě totiž budou správci nuceni spoléhat buď na sebe, nebo na různé poradenské společnosti, v jejichž zájmu často bude správce přesvědčit, že k zajištění souladu s GDPR je potřeba co nejvíce opatření, jejichž realizaci pro správce zajišťují. V této souvislosti je tedy třeba myslet na to, co uvedl generální advokát Bobek ve věci *Rigas Satiksme*:

„94. Není pochyb o tom, že ochrana osobních údajů má v digitálním věku prvořadý význam. Soudní dvůr je v čele vývoje judikatury v této oblasti a činí tak oprávněně.

95. V citovaných případech se však věrně odráží hlavní problém ochrany osobních údajů, kvůli němuž byla ochrana původně zavedena a musí být důsledně dodržována, a sice zpracovávání osobních údajů ve velkém měřítku pomocí mechanických, digitálních prostředků ve všech podobách, jako je například sestavování, správa a použití velkých datových souborů, předávání datových soborů pro jiné než legitimní účely, shromažďování a archivování metadat atd.

96. Stejně jako v jakékoli jiné oblasti práva musí být pravidla upravující určitou činnost dostatečně flexibilní, aby zahrnovala všechny možnosti, které by mohly vzniknout. Mohlo by to však vést k nebezpečí velmi širokého výkladu a uplatňování těchto pravidel. Výsledkem by mohlo být jejich uplatnění i v situaci, ve které je souvislost s původním účelem poněkud nejasná a diskutabilní. Velmi široké uplatnění a určitý „aplikační absolutismus" by mohly mít případně za následek rovněž diskreditaci původní myšlenky, která byla sama o sobě velmi důležitá a legitimní."

Plošné uchovávání komunikačních metadat pak představuje právě takový druh rozsáhlého zpracování osobních údajů, o kterém generální advokát hovoří v bodě 95 stanoviska. V případě uchovávání provozních a lokalizačních údajů by tak mělo být plnění povinností správce vyžadováno v maximální možné míře, zejména co se požadavků na jejich zabezpečení týče.

2.2.2.8 Předávání údajů do třetích zemí

Aby nebyla úroveň ochrany osobních údajů zajišťovaná v EU podstatně snížena předáním údajů do třetích zemí, stanoví GDPR, stejně jako před ním směrnice 95/46, pro taková předání poměrně přísné podmínky. GDPR obsahuje tři vzájemně subsidiární režimy, ve kterých k takovému předání může dojít. Prvním a rozhodně nejideálnějším případem je předání do takové třetí země, u níž Komise v prováděcím rozhodnutí dle čl. 45 GDPR konstatovala, že je v této zemi zajištěna odpovídající úroveň ochrany osobních údajů. Za odpovídající je přitom třeba považovat takovou úroveň ochrany, která sice není s tou unijní totožná, ale je alespoň rovnocenná.[147] V případě, že takové rozhodnutí neexistuje, je předání možné dle čl. 46 GDPR za podmínky, že správce nebo zpracovatel poskytl vhodné záruky, a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů. Ty mohou mít např. podobu standardních smluvních doložek vycházejících z prováděcího rozhodnutí Komise přijatého postupem dle čl. 93 odst. 2 GDPR, závazných podnikových pravidel dle čl. 47 GDPR,[148] kodexů chování schválených dozorovými úřady dle čl. 40

[147] Srov. rozsudek *Schrems*, bod 73.

[148] Jde o pravidla upravující předávání osobních údajů v rámci nadnárodní skupiny podniků, která podléhají schválení dozorovým úřadem. Srov. NULÍČEK, Michal et al. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář*, 2017, s. 390.

GDPR[149] apod. Nejsou-li žádné takové záruky poskytnuty, je předání možné na základě čl. 49 GDPR v rámci „výjimek pro specifické situace“. Těchto výjimek pro specifické situace nicméně GDPR připouští poměrně mnoho. Předání je tak možné např. v případě výslovného souhlasu poskytnutého na základě důkladného poučení o rizicích takového předání či v případě nezbytnosti pro účely plnění smlouvy.

V současnosti existuje 12 rozhodnutí o odpovídající úrovni ochrany, přičemž rozhodnutí konstatující adekvátní úroveň ochrany v USA bylo nedávno Soudním dvorem již podruhé zrušeno. Poprvé došlo ke zrušení rozhodnutí nazývaného Bezpečný přístav[150] v roce 2015 ve věci *Schrems*, v níž se žalobce domáhal, aby irský dozorový úřad zakázal společnosti Facebook Ireland předávat jeho osobní údaje do USA z důvodu, že v USA není zajištěna ochrana osobních údajů před sledováním orgány veřejné moci, přičemž se odvolával na informace poskytnuté Edwardem Snowdenem ohledně činnosti NSA. Soudní dvůr shledal dotčené rozhodnutí neplatným, jelikož jeho podmínky zavazovaly pouze příjemce údajů, nikoliv příslušné orgány USA. Příjemcům údajů navíc rozhodnutí dokonce výslovně umožňovalo upřednostnit požadavky příslušných orgánů USA v oblasti bezpečnosti státu, veřejného zájmu nebo prosazování zákonů před podmínkami rozhodnutí. V neposlední řadě nezajišťovalo rozhodnutí subjektům údajů jakékoliv účinné prostředky nápravy.[151] Rozhodnutí Soudního dvora bylo předmětem poměrně hojné akademické diskuze, v rámci které bylo zpravidla kvitováno. Někteří autoři nicméně vcelku legitimně poukazovali na skutečnost, že regulace přístupu zpravodajských služeb k osobním údajům nespadá působnosti unijního práva, které tak ani nemůže stanovit společný standard, se kterým by bylo možné právní úpravu USA porovnávat a ověřovat její odpovídající úroveň.[152] S tímto konstatováním lze souhlasit, nicméně vzhledem k tomu, že odchýlení se od zásad Bezpečného přístavu bylo předpokládáno za mnohem širším okruhem účelů a závěry Soudního dvora byly taktéž formulovány poměrně

[149] Jde o samoregulační dokumenty upřesňující uplatňování GDPR v rámci jednotlivých odvětví, které by měly vyplnit mezery a nejasnosti, které při zpracování osobních údajů v daném odvětví vznikají a potvrzují soulad určitých postupů s nařízením. Tyto kodexy se předkládají ke schválení dozorovému úřadu, přičemž GDPR pak se schválením kodexu spojuje určité právní následky, např. právě v oblasti předávání údajů do třetích zemí. Dohled nad dodržováním kodexu pak může být dozorovým úřadem svěřen určitým akreditovaným subjektům. Srov. NULÍČEK, Michal et al. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář*, 2017, s. 355.

[150] Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států (oznámeno pod číslem K(2000) 2441).

[151] Srov. rozsudek *Schrems*, body 79-106.

[152] AZOULAI, Loic a VAN DER SLUIS, Marijn. Institutionalizing personal data protection in times of global institutional distrusts: Schrems. *Common Market Law Review.* 2016, s. 1364-1367.

obecně, mám za to, že rozhodnutí Soudního dvora i ve světle této kritiky obstojí. Jedná se však o skutečnost, kterou je dobré mít na paměti, až budeme hovořit o dopadech unijní úpravy na zajišťování národní bezpečnosti v souvislosti s data retention.

Rozhodnutí Bezpečný přístav bylo v roce 2016 nahrazeno rozhodnutím Štít soukromí, které mělo zohledňovat výtky Soudního dvora.[153] V mezidobí však byli správci údajů nuceni využívat k předávání údajů do USA jiné tituly, např. standardní smluvní doložky vycházející z příslušného rozhodnutí Komise, což bylo případem mj. i společnosti Facebook.[154] Proti takovému předání podal Maxmilian Schrems opět stížnost, ve které namítal, že údaje předané společností Facebook jsou získávány orgány USA v rámci různých sledovacích programů způsobem neslučitelným s články 7, 8 a 47 Listiny, takže rozhodnutí o standardních smluvních doložkách nemůže být základem pro předávání těchto údajů do Spojených států.

Soudní dvůr ve věci *Facebook Ireland a Schrems* konstatoval, že ačkoliv v původním řízení byla zpochybněna platnost rozhodnutí o standardních smluvních doložkách, tak vzhledem k tomu, že se předkládající soud táže Soudního dvora obecně na ochranu, jaká musí podle článků 7, 8 a 47 Listiny být zajištěna v kontextu předávání osobních údajů do USA, je třeba zohlednit, že v mezidobí bylo přijato rozhodnutí o Štítu soukromí. Soudní dvůr jednak ve vztahu k úrovni ochrany zajištěné Štítem soukromí konstatoval, že právo USA nadále stanoví v souvislosti se zajišťováním bezpečnostních zájmů USA výjimky z ochrany osobních údajů, které neodpovídají požadavkům unijního práva. Problematickou shledal zejména obecnost sledovacích programů a absenci účinných prostředků nápravy pro subjekty údajů. Soudní dvůr proto rozhodnutí Štít soukromí prohlásil za neplatné.[155]

Soudní dvůr dále konstatoval, že nejsou dány důvody pro konstatování neplatnosti rozhodnutí Komise o standardních smluvních doložkách. Toto rozhodnutí totiž nebrání tomu, aby příslušný dozorový orgán zakázal předávání osobních údajů do třetí země, pokud požadavky unijního práva nemohou být v dané třetí zemi dodrženy v důsledku povinností vyplývajících z vnitrostátního práva.[156] Vzhledem k závěrům Soudního dvora k odpovídající úrovni ochrany je přitom zřejmé, že právě o takovou situaci se jedná v případě USA, takže do USA není možné údaje na základě standardních smluvních doložek předat.

---

[153] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající úrovni ochrany poskytované štítem EU–USA na ochranu soukromí (oznámeno pod číslem C(2016) 4176).
[154] Rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46.
[155] Srov. rozsudek *Facebook Ireland a Schrems*, body 168-202.
[156] Srov. ibidem, body 122-149.

Co se týče výtek Soudního dvora vůči rozhodnutí Štít soukromí, ty považuji za oprávněné. Na tomto rozhodnutí Soudního dvora však shledávám problematické to, že Soudní dvůr dovodil, že předání údajů na základě standardních smluvních doložek je taktéž podmíněno rovnocennou úrovní ochrany ve třetí zemi, což dle mého názoru nejenže nevyplývá z textu GDPR, ale ani z jeho systematiky. Předání na základě dodatečných záruk (kterými jsou právě např. standardní smluvní doložky) má být možné právě za situací, kdy neexistuje rozhodnutí o adekvátní ochraně. Z mého pohledu by tak smluvní doložky měly sloužit pro případy, kdy sice není možné zajistit úroveň ochrany ve vztahu k činnosti příslušných orgánů třetí země (tedy konstatovat odpovídající úroveň ochrany ve třetí zemi), ovšem i tak je vhodné, aby se správce či zpracovatel údajů alespoň sám zavázal dodržovat pravidla GDPR v rámci zpracování probíhajících ve třetí zemi. Přístupem Soudního dvora se rozdíly mezi oběma tituly pro předávání naprosto stírají, což je škoda, jelikož i ve standardních smluvních doložkách, přestože zavazují pouze soukromé subjekty a nikoliv orgány státu, lze spatřovat významnou přidanou hodnotu. Výsledkem přístupu Soudního dvora navíc může být, přinejmenším dočasně, naopak snížení úrovně ochrany předávaných údajů, jelikož k předávání bude docházet na základě souhlasu a bez dodatečných záruk. Samozřejmě lze namítat, že předávání na základě souhlasu jakožto „výjimka pro specifické situace“ nemůže plně nahradit ostatní tituly pro předávání, avšak vzhledem k tomu, že výslovné omezení počtu předání na základě souhlasu GDPR neobsahuje, lze předpokládat, že přinejmenším někteří správci takové řešení zvolí. Z hlediska nadpisu čl. 49 GDPR a systematiky GDPR by však takové řešení nemělo být považováno za správné.[157] Otázkou však je, zda v současnosti existuje z pohledu GDPR alternativa, která by nevedla k prakticky úplnému ochromení toků údajů mezi EU a USA.

2.2.2.9 Dozorové úřady

Klíčovým prvkem celého systému ochrany osobních údajů v EU byly již od přijetí směrnice 95/46 nezávislé dozorové úřady. Stejně jako dříve směrnice 95/46, i GDPR svěřuje ve svých čl. 57 a 58 dozorovým úřadům celou řadu úkolů a pravomocí za účelem jeho monitorování a uplatňování. Mezi ty nejdůležitější patří především pravomoc zabývat se stížnostmi subjektů údajů, provádět šetření a v případě zjištění porušení ukládat napomenutí, sankce či opatření k nápravě. Krom těchto pravomocí disponují úřady také řadou povolovacích, akreditačních

[157] Srov. European Data Protection Board. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 2020, s. 2. Pro odlišný pohled srov. např. VAN EIJK, Rob. Schrems II: Article 49 derogations may not be so narrow and restrictive after all? *Future of Privacy Forum*, 2021.

a konzultačních pravomocí, které však není nezbytné pro účely této práce detailněji rozebírat. GDPR nově vyžaduje, aby se dozorové úřady mohly v určitých případech souvislosti s porušením GDPR obrátit na soud.

Posledně zmíněná pravomoc má základ v rozsudku ve věci *Schrems*, ve kterém byly řešeny mj. i dopady rozhodnutí Komise o odpovídající úrovni ochrany na pravomoci dozorových úřadů. Soudní dvůr rozhodl, že i v případě existence takového rozhodnutí může dozorový úřad dospět k závěru, že předávání údajů není v souladu s právem Unie, a nařídit jeho skončení. Otázkou však bylo, jak lze v této situaci dospět k případnému zneplatnění rozhodnutí Komise, když neplatnost může konstatovat pouze Soudní dvůr. Soudní dvůr proto rozhodl, že v případech, kdy se dozorový orgán domnívá, že je rozhodnutí Komise neplatné, musí mít možnost obrátit se na vnitrostátní soud, který následně může podat předběžnou otázku.[158] V čl. 58 odst. 5 GDPR je v návaznosti na tento rozsudek uvedeno, že dozorový úřad musí mít pravomoc na porušení nařízení „*upozornit*" justiční orgány a „*ve vhodných případech*" zahájit Soudní řízení. Mám za to, že požadavek na zakotvení pravomoci dozorových úřadů zahájit řízení u soudu by měl být skutečně omezen jen na specifické případy, jako je právě např. právě potřeba posoudit platnost rozhodnutí Komise o odpovídající úrovni ochrany. Požadavek na zakotvení této pravomoci v obecné rovině by totiž vedl k situaci, kdy správní orgán, který je v určité věci oprávněn rozhodovat, má dle GDPR také „alternativní" možnost namísto svého rozhodnutí podat žalobu k vnitrostátnímu soudu, což z mého pohledu poměrně významně naráží na to, jak je v řadě členských států koncipován systém správního soudnictví.

Čl. 51-54 GDPR stanoví základní pravidla pro jmenování členů dozorových úřadů a výkon jejich funkce, mj. např. co se týče požadavků na jejich kvalifikaci. Klíčovou roli nicméně hrají především vysoké požadavky na nezávislost dozorových úřadů a jejich členů, které vycházejí mj. i z předchozí judikatury Soudního dvora, která vylučuje prakticky jakýkoliv dohled ze strany jiných orgánů státu, který by mohl vést byť jen k riziku ovlivnění činnosti úřadu.[159]

Klíčovou změnou oproti směrnici 95/46 bylo zavedení *one-stop shop* principu k příslušnosti dozorových úřadů v případě přeshraničních zpracování, tj. zpracování probíhajících v souvislosti s činností provozoven správce ve více členských státech či podstatně se dotýkající subjektů ve více členských státech. Pravidla směrnice 95/46 totiž umožňovala,

[158] Srov. rozsudek ve věci *Schrems*, body 51-66.
[159] Srov. rozsudek ze dne 9. března 2010, *Komise v. Německo*, C-518/07, EU:C:2010:125 či rozsudek ze dne 16. října 2012, *Komise v. Rakousko*, C-614/10, EU:C:2012:631.

aby vzhledem k témuž přeshraničnímu zpracování bylo příslušných i několik dozorových úřadů. K takovým případům přitom v praxi často docházelo, mj. s ohledem na široký výklad pojmu „v souvislosti s činností provozovny“ zastávaný Soudním dvorem a skutečnost, že ne všechny úřady v rámci EU byly při vynucování pravidel GDPR stejně aktivní, např. co se týče dceřiných společností amerických technologických gigantů sídlících v Irsku.[160] Takový stav nicméně zjevně neodpovídal harmonizačním cílům dotčené úpravy, a proto čl. 56 GDPR obsahuje pravidla pro určení jednoho hlavního dozorového úřadu. Čl. 60 GDPR pak obsahuje pravidla pro to, aby se do jeho rozhodovací činnosti mohly zapojit další dotčené úřady. Případy před Soudním dvorem nicméně ukazují, že pro některé dozorové úřady bude těžké takové rozložení příslušnosti akceptovat, zejména právě co se týče zpracování společnostmi jako jsou Google či Facebook. Např. belgický dozorový úřad se nedávno pokusil dotčená pravidla příslušnosti obejít tím, že namísto výkonu své správní pravomoci podal proti společnosti Facebook žalobu u vnitrostátního soudu.[161] Akceptovat takový přístup by však znamenalo otevřít prostor pro obcházení *one-stop shop* principu, a tudíž značně oslabit jeden z klíčových nových institutů GDPR. Proto nelze než doufat, že Soudní dvůr rozhodne, že dotčená pravidla příslušnosti se vztahují i na případy, kdy se dozorový úřad rozhodne obrátit na soud.

Novinkou v GDPR je také zřízení Evropského sboru pro ochranu osobních údajů tvořeného zástupci dozorových úřadů z jednotlivých členských států a evropského inspektora ochrany údajů, jehož cílem je právě přispívat k jednotnému uplatňování GDPR v EU, např. vydáváním pokynů k jeho výkladu, kterých již byla vydána celá řada.[162] Tuto funkci v minulosti plnila Pracovní skupina zřízená dle čl. 29 směrnice 95/46, kterou Evropský sbor pro ochranu osobních údajů nahradil.

2.2.2.10 Odpovědnost a sankce

GDPR v neposlední řadě stanoví pravidla pro uplatňování odpovědnosti za jeho porušení. Subjekt údajů má v případě porušení GDPR v prvé řadě právo podat stížnost k dozorovému úřadu (čl. 77 GDPR), jakož i právo na soudní přezkum rozhodnutí o takové stížnosti (čl. 78 GDPR). GDPR dále stanoví právo subjektu údajů domáhat se odpovědnosti za porušení GDPR soudní cestou přímo proti správci nebo zpracovateli (čl. 79 GDPR). Ti jsou pak odpovědni mj. za majetkovou i nemajetkovou újmu způsobenou porušením jejich povinností (čl. 82

[160] Srov. rozsudek *Wirtschaftsakademie Schleswig-Holstein*, body 45-64.
[161] Srov. řízení před Soudním dvorem ve věci C-645/19 *Facebook Ireland a další.* Předkládací rozhodnutí v této věci je dostupné z https://curia.europa.eu/.
[162] Tyto pokyny jsou k dispozici na https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en.

GDPR). GDPR v neposlední řadě upravuje také problematiku ukládání sankcí dozorovými úřady. Ty mohou nově dosahovat výše až 20 000 000 EUR či 4 % celosvětového ročního obratu podniku (čl. 83 GDPR).

2.2.3 Směrnice 2016/680

Jak bylo uvedeno výše, v okamžiku přijímání směrnice 95/46 nemělo Společenství pravomoc přijímat předpisy regulující zpracování osobních údajů jako takové. Směrnice 95/46 tak musela být přijata na „tržně-harmonizačním" právním základě, kterým byl tehdejší čl. 100a SES, později nahrazený čl. 95 SES.[163] To sice nezabránilo Soudnímu dvoru, aby působnost směrnice vykládal velice široce a vztáhnul ji i na situace, ve kterých nebyl žádný přeshraniční či obchodní prvek přítomen.[164] Avšak co se týče činnosti státních orgánů v oblasti trestního práva či národní bezpečnosti, byly výjimky z působnosti směrnice 95/46 formulovány poměrně jednoznačně, a není tedy divu, že Soudní dvůr již ve své ranné judikatuře uznal, že na tyto oblasti se směrnice 95/46 nevztahuje.[165] Základním harmonizačním prvkem v této oblasti proto byla pouze Úmluva 108, resp. Doporučení R (87) 15. V praxi se proto jednalo o značně fragmentovanou oblast.[166]

Požadavek na společnou úpravu této problematiky alespoň prostřednictvím nástrojů tehdejšího třetího pilíře byl ze strany Evropského parlamentu vznesen již v roce 2003, a následně zopakován v rámci legislativního procesu vedoucího k přijetí směrnice 2006/24 upravující problematiky data retention.[167] K přijetí tohoto nástroje nicméně nedošlo. Potřeba takového opatření nicméně zjevně narůstala spolu s mírou spolupráce v této oblasti. Tato spolupráce totiž byla ve značné míře založena právě na sdílení a předávání osobních údajů mezi příslušnými orgány členských států. Důležitým krokem v tomto ohledu tak bylo přijetí rámcového rozhodnutí 2008/977/JHA. Toto rozhodnutí přenášelo některé klíčové principy obsažené ve směrnici 95/46 i na oblast policejní a justiční spolupráce. Stále se však nevztahovalo na činnost příslušných orgánů mimo rámec této spolupráce, tedy v rámci běžného plnění jejich úkolů.[168]

Klíčovým krokem směrem ke společné úpravě této problematiky byl čl. 16 odst. 2 SEU ve znění Lisabonské smlouvy, díky kterému získala Unie obecnou pravomoc přijímat pravidla

---

[163] Viz kapitola 2.1.2.2.
[164] Viz kapitola 2.2.2.3.
[165] Srov. rozsudek *Lindqvist*, bod 43.
[166] Srov. SAJFERT, Juraj a QUINTEL, Teresa. *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, 2017, s. 2.
[167] PAJUNOJA, Lauri. *The Data Protection Directive on Police Matters 2016/680 protects privacy – The evolution of EU´s data protection law and its compatibility with the right to privacy*, 2017, s. 50.
[168] Srov. čl. 1 rozhodnutí 2008/977/SVV.

pro zpracování osobních údajů v oblastech spadajících do působnosti unijního práva. Že však pravděpodobně nebude na místě jedno společné řešení pro všechny tyto oblasti, naznačovala již deklarace č. 21 připojená k Lisabonské smlouvě, dle které „*Konference uznává, že zvláštní pravidla pro ochranu osobních údajů a volný pohyb těchto údajů v oblastech justiční spolupráce v trestních věcech a policejní spolupráce, založená na článku 16b Smlouvy o fungování Evropské unie, by se mohla vzhledem ke specifické povaze těchto oblastí ukázat jako nezbytná.*“ V roce 2012 pak Komise spolu s návrhem GDPR předložila také samostatný návrh směrnice regulující zpracování osobních údajů příslušnými orgány v oblasti trestního práva, která měla nahradit rámcové rozhodnutí 2008/977/JHA. Na rozdíl od tohoto rámcového rozhodnutí však návrh směrnice neupravoval pouze oblast přeshraniční spolupráce, ale zpracování osobních údajů příslušnými orgány obecně. Přestože s ohledem na citlivost dané oblasti nebyl legislativní proces snadný,[169] byla směrnice následně – byť s podstatnými změnami oproti původnímu návrhu – přijata jako součást balíčkového kompromisu spolu s GDPR.[170]

Směrnice 2016/680 bývá velice často označována za *lex specialis* vůči GDPR,[171] což však nepovažuji za úplně přesné, jelikož upravuje oblast, která je z působnosti GDPR vyňata. Nelze proto hovořit o subsidiární aplikaci GDPR jakožto obecného předpisu. Z tohoto důvodu nejde o stejný vztah speciality, jaký existuje např. mezi GDPR a směrnicí 2002/58. Výše uvedené nic nemění na tom, že základní definice, pravidla a principy obsažené ve směrnici 2016/680 jsou skutečně velice podobné těm v GDPR. Tato kapitola se tak bude soustředit spíše na ty aspekty, ve kterých se směrnice 2016/680 od GDPR liší.

Mohlo by se zdát, že směrnice 2016/680 z hlediska zaměření této práce vyžaduje podstatně podrobnější zkoumání než GDPR či směrnice 2002/58, jelikož se na rozdíl od GDPR týká přímo oblasti trestního práva. Opak je však pravdou, jelikož směrnice 2016/680 reguluje pouze činnost příslušných orgánů, tj. následné zpracování komunikačních metadat po jejich předání poskytovateli služeb. Jak však bude vidět v následujících kapitolách, v souvislosti s data retention jsou nejvíce kontroverzní právě otázky uchovávání komunikačních metadat poskytovateli služeb, resp. podmínky předání těchto údajů příslušným orgánům. Jak

[169] Srov. GUILD, Elspeth a CARRERA, Sergio. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. *CEPS Liberty and Security in Europe Papers*, 2014, s. 10.
[170] Srov. LEISER, Mark a CUSTERS, Bart. The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680. *European Data Protection Law Review*, 2019, s. 368.
[171] Srov. např. HUDOBNIK, Matthias. Data protection and the law enforcement directive: a procrustean bed across Europe? *ERA Forum*, 2020, s. 486 či QUINTEL, Teresa. Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive, *European Data Protection Law Review*, 2018, s. 104.

problematika uchovávání těchto údajů, tak problematika přístupu příslušných orgánů k těmto údajům, je pak v judikatuře zkoumána primárně optikou předpisů bývalého prvního pilíře, zejména směrnice 2002/58.[172] To však neznamená, že by pravidla směrnice 2016/680 mohla být v této souvislosti zcela ignorována, jelikož záruky týkající se následného zpracování provozních a lokalizačních údajů příslušnými orgány jsou důležité pro posouzení přiměřenosti systému data retention jako celku. To ostatně potvrzuje např. judikatura ESLP, která otázku záruk proti zneužití v oblasti nakládání příslušných orgánů s osobními údaji často klade do popředí přezkumu přiměřenosti režimů skrytého sledování.[173]

První důležitý rozdíl mezi směrnicí 2016/680 a GDPR je jejich právní forma. Činnost příslušných orgánů v oblasti trestního práva je stále poměrně citlivou oblastí, v níž členské státy nebyly ochotny přijmout unijní regulaci ve formě nařízení. Důsledkem tohoto přístupu však je, že ve vnitrostátním právu členských států budou pravděpodobně existovat tři odlišné režimy ochrany osobních údajů. První režim bude představovat GDPR a vnitrostátní předpisy na něj navazující. Jak bylo uvedeno výše, GDPR je nařízením, které vyžaduje ještě poměrně značné množství adaptační práce. Samotná pravidla GDPR, jako jsou např. příslušné definice, však do vnitrostátního práva převáděny být nesmí, a příslušné vnitrostátní předpisy tak bez současného čtení GDPR pravděpodobně nebudou dávat příliš velký smysl. Druhým režimem bude režim transponující směrnici 2016/680, v rámci kterého musí být všechna potřebná pravidla, včetně definic, která jsou navíc ve značné míře podobná těm z GDPR, přenesena do vnitrostátního právního řádu.[174] Posledním režimem je režim zpracování osobních údajů v oblasti národní bezpečnosti, ve které se unijní právo neuplatní. Existence těchto tří paralelních režimů může být značně matoucí pro adresáty příslušných právních předpisů, obzvlášť v případech, kdy jsou všechny tři režimy zpracování upraveny v jednom vnitrostátním právním předpise, jak je tomu v ČR.[175]

Zároveň je třeba říct, že ne za každé situace budou hranice působnosti směrnice 2016/680 zcela jasné, a to z „obou stran“, tedy jak vzhledem k GDPR, tak vzhledem k vnitrostátním předpisům upravující zpracování osobních údajů v oblasti národní bezpečnosti. Činnosti příslušných orgánů se v členských státech mohou různě prolínat a v některých hraničních oblastech jako jsou např. kontrola ilegální migrace, boj proti daňovým únikům či boj

[172] Viz kapitola 4.1.2.
[173] Viz kapitola 4.2.2.4.
[174] Nutno dodat, že některé vnitrostátní transpoziční právní úpravy, včetně té české, v této souvislosti toliko odkazují na definice GDPR, které jsou totožné s těmi ve směrnici 2016/680.
[175] Zákon č. 110/2019 Sb. o zpracování osobních údajů.

proti praní špinavých peněz nemusí být vždy zcela jisté, které orgány by měly spadat ještě do režimu GDPR, a které již do působnosti policejní směrnice. V praxi se tak orgány, které se v jednom členském státě řídí GDPR, mohou v jiném členském státě řídit pravidly směrnice, a naopak.[176] Totéž platí pro boj proti terorismu, kde zase dochází ke smazávání rozdílů mezi oblastí boje proti trestné činnosti a oblastí zajišťování národní bezpečnosti. Kapitola sama o sobě jsou případy, kdy jsou údaje předávány z jednoho režimu do druhého, příp. uchovávány v jednom režimu za účelem budoucího předání do režimu druhého. Přesně to je i případ data retention, kdy poskytovatelé telekomunikačních služeb, jež zpravidla budou podléhat GDPR a směrnici 2002/58, uchovávají údaje za účelem jejich předání příslušným orgánům, a to jak těm působícím v oblasti trestního práva, tak těm zajišťujícím národní bezpečnost. Tato problematika byla v judikatuře Soudního dvora týkající se data retention podrobně řešena, přičemž závěry Soudního dvora budou analyzovány a komentovány v následujících kapitolách.[177] V neposlední řadě je třeba upozornit, že i na orgány členských států činné v oblasti trestního práva se směrnice 2016/680 použije pouze v rozsahu plnění jejich úkolů v této oblasti. Ostatní činnosti těchto orgánů, jako např. personální agenda, budou spadat do působnosti GDPR.

S rozdíly v právní formě obou předpisů souvisí i rozdílná míra harmonizace, kterou tyto předpisy zavádějí. Zatímco GDPR je nařízením, které zavádí v zásadě maximální harmonizaci s cílem zajistit rovnocennou úroveň ochrany fyzických osob, a tím mj. odstranit překážky bránící pohybu osobních údajů v rámci Unie, směrnice 2016/680 představuje dle svého čl. 1 odst. 3 pouze harmonizaci minimální. Nebrání tak tomu, aby členské státy v souvislosti se zpracováním osobních údajů příslušnými orgány v oblasti trestního práva stanovily přísnější pravidla, samozřejmě za podmínky, že tato pravidla nebudou bránit výměně informací, kterou v této oblasti požadují jiné unijní předpisy (viz čl. 1 odst. 2 směrnice).

Definice základních pojmů i zásady zpracování jsou ve směrnici 2016/680 obsaženy v čl. 3 a 4 a jsou prakticky totožné s těmi v GDPR. Údaje musí být zpracovány korektně a zákonným způsobem, za legitimním, výslovně vyjádřeným účelem a v míře odpovídající tomuto účelu. Musí být pokud možno přesné a aktualizované a musí být adekvátně zajištěna jejich bezpečnost. Stejně jako v případě GDPR musí být správce schopen dodržení těchto zásad

[176] CARUANA, Mireille. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology*, 2019, s. 253.
[177] Viz kapitola 4.1.2.

doložit. V určitých případech jsou tyto zásady ještě konkretizovány prostřednictvím specifických pravidel, např. povinnosti pravidelně přezkoumávat dobu uložení údajů či pravidelně ověřovat jejich kvalitu. Čl. 6 a 7 směrnice dále ukládají povinnost v rámci zpracování rozlišovat mezi jednotlivými kategoriemi subjektů údajů (např. mezi svědky a obviněnými) jakož i povinnost rozlišovat osobní údaje založené na faktech od údajů založených na subjektivních hodnoceních. To nemusí vždy být zcela snadné, jelikož se povaha subjektů údajů i samotných údajů může v průběhu trestního řízení měnit. Z podezřelého se může stát svědek a svědecká výpověď, která byla považována za fakt, se může stát spíše subjektivním hodnocením situace.[178] Takové rozlišování je tak požadováno pouze v rozsahu, v jakém je to v daném kontextu možné.

Směrnice 2016/680 obsahuje stejně jako GDPR specifická pravidla pro zacházení se speciálními kategoriemi údajů (resp. s citlivými údaji), které mohou být dle jejího čl. 10 zpracovány pouze tehdy, je-li to zcela nezbytné pro sledované účely, v případě potřeby ochrany životně důležitých zájmů subjektu údajů nebo jedná-li se o údaje zjevně zveřejněné subjektem údajů. Na rozdíl od GDPR čl. 11 směrnice zcela nezapovídá, aby bylo na zpracování zvláštních kategorií údajů založeno automatizované rozhodování, jsou-li v daném případě přijata vhodná doprovodná opatření a nevede-li takové automatické rozhodování k diskriminaci. Vždy však musí být zajištěno právo subjektu údajů na lidský zásah předtím, než bude přijato rozhodnutí, jež má pro něj nepříznivé právní účinky či se ho jinak významně dotýká.

Na rozdíl od GDPR umožňuje směrnice pouze jeden titul pro zpracování osobních údajů, a tím je plnění úkolů v oblasti prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, v rozsahu nezbytném pro tyto účely a pokud má základ v právu Unie nebo členského státu.

Směrnice 2016/680 stejně jako GDPR zakotvuje v čl. 12-18 právo subjektu údajů na informace o zpracování, přístup k údajům, jejich opravu a výmaz. Jelikož výkon těchto práv bude v řadě případů způsobilý nepříznivě ovlivnit účel zpracování, obsahují příslušná ustanovení i konkrétnější povahu možných omezení výkonu těchto práv, aby bylo možné takovým nepříznivým důsledkům předejít.[179] Nicméně platí, že subjekt údajů musí mít ve všech případech, kdy dojde k omezení jeho práv vyplývajících ze směrnice, minimálně možnost podat

[178] Srov. LEISER, Mark a CUSTERS, Bart. The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680. *European Data Protection Law Review*, 2019, s. 368.
[179] Srov. čl. 12-18 směrnice 2016/680.

stížnost u dozorového úřadu nebo žádat soudní ochranu. Např. v případě nesdělení důvodů pro odmítnutí poskytnutí informací o zpracování (včetně informace, zda k němu vůbec dochází, či nikoliv) je však potenciál pro efektivní výkon těchto práv poměrně nízký. Směrnice nicméně na tyto případy pamatuje, a vyžaduje, aby členské státy stanovily povinnost příslušných orgánů zdokumentovat důvody odmítnutí a zpřístupnit je dozorovým úřadům. Subjekty údajů pak dle směrnice mají mít možnost vykonávat výše uvedená práva prostřednictvím dozorových úřadů, s tím, že příslušný dozorový úřad musí subjekt údajů informovat vždy přinejmenším o tom, že provedl přezkum a neshledal porušení, jakož i o možnosti obrátit se na soud. S ohledem na vysokou úroveň nezávislosti dozorových úřadů by mohlo být zajišťování práv subjektu údajů tímto způsobem velmi efektivním nástrojem kontroly příslušných orgánů, avšak pro hodnocení jeho účinnosti bude třeba ještě vyčkat na konkrétnější informace o jeho fungování v praxi.

Také co se povinností správce a zpracovatele týče, přebírá směrnice 2016/680 z velké části pravidla GDPR, včetně nově zaváděných institutů jako je povinnost jmenovat pověřence pro ochranu osobních údajů (čl. 32-33 směrnice), povinnost provádět posouzení vlivů na ochranu osobních údajů (čl. 27 směrnice), povinnost zavést vhodná technická a organizační opatření k zabezpečení údajů či hlásit případy porušení zabezpečení dozorovému úřadu či subjektu údajů (čl. 29-31 směrnice). Nad rámec GDPR čl. 25 směrnice 2016/680 výslovně zavádí povinnost vést záznamy (tzv. *logy*) o téměř veškerých operacích v rámci zpracování, přičemž v případě operací spočívajících v nahlédnutí a sdělení údajů musí tyto logy umožňovat zjištění důvodů těchto operací, datum a čas, kdy byly učiněny, a je-li to možné, totožnost osoby, která do osobních údajů nahlédla nebo která je zpřístupnila. Opět lze konstatovat, že v případě správného provedení a vynucování půjde o velmi efektivní nástroj, jak snížit rizika neoprávněného zpracování, která jsou z hlediska zajišťování přiměřenosti systémů data retention velice důležitá.

Zatímco podmínky sdílení údajů mezi příslušnými orgány členských států upravují speciální předpisy, podmínky předávání osobních údajů do třetích států a mezinárodních organizací jsou obsaženy v čl. 35-40 směrnice 2016/680. Stejně jako GDPR, i směrnice 2016/680 obsahuje několik vzájemně subsidiárních režimů předávání, které se v zásadě kryjí s těmi dle GDPR. Primárně je možné údaje předávat do třetích států či mezinárodních organizací, u nichž Komise konstatovala existenci adekvátní úrovně ochrany. Žádné takové

rozhodnutí však doposud přijato nebylo, takže tento titul pro předávání využíván být nemůže.[180] Dále je možné předávat údaje na základě existence vhodných záruk, které mohou být stanoveny právně závazným nástrojem (na rozdíl od případů zpracování dle GDPR zde půjde zpravidla o smlouvy o mezinárodní spolupráci), ale také pouze konstatovány na základě správcova posouzení všech okolností daného předání. V takových případech však musí být informován dozorový úřad. Konečně je možné předávat i na základě výjimek pro tzv. specifické situace. Ty jsou přitom definovány poměrně volně – krom pochopitelných situací, kdy je takové předání nezbytné k ochraně životně důležitých zájmů subjektu údajů nebo jiné osoby, může jít i o situace, kdy je takové předání jednoduše nezbytné pro účely prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. V těchto případech je sice předání podmíněno vážením veřejného zájmu na předání a práv subjektu údajů, avšak toto vážení provádí sám správce. Dozorovému úřadu je dokumentace související s těmito případy předání poskytována pouze na jeho žádost.

Co se týče dozorových úřadů obecně, požadavky na jejich nezávislost a způsob jejich ustavení se v zásadě neliší od pravidel GDPR. Směrnice 2016/680 také umožňuje, aby dozor v režimu GDPR i směrnice prováděl stejný úřad, přičemž lze očekávat, že ve většině členských států bude zvoleno právě takové řešení. Konkrétní pravomoci dozorových úřadů se pak podobají těm v GDPR, s tím, že jsou zohledněna určitá specifika dané oblasti. Co se týče vyšetřovacích pravomocí, zatímco např. v režimu GDPR mají dozorové úřady pravomoc „*získat přístup do všech prostor, v nichž správce a zpracovatel působí, včetně přístupu k veškerému zařízení a prostředkům určeným ke zpracování údajů*“, v případě směrnice 2016/680 takto silná pravomoc chybí a je pouze vyžadováno, aby měl dozorový úřad pravomoc „*získat od správce a zpracovatele přístup ke všem zpracovávaným osobním údajům a k veškerým informacím, které potřebuje k plnění svých úkolů*.“ Stejně tak i nápravné pravomoci dozorových úřadů nejsou tak široké vzhledem k citlivosti dané oblasti, i přesto si však dozorové úřady ponechaly důležitou pravomoc nařídit správci či zpracovateli provést opravu nebo výmaz osobních údajů či omezení zpracování. V režimu směrnice 2016/680 se dále logicky neuplatní princip *one-stop shop*, nicméně i zde jsou stanovena určitá pravidla

[180] V této souvislosti je možná vhodné zmínit Dohodu mezi Spojenými státy americkými a Evropskou unií o ochraně osobních informací v souvislosti s prevencí, vyšetřováním, odhalováním a stíháním trestných činů, která vstoupila v platnost roku 2017. Tato dohoda stanoví rámec pro ochranu osobních údajů při jejich předávání mezi Spojenými státy americkými a EU (resp. členskými státy), avšak sama o sobě neslouží jako titul pro takové předávání.

pro vzájemnou spolupráci dozorových úřadů z různých členských států, jež zahrnuje zejména žádosti o informace a opatření v oblasti dozoru, například žádosti o provedení konzultací, inspekcí a šetření.

Závěrem lze konstatovat, že ačkoliv jsou pravidla směrnice 2016/680 v mnoha ohledech mírnější oproti GDPR s ohledem na specifika regulované oblasti, nelze pochybovat o tom, že při řádné implementaci půjde o naprosto zásadní nástroj ke zvýšení ochrany osobních údajů při jejich zpracování orgány činnými v oblasti trestního práva. Vyzdvihnout lze v tomto ohledu především povinnosti zabezpečení údajů, jmenování pověřence, vedení *logů* a zapojení dozorových úřadů v případech, kde dochází k omezení práv subjektu údajů.

2.3 Ochrana soukromí v elektronických komunikacích v sekundárním právu EU

Již v polovině devadesátých let se k obecné komunitární právní úpravě na ochranu osobních údajů přidala také speciální právní úprava pro ochranu soukromí v oblasti elektronických komunikací. Tato právní úprava jednak stanovila některá pravidla týkající se zpracování osobních údajů při poskytování služeb elektronické komunikace, ale zároveň upravovala i jiné otázky související s problematikou práva na soukromí, jako např. otázky týkající se způsobu vyúčtování, obtěžujících telefonních hovorů či e-mailového spamu. Pro účely této práce je právní úprava ochrany soukromí v elektronických komunikacích důležitá z důvodu, že právě v ní se poprvé objevila možnost členských států zavést do svých vnitrostátních právních řádů data retention. Pro přezkum vnitrostátních právních úprav data retention jsou navíc unijní předpisy v této oblasti klíčové dodnes.

2.3.1 Směrnice 97/66

Ačkoliv do masivního rozmachu internetové komunikace zbývalo ještě pár let, již na konci osmdesátých let bylo zjevné, že budoucnost komunikace leží v její digitalizaci. Ta však s sebou nesla pro uživatele telekomunikačních služeb nejen výhody (např. co se týče možnosti položkového vyúčtování, zjištění čísla volajícího, zpětného volání apod.), ale také určitá rizika pro jejich soukromí, spojená zejména s tím, jak snadné je data v digitální podobě ukládat a analyzovat.[181] Proto Komise, která počítala s velkým rozmachem digitalizace telekomunikací v první polovině devadesátých let, předložila v roce 1990 spolu s návrhem směrnice 95/46 i návrh další směrnice, který byl později přijat jako směrnice 97/66 o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací.

[181] European Commission. *Proposal for a Council directive concerning the protection of personal data and privacy in the context of public digital telecomunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks – Explanatory memorandum*, 1990, s. 82.

Cílem této směrnice bylo dle jejího čl. 1 odst. 2 „*upřesnit a doplnit*“ pravidla směrnice 95/46 pro sektor telekomunikací. Směrnice souvisela spíše se širší problematikou soukromí než s problematikou ochrany osobních údajů, a reagovala tak na některá specifická rizika, která z různých důvodů nebyla dostatečně zohledněna směrnicí 95/46. Směrnice 97/66 v prvé řadě stanovila povinnost členských států zajistit důvěrný charakter sdělení přenášených skrze tyto sítě, zejména tím, že zakážou zachycování těchto sdělení bez souhlasu dotčených uživatelů či jiného zákonného podkladu (čl. 5 směrnice). Krom obsahu sdělení směrnice upravovala i nakládání komunikačními metadaty, s ohledem na tehdejší stav technologií zatím pouze ve formě provozních údajů a údajů nezbytných pro vyúčtování (čl. 6 směrnice). Ty s výjimkou případů, kdy bylo jejich uchování nezbytné pro vyúčtování (a příp. vymáhání souvisejících nároků) či marketing (ovšem pouze se souhlasem uživatele) měly být smazány po ukončení hovoru. Směrnice také v čl. 7 zakotvila právo uživatelů na vyúčtování bez podrobného rozpisu položek (aby nebyla zjevná jednotlivá volaná čísla) a s určitými výjimkami i právo při volání znemožnit identifikaci volající linky (tj. telefonovat anonymně). Směrnice zároveň zakazovala nevyžádaná marketingová sdělení prostřednictvím automatických telefonních přístrojů či faxu (čl. 12 směrnice).

Věcná působnost směrnice 97/66 byla omezená podobně jako v případě směrnice 95/46 tak, že se dle jejího čl. 1 odst. 3 její pravidla neuplatnila mj. na činnosti stanovené v hlavách V a VI tehdejší SEU, a v žádném případě na činnosti týkající se veřejné bezpečnosti, obrany, bezpečnosti státu a činnosti státu v oblasti trestního práva. Příslušný bod odůvodnění v této souvislosti dodával, že se směrnice nedotýká práva členských států provádět zákonné odposlechy telekomunikace za těmito účely. Po vzoru čl. 13 směrnice 95/46 (dnešní čl. 23 GDPR) obsahovala i směrnice 97/66 ustanovení umožňující omezit práva a povinnosti z ní vyplývající, včetně povinností poskytovatele služeb spočívajících v zajištění důvěrnosti komunikace, jsou-li taková opatření nezbytná k zajištění národní bezpečnosti, obrany, veřejné bezpečnosti, prevence, vyšetřování, odhalování a stíhání trestných činů (čl. 14 směrnice).

Problémem směrnice 97/66 bylo, že kvůli nezvykle dlouhému legislativnímu procesu a rapidnímu technologickému rozvoji v mezidobí byla již v okamžiku svého přijetí zastaralá.[182] Hlavní potíž představoval rozsah směrnicí pokrytých technologií, který odpovídal situaci na počátku devadesátých let. Směrnice totiž mířila především na digitální hovory činěné

[182] PAPAKONSTANTINOU, Vagelis a DE HERT, Paul. The amended eu law on eprivacy and electronic communications after its 2011 implementation; new rules on data protection, spam, data breaches and protection of intellectual property rights. *Marshall Journal of Computer and Information Law*, 2011, s. 40.

prostřednictvím tradičních obvodů veřejné telefonní sítě, příp. na tzv. „vytáčené“ internetové připojení. Směrnice 97/66 proto byla následně nahrazena směrnicí 2002/58, jejímž hlavním cílem bylo rozšířit pravidla směrnice 97/66 na jakékoliv veřejně dostupné služby elektronických komunikací ve veřejných komunikačních sítích.

2.3.2 Směrnice 2002/58

Cílem směrnice 2002/58 nebylo změnit základní pravidla zavedená směrnicí 97/66, ale pouze tato pravidla rozšířit na nové prostředky elektronické komunikace, a tím zajistit technologickou neutralitu těchto pravidel. Proto tam, kde směrnice 97/66 hovořila o telekomunikačních službách, hovoří směrnice 2002/58 o službách elektronické komunikace. Tam, kde směrnice 97/66 hovořila o nevyžádaných hovorech, hovoří směrnice 2002/58 o nevyžádaných sděleních apod. Podstata pravidel však zůstala zpravidla stejná, pouze přizpůsobená širší věcné působnosti směrnice.

Směrnice však obsahovala několik dalších, pro účely této práce významných změn a upřesnění. V prvé řadě směrnice explicitně uvádí, že pravidla o důvěrnosti sdělení a zákazu zachytávání se nevztahují pouze na samotný obsah sdělení, ale taktéž na provozní údaje, které definuje jako „*jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování*“. Směrnice dále definuje lokalizační údaje jako „*jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací*“. Důvodem pro tuto definici je skutečnost, že některé (zpravidla přesnější) lokalizační údaje neslouží pro účely přenosu sdělení, ale k poskytování některých dalších služeb (např. navigace, předpověď počasí apod.), a nelze je proto považovat za provozní údaje. Zpracování těchto lokalizačních údajů směrnice povoluje pouze se souhlasem uživatele a v míře nezbytné pro poskytování tohoto druhu služeb. Směrnice dále upravovala některé z tehdejšího pohledu nové fenomény spojené s nástupem internetu, jako např. *cookies*[183], jejichž použití bylo povoleno pouze za podmínky, že dotčené osoby byly jasně a úplně informovány v souladu se směrnicí 95/46/ES a že mohly jejich použití odmítnout. Tento *opt-out* režim byl však při následné revizi směrnice změněn na režim *opt-in* v případě *cookies*, jejichž použití není možné odůvodnit

[183] Datové soubory malé velikosti, které jsou při návštěvě webové stránky bez aktivního jednání ze strany uživatele ukládány do prohlížeče zařízení. Odtud pak s jejich pomocí dochází ke shromažďování různých dat o uživateli, mezi jinými i dat o jeho chování na internetu. Data získaná pomocí cookies jsou využívána jednak k samotnému poskytnutí internetové služby, resp. k usnadnění jejího dalšího užívání (např. využívání emailu, automatického přihlašování či předvyplnění některých údajů při online nákupu), ale také pro vytváření jakéhosi profilu uživatele internetu, pomocí kterého lze daleko účinněji cílit reklamu. Viz např. KOPEČKOVÁ, Andrea. Právní povaha cookies. *Epravo.cz*, 2015.

např. oprávněným zájmem na funkčnosti webové stránky. Vhodnost takového řešení je však v současnosti velmi zpochybňována, jelikož vyžadování souhlasu na téměř každé webové stránce vede k tzv. souhlasovému vyčerpání („*consent fatigue*"), tj. stavu, kdy jsou souhlasy beztak bezmyšlenkovitě udělovány.

Pro účely této práce jsou klíčové především čl. 1 odst. 3, čl. 5 a čl. 15 směrnice 2002/58. Co se týče čl. 1 odst. 3 směrnice, ten vymezuje působnost směrnice mj. vzhledem k „bezpečnostním" činnostem členských států. Dle tohoto ustanovení se tak se směrnice 2002/58 nevztahuje mj. na „*činnosti, které nespadají do oblasti působnosti Smlouvy o založení Evropského společenství, jako činnosti uvedené v hlavě V a VI Smlouvy o založení Evropské unie, a v žádném případě na činnosti týkající se veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a na činnosti státu v oblasti trestního práva.*"

Čl. 5 pak zakotvuje z hlediska data retention klíčovou zásadu důvěrnosti sdělení, a ukládá členským státům, aby zajistily „*důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů. Zejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1. Tento odstavec nebrání technickému uchovávání, které je nezbytné pro přenos sdělení, aniž by tím byla dotčena zásada důvěrnosti*."

V čl. 15 odst. 1 směrnice se pak výslovně objevuje možnost zavedení data retention. Toto ustanovení nově uvádělo, že „*[č]lenské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/64/ES. Členské státy mohou mimo jiné přijmout právní opatření umožňující zadržení údajů na omezenou dobu na základě důvodů uvedených v tomto odstavci. Veškerá opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o založení Evropské unie.*"

Nelze si nevšimnout zjevného napětí mezi čl. 1 odst. 3 směrnice 2002/58, který „bezpečnostní" činnosti z působnosti směrnice zcela vyjímá, a čl. 15 odst. 1 směrnice, který

pro omezení zásady důvěrnosti sdělení za stejným účelem stanovuje určité podmínky. Není proto divu, že otázka, zda a v jaké míře vnitrostátní právní předpisy data retention spadají do působnosti směrnice 2002/58 (a tudíž i Listiny), byla v judikatuře Soudního dvora týkající se data retention poměrně intenzivně řešena. Této judikatuře se podrobně věnuje kapitola 4.1.

Směrnice 2002/58 sdílela osud své předchůdkyně v tom smyslu, že v návaznosti na rozvoj technologií přestala být její pravidla aktuální a technologicky neutrální. Z těchto důvodů Komise spolu s nařízením GDPR předložila také návrh nařízení, které mělo směrnici 2002/58 nahradit a problematické otázky řešit. Legislativní proces se však ukázal jako nadmíru problematický a ani po více než pěti letech nelze tvrdit, že by byl konsensus na dosah. Důležitý pokrok v tomto smyslu představuje mandát Rady z 10. února 2021.[184] Avšak s ohledem na počet a povahu Radou navrhovaných změn lze očekávat, že dosažení shody s Evropským parlamentem nebude snadné. Pro účely této práce je každopádně třeba zmínit, že jednou ze zásadních problematických otázek je i revize ustanovení týkajících se data retention, v nichž Rada provedla zásadní úpravy, mj. reagující na aktuální judikaturu Soudního dvora v této oblasti. Tyto návrhy budou podrobněji rozebrány v části práce zabývající se problematikou data retention.[185]

2.4 Lidskoprávní rovina ochrany soukromí a osobních údajů v právu EU

Problematika ochrany osobních údajů má zřetelnou lidskoprávní rovinu. Ta je dána jednak tím, že ochrana osobních údajů sdílí společné historické kořeny se základním právem na soukromý život, ale především tím, že již první unijní předpisy týkající se problematiky ochrany osobních údajů uváděly jako jeden ze svých cílů zajištění vysoké úrovně ochrany základních práv, zejména práva na soukromí ve smyslu čl. 8 Úmluvy. Později byla lidskoprávní rovina ochrany osobních údajů stvrzena a posílena zakotvením základního práva na ochranu osobních údajů v čl. 8 Listiny, jehož svébytný obsah je však po více než dvaceti letech od vyhlášení Listiny stále nejasný.

V následujících kapitolách bude nejprve popsán obsah čl. 8 Úmluvy a související judikatura ESLP jakožto určitý „startovní bod“ pro lidskoprávní argumentaci týkající se ochrany soukromí a osobních údajů v unijním právu a judikatuře Soudního dvora. Následně bude pozornost věnována změnám, které v tomto ohledu přináší Listina, zejména s ohledem

[184] Rada Evropské unie. *Návrh nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) – mandát Rady*, 2021.
[185] Viz kapitola 3.2.2.3.

na zakotvení práva na ochranu osobních údajů jako svébytného základního práva odděleného od práva na soukromí.

2.4.1 Právo na respektování soukromého života dle čl. 8 Úmluvy

Právo na respektování rodinného a soukromého života

1. Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.

Již při letmém pohledu na strukturu čl. 8 Úmluvy je vidět, že obsahuje 4 celkem samostatné, avšak prolínající se chráněné oblasti: (1) soukromý život (2) rodinný život (3) obydlí a (4) korespondenci. Mezi těmito oblastmi v judikatuře není vždy ostrá hranice a soud v praxi často výslovně neuvádí, o kterou z těchto oblasti v daném konkrétním případě jde. Ostatně, zásah do třech posledně jmenovaných oblastí bude téměř vždy představovat zásah do soukromého života jako takového.

Co se týče bližšího vymezení chráněných oblastí, ESLP opakovaně zdůrazňuje, že pojem soukromého života je velmi široký a nepodléhá vyčerpávající definici.[186] Tento přístup plně odpovídá problémům, na které při snaze poskytnout vyčerpávající definici soukromí naráží odborná literatura[187] a které zřejmě není možné překonat, aniž by zároveň došlo k nežádoucímu omezení obsahu tohoto pojmu. Tato skutečnost také mj. odráží povahu Úmluvy jako tzv. „živého nástroje“ a umožňuje výklad Úmluvy přizpůsobovat společenskému a technologickému vývoji.[188] To však neznamená, že by ESLP v průběhu let nestanovil vůbec žádná vodítka pro pochopení obsahu tohoto pojmu. Z judikatury vyplývá, že pod pojem soukromý život spadá fyzická, psychologická a morální integrita identita jednotlivce.[189] Nejedná se tak pouze o možnost skrýt určitou část svého života před ostatními (tedy ono „právo být nechán na pokoji“), ale také o právo na „sebeurčení“ ve smyslu osobnostního rozvoje, které

[186] Srov. např. rozsudek ESLP ze dne 16. prosince 1992, *Niemetz proti Německu*, stížnost č. 13710/88, CE:ECHR:1992:1216JUD001371088, bod 29.
[187] Srov. např. SOLOVE, Daniel J. *Understanding Privacy*, 2008, s. 1-11.
[188] Srov. LETSAS, George. *The ECHR as a Living Instrument: Its Meaning and its Legitimacy*, 2012.
[189] Srov. např. rozsudek ESLP ze dne 25. června 2019, *Nicolae Virgiliu Tănase proti Rumunsku*, stížnost č. 41720/13, CE:ECHR:2019:0625JUD004172013, bod 128 či rozsudek ESLP ze dne 14. ledna 2020, *Beizaras and Levickas proti Litvě*, stížnost č. 41288/15, CE:ECHR:2020:0114JUD004128815, body 109-117.

spočívá v možnosti svobodně navazovat a rozvíjet své vztahy s ostatními.[190] Z dosahu čl. 8 Úmluvy navíc nejsou striktně vyloučeny ani aktivity převážně pracovní či obchodní povahy.[191]

Okruh práv chráněných čl. 8 Úmluvy je tedy extrémně široký. Krom otázek týkajících se rodiny, nedotknutelnosti obydlí a korespondence spadá pod tento pojem také problematika informačního sebeurčení jednotlivce, jeho reputace, jména, občanství, původu, sexuální a genderové identity, jakož i otázky zdravotnických zásahů, reprodukčních práv, domácích porodů, eutanázie, pohřbívání, a v neposlední řadě i problematika životního prostředí.[192] Pro účely této práce je důležité, že součástí soukromého života je i soukromí ve smyslu „práva být nechán na pokoji" a ve smyslu práva na informační sebeurčení, se kterým úzce souvisí i problematika ochrany osobních údajů.

Práva obsažená v čl. 8 Úmluvy nejsou absolutní a je do nich možné zasáhnout, je-li dotčený zásah stanoven zákonem, sleduje-li legitimní cíl a nejde-li nad rámec toho, co je v demokratické společnosti nezbytné. Aby však takový zásah vůbec spadal do věcné působnosti čl. 8 Úmluvy, musí mít nejprve určitou minimální úroveň intenzity. Na zásahy, které jsou z hlediska svých dopadů zcela minimální, se tedy ochrana čl. 8 Úmluvy vztahovat nebude.[193]

Legitimní cíle pro omezení práva na soukromý život jsou pak vyjmenovány v čl. 8 odst. 2 Úmluvy. Omezení je tak možné v zájmu ochrany národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany veřejného pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných. V drtivé většině případů nebývá problematické určit legitimní cíl, o který je možné omezení práva na soukromý život opřít, a klíčovou proto bývá zpravidla až otázka nezbytnosti zásahu v demokratické společnosti. ESLP tak nebývá v hodnocení existence legitimního cíle přísný, spíše naopak. V této souvislosti vyvolal poměrně intenzivní debaty např. jeho rozsudek týkající se francouzského zákona zakazujícího zahalování obličeje na veřejných prostranstvích, ve kterém ESLP mj. uznal, že tento zákon sleduje legitimní cíl ochrany společenského soužití,

[190] Srov. např. rozsudek ESLP ze dne 5. září 2017, *Bărbulescu proti Rumunsku*, stížnost č. 61496/08, CE:ECHR:2017:0905JUD006149608, bod 71.
[191] Ibidem.
[192] Srov. European Court of Human Rights. *Guide on Article 8 of the Convention – Right to respect for private and family life,* 2020.
[193] Srov. např. rozsudek ESLP ze dne 31. října 2019, *Vučina proti Chorvatsku*, stížnost č. 58955/13, CE:ECHR:2019:0924DEC005895513, body 42-51.

resp. ochrany práv a svobod jiných v podobě „*respektování minimálních požadavků na život ve společnosti*“.[194]

Co se týče požadavku na to, aby byl zásah stanoven zákonem, ten není aplikován formalisticky jako požadavek na zákonnou formu dotčených vnitrostátních pravidel. Tento požadavek je proto splněn za podmínek, že tato pravidla jsou jasná, předvídatelná a odpovídajícím způsobem dostupná. Jinými slovy, jednotlivci z těchto pravidel musí být schopni seznat jak limity vlastního chování, tak limity diskrece orgánů státu.[195] Oba tyto aspekty jsou klíčové právě v oblasti skrytého sledování.

Posuzování toho, zda je určité opatření nezbytné v demokratické společnosti, pak spočívá v zásadě ve vážení práva na soukromý život a konkurenčních práv či veřejných zájmů. S Úmluvou tak budou slučitelná pouze opatření, která jsou skutečně nezbytná k řešení určité naléhavé společenské potřeby, nikoliv pouze opatření, která se jeví vhodná či užitečná. Jak však bude uvedeno níže konkrétně v souvislosti s problematikou data retention, určit jasnou hranici mezi „velmi užitečným“ a „nezbytným“ mnohdy nebývá snadné – obzvlášť v kontextu moderních bezpečnostních hrozeb.[196]

Striktnost posuzování splnění požadavku nezbytnosti úzce souvisí s prostorem pro uvážení („*margin of appretiation*“), který mají smluvní strany k dispozici. Šíře tohoto prostoru není v každém případě stejná a závisí na mnoha faktorech – např. cílech sledovaných opatřením (v citlivé oblasti jako je např. zajišťování národní bezpečnosti bude prostor pro uvážení zpravidla větší), povaze zásahu (v případě významných zásahů do klíčových práv chráněných Úmluvou bude prostor pro uvážení nižší) ale i třeba existenci konsensu mezi smluvními stranami (nepanuje-li mezi smluvními stranami širší shoda v určité oblasti, bude prostor pro uvážení zpravidla vyšší). Platí, že čím větší prostor pro uvážení, tím „mírnější“ je ESLP při přezkumu toho, zda je opatření v daném kontextu opravdu nezbytné.[197] Doktrína prostoru pro uvážení úzce souvisí s funkcí ESLP, jež spočívá v zajišťování minimálního standardu ochrany základních práv. Role ESLP tak nespočívá nutně v harmonizaci úrovně

---

[194] Srov. rozsudek ESLP ze dne 1. července 2014, *S.A.S. proti Francii*, stížnost. č. 43835/11, CE:ECHR:2014:0701JUD004383511, bod 122.

[195] Srov. např. rozsudek ESLP ze dne 25. března 1983, *Silver a další proti Spojenému království*, stížnosti č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, CE:ECHR:1983:0325JUD000594772, bod 87 či rozsudek ESLP ze dne 19. října 2017, *Lebois proti Bulharsku*, stížnost č. 67482/14, CE:ECHR:2017:1019JUD006748214, body 66-67.

[196] Srov. např. rozsudek ESLP ze dne 22. října 1981, *Dudgeon proti Spojenému království*, stížnost č. 7525/76, CE:ECHR:1981:1022JUD000752576, body 42-62.

[197] Srov. McGOLDRICK, Dominic. A defence of the margin of appreciation and an argument for its application by the human rights committee. *International & Comparative Law Quarterly*, 2016, s. 26.

ochrany základních práv napříč smluvními stranami, nýbrž v zajištění, že se úroveň ochrany nedostane pod určitou, mezi smluvními stranami obecně akceptovanou mez.[198]

Nutno však dodat, že doktrína prostoru pro uvážení bývá občas kritizována. Je tomu tak jak z principiálního hlediska, dle kterého vede k přílišné relativizaci obsahu základních práv garantovaných Úmluvou, tak z hlediska praktického, dle kterého se jedná pouze o rétorické zdůvodnění konečného výsledku vážení zájmů, bez reálného dopadu na samotný proces vážení a jeho výsledek.[199]

V neposlední řadě je třeba poznamenat, že ačkoliv čl. 8 Úmluvy stanoví pro stát primárně negativní povinnosti (spočívající v povinnosti zdržet se zásahu do chráněných oblastí), v mnohých případech soud dovodil i pozitivní povinnost přijmout opatření k zajištění efektivní ochrany těchto zájmů.[200] Jelikož by tyto pozitivní obligace neměly spočívat v ukládání nepřiměřených povinností, je smluvním stranám zpravidla ukládáno pouze určitým způsobem jednat (např. zajistit účinné vyšetřování trestného činu) spíše než dosáhnout určitého výsledku (např. odsouzení pachatele).[201]

2.4.2 Právo na respektování soukromého života dle čl. 7 Listiny

Respektování soukromého a rodinného života

Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.

Text předmětného ustanovení v podstatě kopíruje čl. 8 Úmluvy, ovšem se dvěma rozdíly. Tím prvním je nahrazení slova „korespondence“ širším pojmem „komunikace“, což je s ohledem na dobu, ve které byla Listina přijata, zcela pochopitelné. V praxi jde však toliko o kosmetickou odlišnost. I čl. 8 Úmluvy je ze strany ESLP vykládán s přihlédnutím k technologickému vývoji tak, že se vztahuje i na moderní způsoby komunikace. Druhým rozdílem je absence ustanovení stanovujících podmínky pro omezení dotčeného základního práva, to je však dáno tím, že autoři Listiny považovali za vhodnější zakotvit podmínky omezení společně pro všechna práva v čl. 52 odst. 1 Listiny. Ani v režimu Listiny tak právo na soukromí není absolutní.[202]

---

[198] Srov. ibidem, s. 28.
[199] Srov. ibidem, s. 37-39.
[200] Srov. např. rozsudek *Bărbulescu v. Rumunsko*, body 108-111.
[201] BEIJER, Malu. Active Guidance of Fundamental Rights Protection by the Court of Justice of the European Union: Exploring the Possibilities of a Positive Obligations Doctrine. *Review of European Administrative Law*, 2015, s. 146.
[202] Ke střetu práv na soukromí a ochranu osobních údajů s některými jinými právy a veřejnými statky, jako např. svoboda projevu, duševní vlastnictví či přístup k informacím viz např. rozsudek Soudního dvora ze dne 16. prosince 2008, *Satakunnan Markkinapörssi a Satamedia*, C-73/07, EU:C:2008:727; rozsudek Soudního dvora

Z čl. 52 odst. 3 dále vyplývá, že obsah práva na respektování soukromého a rodinného života dle čl. 7 Listiny odpovídá obsahu téhož práva dle čl. 8 Úmluvy, což následně jednoznačně potvrzují taktéž vysvětlivky k Listině a v neposlední řadě i judikatura Soudního dvora.[203]

Výše uvedené nicméně neznamená, že by Soudní dvůr a ESLP musely v souvislosti s každou konkrétní otázkou týkající se práva na soukromí dospět k týž závěrům. Rozdíly v přístupech obou soudů se v některých oblastech objevují, přičemž jsou zpravidla podrobeny široké akademické diskusi zabývající se důvody takových odchylek a dopady těchto odchylek.[204] Situace, ve kterých judikatura Soudního dvora vede k poskytnutí vyšší úrovně ochrany, nejsou v tomto ohledu příliš problematické, jelikož režim Úmluvy představuje toliko minimální standard ochrany dotčených základních práv v rámci Rady Evropy.[205] Ostatně, čl. 52 odst. 3 Listiny výslovně uvádí, že unijní právo může poskytovat vyšší úroveň ochrany. Problematičtější situace nastává ve chvíli, kdy unijní právo poskytuje nižší úroveň ochrany, k čemuž může dojít např. v případech konfliktů dvou základních práv či základního práva a určitého jiného veřejného statku uznávaného právem EU, včetně základních svobod vnitřního trhu.[206]

Co se týče data retention, sama skutečnost, že Soudní dvůr v této souvislosti vyžaduje velmi vysokou úroveň ochrany práva na soukromí, by tedy optikou režimu Úmluvy neměla představovat větší problém. Některé členské státy nicméně argumentují tím, že plošná data retention představuje nástroj pro plnění pozitivních povinností vyplývajících z práva na bezpečnost ve smyslu čl. 5 Úmluvy.[207] Pokud by vysoká úroveň ochrany soukromí vedla k tomu, že členské státy skutečně nemohou zajišťovat bezpečnost v míře vyžadované judikaturou ESLP, nastal by v tomto ohledu poměrně závažný problém. Oprávněnosti této argumentace se práce věnuje v kapitole 4.2.2.3.

---

ze dne 29. ledna 2008, *Promusicae*, C-275/06, EU:C:2008:54 či rozsudek Soudního dvora ze dne 29. června 2010, *Bavarian Lager*, C-28/08 P, EU:C:2010:378.

[203] Srov. např. rozsudek Soudního dvora ze dne 9. listopadu 2010, *Volker und Markus Schecke a Eifert*, spojené věci C-92/09 a C-93/09, EU:C:2010:662, bod 51.

[204] A to i co se týče výkladu práva na soukromí, např. v souvislosti s prohlídkami prostor společností při vyšetřování porušení pravidel hospodářské soutěže. Srov. GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014, s. 170-173.

[205] Srov. např. O'LEARY, Síofra. A Tale of Two Cities: Fundamental Rights Protection in Strasbourg and Luxembourg. *Cambridge Yearbook of European Legal Studies*, 2018, s. 8.

[206] K řešení tohoto druhu konfliktu viz např. rozsudek Soudního dvora ze dne 12. června 2003, *Schmidberger*, C-112/00, EU:C:2003:333.

[207] Srov. např. rozsudek *La Quadrature du Net*, body 125-126.

2.4.3 Právo na ochranu osobních údajů dle čl. 8 Listiny

Ochrana osobních údajů

1. Každý má právo na ochranu osobních údajů, které se ho týkají.

2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.

3. Na dodržování těchto pravidel dohlíží nezávislý orgán.

Počátky ochrany osobních údajů jsou úzce spojeny s problematikou ochrany soukromí, jelikož ve svých prvopočátcích nebyla diskuse o ochraně osobních údajů ničím jiným než diskusí o ochraně soukromí v éře počítačů.[208] To ostatně dokládají i první unijní předpisy v této oblasti, které se sice odvolávaly na lidskoprávní rovinu ochrany osobních údajů, avšak tu spatřovaly především v právu na soukromí dle čl. 8 Úmluvy.[209] Právo jednotlivce rozhodovat o tom, jak bude nakládáno s jeho osobními údaji, je dlouhodobě považováno za součást práva na informační sebeurčení, které spadá pod právo na soukromí.

Důvody, proč byla ochrana osobních údajů v Listině povýšena na svébytné základní právo, nejsou jednoznačné. Vysvětlivky k Listině toliko uvádí, že čl. 8 Listiny „*je založen na článku 286 Smlouvy o založení Evropského společenství a směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a rovněž na článku 8 EÚLP a na Úmluvě Rady Evropy ze dne 28. ledna 1981 o ochraně osob s ohledem na automatizované zpracování osobních údajů, která byla ratifikována všemi členskými státy. Článek 286 Smlouvy o ES je nyní nahrazen článkem 16 Smlouvy o fungování Evropské unie a článkem 39 Smlouvy o Evropské unii. Odkazuje se rovněž na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů. Směrnice a nařízení uvedené výše obsahují podmínky a omezení pro výkon práv na ochranu osobních údajů.*“ Z vysvětlivek se tedy dozvídáme, že čl. 8 Listiny je založen na primárním a sekundárním právu EU týkajícím se ochrany osobních údajů a čl. 8 Úmluvy, avšak nedozvídáme nic o důvodech pro „povýšení“ ochrany osobních údajů na úroveň základního práva, a co je nejdůležitější, ani o jeho vztahu k právu na soukromí dle čl. 7 Listiny,

[208] Viz kapitola 2.1.2.
[209] Viz kapitola 2.2.1.

resp. čl. 8 Úmluvy. Odpovědi na tyto otázky není možné nalézt ani v přípravných pracích. Oporu pro rozlišení obou práv neposkytuje judikatura Soudního dvora z období před přijetím Lisabonské smlouvy, ve kterých je ochrana osobních údajů soustavně ztotožňována s ochranou soukromí, a to zejména pod vlivem judikatury ESLP k článku 8 Úmluvy.[210]

Především v odborné literatuře pak existuje shoda na tom, že ochrana soukromí a ochrana osobních údajů nejsou totéž, resp. že není správné chápat ochranu osobních údajů pouze jako podmnožinu ochrany soukromí. Ochrana osobních údajů je totiž v určitých ohledech ochranou širší. Je tomu tak z důvodu, že ne každé zpracování osobních údajů je zároveň zásahem do soukromí. To lze dobře ilustrovat např. na judikatuře ESLP, dle které běžné monitorování veřejných prostranství videokamerami nemusí vždy představovat zásah do práva na soukromý život osob, které se na těchto veřejných prostranstvích pohybují.[211] Nemůže však být pochyb o tom, že se jedná o zpracování osobních údajů dle příslušné unijní legislativy. V některých aspektech je však ochrana osobních údajů naopak užší, jelikož dopadá v zásadě pouze zpracování osobních údajů prostřednictvím automatizovaných prostředků a týká se pouze fyzických osob. Ochrana soukromí dle čl. 8 Úmluvy a čl. 7 Listiny přitom taková omezení neobsahuje. Současná akademická literatura k této problematice se proto kloní k závěrům, že přestože se problematika soukromí (zejména ve smyslu práva na informační sebeurčení) a problematika ochrany osobních údajů překrývají, není tomu tak zcela.

Přední akademici se zároveň v zásadě shodují, že na rozdíl od ochrany soukromí má ochrana osobních údajů podstatně více pragmatický, proaktivní a procedurální charakter. Její těžiště spočívá v nastavení základních zásad a požadavků pro zpracování údajů. Ochrana osobních údajů pak neusiluje o zabránění jakémukoliv zpracování osobních údajů, ale pouze takovému, které těmto zásadám a požadavkům neodpovídá (pragmatický charakter).[212] Za tímto účelem je subjektu údajů poskytnuta řada procesních nástrojů, kterými může subjekt proaktivně ovlivňovat, jak bude nakládáno s jeho osobními údaji (proaktivní a procedurální charakter).[213]

---

[210] Srov. MÁDR, Petr. *Právo na ochranu osobních údajů dle článku 8 Listiny základních práv Evropské unie*, 2016, s. 26.
[211] Srov. např. rozsudek ESLP ze dne 28. ledna 2003, *Peck proti Spojenému království*, stížnost č. 44647/98, CE:ECHR:2003:0128JUD004464798, bod 59 a zde citovaná judikatura.
[212] Srov. ibidem, s. 42.
[213] Srov. LYNSKEY, Orla. *The Foundations of EU Data Protection Law*, 2015, s. 130; DE HERT, Paul a Serge GUTWIRTH. Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In: CLAES Erik, Antony DUFF a Serge GUTWIRTH (eds). *Privacy and the Criminal Law*, 2006 či MÁDR, Petr. *Právo na ochranu osobních údajů dle článku 8 Listiny základních práv Evropské unie*, 2016, s. 43-45.

S výše uvedeným pojetím rozdílů mezi ochranou soukromí a ochranou osobních údajů poměrně dobře koresponduje samotný text čl. 8 Listiny, který je v porovnání s jinými právy velmi podrobný a ve kterém je poměrně snadné identifikovat šest klíčových prvků tohoto základního práva. Jde o (1) korektnost zpracování, (2) přesně stanovený účel zpracování a (3) souhlas či jiný zákonem stanovený důvod pro zpracování jakožto důležité hmotněprávní zásady zpracování. Dále jde o (4) právo na přístup k údajům, (5) opravu údajů a (6) dohled nezávislého orgánu jakožto důležité procesní záruky zpracování. Tyto prvky pak odpovídají zásadám a požadavkům na zpracování (prvky 1 až 3) či právním institutům (prvky 4 až 6) v unijní sekundární legislativě, na níž ostatně vysvětlivky odkazují. Pravděpodobně není náhoda, že se jedná o prvky obsažené i v právních předpisech upravujících zpracování osobních údajů v oblasti trestního práva, a to nejen v současné,[214] ale i dřívější právní úpravě,[215] resp. dokonce již v Doporučení R (87) 15.[216]

Nabízelo by se tedy předpokládat, že autoři Listiny vybrali z unijní sekundární legislativy v oblasti ochrany osobních údajů prvky, které považovali skutečně za základní, a ty následně povýšili na úroveň základního práva. K zásahu do čl. 8 Listiny by pak docházelo v případech, kdy některá z výše uvedených zásad či záruk není dodržena. K porušení čl. 8 Listiny by pak docházelo v případech, kdy zásah neodpovídá požadavkům čl. 52 odst. 1 Listiny, tedy pokud nebyl stanoven zákonem či nebyl v souladu se zásadou proporcionality. Takový přístup by pak umožnil poměrně snadno rozlišovat mezi porušením pravidel na ochranu osobních údajů stanovených sekundárním právem, porušením základního práva na ochranu osobních údajů dle čl. 8 Listiny a porušením základního práva na soukromí dle čl. 7 Listiny. V řadě případů by jistě mohla být přítomna všechna tři porušení, v řadě jiných pouze jedno nebo dvě.[217]

Problém s výše nastíněným přístupem k obsahu čl. 8 Listiny je, že judikatura Soudního dvora takový výklad nepřijala. Jak vyplývá z vyčerpávající analýzy provedené Mádrem,

---

[214] Srov. čl. 4, 14, 16 a 41-49 Směrnice 2016/680. Viz také kapitola 2.2.3.
[215] Srov. čl. 3, 17, 18 a 25 rámcového rozhodnutí Rady 2008/977/SVV.
[216] Srov. bod 1.1, 2.1, 6.2 a 6.3 Doporučení R (87) 15.
[217] Např. neumožnění využití práva na přenositelnost v případě některých údajů by sice mohlo znamenat porušení čl. 20 GDPR, ale nemuselo by se jednat o zásah do základního práva na ochranu osobních údajů (jelikož nebyl porušen žádný z výše uvedených základních prvků) ani práva na soukromí (jelikož se nejedná o zásah, který by přesahoval určitou nezbytnou míru intenzity). Neumožnění přístupu k běžnému bezpečnostnímu videozáznamu z veřejného prostranství jako je např. nádraží by mohlo znamenat porušení čl. 15 GDPR i zásah do základního práva na ochranu osobních údajů (jelikož právo na přístup patří mezi jeho základní prvky), avšak nikoliv nutně zásah do práva na soukromí (jelikož se nejedná o zásah, který by přesahoval určitou nezbytnou míru intenzity). Zpracování citlivých údajů bez legitimního účelu by pak znamenalo porušení pravidel GDPR i zásah do obou dotčených základních práv.

se kterou plně souhlasím, Soudní dvůr ve své judikatuře autonomní povahu práva na ochranu osobních údajů nezohledňuje a jeho judikatura tíhne k souběžné aplikaci čl. 7 a 8 Listiny, ale bez vyjasnění jejich obsahu a provázanosti.[218] Používání čl. 8 Listiny je v naprosté většině případů pouze proklamativní, a to na úkor vymezování jeho věcného obsahu.[219] Po separátním konstatování zásahu do práv dle čl. 7 a 8 Listiny totiž zpravidla následuje společný přezkum přiměřenosti takového zásahu, jakoby obě práva měly tentýž obsah.[220] Diskutabilní je taktéž skutečnost, že Soudní dvůr shledává zásah do práva na ochranu osobních údajů ve smyslu čl. 8 Listiny pokaždé, kdy dochází ke zpracování osobních údajů, bez ohledu na to, zda v daném případě byly či nebyly dodrženy zásady a záruky vyjmenované v čl. 8 Listiny.[221]

Výše uvedené nedostatky v přístupu Soudního dvora k obsahu čl. 8 Listiny však Soudnímu dvoru nezabránily, aby v této oblasti svým výkladem přispíval k velmi vysoké úrovni ochrany osobních údajů, a to jak co se týče zpracováním osobních údajů soukromými subjekty,[222] tak co se týče jejich zpracování orgány státu.[223] Tato skutečnost však nic nemění na tom, že přístup Soudního dvora k samostatnému obsahu čl. 8 Listiny je značně nevyhovující. Čím dříve tedy Soudní dvůr přistoupí k určitým změnám ve svém postoji a obsah tohoto práva vyjasní, tím lépe. Jedním z cílů této práce bude zjistit, zda k takovému posunu došlo v poslední judikatuře týkající se problematiky data retention.

2.5 ZÁVĚR

Účelem této části práce bylo vysvětlit základní pravidla ochrany soukromí a osobních údajů v EU předtím, než dojde ke zkoumání problematiky data retention jakožto zásahu do soukromí a zpracování osobních údajů. Bylo vysvětleno, že ochrana soukromí a ochrana osobních údajů sdílí společné kořeny, přičemž přijetí prvních předpisů v oblasti ochrany osobních údajů bylo zdůvodněno potřebou chránit soukromí jednotlivců v éře počítačů, mj. v souvislosti s ukládáním osobních údajů v databázích veřejného sektoru. Zároveň bylo demonstrováno, že ačkoliv se dnes jedná o dvě samostatná základní práva v Listině, v rozhodovací praxi

[218] Srov. MÁDR, Petr. *Právo na ochranu osobních údajů dle článku 8 Listiny základních práv Evropské unie*, 2016, s. 37.
[219] Ibidem, s. 62.
[220] Ibidem, s. 31.
[221] Ibidem, s. 43.
[222] Viz kapitola 2.2.2.
[223] Viz zejména kapitola 4.1. Srov. také např. rozsudek Soudního dvora ze dne 9. listopadu 2010, *Volker und Markus Schecke a Eifert*, spojené věci C-92/09 a C-93/09, EU:C:2010:662. V tomto rozsudku Soudní dvůr zrušil ustanovení sekundárního práva vyžadující publikaci informací o příjemcích veřejných podpor s poukazem na čl. 7 a 8 Listiny.

Soudního dvora je rozlišování mezi oběma právy spíše formálního charakteru, a skutečný samostatný obsah základního práva na ochranu osobních údajů zůstává nadále velmi nejasný.

Výše uvedené nicméně nezabránilo vzniku značně progresivní judikatury Soudního dvora v této oblasti, jež vede k vysoké úrovni ochrany výše uvedených základních práv. Extenzivní právní výklad ve prospěch vyšší úrovně ochrany se přitom projevil nejen při výkladu jednotlivých definic a právních institutů v příslušných unijních předpisech, ale i v jejich Soudním dvorem dovozené široké působnosti.

Co se týče data retention, bylo vysvětleno, že i provozní a lokalizační údaje představují osobní údaje ve smyslu unijní právní úpravy, přičemž v některých případech mohou mít dokonce charakter citlivých údajů. Samotné uložení údajů pak představuje jejich zpracování (a tudíž optikou Soudního dvora i zásah do práva na ochranu osobních údajů ve smyslu čl. 8 Listiny) a zpravidla také zásah do práva na soukromí dle čl. 8 Úmluvy a čl. 7 Listiny. V neposlední řadě byly nastíněny třecí plochy mezi plošným uchováváním údajů a základními zásadami unijní legislativy v oblasti zpracování osobních údajů (zejména zásadami účelového omezení a minimalizace údajů) a zajišťování soukromí v elektronických komunikacích (zásadou důvěrnosti komunikace). Také byly nastíněny i problémy týkající se působnosti práva EU v oblastech, kdy dochází k uchovávání údajů soukromými subjekty, avšak za účelem spojeným s činností státních orgánů v oblasti trestního práva a zajišťování národní bezpečnosti, což je případ právě data retention.

3 DATA RETENTION

Cílem této části práce je popis a analýza data retention jakožto účinného nástroje v boji proti bezpečnostním hrozbám na straně jedné, avšak i významného zásahu do práv na soukromí a ochranu osobních údajů na straně druhé. Budou popsány základní společné aspekty právních úprav data retention a shrnuty hlavní argumenty jejích kritiků i zastánců. Následně dojde k popisu a analýze současného unijního právního rámce data retention, přičemž hlavní důraz bude věnován legislativní historii a obsahu směrnice 2006/24. Ta sice již byla Soudním dvorem zrušena, avšak její pravidla se nadále významně promítají do platných právních úprav data retention v členských státech.

3.1 ÚVOD DO PROBLEMATIKY DATA RETENTION

Cílem této kapitoly je vysvětlení základních parametrů data retention a přiblížení hlavních třecích ploch mezi data retention, právem na soukromí a právem na ochranu osobních údajů. Máme-li se totiž následně zabývat přístupem Soudního dvora a ESLP k problematice data retention, je klíčové nejprve pochopit, v čem vlastně data retention spočívá. Ačkoliv jistě platí, že není data retention jako data retention a jednotlivé vnitrostátní právní úpravy se mohou v mnohých ohledech lišit, jejich základní parametry, a tudíž i hlavní třecí plochy s ochranou soukromí a osobních údajů, budou ve všech případech velmi podobné.

V prostém překladu z angličtiny znamená pojem data retention prostě uchovávání či zadržování údajů. V současnosti se však tento pojem nejčastěji používá v souvislosti s právní povinností uloženou poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí uchovávat provozní, lokalizační a související údaje s cílem zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů či příp. jiných bezpečnostních hrozeb. Jinými slovy, poskytovatelům vybraných služeb je přikázáno uchovávat určitá komunikační metadata za účelem jejich možného zpřístupnění orgánům činným v oblasti trestního práva či v oblasti zajišťování národní bezpečnosti. Ruku v ruce s touto povinností tedy nutně jdou i podmínky pro přístup příslušných orgánů k takto uchovávaným údajům. Jak v této souvislosti uvádí Myška – jednoduchý a výstižný český ekvivalent k pojmu data retention by se hledal poměrně těžko.[224] Práce proto pracuje primárně s tímto zažitým anglickým pojmem.

[224] Srov. MYŠKA, Matěj. Aktuální otázky data retention. *Revue pro právo a technologie*, 2010, s. 13.

V dnešní době je čím dál více komunikace realizováno na dálku prostřednictvím informačních a komunikačních technologií. V rámci takové komunikace není vytvářen a přenášen pouze samotný obsah sdělení, nýbrž i tzv. komunikační metadata. Těmi jsou na jedné straně údaje nezbytné pro samotnou realizaci komunikace (např. identifikace volajícího a volaného), na straně druhé údaje nezbytné pro řádné vyúčtování poskytovaných služeb (např. délka hovoru). Krom toho, že jsou tyto údaje nezbytné pro výše uvedené účely, jsou také velmi užitečné pro účely jiné, a to jak pro komerční subjekty, kteří je mohou využít např. pro účely marketingu, tak pro orgány státu. Velký potenciál využití těchto údajů totiž existuje v oblastech boje proti trestné činnosti a zajišťování národní bezpečnosti. Z komunikačních metadat lze totiž např. vyčíst, zda se určitá osoba v době spáchání trestného činu nacházela na místě činu či s kým v dotčené době komunikovala. O tom, že takové údaje mohou být velmi užitečné např. pro policii či zpravodajské služby, nemůže být pochyb.

Otázka, zda by orgány státu měly mít za určitých podmínek k tomuto druhu údajů přístup, nebývá sama o sobě příliš kontroverzní. Ostatně, ani ve vyspělých demokratických státech nebývá zpochybňováno, že orgány státu mohou v některých úzce vymezených případech a při splnění přísných podmínek přistoupit k odposlechu telefonních hovorů, tedy získat přístup k obsahu komunikace. Totéž lze tvrdit i o komunikačních metadatech. Samozřejmě můžeme debatovat o tom, jaké by tyto podmínky měly být (např. opravdová nezbytnost pro vyšetřování závažné trestné činnosti, předchozí souhlas soudu apod.), samotná možnost přístupu však nebývá v případě data retention považována za hlavní „kámen úrazu“.

Onen „kámen úrazu“ v případě data retention je nicméně v tom, že data retention nespočívá pouze v povinnosti zpřístupnit tyto údaje, nýbrž v povinnosti je preventivně uchovávat. Jinými slovy, data retention znamená povinnost poskytovatelů služeb za účelem jejich potenciálního pozdějšího vyžádání ze strany orgánů státu uchovávat údaje, které by pro své vlastní účely uchovávat nemuseli, nechtěli či v některých případech ani nemohli. A to zpravidla o všech jejich zákaznících, tedy o všech osobách využívajících prostředky komunikace na dálku, bez ohledu na spojitost těchto osob s jakoukoliv konkrétní hrozbou.

Ve výše uvedeném přitom spočívá hlavní síla data retention i hlavní rizika s ní spojená. Zatímco např. u odposlechů telefonních hovorů musí policie nejprve určit osobu, jejíž odposlech je nezbytný pro účely vyšetřování, aby následně mohla přistoupit k odposlechu mobilního telefonu, data retention umožňuje policii pohlédnout do života této osoby zpravidla i několik měsíců předtím, než se vůbec stala podezřelou. Takový „pohled do minulosti“ pak

může být pro úspěch vyšetřování zcela klíčový. Je však vykoupen preventivním uchováváním údajů o všech uživatelích prostředků elektronické komunikace.

Vzhledem k výše uvedenému data retention její kritici často označují za nástroj pro preventivní sledování celé populace, resp. za „*plošné sledování komunikace*“[225] či *de facto* „*plošné odposlechy*“.[226] Realita je však komplikovanější – záleží totiž na tom, zda bychom za „sledování“ či „odposlech“ měli považovat již samotné uchování údajů, či až přístup k nim.

3.1.1 Uchovávání v. přístup

Přestože data retention znamená v prostém překladu pouze zadržování či uchovávání údajů, je třeba si uvědomit, že každá právní úprava data retention vždy bude mít dvě oddělené roviny, které spolu nicméně úzce souvisí. Rovinu uchovávání a rovinu přístupu k údajům.

Rovina uchovávání údajů spočívá ve vymezení toho, jaké údaje mají být uchovávány (např. URL navštívených stránek, lokalita zařízení apod.), jak dlouho (např. na 6 měsíců od jejich vzniku), kým (tj. poskytovateli jakých konkrétních služeb) a o kom (o všech uživatelích, o uživatelích v určité geografické lokalitě apod.). Co se týče posledního kritéria, právní úpravy data retention nejsou v tomto ohledu obvykle jakkoliv omezeny, a zpravidla tedy vyžadují uchovávání údajů o všech uživatelích bez výjimky.

Tento plošný a preventivní charakter uchovávání je na jedné straně příslušnými orgány státu vnímán jako nezbytný pro zachování účinnosti data retention, na druhé straně je však hlavním terčem kritiky ze strany odpůrců data retention. Je nicméně třeba zdůraznit, že data retention spočívá skutečně v uchovávání, nikoliv sbírání či vytváření údajů. To znamená, že poskytovatelům služeb není ukládána povinnost získávat či vytvářet osobní údaje pouze za účelem vyhovění požadavkům data retention legislativy. Pokud tedy není určitý údaj generován pro účely přenosu sdělení či pro účely poskytování služeb, nebude následně k dispozici ani orgánům státu.

Rovina přístupu k údajům pak spočívá ve vymezení toho, jaké orgány státu budou mít přístup k těmto údajům (např. policie, státní zastupitelství, zpravodajské služby apod.), za jakým účelem (např. za účelem vyšetřování závažných trestných činů, předcházení hrozeb v oblasti národní bezpečnosti apod.) a za jakých podmínek (např. pouze s předchozím povolením soudu, s povinností následného informování dotčených osob apod.).

---

[225] VOBOŘIL, J. Ústavní soud posvětil plošné sledování elektronické komunikace. *Lupa.cz*, 2019.
[226] Srov. MYŠKA, Matěj. Aktuální otázky data retention. *Revue pro právo a technologie*, 2010, s. 15.

Plošné a preventivní uchovávání se tedy bez dalšího nerovná plošný a preventivní přístup k těmto údajům. Data retention totiž skutečně spočívá v preventivním a plošném uchovávání údajů velkého množství osob, ovšem v praxi bude k přístupu k těmto údajům docházet jen v opravdu nepatrném zlomku případů. Podstatou data retention, alespoň tedy v její typické podobě vycházející ze směrnice 2006/24, není vytvoření databáze údajů o celé populaci, ve které by mohly orgány státu volně vyhledávat. Tyto údaje jsou uloženy u poskytovatelů služeb a pokud v určité, zpravidla několikaměsíční lhůtě od vzniku údajů není nalezena souvislost těchto údajů s konkrétním trestným činem či hrozbou v oblasti národní bezpečnosti, dojde k jejich automatickému smazání.

Samozřejmě nemůže být pochyb o tom, že již samotné uchovávání znamená určitý zásah do práv na soukromí a ochranu osobních údajů. Nicméně je třeba si uvědomit, v čem přesně takový zásah spočívá. Jak bude uvedeno dále, kritici data retention stejně jako Soudní dvůr uvádí, že z uchovaných údajů lze „*vyvozovat velmi přesné závěry o soukromém životě osob*“.[227] Je však zjevné, že tyto závěry lze vyvozovat až na základě přístupu k těmto údajům. Jak přitom již bylo uvedeno výše, ani ve vyspělých demokratických státech nebývá zpochybňováno, že v určitých případech je přístup k tomuto druhu údajů žádoucí.

Pokud bychom tedy žili v ideálním světě, ve kterém si můžeme být jisti, že k uchovávaným údajům bude přistupováno jen v zákonem vymezených případech, veškeré otázky o nezbytnosti a přiměřenosti právní úpravy data retention by se soustředily na to, jak tyto oprávněné případy vymezit. Rizika spojená se samotným uchováváním údajů by zcela odpadla. Problém je nicméně v tom, že v reálném světě nikdy takovou jistotu mít nemůžeme. A právě v tom spočívá zásah do práv na soukromí a ochranu osobních údajů způsobený již samotným uchováváním údajů – v tom, že riziko neoprávněného přístupu nelze nikdy vyloučit.

Samo riziko zneužití by však nemělo vést k tomu, abychom o data retention hovořili jako o nástroji pro sledování či odposlech celé populace. Samozřejmě, s uchováváním údajů o celé populaci jde ruku v ruce riziko, že u kohokoliv může dojít k neoprávněnému zpracování osobních údajů. Jedná se však o riziko zneužití tohoto nástroje, nikoliv podstatu jeho fungování. Míra tohoto rizika je přitom značně odvislá od dvou faktorů – od nastavení podmínek pro přístup k údajům a míry, v jaké jsme schopni zajistit, že tyto podmínky budou dodržovány. To samozřejmě nebrání tomu, abychom dospěli k závěru, že i za velmi striktních podmínek pro přístup a velmi účinných nástrojů proti zneužití je výše uvedené riziko neoprávněného

[227] Srov. rozsudek *Tele2 Sverige*, bod 99 či rozsudek *Digital Rights Ireland*, bod 27.

přístupu příliš vysoké na to, aby bylo data retention možné považovat za slučitelnou s právy na soukromí a ochranu osobních údajů. Ostatně – zamyšlení nad touto otázkou je v mnoha ohledech jádrem této práce.

Nesmíme však zapomínat, že riziko zneužití je spojeno i se všemi dalšími nástroji pro boj proti trestné činnosti a hrozbám v oblasti národní bezpečnosti. Stejně jako nemůžeme zaručit, že nedojde k neoprávněnému přístupu k uchovávaným metadatům, nemůžeme zaručit, že nedojde k neoprávněnému odposlechu. Tyto skutečnosti je třeba mít na paměti, uvažujeme-li o míře zásahu do práv na soukromí a ochranu osobních údajů v případě data retention.

Ačkoliv tedy nelze v žádném případě podceňovat rizika spojená s data retention, je označení data retention jako nástroje pro sledování celé populace příliš zjednodušující, jelikož je založeno na směšování roviny uchovávání a roviny přístupu. Data retention by jako nástroj sice umožňující plošné uchovávání, ale pouze adresný přístup, proto neměla být zaměňována s opatřeními umožňujícími hromadný přístup k údajům, jako např. právní úpravy vyžadující pravidelné hromadné předávání komunikačních metadat příslušným orgánům[228] či hromadnou analýzu obsahu komunikace v reálném čase pomocí klíčových slov.[229]

3.1.2 Metadata v. obsah komunikace

Data retention se dále týká pouze tzv. komunikačních metadat. Jde o údaje, které nezahrnují obsah sdělení, ale spíše jeho „kontext".[230] Jedná se např. o informace o zdroji komunikace (o zařízeních a uživatelích), lokalizační údaje, časové údaje (čas zahájení hovoru, délka jeho trvání, okamžik odeslání zprávy) apod. Jednoduše řečeno, nejde o informace *uvnitř* sdělení, ale informace *o* sdělení.[231] Tím se data retention podstatně liší od ostatních metod, kterými mohou příslušné orgány státu za účelem boje proti trestné činnosti a hrozbám v oblasti národní bezpečnosti zasáhnout do práv na soukromí a ochranu osobních údajů (např. telefonní odposlechy, prostorové odposlechy apod.).

Zastánci data retention často poukazují na to, že uchovávání a přístup metadatům představují menší zásah do práv na soukromí a ochranu osobních údajů, než uchovávání a přístup k obsahu komunikace, a to právě z toho důvodu, že jde pouze o metadata. Toto tvrzení bylo v minulosti potvrzeno i Soudním dvorem, který z této skutečnosti dovozuje, že data

---

[228] Srov. rozsudek *Privacy International*, bod 23.
[229] Srov. rozsudek *Facebook Ireland Schrems*, bod 62.
[230] Srov. NI LOIDEAIN, Nora. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, 2015, s. 2.
[231] Srov. WHITLEY, Edgar a HOSEIN, Ian. Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy*, 2005, s. 860.

retention nemůže zasáhnout do podstaty těchto základních práv.[232] Jedná se však o poměrně zjednodušující pohled, a to z několika důvodů.

Zaprvé, hranice mezi obsahem komunikace a komunikačními metadaty není vždy zcela jasná. Typickým příkladem je údaj o adresách navštívených webových stránek. Ačkoliv se podle některých vnitrostátních právních úprav jedná o metadata, lze z nich mnohdy přinejmenším dovozovat důležité informace i o obsahu sdělení.[233] Jako příklad může sloužit např. informace o tom, že určitá osoba opakovaně navštívila stránky internetové poradny pro pacienty s HIV apod. U tohoto druhu metadat tak dochází k určitému (i když ne úplnému) stírání rozdílů mezi obsahem a kontextem sdělení.

Zadruhé, přístup k metadatům může v určitých případech znamenat naopak větší zásah do práv na soukromí a ochranu osobních údajů než přístup k samotnému obsahu komunikace. Velmi totiž záleží na kontextu. Přístup k *obsahu* nákupního seznamu může představovat podstatně menší zásah do soukromí než přístup k *lokalizačnímu údaji* potvrzující přítomnost mobilního telefonu v bydlišti milenky či na místě, kde došlo ke spáchání trestného činu.

Zatřetí, metadata se od obsahu komunikace liší tím, že jsou za současného stavu technologie mnohem snadněji zpracovatelná pomocí nástrojů pro automatickou analýzu dat. Jak uvádí např. Myška, „*zatímco vyhodnocovat odposlechy telekomunikačního provozu musí stále provádět fyzická osoba, z uchovaných dat lze pomocí sofistikovaných programů vytvářet např. tzv. ‚komunikační profily' jednotlivce. Z nich pak lze s vysokou pravděpodobností dovozovat i samotný obsah komunikace. Dají se ale použít např. k identifikaci sociálních vazeb jednotlivce či např. k rozkrývání hierarchických vazeb v organizacích*".[234] To se projeví především v případech, kdy bychom usilovali o získání ucelenějšího obrazu o soukromém životě osob – jejich zájmech, zvycích a sociálních kontaktech. Zejména v situacích, kdy jsou analyzována metadata za určité delší období, může jejich analýza o soukromém životě jednotlivce prozradit mnohem více než analýza samotného obsahu komunikace, resp. přinejmenším za využití podstatně méně úsilí, než které by bylo třeba v případě analýzy obsahu sdělení. Analýza obsahu sdělení se pak v mnohých případech jeví jako nadbytečná či (časově a technologicky) příliš náročná.[235] Podstatou právních úprav data retention v pravém

[232] Srov. rozsudek *Tele2 Sverige*, bod 101 či rozsudek *Digital Rights Ireland*, bod 39.
[233] DE HERT, Paul et al. The Proposed ePrivacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads? *Brussels Privacy Hub Working Paper*, 2020, s. 12.
[234] MYŠKA, Matěj. Aktuální otázky data retention. *Revue pro právo a technologie*, 2010, s. 14.
[235] Srov. NI LOIDEAIN, Nora. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, s. 2.

slova smyslu nicméně v žádném případě není provádění takových analýz či profilů – ať už na úrovni jednotlivce či celé populace.

Z výše uvedeného vyplývá, že přístup „komunikační metadata = menší zásah, obsah komunikace = větší zásah“ není na místě, tedy alespoň ne paušálně. Vždy je třeba zamyslet se nad konkrétními okolnostmi každého zpracování – účelem zpracování, možnostmi správce, rozsahem uchovávaných údajů apod.

3.1.3 Základní parametry právních úprav data retention

Jak již bylo zmíněno výše, jednotlivé právní úpravy data retention se mohou velmi lišit – cílem této kapitoly je tak pouze poukázat na hlavní společné parametry těchto úprav, příp. upozornit na oblasti, ve kterých členské státy disponují určitým manévrovacím prostorem. Bližší popis unijní úpravy data retention pak bude předmětem dalších kapitol.[236] Veškeré sporné aspekty, na které je níže upozorněno, budou podrobněji řešeny v následujících kapitolách, zejména v rámci analýzy relevantní judikatury Soudního dvora a ESLP.[237]

Každá právní úprava data retention bude upravovat jak rovinu uchovávání údajů, tak rovinu následného přístupu k uchovaným údajům. Co se týče roviny uchovávání, jsou klíčové především čtyři aspekty – jaké subjekty mají povinnost údaje uchovávat, jaké typy údajů mají uchovávat, jak dlouho je mají uchovávat a jaká bezpečnostní opatření mají v této souvislosti přijmout. Kategorie povinných subjektů bývá vymezena tak, aby s ohledem na cíle sledované data retention bezezbytku pokryla dva základní způsoby komunikace na dálku – a tedy komunikaci prostřednictvím (pevné i mobilní) telefonní sítě a komunikaci prostřednictvím internetového připojení. Proto jsou povinnými osobami obvykle operátoři telekomunikačních sítí a poskytovatelé služeb přístupu k internetu. Vymezení pokrytých služeb však může být mnohdy problematické, zejména s ohledem na rychlý vývoj technologií. Určité komunikační kanály proto mohou dosahu těchto právních úprav unikat, což bude níže demonstrováno na příkladu směrnice 2006/24 a skutečnosti, že se nevztahovala např. na tzv. *over-the-top messaging*.

Právní úpravy data retention obvykle neukládají poskytovatelům telekomunikačních služeb povinnost generovat či sbírat údaje nad rámec těch, které generují a sbírají pro svou vlastní potřebu. Základním východiskem pro určení kategorií uchovávaných údajů tedy je, že se vždy musí jednat o údaje původně nezbytné k přenosu sdělení a vyúčtování služeb.

[236] Viz kapitola 3.2.
[237] Viz kapitola 4.

Z těchto údajů jsou pak povinně uchovávány pouze ty, které mohou přispět k cílům sledovaným právní úpravou data retention. Půjde proto především o údaje, ze kterých lze zjistit totožnost komunikujících osob a jejich lokaci v konkrétním čase. S tím souvisí i nejčastější způsob kategorizace těchto údajů – na údaje provozní a na údaje lokalizační.

Zejména v poslední době však bývá vyčleňována ještě další specifická kategorie nazývaná údaje o předplatitelích („*subscriber data*"), mezi které jsou nejčastěji řazeny údaje o totožnosti uživatelů (jejich jméno, adresa apod.). Zásah do základních práv způsobený uchováváním a zpřístupněním těchto údajů bývá často považován za méně závažný, jelikož tyto údaje *samy o sobě* neumožňují zjistit datum, čas, dobu trvání, četnost a adresáta uskutečněné komunikace či místo, kde se tato komunikace uskutečnila.[238] Proto i podmínky pro uchovávání těchto údajů a pro přístup k nim bývají často mírnější.

Nepanuje však shoda nad tím, zda by za údaje o předplatitelích měly být považovány také údaje jako je IP adresa či číslo SIM, které budou často tvořit právě nezbytný mezičlánek mezi údaji, které mají příslušné orgány k dispozici, a identitou uživatele.[239] Dle mého názoru ani IP adresy *samy o sobě* neumožňují zjistit výše uvedené detaily o konkrétních sděleních, a tudíž na ně lze uplatnit stejnou logiku jako na ostatní údaje o předplatitelích. Je si však třeba uvědomit, že údaje o předplatitelích budou zpravidla představovat klíč k propojení určitých sdělení či zařízení s konkrétními uživateli, a tudíž k přiřazení identity k jiným, zpravidla podstatně citlivějším údajům. Proto by z mého pohledu i podmínky pro jejich uchovávání a zpřístupnění by měly podléhat dodatečným zárukám, byť třeba ne tak přísným jako v případě lokalizačních údajů, které jsou svou povahou jistě citlivější. Umožnění přístupu k těmto údajům např. i za účelem řešení přestupků a bez předchozího souhlasu soudu, což některé vnitrostátní právní úpravy umožňují, se jeví jako příliš problematické.[240]

Jaké konkrétní provozní a lokalizační údaje budou v jednotlivých případech uchovávány, značně souvisí se zvoleným způsobem komunikace. V případě mobilního telefonního hovoru tak zpravidla půjde mj. o následující údaje: telefonní číslo volaného a volajícího; identifikátor IMSI; identifikátor IMEI; datum, čas a délka hovoru; jednotlivé vysílače (BTS stanice), přes které hovor začal a skončil; typ komunikace (hovor, videohovor, SMS atd.); úspěšnost komunikace a v neposlední řadě jméno, příjmení a adresa předplatitele.

---

[238] Srov. rozsudek *La Quadrature du Net*, bod 157.
[239] Srov. Europol. *Data categories to be retained for law enforcement purposes – Working paper*, 2017, s. 2 či European Commission. *Data Retention for law enforcement purposes – Final report*, s. 48.
[240] Srov. Council of the European Union. *Data retention – State of play*, 2018, s. 14.

V případě e-mailu odeslaného z počítače pak zpravidla půjde mj. o následující údaje: IP adresa počítače; identifikátor uživatelského účtu; e-mailové adresy odesílatele a adresátů; datum a čas odeslání zprávy a v neposlední řadě opět jméno, příjmení a adresa zákazníka. Není však nezbytné podávat důkladný výčet kategorií údajů uchovávaných při každém způsobu komunikace. Zjednodušeně lze uvést, že půjde o údaje sloužící k identifikaci zařízení (např. identifikátor IMEI), k identifikaci uživatele (např. telefonní číslo, IP adresa, e-mailová adresa, jméno a příjmení, adresa), časové údaje (okamžik odeslání zprávy či začátek a konec hovoru), lokalizační údaje (identifikátor BTS stanice) a údaje o způsobu komunikace.[241]

Co se týče délky uchovávání, zde opravdu existuje značný prostor pro jednotlivé právní úpravy. Lze si tak představit poměrně krátké doby uchovávání (několik týdnů) či doby velmi dlouhé (několik let). Samozřejmě lze dobu uchovávání stanovit i odlišnou pro jednotlivé kategorie údajů, což se vzhledem k jejich odlišné citlivosti i užitečnosti jeví jako žádoucí.

Dalším klíčovým aspektem právních úprav data retention jsou požadavky na zabezpečení těchto údajů. Nelze pochybovat o tom, že by poskytovatelé telekomunikačních služeb měly předmětná data zabezpečit přinejmenším tak, jako ostatní osobní údaje, se kterými disponují, což bývá v případě vnitrostátních právních úprav standardem. Nicméně lze si rozumně představit i přísnější požadavky za účelem vyloučení neoprávněného přístupu – a to jak ze stran zaměstnanců samotného poskytovatele služeb, tak orgánů státu a příp. i třetích osob. Může jít např. o povinnost pseudonymizace dat, vedení *logů*, oddělené uchovávání různých typů metadat, pravidelné testování úrovně zabezpečení, pravidlo čtyř očí při nahlížení do databáze apod. Co se týče zabezpečení mechanismu předávání, nabízí se např. inspirace rakouským předávacím systémem „*durchlaufstelle*“, který umožňoval zabezpečenou a oboustranně zašifrovanou komunikaci mezi příslušnými orgány a poskytovateli služeb, sbíral a generoval statistiky o počtu podaných a vyřízených žádostí, aniž by však údaje centrálně uchovával či umožňoval centralizovaný přístup k nim (klíče k obsahu totiž neměl centrální provozovatel *durchlaufstelle*, ale jen dožadující orgán a dožadovaný poskytovatel).[242] Je samozřejmě naprosto správné, aby náklady na takto robustní zabezpečení systém hradil stát, má-li o tyto údaje kvůli jejich nepostradatelnosti zájem.

[241] Pro podrobný výčet a popis zpracovávaných kategorií údajů při každém jednotlivém typu komunikace v českém prostředí srov. JIROVSKÝ, Lukáš. *Data retention – ukládání provozních a lokalizačních údajů*, 2015, s. 52 a násl.
[242] Srov. MYŠKA, Matěj. Právní úprava data retention v Rakousku. In: MYŠKA, Matěj. *Data Retention Reloaded: zkušenosti, problémy a aplikační praxe*, 2013, s. 49-51.

Mezi klíčové parametry v oblasti přístupu k údajům pak bude patřit zejména to, jaké orgány, k jakým účelům a za jakých podmínek mají mít k uchovávaným údajům přístup. Co se týče prvního zmíněného parametru, půjde zpravidla jak o orgány působící v oblasti trestního práva (o policii, státní zastupitelství a soudy), tak orgány působící v oblasti národní bezpečnosti či bezpečnosti státu (o zpravodajské služby či příp. armádu). Vymezení oprávněných orgánů jde samozřejmě ruku v ruce s vymezením cílů, jež má předmětná vnitrostátní právní úprava sledovat. V této souvislosti lze uvést, že poměrně kontroverzní se v minulosti ukázala otázka, zda by uchovávaná data měla být využívána nejen za účelem objasňování trestné činnosti, ale také za účelem její prevence. Přístup za účelem preventivního zásahu naopak bývá charakteristický pro oblast zajišťování národní bezpečnosti. Velmi diskutovaná byla také otázka, zda by přístup k údajům měl být umožněn při vyšetřování všech trestných činů, či pouze omezeného výčtu závažných trestných činů, příp. na základě jakých kritérií a jak přesně by měl být takový výčet vymezen. Nutno také dodat, že některé vnitrostátní právní úpravy také umožňují přístup k uchovávaným údajům i za jinými účely, např. za účelem pátrání po nezvěstných osobách či za účelem dohledu nad finančním trhem.

V oblasti podmínek přístupu jsou samozřejmě klíčové záruky proti zneužití. Právní úpravy data retention tak mohou stanovit např. kdy je možné o uchované údaje žádat (v této souvislosti lze stanovit např. možnost žádat o přístup pouze v případě, že ostatní metody nemohou vést k objasnění trestného činu), povinnost získání soudního povolení k přístupu k uchovávaným údajům, povinnost následného informování dotčených osob či nezávislý dohled nad činností oprávněných orgánů. Vzhledem ke specifikům činnosti zpravodajských služeb bývají stanovené záruky v oblasti národní bezpečnosti zpravidla volnější, než je tomu u orgánů působících v oblasti trestního práva.

3.1.4 Kritika data retention

Jak bylo zmíněno výše, máme-li k dispozici komunikační metadata za delší časové období, často nám to umožní činit poměrně přesné závěry o životech osob – jaká místa navštěvují, s jakými osobami se stýkají, jaké jsou jejich zájmy. Samozřejmě není vyloučeno, že z metadat půjdou vyčíst i poměrně citlivé údaje o zdravotním stavu, sexuální orientaci či náboženském a politickém přesvědčení. To vše se totiž odráží v tom, kde se pohybujeme, s kým komunikujeme a jaké webové stránky navštěvujeme. Kritici v této souvislosti proto často o data retention hovoří jako o ztělesnění orwellovského Velkého bratra, tedy jakéhosi nástroje totální společenské kontroly, stále sledujícího celou populaci a pátrajícího z hlediska společenského

řádu nežádoucím chování. Slova o „*totálním dohledu*“[243] či „*politickém ovládání ze strany státních agentur*“[244] nejsou v rámci debaty o data retention neobvyklá, přestože ve značné míře ignorují účel nástroje data retention v evropských státech (boj proti závažné trestné činnosti) i záruky, které se k němu zpravidla pojí (použití pouze v případě nezbytnosti v konkrétním vyšetřování, souhlas soudu, povinnost informovat subjekt údajů a následný soudní přezkum). Současná praxe fungování data retention má totiž k orwellovskému Velkému bratru skutečně velmi daleko.

To však neznamená, že bychom měli kritiku plošnosti uchovávání ignorovat. Rizika spojená se zneužitím přístupu k plošně uchovávaným údajům sice můžeme minimalizovat, ovšem nikdy je nemůžeme zcela vyloučit. Není možné zcela vyloučit, že státní orgány získají přístup k citlivým osobním údajům o osobě, která se nakonec ukáže být nevinnou. Není možné zcela vyloučit, že určité příslušné osoby zneužijí přístup k uchovávaným datům k soukromým záležitostem.[245] K takovému zneužívání může docházet i v rámci širší praxe státních orgánů.[246] Dále platí, že k neoprávněnému přístupu nemusí dojít jen ze strany státních orgánů, ale i ze strany samotných poskytovatelů služeb či dokonce třetích osob. Databáze provozních a lokalizačních údajů v tomto ohledu mohou představovat významný cíl např. pro hackerské útoky.[247] I při sebelepším zabezpečení přitom nelze vyloučit, že taková databáze bude prolomena a osobní údaje z ní budou odcizeny, zneužity třetími osobami či zveřejněny. Jinými slovy, jsou-li dotčené údaje uchovány, nelze nikdy s absolutní jistotou vyloučit, že budou v budoucnu zpracovány, ať už v souladu se zákonem (např. při odůvodněném, avšak nepotvrzeném podezření), v rozporu se zákonem (např. při zneužití přístupu či odcizení dat), nebo někde na pomezí těchto situací (např. při zbytečném nadužívání dotčeného nástroje ze strany orgánů státu).

---

[243] Srov. SARRE, Rick. Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia. *Asian Journal of Criminology*, 2017, s. 169.
[244] Srov. BREYER, Patrick. Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, 2005, s. 371.
[245] V této souvislosti lze uvést jako příklad policisty, který v roce 2009 a 2010 dostal od Okresního soudu v Děčíně souhlas ke zpřístupnění provozních a lokalizačních údajů týkajících padesáti čísel, mezi nimiž byl předseda ústavního soudu, kancléř prezidenta, manažer ČEZ či novináři MF Dnes a to pod záminkami jako prověřování obchodu s lidmi. Z tohoto důvodu by mělo být vyžadováno, aby v případech, kdy je jméno dotčené osoby známo, bylo v žádosti uvedeno. Srov. JIROVSKÝ, Lukáš. *Data retention – ukládání provozních a lokalizačních údajů*, 2015, s. 62. Případy zneužití poskytovatelem služeb byly odhaleny v Německu. V Polsku bylo zase odhaleno nezákonné zpracování dotčených údajů zpravodajskými službami. Srov. European Digital Righs. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, s. 18.
[246] Srov. NI LOIDEAIN, Nora. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication*, s. 3.
[247] Srov. CLARKE, Roger. Data retention as mass surveillance: the need for an evaluative framework. *International Data Privacy Law*, 2015, s. 128.

Právě z tohoto důvodu může už samotné uchovávání zasahovat do soukromé sféry jednotlivců a mít dopad na jejich chování. Data retention je v tomto ohledu je často přirovnávána k *Panopticonu* Jeremyho Benthama, filosofickému konceptu vycházejícího z toho, že již pouhá možnost, že je vězeň sledován dozorcem, postačí k ovlivnění jeho chování, není-li možné ze strany vězně zjistit, zda ke sledování opravdu dochází.[248] Podobné dopady může mít i jen potenciál skrytého sledování ze strany státu na chování veřejnosti. Pokud si totiž nemůžeme být jisti, že naše chování v soukromí zůstane v soukromí napořád, může to vést k tomu, že se začneme v soukromí chovat stejně jako na veřejnosti. Někteří autoři v této souvislosti hovoří o změně perspektivy z první do třetí osoby[249] či o ztrátě soukromé a zachování pouze veřejné roviny osobnosti.[250] Nejčastěji je v této souvislosti používán pojem „*chilling effect*“, jež označuje nežádoucí účinek, kdy právní úprava zaměřená na potírání určitého nežádoucího chování vede k omezení chování v demokratických státech povoleného či dokonce žádoucího, např. aktivního zapojení se do diskuze o politických otázkách.[251]

K výše uvedené kritice týkající se závažnosti zásahu do soukromí se pak často přidává i kritika poukazující na údajnou neúčinnost data retention při dosahování vytyčených cílů. Kritici v této souvislosti upozorňují, že přestože mají státní orgány tento nástroj k dispozici už delší dobu a hojně jej využívají, statistiky neukazují, že by se to odrazilo i v míře objasněnosti trestných činů či míře jejich páchání.[252] Vskutku, členské státy ani Komise zatím nebyly sto předložit studii, jež by prokazatelně demonstrovala, že data retention má reálný dopad na celkovou míru objasněnosti trestných činů.[253] A to i přesto, že příslušné orgány tento nástroj využívají poměrně hojně.[254] Osobně mne však tento argument příliš nepřesvědčuje – potírání trestné činnosti napříč členskými státy je extrémně komplexní problematika a z mého pohledu nelze neúčinnost data retention dovozovat pouze z toho, že její zavedení či zrušení nemá jasné dopady na celkové roční statistiky objasněnosti trestných činů, obzvlášť když

[248] Srov. SPINA, Alessandro. Risk Regulation of Big Data: Has the Time Arrived for a paradigm Shift in EU Data Protection Law? *European Journal of Risk Regulation*, 2014, s. 251.
[249] ROBERTS, Andrew. Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. *Modern Law Review*, 2015, s. 543.
[250] DESIMONE, Christian. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, 2010, s. 294.
[251] Srov. např. PENNEY, W. Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review*, 2017, s. 1.
[252] Srov. např. European Digital Righs. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, s. 7.
[253] Srov. stanovisko generálního advokáta Saugmandsgaarda Øe ze dne 19. července 2016 spojených věcech *Tele2 Sverige a Watson a další*, C-203/15 a C-698/15, EU:C:2016:572, bod 209 (dále jen „*stanovisko GA ve věci Tele2 Sverige*“) či nález Ústavního soudu ze dne 22. března 2011, Pl. ÚS 24/10, bod 56 a zde citované statistiky.
[254] Srov. nález Ústavního soudu ze dne 22. března 2011, Pl. ÚS 24/10, bod 49.

příslušné orgány zpravidla nemají problém nepostradatelnost data retention demonstrovat na konkrétních případech.

Řada kritiků taktéž uvádí, že data retention není potřeba, jelikož i v členských státech, kde tato povinnost z nějakého důvodu zavedena není, příslušné orgány členských států nemají zpravidla problém potřebná metadata získávat, jelikož si je poskytovatelé služeb uchovávají pro vlastní účely. Vskutku, např. v Německu po zrušení právní úpravy data retention ústavním soudem příslušné orgány zjistily, že se k potřebným údajům nedostanou zhruba pouze ve 4 % případů.[255] Obdobné zkušenosti mají taktéž v Dánsku[256], České republice[257] i řadě dalších států.[258] Pravděpodobně se bude jednat i o důvod, proč samotné zrušení data retention se neprojevuje na celkových statistikách objasněnosti trestných činů.

Z mého pohledu se však nejedná o argument proti data retention, ale spíše na její podporu. Dokládá totiž, že „dodatečný" zásah do základních práv způsobený data retention se jen velmi málo liší od rozsahu zásahu do základních práv způsobeným uchováváním údajů pro komerční účely. Tento dodatečný zásah má však vysokou přidanou hodnotu, jelikož vylučuje, aby se úspěšnost vyšetřování odvíjela *de facto* od náhody, zda údaje nezbytné pro vyšetřování nebudou právě v tom malém procentu údajů, které se poskytovatel služeb rozhodl neuchovávat. Takové případy přitom v praxi prokazatelně nastávají.[259]

3.1.5 Obhajoba data retention

Obhájci data retention na druhé straně vyzdvihují přínos tohoto nástroje v boji se závažnou trestnou činností a hrozbami v oblasti národní bezpečnosti, přičemž se odvolávají mj. na „druhou" lidskoprávní rovinu dotčené problematiky, tj. právo každého na bezpečnost ve smyslu čl. 5 Úmluvy a čl. 6 Listiny základních práv EU.

Jak bylo uvedeno výše, v současnosti neexistují studie prokazující, že by data retention vedla k celkově menšímu množství páchaných či většímu množství úspěšně vyšetřených trestných činů. Státní orgány nicméně obvykle nemají problém dokladovat efektivitu tohoto nástroje na konkrétních příkladech. Dojde-li např. k sérii vloupání, můžeme data retention použít ke zjištění, zda se určitý mobilní telefon v rozhodnou dobu nacházel na více místech činu. Dojde-li k únosu, může být nenahraditelná možnost lokalizovat telefon oběti. V případě

[255] Srov. European Digital Rights. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, s. 13.
[256] Srov. ibidem, s. 14.
[257] Srov. nález Ústavního soudu ze dne ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17, bod 34.
[258] Srov. European Commission. *Data Retention for law enforcement purposes – Final report*, 2020, s. 17.
[259] Srov. ibidem, s. 41 či nález Ústavního soudu ze dne ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17, bod 22.

vraždy může být zase zcela zásadní zjistit, s kým oběť komunikovala bezprostředně před tím, než byla usmrcena. Obdobných případů, z nichž je užitečnost data retention zcela zjevná, lze přitom uvést nespočet. Provozní a lokalizační údaje mohou být v některých případech klíčovým důkazem, v jiných případech pouze dílem mozaiky spolu s dalšími důkazy.[260] Mohou být užitečné jak v případech, kdy policie vyžaduje informace o konkrétním uživateli (např. výpis hovorů z jeho telefonního čísla), tak v případech, kdy policie konkrétního uživatele hledá (a vyžádá si tedy např. výpis čísel, které v okamžiku spáchání trestného činu odeslali zprávu z místa činu, jakož i identifikační údaje vlastníků těchto čísel).

Význam data retention navíc roste v souvislosti s tím, jak roste význam elektronické komunikace v každodenním životě. V dnešní době lze jen těžko očekávat, že by komunikace mezi pachateli trestného činu či mezi obětí a pachatelem byla zachycena v jiné než elektronické podobě. Samo páchání trestných činů se mnohdy přesouvá do kyberprostoru, přičemž dochází ke vzniku řady nových, značně společensky nebezpečných trestných činů, jež jsou páchány převážně či výhradně prostřednictvím internetu.[261] Prostředí internetu je přitom charakteristické tím, že v něm žádné stopy nevznikají náhodně. Zatímco v případě „běžného" trestného činu lze spoléhat na to, že onen „pohled do minulosti" poskytnou příslušným orgánům výpovědi svědků, stopy v blátě či otisky prstů, v prostředí internetu žádná obdobná stopa nevznikne, resp. ne bez jasně daného technologického pravidla. Těchto skutečností si jsou pachatelé samozřejmě dobře vědomi, a proto dnes hojně využívají prostředků komunikace na dálku. Zatímco tedy v minulosti bychom o data retention hovořili jako o užitečném nástroji pro boj proti bezpečnostním hrozbám, s tím, jak se celý náš život (včetně trestné činnosti a terorismu) přesouvá do kyberprostoru, stává se z data retention nástroj nejen užitečný, ale – alespoň z pohledu jejích zastánců – také nezbytný.

Krom nepostradatelnosti data retention při zajišťování bezpečnosti její zastánci také zdůrazňují rozdíl mezi uchováváním údajů a přístupem k nim. Ačkoliv dochází k uchovávání údajů o všech uživatelích elektronické komunikace, k přístupu k těmto údajům dojde jenom v nepatrném zlomku odůvodněných případů, přičemž zbylé údaje budou po uplynutí několika měsíců bez dalšího vymazány. Zastánci data retention uvádějí, že riziko neoprávněného přístupu k předmětným údajům lze minimalizovat právě prostřednictvím přísných podmínek

[260] Srov. RAUHOFER, Judith. Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union. *SCRIPTed: Journal of Law, Technology and Society*, 2006, s. 328.
[261] Srov. WHITLEY, Edgar. Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy*, 2005, s. 860.

pro přístup a důkladnou kontrolou jejich dodržování.[262] V této souvislosti také bývá zmiňováno, že v mnohých případech může využití provozních a lokalizačních údajů v konečném důsledku vést k menšímu zásahu do soukromí jednotlivců, jelikož nebude třeba přistupovat k intrusivnějším metodám, jako jsou např. odposlechy či sledování osoby. V neposlední řadě zastánci data retention upozorňují – jak bylo uvedeno výše – na skutečnost, že velká část údajů je poskytovateli služeb uchovávána pro jejich vlastní komerční účely, byť v některých případech jen po kratší dobu.

3.1.6 Alternativy plošné data retention

Otázku nezbytnosti plošné data retention nelze oddělit od otázky, zda existují nějaké alternativní nástroje, které by umožňovaly dosažení téhož cíle a zároveň představovaly menší zásah do základních práv jednotlivců. V tomto ohledu bývají zmiňovány v zásadě pouze dva nástroje, které by plošné data retention mohly konkurovat – zaprvé jde o tzv. „*quick freeze*“, zadruhé o cílenou data retention.

Quick freeze, jehož zavedení v členských státech vyžaduje např. Úmluva o počítačové kriminalitě,[263] spočívá v oprávnění státních orgánů (zpravidla policie či státního zastupitelství) uložit poskytovateli služeb povinnost uchovávat určité provozní a lokalizační údaje, existuje-li předpoklad, že tyto údaje budou potřeba pro konkrétní vyšetřování. V závislosti na parametrech konkrétní úpravy může jít buď o povinnost uchovávat provozní a lokalizační údaje pouze do budoucna, nebo i o povinnost zachovat veškeré údaje o dané osobě, které má v daném okamžiku poskytovatel služeb k dispozici (někdy také označováno jako tzv. „*quick freeze plus*“).[264] V tom, co následuje dále, se *quick freeze* velmi podobá data retention – zpravidla půjde o možnost přístupu k uchovaným údajům na základě souhlasu soudu za účelem vyšetřování závažné trestné činnosti, následná povinnost informovat subjekt údajů a související možnost u soudu či dozorového úřadu napadat odůvodněnost přístupu.

Cílená data retention se pak co do účinnosti a míry zásahu do základních práv nachází někde na půli cesty mezi *quick freeze* a plošnou data retention. Podstata tohoto nástroje spočívá v tom, že povinnost uchovávat údaje není stanovena plošně pro všechny uživatele elektronických komunikací, ale pouze pro určitý okruh uživatelů, jejichž údaje mohou vykázat minimálně nepřímou souvislost s ohrožením veřejné bezpečnosti. V této souvislosti může jít

[262] Srov. např. stanovisko GA ve věci *Tele2 Sverige*, bod 193.
[263] Srov. čl. 16 Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s., o sjednání Úmluvy o počítačové kriminalitě.
[264] Srov. MIKOLASCH, Felix. *Data Retention in the European Union*, 2019, s. 33.

např. o vymezení územních oblastí, v nichž existuje vyšší riziko páchání závažné trestné činnosti. Opět platí, že způsob využití uchovaných údajů se neliší od plošné data retention.

Z výše uvedeného popisu obou nástrojů jsou zjevné jejich limity ve srovnání s plošnou data retention. *Quick freeze* nenabízí onen „pohled do minulosti", ve kterém spočívá hlavní užitečnost data retention. *Quick freeze plus* jej v určitých případech nabízet může, ovšem tato možnost se odvíjí výhradně od toho, zda sám poskytovatel služby potřebné provozní a lokalizační údaje uchovával pro vlastní účely, či nikoliv. V případě cílené data retention pak sice ve srovnání s *quick freeze* odpadá nutnost podezřívat konkrétní osobu či skupinu osob, zároveň však platí, že k závažné trestné činnosti může docházet na celém území státu, a omezení uchovávání údajů pouze na některé oblasti tak významně snižuje účinnost tohoto nástroje. V případě trestných činů páchaných prostřednictvím internetu pak místní kritérium ztrácí význam úplně.

Nemůže však být pochyb o tom, že jsou obě metody šetrnější k soukromí jednotlivců. V tomto ohledu je nejšetrnější samozřejmě *quick freeze*, jelikož k uchovávání nedochází plošně, nýbrž až v souvislosti s konkrétní hrozbou. Nelze tedy očekávat, že by některá z těchto alternativ mohla u obyvatelstva vyvolávat zmíněný *chilling effect* v míře, v jaké tomu může být v případě plošné data retention. U cílené data retention jsou negativní dopady uchovávání sice širší než v případě *quick freeze*, ale oproti plošné data retention stále alespoň omezeny pouze na určité oblasti. Zatímco metoda *quick freeze* je ve státech, které nestanoví plošnou data retention, poměrně běžná (obsahuje ji mj. slovenská či rakouská úprava), cílená data retention v členských státech v současnosti uplatňována není, právě kvůli tomu, že zaměření data retention pouze na určité oblasti není v praxi funkční.[265]

3.2 DATA RETENTION V SEKUNDÁRNÍM PRÁVU EU

3.2.1 Situace před přijetím směrnice 2006/24

Ačkoliv lze počátky diskuze o data retention vystopovat již na konec devadesátých let, nelze pochybovat o tom, že to byly právě teroristické útoky z počátku 21. století, které vedly ke značnému zvýšení poptávky po jejím zavedení v členských státech EU. Tato poptávka přicházela nejen od příslušných orgánů, politiků a veřejnosti uvnitř členských států, ale taktéž zvenčí. Již v říjnu 2001 se např. na tehdejšího předsedu Komise obrátil americký prezident G. W. Bush, aby mu doporučil zvážit revizi směrnice 97/66 tak, aby výslovně umožnila

[265] Srov. Eurojust. *Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report*, 2017, s. 6 a 12.

uchovávání údajů na určitou nezbytně nutnou dobu za účelem boje proti terorismu.[266] Toto doporučení v zásadě reflektovalo pozici některých členských států.[267] Např. Spojené království v dotčeném období zavádělo data retention do svého právního řádu, aniž by však na vnitrostátní úrovni existovala jednoznačná shoda ohledně toho, zda to tehdejší směrnice 97/66 umožňovala.[268] Ta totiž sice členským státům umožňovala přijmout opatření k omezení práv vyplývajících z této směrnice za účelem zajišťování veřejné a národní bezpečnosti, avšak výslovně nezmiňovala data retention jako jedno z opatření, které členské státy mohou v této souvislosti přijmout.

To bylo napraveno ve směrnici 2002/58, která již možnost uložit povinnost uchovávání údajů výslovně zmiňovala.[269] Některé členské státy, včetně např. České republiky, této možnosti využily a data retention zavedly dříve než v rámci transpozice směrnice 2006/24. Komise později v rámci legislativního procesu vedoucího k přijetí směrnice 2006/24 uvedla, že jediným důvodem, proč nebyla již ve směrnici 2002/58 data retention koncipována jako povinnost, byla skutečnost, že se členské státy nemohly shodnout na délce uchovávání údajů.[270] Tomu se ovšem poměrně těžko věří s ohledem na to, že následně při přijímání směrnice 2006/24 se jako velmi kontroverzní ukázala celá řada dalších aspektů.[271]

3.2.2 Směrnice 2006/24

3.2.2.1 Směrnice 2006/24 – legislativní historie

Klíčovým impulsem pro to, aby se z data retention stala pro členské státy povinnost, byly teroristické útoky v Madridu a Londýně. V návaznosti na tyto útoky uložila Evropská rada Radě, aby prozkoumala „*návrhy na zavedení pravidel o uchovávání provozních údajů*

---

[266] Srov. WHITLEY, Edgar. Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy*, 2005, s. 865. V tomto ohledu se unijní úprava podstatně lišila od té americké, která neobsahovala povinnost operátorů údaje mazat. Srov. BIGNAMI, Francesca. Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, 2007, s. 238.

[267] Srov. BROWN, Ian. Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, 2010, s. 95-96.

[268] RAUHOFER, Judith. Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union. *SCRIPTed: Journal of Law, Technology and Society*, 2006, s. 331-332.

[269] Viz kapitola 2.3.2.

[270] Evropská komise. *Důvodová zpráva k návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES*, 2005, s. 8.

[271] Viz kapitola 3.2.2.

o komunikaci ze strany poskytovatelů služeb“ s cílem jejich přijetí v roce 2005.[272] Samozřejmě nelze pochybovat o tom, že značnou roli sehrál taktéž tehdejší rapidní technologický rozvoj, a to nejen v tom smyslu, že bylo stále snadnější uchovávat a třídit velká množství dat, ale také v tom smyslu, že v souvislosti s nástupem paušálních telefonních tarifů a internetové komunikace se podstatně změnila struktura dat, které si poskytovatelé služeb uchovávali pro vlastní potřebu. Některé údaje důležité pro bezpečnostní složky již nebyly poskytovateli služeb dobrovolně uchovávány, resp. nebyly uchovávány spolehlivě či dostatečně dlouho.[273]

Směrnice 2006/24 nicméně nebyla původně koncipována jako směrnice založená na tehdejším čl. 95 SES, ale jako rámcové rozhodnutí navrhované v rámci tehdejšího třetího pilíře společně Spojeným královstvím, Francií, Švédskem a Irskem.[274] Volba tohoto právního základu odpovídala hlavnímu cíli dotčeného opatření, kterým byl bezesporu boj proti terorismu a jiné závažné trestné činnosti. S tímto přístupem však nesouhlasila Komise, která měla – na rozdíl od toho, co v souvislosti s data retention uváděla v legislativním procesu vedoucím k přijetí směrnice 2002/58[275] – za to, že uchovávání údajů představovalo zásah do zásady důvěrnosti komunikace stanovené směrnicí 2002/58, a tudíž nemohlo být nařízeno v rámci třetího pilíře.[276] Nesprávný právní základ namítal taktéž Evropský parlament, který navíc navrhovaná opatření považoval za nepřiměřený zásah do práva na soukromí.[277] Tento názor sdílel i Evropský inspektor ochrany údajů, pracovní skupina WP29[278] a řada nevládních organizací zabývajících se ochranou osobních údajů.[279] Oproti konečné formě směrnice obsahoval návrh rámcového rozhodnutí širší vymezení účelů, pro něž mají být údaje uchovávány (včetně prevence „běžné“ trestné činnosti) a delší lhůty pro uchovávání (až 36 měsíců). Zároveň vyžadoval uchovávání údajů o navštívených webových stránkách.

Ve světle těchto výhrad byl nakonec návrh rámcového rozhodnutí opuštěn ve prospěch návrhu směrnice založené na ex čl. 95 SES. Klíčovou roli v tomto ohledu sehrálo stanovisko

---

[272] Srov. Evropská komise. *Důvodová zpráva k návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES*, 2005, s. 2.
[273] Ibidem.
[274] Srov. BIGNAMI, Francesca. Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, 2007, s. 239.
[275] Viz kapitola 4.1.2.3.
[276] Srov. FENELLY, David. Data retention: the life, death and afterlife of a directive. *ERA Forum*, 2018, s. 676.
[277] RAUHOFER, Judith. Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union. *SCRIPTed: Journal of Law, Technology and Society*, 2006, s. 333.
[278] Srov. DESIMONE, Christian. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, 2010, s. 302.
[279] Ibidem, s. 306.

právní služby Rady, které s ohledem na aktuální judikaturu Soudního dvora týkající se trestních sankcí v oblasti životního prostředí konstatovalo, že pokud by Evropský parlament rámcové rozhodnutí napadl u Soudního dvora, měl by velkou šanci se svou žalobou uspět.[280]

Pro formu směrnice zde hovořily i další, bohužel podstatně méně legitimní důvody. Zaprvé šlo o to, že přijetí rámcového rozhodnutí záviselo na dosažení konsensu v Radě, který však v dotčeném okamžiku nebyl vůbec jistý kvůli váhavému postoji Německa a Rakouska.[281] Takový přístup je však extrémně problematický, jelikož nijak nesouvisí s obsahem aktu, který by měl být pro volbu právního základu klíčový. Zadruhé, forma směrnice znamenala taktéž zapojení Evropského parlamentu, a tedy zvýšení demokratické legitimity dotčeného opatření, což bylo s ohledem na závažnost zásahu do základních práv způsobeného data retention vnímáno jako důležité.[282] Takový přístup je dle mého názoru také nesprávný, jelikož právní základ opět nevychází z obsahu aktu, ale naopak z procedury, která se v daném případě jeví jako vhodnější.[283]

Návrh směrnice volbu právního základu zdůvodňoval tak, že rozdíly v právních, regulativních a technických předpisech členských států, které upravují uchovávání provozních údajů, představují překážku vnitřního trhu, jelikož se poskytovatelé služeb potýkají s různými požadavky, pokud jde o to, jaké údaje se mají uchovávat a za jakých podmínek.[284] Z celé legislativní historie popsané výše je však zřejmé, že skutečným důvodem pro přijetí dotčené úpravy nebyly problémy potíže poskytovatelů služeb elektronických komunikací, ale boj proti bezpečnostním hrozbám, přičemž přeshraniční prvek spočíval v přeshraničním charakteru terorismu a závažné trestné činnosti. Ten vyvolával potřebu spolupráce mezi příslušnými orgány členských států, jejímž předpokladem je vůbec existence údajů, které mohou být sdíleny napříč tehdejším Společenstvím.

---

[280] Srov. SERVENT, Ariadna Ripoll. Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, 2013, s. 977 či RAUHOFER, Judith. Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union. *SCRIPTed: Journal of Law, Technology and Society*, 2006, s. 334.

[281] Srov. DESIMONE, Christian. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, 2010, s. 301.

[282] Srov. BIGNAMI, Francesca. Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, 2007, s. 240.

[283] Formálně čistějším řešením by tak byla zvažovaná *passerelle* procedura či přijetí nástroje pro ochranu údajů i v rámci třetího pilíře, pro kterou však nebyla nalezena dostatečná podpora. Srov. SERVENT, Ariadna R. Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, 2013, s. 978.

[284] Srov. Evropská komise. *Důvodová zpráva k návrhu směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES*, 2005, s. 2.

Zároveň si musíme uvědomit, že čl. 15 odst. 1 směrnice 2002/58 nadále umožňoval členským státům požadovat uchovávání údajů, jejichž uchovávání směrnice 2006/24 nevyžaduje. Taktéž podmínky přístupu byly ponechány na členských státech. Harmonizační účinek směrnice tak byl, budeme-li se na něj dívat výhradně optikou obtíží, které mohou odlišné předpisy působit přeshraničně působícím poskytovatelům služeb, naprosto marginální, nebo spíše záporný. Před přijetím směrnice se museli poskytovatelé služeb vypořádat jen s pěti odlišnými vnitrostátními právními úpravami data retention (ostatní státy takovou právní úpravu neměly), po jejím přijetí bylo takových úprav 25, vzhledem k výše uvedenému nadále velmi odlišných.[285] Otázkou navíc zůstává, do jaké míry byla směrnice nezbytná i k jejímu skutečnému cíli, jelikož se následně ukázalo, že jen necelé 1 % přístupů k údajům se týkalo komunikačních metadat uchovávaných v jiném členském státě.[286]

V každém případě se tato dichotomie mezi deklarovaným a skutečným účelem směrnice 2006/24 následně stala jedním z klíčových problémů této směrnice, jak bude demonstrováno v kapitole zabývající se analýzou judikatury Soudního dvora v této oblasti.[287] Důsledkem volby dotčeného právního základu totiž bylo, že problematika přístupu k údajům byla ponechána zcela na členských státech, jelikož Rada i Komise (na rozdíl od Evropského parlamentu)[288] měly za to, že opatření založené pouze na ex čl. 95 SES nemůže tuto problematiku upravovat.[289]

Zapojení Komise a Evropského parlamentu se i tak projevilo ve zmírnění intenzity zásahu do základních práv oproti původnímu návrhu v několika ohledech. Doba uchovávání byla oproti návrhu rámcového rozhodnutí v návrhu směrnice omezena na 1 rok, v případě údajů o internetové komunikaci dokonce na 6 měsíců. Takto restriktivní přístup byl ale nakonec v legislativním procesu odmítnut ve prospěch konečného kompromisu spočívajícího v době uchovávání v délce 6 až 24 měsíců pro všechny údaje. Z povinně uchovávaných údajů byly vypuštěny údaje o neúspěšných hovorech a webových adresách. Účel uchovávání údajů byl omezen pouze na závažné trestné činy, ovšem tento pojem nebyl ve směrnici definován, jelikož Evropským parlamentem navrhovaný odkaz na rámcové rozhodnutí o evropském zatýkacím rozkazu nebyl přijat. Z důvodu obav ohledně preventivního zpracovávání údajů za účelem identifikace jedinců, kteří by měli spáchat trestné činy v budoucnu, byla z účelů uchovávání

[285] Srov. European Digital Righs. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, s. 5.
[286] Ibidem, s. 11.
[287] Viz kapitola 4.1.2.
[288] Srov. PEERS, Steve. The European Parliament and data retention: Chronicle of a 'sell-out' foretold? *Statewatch*, 2005, s. 6.
[289] Srov. FENELLY, David. Data retention: the life, death and afterlife of a directive. *ERA Forum*, 2018, s. 677.

vypuštěna prevence závažné trestné činnosti.[290] V této souvislosti je však třeba zdůraznit, že vyloučení těchto účelů uchovávání ze směrnice 2006/24 nemělo za důsledek to, že by členské státy nemohly přijmout vnitrostátní právní úpravu data retention za těmito účely – k takovému postupu je nadále opravňoval čl. 15 odst. 1 směrnice 2002/58.

Přestože mezi Radou a Evropským parlamentem v průběhu legislativního procesu existovaly velmi rozdílné názory na přiměřenost dotčených opatření, směrnice byla nakonec přijata poměrně rychle. Jak uvádí DeSimone, jednalo se paradoxně o jednu z nejrychlejších spolurozhodovacích procedur.[291] To bylo dáno především tím, že plénum Evropského parlamentu se nakonec odklonilo od pozice příslušného parlamentního výboru a přiklonilo se k pozici Rady.[292] Klíčový byl v tomto ohledu postup britského předsednictví, které deklarovalo, že ochota Rady pokračovat cestou směrnice (tj. spolurozhodování) bude záviset na rychlosti, s jakou se bude dařit nalézat kompromis mezi Radou a Evropským parlamentem ohledně sporných otázek. Právě tato strategie vedla k tomu, že se směrnici podařilo přijmout nejen rychle, ale především předtím, než předsednictví převzalo Rakousko, které bylo k problematice data retention mnohem kritičtější.[293]

3.2.2.2 Směrnice 2006/24 – obsah

Čl. 1 směrnice 2006/24 upravoval její předmět a oblast působnosti. První odstavec vystihoval pro budoucí judikaturu klíčovou dichotomii cílů směrnice, když uváděl, že jejím „účelem" je harmonizovat předpisy členských států týkající se povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, s „cílem" zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak jsou vymezeny každým členským státem v jeho vnitrostátních právních předpisech. I přes tuto dichotomii však byla směrnice založena pouze na právním základu, který odpovídal jejímu „účelu", tj. na čl. 95 tehdejší SES.

---

[290] Pro přehledný popis rozdílů mezi původním návrhem Komise, postojem Evropského parlamentu a výsledným textem viz SERVENT, Ariadna R. Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, 2013, s. 975 či PEERS, Steve. The European Parliament and data retention: Chronicle of a 'sell-out' foretold? *Statewatch*, 2005.

[291] Srov. DESIMONE, Christian. Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, 2010, s. 304.

[292] SERVENT, Ariadna Ripoll. Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy*, 2013, s. 977.

[293] Srov. RAUHOFER, Judith. Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union. *SCRIPTed: Journal of Law, Technology and Society*, 2006, s. 336.

Druhý odstavec čl. 1 směrnice vymezoval rozsah údajů, na nějž se směrnice vztahovala. Krom provozních a lokalizačních údajů výslovně hovořil i o tzv. souvisejících údajích, které jsou nezbytné k identifikaci účastníka nebo registrovaného uživatele. Čl. 2 pak obsahoval definice základních pojmů, jako např. údaje, účastníka, telefonní služby apod. Ohledně pojmů, které zde nebyly definovány, bylo odkazováno na směrnice 95/46 a 2002/21.[294]

Klíčovým ustanovením byl čl. 3, který nejenže ukládal členským státům přijmout právní předpisy ukládající povinnost uchovávání údajů, ale především upřesňoval, že se tato povinnost měla vztahovat na údaje vytvářené nebo zpracovávané poskytovateli veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí. S ohledem na širokou škálu způsobů elektronické komunikace i množství poskytovatelů služeb, které se často musí k přenosu zprávy zapojit na straně odesílatele i příjemce, nemusí být z takového vymezení zcela jasné, kdo přesně je v jednotlivých případech povinen údaje uchovávat. Právě v souvislosti s definicí těchto pojmů bylo třeba obrátit se na směrnici 2002/21, dle které se „*službou elektronických komunikací rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové vysílání, s výjimkou služeb poskytujících obsah nebo vykonávajících redakční dohled nad obsahem přenášeným prostřednictvím sítí a služeb elektronických komunikací; pojem nezahrnuje služby informační společnosti, jak jsou definovány v článku 1 směrnice 98/34/ES, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací;*“ a „*veřejnou komunikační sítí rozumí síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací a která podporuje přenos informací mezi koncovými body sítě;*“. Ani tyto definice však nejsou na první pohled zcela jednoznačné, abychom byli schopni v případě jednotlivých druhů komunikace určit, jaký subjekt bude nucen údaje uchovávat. V této souvislosti je klíčové, že aby mohl být subjekt považován za poskytovatele těchto služeb, musí mít především odpovědnost za přenos signálu.[295] Zjednodušeně řečeno, je třeba rozlišovat mezi přenosem signálu a obsahem konkrétní služby.

Proto v drtivé většině případů dopadala povinnost uchovávání údajů na poskytovatele internetového připojení či operátory mobilní sítě (tj. společnosti jako Vodafone, O2, T-Mobile

[294] Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).
[295] Rozsudek Soudního dvora ze dne 30. dubna 2014, *UPC DTH*, C-475/12, EU:C:2014:285, bod 43.

či UPC), nikoliv poskytovatele konkrétních webových služeb (společnosti Google, Seznam, Facebook apod.).[296] Nedopadala tak ani na služby umožňující zasílání e-mailu prostřednictvím webového klienta (tzv. „*freemail*“) či na tzv. *over-the-top messaging* služby jako je WhatsApp, Skype či Viber. Někteří poskytovatelé webových služeb, např. Google, se nicméně v minulosti přesto (neoprávněně) odvolávaly na povinnosti vyplývající ze směrnice 2006/24, aby odůvodnily rozsah provozních a lokalizačních údajů, které uchovávaly.[297] K rozšíření působnosti směrnice 2006/24 i na internetové vyhledávače po jejím přijetí vyzval Evropský parlament, a to za účelem zefektivnění boje proti šíření dětské pornografie, avšak nikdy k němu nedošlo.[298] Povinnosti vyplývající ze směrnice 2006/24 dopadaly nicméně taktéž na tzv. VoIP telefonii (tj. způsob telefonního spojení, při kterém hovor probíhá po internetové síti).[299] Dnes se jedná – právě ve srovnání s *over-the-top* službami – o poměrně marginální způsob komunikace.

Ačkoliv to text směrnice neumožňoval, některé členské státy se rozhodly z povinnosti uchovávání vyjmout malé poskytovatele služeb.[300] To je ovšem zcela pochopitelné, jelikož *stricto sensu* měly povinnosti ze směrnice dopadat např. i na internetové kavárny či restaurace, které svým zákazníkům nabízely možnost připojení k internetu.[301] V případě takových subjektů však nejenže neexistovala velká šance, že by se na ně příslušné orgány obrátily se žádostí o přístup k údajům, zároveň jistě nebylo v jejich silách uchovávání (a především zabezpečení) těchto údajů reálně zajistit.

Čl. 4 se pak věnoval problematice přístupu k údajům. Ačkoliv měl zákonodárce za to, že s ohledem na svůj právní základ nemůže směrnice tyto otázky regulovat, nebylo vynětí těchto otázek z působnosti směrnice důsledné. Čl. 4 v této souvislosti přeci jen určité podmínky stanovil, jelikož např. uváděl, že k přístupu k údajům může dojít pouze v konkrétních případech, v souladu s požadavky nezbytnosti a přiměřenosti a za podmínek dodržení ostatních

---

[296] Srov. FEILER, Lukas. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *European Journal of Law and Technology*, 2010, s. 3. Roberts. K rozšíření působnosti směrnice 2006/24 i na internetové vyhledávače po jejím přijetí vyzval Evropský parlament, a to za účelem zefektivnění boje proti šíření dětské pornografie. Srov. Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011, s. 13.

[297] Srov. ROBERTS, Hal. The EU Data Retention Directive in an Era of Internet Surveillance. In: DEIBERT, Ronald et al. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, 2010, s. 44.

[298] Srov. Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011, s. 13.

[299] Za službou elektronických komunikací je zároveň třeba považovat službu SkypeOut, která umožňuje uživateli volat na pevnou linku nebo mobilní telefon. Srov. rozsudek Soudního dvora ze dne 5. června 2019, *Skype Communications*, C-142/18, EU:C:2019:460.

[300] Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011, s. 9.

[301] Srov. VOBOŘIL, Jan. Využívání provozních a lokalizačních údajů ze strany oprávněných orgánů, zejména Policie ČR. In: MYŠKA, Matěj. *Data Retention Reloaded: zkušenosti, problémy a aplikační praxe*, 2013, s. 14.

příslušných ustanovení práva EU nebo mezinárodního práva veřejného, zejména Úmluvy, jak ji vykládá ESLP. Toto ustanovení tedy vykazovalo obdobnou nejasnost, jakou vykazuje čl. 15 odst. 1 směrnice 2002/58.[302]

Otázka oprávněných orgánů a podmínek přístupu byla jednotlivými členskými státy řešena poměrně různě, jak vyplývá z hodnotící zprávy publikované Komisí v roce 2011. Přístup k uchovávaným údajům mohly téměř ve všech členských státech získat policie i státní zástupci. Čtrnáct členských států umožňovalo získat přístup i zpravodajským službám a armádě. Šest členských států pak mezi příslušné orgány zařadilo dokonce i daňovou nebo celní správu a tři rovněž pohraniční orgány. Co se týče soudního povolení jako podmínky přístupu k údajům, to vyžadovalo za všech okolností jen jedenáct členských států. Ve třech členských státech bylo soudní povolení vyžadováno ve většině případů. Pět dalších členských států vyžadovalo povolení nadřízeného orgánu, nikoliv však soudce. Ve dvou členských státech byla jedinou podmínkou je písemná žádost na poskytovatele služeb.[303]

Čl. 5 pak obsahoval výčet kategorií údajů, které mají být uchovávány. Jak již bylo naznačeno výše, jde o údaje potřebné k dohledání a identifikaci zdroje sdělení; údaje potřebné k identifikaci adresáta sdělení; údaje potřebné ke zjištění data, času a doby trvání komunikace; údaje potřebné k určení typu sdělení; údaje potřebné k identifikaci komunikačního vybavení uživatelů a v neposlední řadě údaje potřebné ke zjištění polohy mobilního komunikačního zařízení. Konkrétní podoba těchto údajů se pak odvíjela od způsobu komunikace. Z důvodu jejich charakteru podobajícímu se obsahu sdělení neukládala směrnice povinnost uchovávat údaje o webové historii, tj. zejména URL navštívených webových stránek.[304] Uchovávání těchto údajů však nadále mohly členské státy uložit na základě čl. 15 odst. 1 směrnice 2002/58.

Čl. 6 stanovil, že doba uchovávání údajů musí být nejméně 6 a nejvíce 24 měsíců, aniž by – oproti původnímu návrhu Komise – rozlišoval dle jednotlivých kategorií údajů. Zpětně takové řešení nelze považovat za šťastné. Již tehdy se totiž objevovaly informace, že užitečnost provozních a lokalizačních údajů po pár měsících rapidně klesá.[305] To následně potvrdily i statistiky Komise získané v rámci procesu hodnocení směrnice, dle kterých „*zhruba devadesát procent údajů, které byly předmětem přístupu ze strany příslušných orgánů v daném roce,*

[302] Srov. kapitola 4.1.2.3.
[303] Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011, s. 10.
[304] Srov. KOSTA, Eleni. The Retention of Communications Data in Europe and the UK. In: EDWARDS, Lilian. *Law, Policy and the Internet*, 2018, s. 202.
[305] Srov. BROWN, Ian. Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, 2010, s. 106.

nebylo starší šesti měsíců a kolem sedmdesáti procent nebylo starší tří měsíců v okamžiku podání (původní) žádosti o přístup k údajům.“.[306] Nemluvě o tom, že umožnění velmi odlišných dob uchovávání vedlo k omezení harmonizačního účinku směrnice.

Čl. 7, aniž by se dotýkal obecných povinností dle směrnic 95/46 a 2002/58, upravoval otázky zabezpečení uchovávaných údajů a ukládal členským státům zajistit, aby:

- uchovávané údaje měly stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně jako údaje na síti;
- se na údaje se vztahovala vhodná technická a organizační opatření k ochraně údajů před náhodným nebo neoprávněným zničením, náhodnou ztrátou či pozměněním nebo nepovoleným nebo neoprávněným uchováním, zpracováním, přístupem nebo zveřejněním;
- údaje podléhaly příslušným technickým a organizačním opatřením pro zajištění toho, aby k nim mohly přistupovat pouze zvláště zmocněné osoby;
- na konci doby uchovávání údajů se všechny tyto údaje zničily, a to vyjma údajů, k nimž bylo přistoupeno.

Na dodržování těchto požadavků měl dohlížet nezávislý orgán určený dle čl. 9 směrnice, přičemž se mohlo jednat i o dozorový úřad stanovený na základě směrnice 95/46. V praxi často docházelo k tomu, že byly dozorové pravomoci rozděleny mezi regulační orgány v oblasti telekomunikací a dozorové úřady v oblasti ochrany osobních údajů.

Způsobu uchovávání se dále týkal i čl. 8, dle kterého měly být údaje uchovávány tak, aby je bylo možné příslušným orgánům předat bezprostředně. Poměrně zajímavé je, že toto ustanovení hovoří nejen o předávání údajů definovaných v čl. 2 odst. 2 písm. a) směrnice (tj. včetně údajů o totožnosti uživatelů), ale také o souvisejících informacích, které však blíže nedefinuje. Přestože problematika těchto souvisejících informací nebyla nikdy Soudním dvorem řešena, mám za to, že čl. 5 směrnice v tomto ohledu vyvolával důvodné pochybnosti ohledně jasnosti a přesnosti ustanovení, kterou vyžaduje judikatura ESLP a Soudního dvora.[307]

Vzhledem k tomu, jak nové a kontroverzní opatření data retention představovala, byl velmi důležitý čl. 10 směrnice, ukládající členským státům sbírat a předávat Komisi statistiky obsahující:

---

[306] Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011, s. 22-23.
[307] Srov. kapitoly 4.1.3. a 4.2.2.2.

- případy, kdy byly příslušným orgánům poskytnuty informace v souladu s použitelnými vnitrostátními právními předpisy;
- čas, který uplynul ode dne uchování údajů do dne, kdy příslušný orgán požádal o předání údajů;
- a případy, kdy nebylo možné žádosti o poskytnutí údajů vyhovět.

Tyto údaje pak měly sloužit jako hlavní podklad pro hodnocení fungování směrnice.[308]

Čl. 13 nadepsaný „opravné prostředky, odpovědnost a sankce" neukládal členským státům povinnost stanovit sankce za nedodržení povinnosti uchovávat údaje, ale výhradně za porušení povinností v oblasti ochrany údajů, zejména těch vyplývajících ze směrnice 95/46.

Na rozdíl od původního návrhu neobsahovala směrnice 2006/24 pravidla pro kompenzací nákladů poskytovatelů služeb souvisejících s plněním směrnicí uložených povinností. Tato otázka tak byla řešena jednotlivými členskými státy značně odlišně.

Transpoziční lhůta směrnice uplynula 15. září 2007, s tím, že pokud jde o uchovávání komunikačních údajů týkajících se připojení k internetu, internetové telefonie a internetové elektronické pošty, bylo umožněno odložení transpozice o 18 měsíců. Této možnosti využilo 16 členských států.

3.2.2.3 Směrnice 2006/24 – problematická transpozice v členských státech a zrušení Soudním dvorem

Spolehlivým indikátorem kontroverzní povahy směrnice 2006/24 byly problémy, se kterými se řada členských států potýkala již v rámci transpozice. Díky odporu vnitrostátních parlamentů nebyla směrnice včas transponována v Řecku, Irsku, Nizozemsku, Lucembursku, Švédsku a Rakousku.[309] Za neprovedení směrnice ve stanovené lhůtě byly Švédsko,[310] Rakousko,[311] Irsko[312] a Řecko[313] dokonce odsouzeny Soudním dvorem. Rakousko se sice v rámci řízení pro porušení povinnosti bránilo poukazem na to, že směrnice 2006/24 není v souladu s čl. 8 Úmluvy, avšak s ohledem na ustálenou judikaturu Soudního dvora byl tento druh argumentace předem odsouzen k neúspěchu. Irsko pak vůči směrnici podalo žalobu na neplatnost k Soudnímu dvoru, přičemž namítalo nesprávnost zvoleného právního základu. Irsko, které

[308] Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011.
[309] Srov. FEILER, Lukas. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *European Journal of Law and Technology*, 2010, s. 6.
[310] Rozsudek Soudního dvora ze dne 4. února 2010, *Komise v. Švédsko*, C-185/09, EU:C:2010:59.
[311] Rozsudek Soudního dvora ze dne 29. července 2010, *Komise v. Rakousko*, C-189/09, EU:C:2010:455.
[312] Rozsudek Soudního dvora ze dne 26. listopadu 2009, *Komise v. Irsko*, C-202/09, EU:C:2009:736.
[313] Rozsudek Soudního dvora ze dne 26. listopadu 2009, *Komise v. Řecko*, C-211/09, EU:C:2009:73.

svou žalobou sledovalo především cíl ponechat si svou volnější právní úpravu data retention, však s žalobou neuspělo. Argumentace Soudního dvora týkající se právního základu směrnice v této věci bude podrobněji rozebrána v následující kapitole.[314] Ve Švédsku navíc nebyla směrnice implementována ani po vynesení prvního odsuzujícího rozsudku, což vedlo Komisi k podání další žaloby, která opět dospěla až do stadia rozsudku Soudního dvora, kterým byla Švédsku uložena finanční sankce.[315] Ta však nakonec byla Komisí vrácena poté, co Soudní dvůr směrnici zrušil pro její rozpor s čl. 7 a 8 Listiny.[316]

V mnoha členských státech, které transpozici včas stihly, tato skutečnost vedla k podání žalob namítajících protiústavnost transpozičních předpisů – ať už ze strany nevládních organizací zabývajících se ochranou osobních údajů, či ze strany politiků. V několika případech byly vnitrostátní právní předpisy protiústavními skutečně shledány. K tomu došlo v Rumunsku, Německu, Bulharsku, České republice a Kypru. Vnitrostátní soudy – s výjimkou rumunského ústavního soudu – však neshledávaly protiústavnost v provedení samotných požadavků směrnice, ale spíše v tom, jakým způsobem jednotlivé členské státy využily prostor pro uvážení, který jim směrnice poskytovala, např. co se týče délky uchovávání údajů a záruk v oblasti přístupu k údajům.[317]

V roce 2011 Komise vydala hodnotící zprávu ke směrnici 2006/24. Krom shrnutí způsobů transpozice v jednotlivých členských státech měla hodnotící zpráva také posoudit nezbytnost směrnicí zavedených opatření na základě statistických údajů dodaných členskými státy. Tento cíl nebylo možné naplnit, protože většina členských států provedla směrnici až v předcházejících dvou letech, přičemž pro sběr údajů jednotlivé státy použily značně odlišné metodiky. Ze statistik dodaných 19 členskými státy za roky 2008 a 2009 vyplývalo, že celkově v EU bylo každým rokem podáno více než 2 miliony žádostí o údaje, přičemž počet značně kolísal mezi členskými státy, a to od méně než 100 žádostí za rok (Kypr) až k více než 1 milionu (Polsko). Ze statistik také vyplynuly poměrně zásadní poznatky týkající se nezbytné doby uchovávání, jelikož zhruba 90 % údajů, které byly předmětem přístupu ze strany

---

[314] Srov. kapitola 4.1.2.2.
[315] Rozsudek Soudního dvora ze dne 30. května 2013, *Komise v. Švédsko*, C-270/11, EU:C:2013:339.
[316] Srov. FIODOROVA, Anna. *Information Exchange and EU Law Enforcement*, 2018.
[317] Pro stručnou a přehlednou analýzu rozhodnutí ústavních soudů členských států v oblasti data retention viz KOSTA, Eleni. The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection. *SCRIPTed-A Journal of Law, Technology and Society*, 2013, s. 339-363. Srov. také VAINIO, Niklas. Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States. *International Journal of Law and Information Technology*, 2015, s. 293-295. Pro podrobnější zpracování této problematiky viz ZUBIK, Marek et al. *European Constitutional Courts towards Data Retention Laws*, 2021.

příslušných orgánů, nebylo v okamžiku podání žádosti o přístup k údajům starší šesti měsíců a kolem 70 % nebylo starší tří měsíců.

Dodaná data nebyla sto prokázat pozitivní dopady data retention na celkovou míru objasněnosti trestné činnosti, a Komise tudíž při konstatování účinnosti data retention vycházela především z vyjádření členských států a ilustrativních příkladů. Z hodnotící zprávy také vyplynulo, že účinnost data retention snižují nástroje jako VPN[318] či možnost zakoupení anonymních předplacených SIM karet. Hodnotící zpráva se dále zabývala pohledem poskytovatelů služeb, kdy dospěla k závěru, že povinnosti vyplývající ze směrnice mohou poměrně zásadně dopadnout především na menší poskytovatele (přičemž téměř polovina členských států náklady nekompenzovala) a že k harmonizaci podmínek uchovávání došlo pouze částečně.[319] Přestože tedy Komise dospěla k závěru o užitečnosti data retention a vytyčila si i určité cíle v této oblasti do budoucna, rozhodně se nedá hovořit o tom, že by informace poskytnuté členskými státy jednoznačně rozptýlily pochybnosti ohledně data retention.[320]

Výše uvedená neschopnost členských států na tvrdých datech demonstrovat účinnost data retention je z mého pohledu poměrně zásadním problémem nejen tehdejší, ale i současné diskuse o data retention. Ačkoliv se domnívám, že data retention je užitečným a při správném provedení i přiměřeným nástrojem pro boj proti závažné trestné činnosti a hrozbám v oblasti národní bezpečnosti, je legitimní vyžadovat, aby členské státy tvrzení o její nepostradatelnosti podpořily tvrdými daty. Nejde o to, aby data retention vedla ke snížení celkové úrovně zločinnosti či zvýšení celkové objasněnosti trestných činů. Statistiky by nicméně mohly zahrnovat celou řadu dalších aspektů – např. k jakým kategoriím údajů je nejčastěji přistupováno, k jak „starým“ údajům je nejčastěji přistupováno, jakých trestných činů se žádosti týkají, v kolika případech byla získaná metadata stěžejním důkazem, v kolika případech bylo kvůli absenci údajů nutné zastavit vyšetřování, v kolika případech došlo ke zneužití uchovávaných či zpřístupněných údajů, k porušení zabezpečení apod. Taková data bohužel, jak se zdá alespoň z hodnotící zprávy i následných řízení před Soudním dvorem, široce dostupná nejsou. Samozřejmě, výpovědní hodnotu ilustrativních příkladů z praxe nelze zcela ignorovat, avšak je s podivem, že tyto ilustrativní příklady je natolik obtížné podepřít tvrdými

[318] Virtuální soukromá síť, tj. šifrované připojení mezi dvěma sítěmi nebo mezi konkrétním uživatelem a sítí, jež může znesnadnit identifikaci konkrétního uživatele.
[319] Srov. Evropská komise. *Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)*, 2011.
[320] Srov. FENELLY, David. Data retention: the life, death and afterlife of a directive. *ERA Forum*, 2018, s. 679 či GUILD, Elspeth a CARRERA, Sergio. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. *CEPS Liberty and Security in Europe Papers*, 2014, s. 3.

daty. Navíc hovoříme-li o využití provozních a lokalizačních údajů zpravodajskými službami, jsou často i tyto ilustrativní příklady velmi obecné, jelikož se členské státy zdráhají podrobněji popisovat činnost zpravodajských služeb, což také snižuje jejich vypovídací hodnotu. Je však pravdou, že i kritika data retention se ve značné míře nezakládá na tvrdých datech, např. co se skutečných dopadů *chilling effect* týče.[321] Oběma stranám diskuse by tedy hlubší vědecké zkoumání dotčené problematiky jedině prospělo.

3.2.3 Situace po zrušení směrnice 2006/24

Směrnice 2006/24 byla Soudním dvorem v roce 2014 zrušena pro neslučitelnost s čl. 7 a 8 Listiny, přičemž právní úpravy data retention členských států jsou dnes zkoumány optikou čl. 15 odst. 1 směrnice 2002/58 vykládaného ve světle čl. 7, 8 a 11 Listiny.[322] Do budoucna tak může dotčenou problematiku znatelně ovlivnit ePrivacy nařízení, které by mělo v dohledné době nahradit směrnici 2002/58. Původní návrh Komise počítal s tím, že ustanovení týkající se působnosti směrnice a ustanovení umožňující data retention budou převzata bez větších změn, přičemž důvodová zpráva v této souvislosti zohledňovala závěry Soudního dvora ve věci *Tele2 Sverige* a uváděla, že členské budou moci i po přijetí nařízení nadále přijímat „*cílená opatření pro uchovávání údajů, pokud jsou tyto rámce v souladu s právem Unie a zohledňují judikaturu Soudního dvora týkající se výkladu směrnice o soukromí a elektronických komunikacích a Listiny základních práv*“.[323]

Současný návrh z dílny Rady však přistoupil k poměrně razantní úpravě příslušných ustanovení. První důležitou změnou je požadavek, aby bylo možné provozní a lokalizační údaje bez souhlasu subjektu údajů (byť při dodržení určitých podmínek jako je např. pseudonymizace údajů, je-li to s ohledem na účel zpracování možné) zpracovávat také za účelem vědeckého výzkumu, statistickými účely a v neposlední řadě za účelem ochrany životně důležitých zájmů subjektu údajů i třetích osob, např. při boji s epidemiemi. Dále Rada navrhuje, aby z působnosti nařízení byla vyňata jakákoliv zpracování prováděná za účelem zajišťování národní bezpečnosti a obrany, bez ohledu na to, zda je vykonávají příslušné orgány členských států přímo, či prostřednictvím poskytovatele služeb, čímž se zjevně snaží překonat výklad působnosti směrnice 2002/58 zaujatý Soudním dvorem ve věcech *Privacy International* a *La Quadrature*

---

[321] Srov. např. BEDI, Suneal. The Myth of the Chilling Effect. *Kelley School of Business Research Paper*, 2021.
[322] Viz kapitola 4.1.3.
[323] Evropská Komise. *Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)*, s. 3.

du Net.[324] Osobně nicméně nepovažuji za pravděpodobné, že by takto koncipované ustanovení akceptoval Evropský parlament, který bude v daném případě usilovat o zajištění co nejvyšší úrovně ochrany základních práv a který dlouhodobě usiluje o to, aby se i aktivity členských států v oblasti národní bezpečnosti v co největší možné míře řídily unijními pravidly.[325]

Velmi opatrný bych byl také v souvislosti s umožněním přístupu k údajům za účelem boje s epidemiemi. Zásah do základních práv způsobený takovým přístupem by byl bezesporu velmi závažný, jelikož by se z povahy věci jednalo o přístup k lokalizačním údajům za účelem odhalení mezilidských vazeb. Tyto údaje by navíc měly nutně velice citlivou povahu, jelikož by vypovídaly mj. o zdravotním stavu. Navíc je otázkou, v jakém rozsahu by bylo možné zajistit robustní záruky v oblasti přístupu, aby bylo minimalizováno riziko zneužití. Jen stěží si lze představit, že by byl s ohledem na počty nakažených osob takový přístup podmíněn souhlasem soudu či že by případný souhlas soudu nebyl toliko formální. Přestože nelze podceňovat závažnost současné epidemie COVID-19, z mého pohledu by takto závažný zásah do základních práv měl být přípustný pouze v případě, že by se jednalo o extrémně efektivní nástroj z hlediska zvládání epidemie, což by mělo být předem demonstrováno opravdu s velkou přesvědčivostí.

V neposlední řadě je třeba uvést, že ani přijetí nové společné právní úpravy data retention, která by nahradila zrušenou směrnici 2006/24, není zcela vyloučeno. V roce 2019 pověřila Rada Komisi, aby za tímto účelem připravila studii beroucí v potaz krom situace v členských státech i aktuální judikaturu Soudního dvora. Komise tedy oslovila externí konzultantskou společnost a dotčená studie, vycházející především z dat poskytnutých příslušnými orgány a poskytovateli služeb z vybraných deseti členských států, byla publikována v roce 2020.[326] Z této studie mj. vyplývá, že:

- ve většině států nadále existuje povinnost plošné data retention vycházející ze směrnice 2006/24;
- data retention je z pohledu příslušných orgánů členských států nenahraditelným nástrojem pro vyšetřování trestné činnosti;
- *quick freeze* nepředstavuje účinnou alternativu data retention;

[324] Viz kapitola 4.1.2.4.
[325] Srov. CARUANA, Mireille. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology*, 2019, s. 256.
[326] European Commission. *Data Retention for law enforcement purposes – Final report*, 2020.

- příslušné vnitrostátní právní úpravy se značně liší, především v rovině přístupu, řada členských států nadále v některých případech nevyžaduje předchozí souhlas soudu
- podrobné statistiky týkající se dané problematiky nadále chybí;
- v dané oblasti se zároveň objevují nové výzvy, krom *over-the-top messagingu* jde také o zavádění 5G sítí a s ním související metody šifrování, které omezují dostupnost potřebných údajů.

Ačkoliv lze ocenit, že se studie soustředí na některé nové aspekty problematiky data retention (tj. například problematiku zahrnutí *over-the-top mesagingu*), debatu, jak systémy data retention nastavit, aby odpovídaly judikatuře Soudního dvora, posouvá kupředu jen velmi málo. Studie vychází téměř výhradně ze zkušeností poskytovatelů služeb a příslušných orgánů členských států, které nicméně nekonfrontuje s názory nevládních organizací, dozorových úřadů, a především ani s judikaturou Soudního dvora. Ze studie je navíc zřejmé, že řada vnitrostátních právních úprav se nachází ve stadiu, kdy v nich chybí dokonce i základní požadavky na dodatečné záruky vyplývající již z rozsudku *Digital Rights Ireland*, což není příliš potěšující. Sama o sobě tak jako podklad pro novou společnou právní úpravu data retention jistě sloužit nemůže.

3.3 ZÁVĚR

Cílem této části práce bylo vysvětlit základní aspekty data retention jakožto užitečného nástroje pro potírání terorismu a jiné závažné trestné činnosti, avšak taktéž jako opatření významně zasahujícího do práv na ochranu soukromí a osobních údajů. Bylo vysvětleno, že jádro užitečnosti data retention, avšak i hlavní rizika s ní spojená, spočívají v plošném uchovávání údajů. Podstatou data retention a její hlavní výhodou ve srovnání s jinými opatřeními je totiž možnost, aby příslušné orgány „nahlížely do minulosti“ osob, u nichž v rozhodné době ještě nebyla identifikována spojitost s konkrétním trestným činem či jinou hrozbou. Toto nahlížení do minulosti však není možné bez toho, aby docházelo k preventivnímu uchovávání údajů, a tudíž k zásahu do základních práv všech uživatelů elektronické komunikace.

Přestože se takový zásah dotýká extrémně širokého počtu osob, je třeba se zabývat také intenzitou tohoto zásahu. Bylo vysvětleno, že se intenzita zásahu spojená s plošným uchováváním údajů ve značné míře odvíjí od rizika zneužití přístupu k údajům. Byla zdůrazněna klíčová role dodatečných záruk v oblasti uchovávání a přístupu jakožto účinný nástroj pro snižování intenzity zásahu způsobeného data retention. Bylo argumentováno proti příliš zjednodušujícímu nahlížení na data retention jako na nástroj pro sledování či odposlouchávání celé evropské populace, ovšem bylo i varováno před marginalizací dopadů

data retention pouze s poukazem na to, že nedochází k uchovávání obsahu komunikace.

Klíčové rysy právních úprav data retention pak byly blíže vysvětleny v rámci popisu směrnice 2006/24, jejíž pravidla nadále odráží řada platných vnitrostátních právních úprav data retention. Bylo poukázáno na to, že řada problematických aspektů směrnice 2006/24 má původ v kompromisech, ke kterým docházelo v legislativním procesu. V neposlední řadě byly popsány nové iniciativy v oblasti data retention (zejména návrh ePrivacy nařízení) i související výzvy (např. problematika *over-the-top messagingu* či snaha o vynětí problematiky národní bezpečnosti z působnosti nařízení).

4 DATA RETENTION V JUDIKATUŘE

4.1 SOUDNÍ DVŮR

4.1.1 Přehled

Vzhledem k tomu, že následující kapitoly jsou členěny spíše tematicky dle jednotlivých právních otázek, které v souvislosti s data retention musel Soudní dvůr řešit, je vhodné následně analyzovanou judikaturu Soudního dvora nejprve stručně představit v chronologickém pořadí.

Prvním řízením, ve kterém se Soudní dvůr zabýval problematikou data retention, byla věc *Irsko v. Parlament a Rada.*[327] Irsko v daném případě napadlo platnost směrnice 2006/24 z důvodu, že směrnice byla s ohledem na svůj obsah přijata na nesprávném právním základě. Dle Irska bylo jediným či přinejmenším hlavním cílem této směrnice vyšetřování, odhalování a stíhání trestných činů. Dle Irska proto směrnice nemohla být založena na tehdejším čl. 95 SES. Soudní dvůr se však s argumenty Irska neztotožnil a konstatoval, že směrnice 2006/24 mohla být platně založena na čl. 95 SES, jelikož mezi vnitrostátními předpisy o uchovávání údajů v daném okamžiku existovaly právní a technické odlišnosti, které mohly mít přímý dopad na fungování vnitřního trhu. Soudní dvůr v této souvislosti vyzdvihl, že směrnice upravuje pouze povinnosti poskytovatelů služeb (tj. povinnost uchovávat údaje), nikoliv chování příslušných orgánů členských států (tj. podmínky přístupu k údajům). Soudní dvůr proto v roce 2009 rozhodl, že směrnice 2006/24 byla platně založena na čl. 95 SES, aniž by však zkoumal její platnost s ohledem na její soulad s Listinou.

Jak bylo popsáno výše, směrnice 2006/24 byla velmi kontroverzní, a přijímání implementačních předpisů proto v mnohých členských státech poměrně vázlo. To vedlo Komisi k zahájení hned několika řízení pro porušení Smlouvy v souvislosti s neprovedením směrnice, která v některých případech dospěla až do fáze rozsudku Soudního dvora.[328]

Slučitelnost směrnice 2006/24 s požadavky čl. 7 a 8 Listiny se stala předmětem řízení před Soudním dvorem v roce 2012 ve věci *Digital Rights Ireland.* Jednalo se o předběžné otázky položené irským High Court a rakouským Verfassungsgerichtshof. Soudní dvůr rozhodl, že ačkoliv práva vyplývající z čl. 7 a 8 Listiny nejsou absolutní a směrnice 2006/24 sleduje legitimní cíle boje proti závažné trestné činnosti a terorismu, její pravidla překračují meze naprosté nezbytnosti, zejména proto, že nestanoví žádné podmínky pro přístup příslušných

[327] Rozsudek Soudního dvora ze dne 10. února 2009, *Irsko v. Parlament a Rada*, C-301/06, EU:C:2009:68 (dále jen „*rozsudek Irsko v. Parlament a Rada*“).
[328] Viz kapitola 3.2.2.3.

vnitrostátních orgánů k údajům a jejich následné využití. Paradoxně tedy to, co tedy směrnici zachránilo v řízení, ve kterém byl zpochybňován její právní základ, vedlo nakonec k jejímu zrušení v řízení, ve kterém byla posuzována její slučitelnost s Listinou.

Konec směrnice 2006/24 však neznamenal také konec národních úprav směrnici implementujících. Mnoho těchto „osiřelých" právních úprav zůstalo nadále v platnosti i po rozsudku ve věci *Digital Rights Ireland.* To platilo mj. pro švédskou a britskou vnitrostátní právní úpravu data retention, které se poměrně záhy staly předmětem řízení před Soudním dvorem ve věci *Tele2 Sverige.* Zde řešil Soudní dvůr dvě klíčové otázky. Zaprvé šlo o to, do jaké míry po zrušení směrnice 2006/24 spadají vnitrostátní právní předpisy upravující data retention do působnosti unijního práva. Zadruhé se případ týkal otázky, zda plošná povinnost uchovávání údajů je sama o sobě v rozporu s požadavky čl. 7, 8 a 11 Listiny, či zda může být shledána přiměřenou za předpokladu, že budou stanoveny přísné záruky v oblasti přístupu k údajům. Soudní dvůr v prvé řadě rozhodl, že do působnosti směrnice 2002/58 spadají jak vnitrostátní právní předpisy upravující uchovávání údajů, tak předpisy upravující přístup příslušných orgánů k těmto údajům. Soudní dvůr dále rozhodl, že čl. 7, 8 a 11 Listiny brání plošnému uchovávání údajů jako takovému, bez ohledu na dodatečné záruky. Tím tedy Soudní dvůr zpochybnil základní aspekt data retention naprosto zásadním způsobem.

Ani toto rozhodnutí však neznamenalo konec data retention v EU. Řada vnitrostátních právních úprav stanovujících plošné uchovávání je nadále v platnosti. Komise, která před Soudním dvorem vždy zastávala názor, že plošná povinnost data retention není *a priori* v rozporu s Listinou, doposud nezahájila řízení pro porušení Smlouvy s členskými státy, jež si své z pohledu rozsudku *Tele2 Sverige* problematické vnitrostátní právní úpravy ponechaly. Tyto vnitrostátní právní úpravy nicméně byly a nadále jsou průběžně napadány na vnitrostátní úrovni, což vedlo a nadále vede k pokládání dalších předběžných otázek Soudnímu dvoru.[329]

Chronologicky dalším případem týkajícím se data retention byla věc *Ministerio Fiscal.*[330] Ta se týkala žádosti španělské policie o zpřístupnění údajů o majiteli SIM karty, která byla vložena do telefonu odcizeného při loupeži. Na rozdíl od předchozích případů nezajímala

[329] Šlo o právní úpravy Spojeného království (viz věc C-623/17), Belgie (viz věc C-520/18), Francie (viz věci C-511 a C-512/18), Irska (viz věc C-140/20) a Německa (viz věci C-793/19 a C-794/19). Krom právních úprav, které byly předmětem řízení Soudním dvorem, zůstala plošná povinnost uchovávání údajů zachována taktéž v České republice, Estonsku, Maďarsku, Itálii, Lucembursku, Portugalsku a Španělsku. Srov. RIJPMA, Jorrit J. *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*, 2020, s. 233, 256, 342, 364, 402, 424, 511, 578.

[330] Rozsudek Soudního dvora ze dne 2. října 2018, *Ministerio Fiscal*, EU:C:2018:788 (dále jen „*rozsudek Ministerio Fiscal*").

španělský předkládající soud problematika uchovávání, ale výhradně to, co je pro účely přístupu třeba považovat za „závažný trestný čin“. Soudní dvůr v daném případě rozhodl, že na rozdíl od plošného uchovávání veškerých provozních a lokalizačních údajů nepředstavuje samotný přístup k údajům o majiteli SIM karty závažný zásah do práv na soukromí a ochranu osobních údajů, a tudíž je z hlediska práva EU přípustný i v případě „*běžné*“ trestné činnosti. Soudní dvůr se tedy vůbec nezabýval problematikou plošného uchovávání provozních a lokalizačních údajů.

Skutečnými pokračovateli data retention ságy se tak staly až případy *Privacy International* (týkající se právní úpravy Spojeného království) a *La Quadrature du Net a další* (týkající se francouzské a belgické právní úpravy), *Commissioner of the Garda Síochána* (týkající se irské právní úpravy) a *SpaceNet*, resp. *Telekom Deutschland* (týkající se německé právní úpravy). Krom otázky možného přehodnocení závěrů Soudního dvora ohledně nepřípustnosti plošné data retention v některých těchto řízeních navíc vyvstaly otázky, do jaké míry jsou závěry Soudního dvora ve věci *Tele2 Sverige* přenositelné na problematiku zajišťování národní bezpečnosti.

Rozsudky Soudního dvora ve věcech *Privacy International* a *La Quadrature du Net* vynesené na podzim roku 2020 potvrdily, že Soudní dvůr nehodlá své závěry o nepřípustnosti plošné data retention zcela opustit, avšak je v tomto ochotný ohledu činit určité ústupky, a to v případě některých kategorií údajů či určitých výjimečných situací. Na druhé straně Soudní dvůr, jistě k nevůli řady členských států, dospěl k závěru, že omezení vyplývající v této souvislosti z unijního práva se uplatní i na uchovávání a předávání provozních a lokalizačních údajů za účelem zajišťování národní bezpečnosti. Jakým způsobem budou členské státy a zejména Komise na tyto rozsudky reagovat, ještě není zcela jasné. Řízení ve věci *SpaceNet* a *Telekom Deutschland*, která jsou zajímavá tím, že dotčená německá vnitrostátní právní úprava sice stanoví plošnou povinnost uchovávání, ale jinak obsahuje velice přísné dodatečné záruky, doposud běží.

V březnu 2021 byl vynesen doposud poslední rozsudek z oblasti data retention ve věci *Prokuratuur.*[331] Tento případ navazoval na věc *Ministerio Fiscal* a týkal se také primárně roviny přístupu k údajům. Soudní dvůr v této věci rozhodl, že přístup k jiným metadatům než k údajům o předplatitelích je možný pouze za účelem boje proti závažné trestné činnosti, nikoliv „běžné“ trestné činnosti, bez ohledu na to, zda jde o údaje týkající se velmi krátkého časového období.

[331] Rozsudek Soudního dvora ze dne 2. března 2021, *Prokuratuur*, C-746/18, EU:C:2021:152 (dále jen „*rozsudek Prokuratuur*“).

Soudní dvůr také dospěl k závěru, že k přístupu k provozním a lokalizačním údajům nepostačí předchozí souhlas státního zastupitelství, které v daném ohledu nedosahuje dostatečné úrovně nezávislosti a nestrannosti.

4.1.2 Působnost unijních předpisů v oblasti data retention

Jednou ze zásadních otázek v souvislosti s problematikou data retention vždy bylo, zda je zákonodárce Společenství, resp. později zákonodárce Unie, vůbec oprávněn tuto problematiku regulovat. Ještě než se budeme zabývat přístupem Soudního dvora k působnosti unijních předpisů v oblasti data retention, je na místě se blíže podívat na rozsudek Soudního dvora ve věci *Parlament v. Rada a Komise* týkající se problematiky předávání údajů o cestujících v letecké dopravě.[332] Soudní dvůr byl totiž v dané věci postaven před podobnou otázku, jako následně ve věcech týkajících se data retention. Důsledky tohoto rozsudku proto byly často diskutovány právě v řízeních týkajících se působnosti unijních předpisů v oblasti data retention.

4.1.2.1 Parlament v. Rada a Komise

Tyto spojené věci se týkaly jednak rozhodnutí Komise, které prostřednictvím konstatování adekvátní úrovně ochrany umožnilo předávání údajů PNR americkému úřadu pro civilní letectví, a dále pak rozhodnutí Rady o uzavření mezinárodní dohody umožňující předávání těchto údajů. Rozhodnutí Komise o adekvátní úrovni ochrany bylo založeno přímo na směrnici 95/46, rozhodnutí Rady pak na tehdejším čl. 95 SES, který odpovídal předchozímu čl. 100a SES, tedy právnímu základu směrnice 95/46. Parlament obě tato rozhodnutí napadl u Soudního dvora, přičemž namítal především nesprávný právní základ těchto rozhodnutí (účelem předávání osobních údajů do USA totiž byl bezesporu boj proti terorismu a související trestné činnosti), a dále skutečnost, že tato rozhodnutí porušují obecné zásady práva Společenství, konkrétně právo na soukromí dle čl. 8 Úmluvy.

Podstatou napadených rozhodnutí reagujících na teroristické útoky z 11. září 2001 bylo umožnit předávání údajů PNR, které evropští letečtí dopravci sbírali pro vlastní komerční účely, orgánům USA, které je měly využívat k boji proti terorismu. Parlament v této souvislosti namítal, že rozhodnutí Komise nemohlo být platně založeno na čl. 25 směrnice 95/46, jelikož se týkalo zpracování osobních údajů vyňatých z působnosti této směrnice na základě čl. 3 odst. 2 první odrážky této směrnice. Ze stejného důvodu měl Parlament za to, že rozhodnutí Rady nemůže být založeno na čl. 95 SES, jelikož se netýká harmonizace podmínek pro

[332] Rozsudek Soudního dvora ze dne 30. května 2006, *Parlament v. Rada a Komise*, spojené věci C-317/04 a C-318/04, EU:C:2006:346 (dále jen „*rozsudek Parlament v. Rada a Komise*“).

vytváření vnitřního trhu, ale mezinárodní spolupráce v trestních věcech. Parlament mj. argumentoval rozsudkem ve věci *Lindqvist*, když poukazoval na to, že dotčené předávání (přestože jej v praxi provádí letečtí dopravci) se netýká činnosti jednotlivců, ale právě činnosti států v oblasti trestního práva. Komise a Rada naopak argumentovaly tím, že činnosti leteckých dopravců jasně spadají do oblasti působnosti směrnice 95/46, resp. do působnosti práva Společenství. Jsou to totiž právě jednotlivci – letečtí dopravci – kdo v rámci své vlastní komerční činnosti sbírá dotčené údaje a kdo je následně předává třetímu státu.

Soudní dvůr argumentaci Rady a Komise odmítl. Vyšel z toho, že je třeba rozlišovat původní zpracování předmětných údajů pro komerční účely a následné zpracování spočívající v předání těchto údajů orgánům USA. Předmětná rozhodnutí se přitom týkala výhradně zmíněného předávání, jehož jediným účelem bylo zajišťování veřejné bezpečnosti a činností států v oblasti trestního práva. Přestože tedy dotčené zpracování prováděli jednotlivci, spadalo s ohledem na sledovaný účel do rámce zavedeného orgány veřejné moci za účelem zachování veřejné bezpečnosti. Soudní dvůr proto prohlásil obě rozhodnutí za neplatná. Ačkoliv Soudní dvůr dospěl ke stejným závěrům jako před ním generální advokát, byla jeho argumentace o poznání stručnější – k vyřešení této zásadní otázky mu stačilo pouze 8 stručných bodů rozsudku.[333]

Jelikož Soudní dvůr vyhověl již prvnímu žalobnímu důvodu Evropského parlamentu, nezabýval se důvody dalšími, jako např. slučitelností dotčeného režimu s čl. 8 Úmluvy. Soudní dvůr se nezabýval ani (slovy generálního advokáta) „*delikátní*“ otázkou, na jakém právním základě by dotčená dohoda měla být uzavřena, resp. zda je Společenství vůbec oprávněno takovou dohodu uzavřít.[334] Faktem zůstává, že zrušení výše uvedených rozhodnutí vedlo k uzavření nové dohody založené na čl. 24 a 38 tehdejší SEU.[335] Čl. 24 SEU zmocňoval Unii k uzavření dohod v oblasti zahraniční a bezpečnostní politiky, které se dle čl. 38 SEU mohly taktéž dotýkat problematiky policejní a soudní spolupráce v trestních věcech. Otázkou právního základu pro předávání údajů PNR se Soudní dvůr zabýval znovu až v posudku 1/15, tedy až po poměrně zásadní změně primárního práva. Tehdy Soudní dvůr dospěl k závěru,

[333] Srov. rozsudek *Parlament v. Rada a Komise*, body 54-61.
[334] Srov. stanovisko GA Légera ze dne 22. listopadu 2005 ve spojených věcech *Parlament v. Rada a Komise*, C-317/04 a C-318/04, EU:C:2005:710, bod 157.
[335] Srov. Rozhodnutí Rady 2006/729/SZBP/SVV ze dne 16. října 2006 o podpisu, jménem Evropské unie, Dohody mezi Evropskou unií a Spojenými státy americkými o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států.

že dotčená dohoda má být založena na čl. 16 odst. 2 SFEU, ale taktéž na čl. 87 odst. 2 písm. a) SFEU.[336]

Pro účely této práce je však zásadní, že při rozhodování, zda určité zpracování osobních údajů spadá do působnosti aktů Společenství založených na „tržně-harmonizačním" ex čl. 95 SES, Soudní dvůr jednoznačně vycházel z účelu tohoto zpracování. Soudní dvůr rozhodl, že je-li účelem konkrétního zpracování jednání orgánů států v oblasti boje proti trestné činnosti a zajišťování národní bezpečnosti, nespadá takové zpracování do působnosti dotčených unijních předpisů. Rozhodl tak i přesto, že dotčené údaje byly shromážděny soukromými subjekty v rámci jejich vlastní ekonomické činnosti. Tomuto přístupu Soudního dvora lze přitom jen stěží něco vytknout. Soudní dvůr bohužel tento logický přístup velmi brzy opustil, což do budoucna vyvolalo celou řadu otázek ohledně působnosti unijních předpisů v oblasti data retention.

4.1.2.2 Irsko v. Parlament a Rada

Jak bylo uvedeno výše, ex čl. 95 SES byl právním základem také směrnice 2006/24, což bylo zdůvodňováno tím, že směrnice neupravuje otázky přístupu bezpečnostních složek k uchovávaným údajům, které zůstávají v pravomoci členských států, ale pouze problematiku uchovávání těchto údajů poskytovateli služeb.[337] Je však třeba uvést, že směrnice 2006/24 se přístupem bezpečnostních složek k uchovávaným údajům zabývala, i když v minimální míře. Čl. 4 směrnice 2006/24 v této souvislosti apeloval na dodržení požadavků nezbytnosti a přiměřenosti.[338] Toto pojetí právního základu směrnice 2006/24, dle kterého problematika uchovávání údajů spadala do působnosti ex čl. 95 SES, přestože jediným cílem tohoto uchovávání bylo umožnění pozdějšího přístupu bezpečnostních složek k těmto údajům, celkem jednoznačně neodpovídalo přístupu, který Soudní dvůr zaujal k problematice předávání údajů PNR ve věci *Parlament v. Rada a Komise*.

Irsko proto právní základ směrnice napadlo u Soudního dvora, přičemž z pohledu tehdejší judikatury zcela oprávněně tvrdilo, že jediným (či přinejmenším převažujícím) cílem směrnice 2006/24 je usnadnit vyšetřování, odhalování a stíhání trestných činů, a žádné ustanovení tehdejší SES tak nemůže sloužit jako právní základ této směrnice. Nutno dodat, že Irsko v žádném případě neusilovalo o zrušení směrnice na základě lidskoprávních úvah.

---

[336] Srov. posudek Soudního dvora ze dne 26. července 2017, 1/15, EU:C:2017:592.
[337] Srov. BIGNAMI, Francesca. Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, 2007, s. 243.
[338] Viz kapitola 3.2.2.2.

Právě naopak – Irsko ve zrušení směrnice vidělo možnost zachovat si vlastní úpravu data retention, která do soukromí obyvatelstva zasahovala ještě více než směrnice 2006/24.[339]

Soudní dvůr argumenty Irska odmítl – uvedl, že rozdíly mezi jednotlivými vnitrostátními právními předpisy přijatými v oblasti uchovávání údajů o elektronických komunikacích mohly mít přímý dopad na fungování vnitřního trhu a že bylo možné očekávat, že se tento dopad bude zhoršovat. Stejně tak Soudní dvůr upozornil, že předmětem směrnice 2006/24 je v podstatě odchylka od pravidel směrnice 2002/58, která byla taktéž přijata na základě tehdejšího článku 95 SES. Zároveň směrnice 2006/24 neupravovala otázky přístupu příslušných orgánů k uchovávaným údajům, resp. se nijak netýkala činnosti těchto orgánů, a proto nezasahuje do oblastí, které jsou vyhrazeny členským státům. Soudní dvůr v neposlední řadě uvedl, že rozhodnutí přezkoumávaná ve věci *Parlament v. Rada a Komise* se týkala zpracování osobních údajů v rámci systému zavedeného orgány veřejné moci za účelem zajištění veřejné bezpečnosti, zatímco směrnice 2006/24 se týká činností poskytovatelů služeb na vnitřním trhu a neobsahuje žádnou právní úpravu činnosti orgánů veřejné moci za trestněprávními účely. Úvahy Soudního dvora k problematice předávání údajů PNR proto dle Soudního dvora nelze bez dalšího přenést na problematiku data retention.[340]

S tím je poměrně obtížné souhlasit – pokud by totiž Soudní dvůr skutečně zvolil totožnou optiku již ve věci *Parlament v. Rada a Komise*, velmi pravděpodobně by dospěl k tomu, že napadená rozhodnutí mohou být platně založena na čl. 95 SES, resp. na směrnici 95/46. Případná rozdílná ujednání členských států ohledně údajů předávaných do USA mohla zcela jistě představovat určité překážky pro letecké dopravce působící napříč členskými státy; těžiště rozhodnutí PNR se také týkalo činnosti komerčních subjektů, nikoliv orgánů členských států; předávání údajů PNR lze také chápat jako výjimku z pravidel, která stanoví směrnice 95/46 v oblasti ochrany osobních údajů. Nicméně ve věci *Parlament v. Rada a Komise* zvolil Soudní dvůr odlišnou optiku a vycházel výhradně z účelu předmětného zpracování. Pokud by tedy zvolil stejnou optiku v případě směrnice 2006/24, musel by Irsku vyhovět.

4.1.2.3 Tele2 Sverige

Mohlo by se zdát, že ve chvíli, kdy Soudní dvůr ve věci *Irsko v. Parlament a Rada* potvrdil, že právní úprava data retention může být založena na čl. 95 SES, nebude už mnoho sporu o tom,

---

[339] Srov. FABBRINI, Federico. Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S. *Harvard Human Rights Journal*, 2015, s. 76.

[340] Rozsudek *Irsko v. Parlament a Rada*, body 56-94.

zda problematika data retention spadá do působnosti unijního práva. Po zrušení směrnice 2006/24 ve věci *Digital Rights Ireland* se však Soudní dvůr k této problematice musel opět vrátit.

Předmětem sporu ve věci *Tele2 Sverige* byly „pozůstatky" směrnice 2006/24 v podobě jejích transpozičních předpisů ve Švédsku a Spojeném království.[341] Soudní dvůr v těchto spojených věcech mj. řešil, zda a v jakém rozsahu tyto vnitrostátní právní předpisy upravující data retention spadají do působnosti směrnice 2002/58. V důsledku zrušení směrnice 2006/24 se totiž stal unijním právním rámcem data retention právě čl. 15 odst. 1 směrnice 2002/58, který zmiňoval možnost zavedení data retention ještě před přijetím směrnice 2006/24.

Problém se směrnicí 2002/58 jakožto unijním rámcem pro data retention však spočíval ve zjevném napětí mezi jejím čl. 1 odst. 3 a jejím čl. 15 odst. 1. Dle jejího čl. 1 odst. 3 se směrnice 2002/58 nevztahuje mj. na „*činnosti, které nespadají do oblasti působnosti Smlouvy o založení Evropského společenství, jako činnosti uvedené v hlavě V a VI Smlouvy o založení Evropské unie, a v žádném případě na činnosti týkající se veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a na činnosti státu v oblasti trestního práva.*" Z tohoto ustanovení by se tak zdálo, že uchovávání provozních a lokalizačních údajů a jejich zpřístupňování příslušným orgánům členských států činným v oblasti trestního práva spadá mimo působnost směrnice.

Čl. 15 odst. 1 směrnice nicméně uvádí, že „*[č]lenské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/64/ES. Členské státy mohou mimo jiné přijmout právní opatření umožňující zadržení údajů na omezenou dobu na základě důvodů uvedených v tomto odstavci. Veškerá*

[341] Fennelly v tomto ohledu hovoří o „*posmrtném životě*" směrnice 2006/24, Granger zase o „*osiřelých*" vnitrostátních právních úpravách. Srov. FENNELLY, David. Data retention: the life, death and afterlife of a directive. *ERA Forum*, 2019, s. 673 a GRANGER, Marie-Pierre. The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection. *European Law Review*, 2014, s. 848. K otázce dopadů zrušení směrnice 2006/24 v českém kontextu srov. např. KRÁL, Richard. On the Consequences of the Annulment of EU Directives for their Incompability with the EU Charter of Fundamental Rights. In: PÍTROVÁ et al. *Rule of Law and Mechanisms of its Protection Czech Perspective*, 2015, s. 144-151.

opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o založení Evropské unie.“ Zatímco tedy čl. 1 odst. 3 směrnice 2002/58 naznačuje, že dotčená problematika je z působnosti směrnice 2002/58 zcela vyňata, čl. 15 odst. 1 této směrnice naznačuje spíše opak. Toto ustanovení totiž hovoří o *omezení* práv vyplývajících mj. z čl. 5 směrnice, které navíc *podmiňuje dodržením obecných zásad práva Společenství*.

Podíváme-li se na dané ustanovení optikou Krále a Mádra,[342] znění čl. 15 odst. 1 směrnice 2002/68 naznačuje, že se jedná o „*power-granting*“ a „*discretion-delimiting*“ ustanovení, které členské státy zmocňuje k přijetí určitých opatření v rámci působnosti směrnice (a tudíž i obecných zásad Společenství, resp. později Listiny) a vymezuje meze jejich diskrece v tomto ohledu, nikoliv „*power-recognising*“ a „*scope-delimiting*“ ustanovení, jež by pouze deklaratorním způsobem konstatovalo prostor pro legislativní činnost členských států, který zůstává směrnicí nedotčen.

Ve prospěch vnímání čl. 15 odst. 1 – navzdory jeho znění – spíše jako *power-recognising* ustanovení, však hovoří bod 11 odůvodnění směrnice, který popisuje výjimku v čl. 15 odst. 1 spíše jako důsledek toho, že je problematika data retention na základě čl. 1 odst. 3 vyňata z působnosti směrnice, resp. že dotčená problematika nespadala do pravomoci tehdejšího Společenství. Tento bod odůvodnění uvádí, že *„[t]ato směrnice, obdobně jako směrnice 95/46/ES, se netýká ochrany základních práv a svobod ve vztahu k činnostem, které se neřídí právem Společenství. Proto tato směrnice nemění stávající rovnováhu mezi právem jednotlivce na soukromí a možností, aby členské státy přijaly opatření uvedená v čl. 15 odst. 1 této směrnice, která jsou nezbytná pro ochranu veřejné bezpečnosti, obrany, bezpečnosti státu (včetně hospodářské prosperity státu, pokud jsou tyto činnosti spojeny s otázkami bezpečnosti státu) a pro prosazování trestního práva. Tato směrnice se tedy nedotýká možnosti členských států provádět zákonné zachycování elektronických sdělení nebo přijímat jiná opatření, je-li to nezbytné pro některý z těchto účelů a je-li to v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod, jak je vykládána v rozhodnutích Evropského soudu pro lidská práva.“* I tento bod odůvodnění však zanechává určité pochybnosti ohledně *power-recognising* povahy dotčeného ustanovení, jelikož také dodává, že přijatá *„opatření musí být vhodná, plně přiměřená vzhledem k zamýšlenému účelu*

[342] KRÁL, Richard a MÁDR, Petr. On the (In)Applicability of the EU Charter of Fundamental Rights to National Measures Exceeding the Requirements of Minimum Harmonisation Directives. *European Law Review*, 2021.

a nezbytná v demokratické společnosti a musí být předmětem odpovídajících záruk v souladu s Evropskou úmluvou o ochraně lidských práv a základních svobod."

Ve prospěch *power-recognising* povahy dotčeného ustanovení, tj. ve prospěch vynětí dotčené problematiky z působnosti směrnice, hovoří také dokumenty z legislativního procesu, např. vyjádření Komise k navrhovanému znění čl. 15 odst. 1 směrnice, ve kterém Komise uvedla, že směrnice založená na čl. 95 SES nemůže obsahovat žádná pravidla týkající se činnosti příslušných orgánů v oblasti trestního práva, a nemůže tedy „*povolovat ani zakazovat jakákoliv opatření, které členské státy v této oblasti shledávají nezbytnými*". Ovšem i Komise upozornila na to, že členské státy musí dodržovat povinnosti vyplývající z obecných zásad Společenství, včetně těch vyplývajících z Úmluvy.[343]

Protichůdné tendence přitom v této souvislosti vykazovala i tehdejší judikatura. Pro vynětí dotčené problematiky z působnosti směrnice 2002/58 jednoznačně hovořil rozsudek ve věci *Parlament v. Rada a Komise* připomenutý výše. Opačný přístup naopak naznačoval rozsudek *Irsko v. Parlament a Rada*, ve kterém Soudní dvůr dospěl Soudní dvůr k závěru, že úprava uchovávání údajů ve směrnici 2006/24 může být bez problémů založena na čl. 95 SES. Na druhou stranu, Soudní dvůr měl v daném rozsudku také za to, že směrnice 2006/24 vůbec neupravuje problematiku přístupu k údajům, přestože tato směrnice ve svém čl. 4 taktéž uváděla, že právní předpisy upravující problematiku přístupu k údajům musí dodržovat obecné zásady práva Společenství.

Jak tedy tyto třecí plochy – mezi čl. 1 odst. 3 a čl. 15 odst. 1 směrnice 2002/58 na straně jedné, a mezi závěry Soudního dvora ve věcech *Parlament v. Rada a Komise* a *Irsko v. Parlament a rada* na straně druhé – vyřešit? Ve vyjádřeních účastníků řízení vykrystalizovaly v zásadě tři přístupy k dané věci. Česká republika, Francie a Polsko měly za to, že jediným účelem dotčených vnitrostátních právních úprav je boj proti trestné činnosti, a jedná se tudíž o problematiku vyňatou z působnosti směrnice na základě jejího čl. 1 odst. 3.[344] Dle České republiky představoval čl. 15 odst. 1 směrnice toliko (v daném kontextu dosti matoucí) připomenutí lidskoprávních mantinelů vyplývajících pro členské státy z Úmluvy a související judikatury ESLP.

---

[343] Srov. European Commission. *Opinion of the Commission pursuant to Article 251 (2), third subparagraph, point (c) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector amending the proposal of the Commission pursuant to Article 250 (2) of the EC Treaty*, 2002, bod 4. Srov. také European Digital Rights. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011, s. 4.

[344] Srov. stanovisko GA věci *Tele2 Sverige*, bod 88 a rozsudek *Tele2 Sverige*, bod 65.

Spojené království a Komise v daném případě zastávaly určitou „střední cestu“, umožňující částečně skloubit čl. 1 odst. 3 a čl. 15 směrnice 2002/58.[345] V rámci této střední cesty měla do působnosti směrnice 2002/58 spadat problematika uchovávání údajů poskytovateli služeb, zatímco problematika přístupu bezpečnostních složek zůstávala mimo její působnost. Tento přístup by jednak zachoval alespoň určité účinky obou výše uvedených ustanovení, zároveň by víceméně odpovídal tomu, co Soudní dvůr uvedl v rozsudku *Irsko v. Parlament a Rada*. Praktickým problémem takového řešení bylo, že vyžadovalo, aby Soudní dvůr „odevzdal“ problematiku přístupu k údajům do rukou členských států, a vzdal se svého nároku na kontrolu těchto aspektů. Bylo jasné, že Soudní dvůr bude takové řešení akceptovat jen těžko. Ostatně, jak bude uvedeno níže, ve věci *Digital Rights Ireland* jednoznačně odmítl, že by unijní úprava mohla stanovit povinnost uchovávání údajů, aniž by zároveň stanovila záruky v oblasti přístupu k údajům.

Dle třetího pojetí, zastávaného ostatními účastníky řízení, spadala do působnosti směrnice 2002/58 jak otázka uchovávání, tak otázka přístupu.[346] Problémem tohoto pojetí nicméně bylo, že ve značné míře, alespoň co se problematiky data retention týče, zbavovalo užitečného účinku čl. 1 odst. 3 směrnice 2002/58 a neodpovídalo bodu 11 jejího odůvodnění. Zároveň nebylo takové pojetí v souladu s tím, co Soudní dvůr uvedl ve věci *Irsko v. Parlament a Rada*, ve které považoval skutečnost, že směrnice 2006/24 neupravovala otázky přístupu, jako klíčovou pro to, aby mohla být platně založena na čl. 95 SES. A už vůbec neodpovídalo tomu, jak Soudní dvůr přistupoval k problematice předávání údajů PNR ve věci *Parlament v. Rada a Komise*.

Soudní dvůr se přesto přiklonil k posledně uvedenému pojetí. Co se týče roviny uchovávání, Soudní dvůr uvedl, že čl. 15 odst. 1 směrnice 2002/58 umožňuje přijetí opatření upravujících uchovávání údajů pouze za dodržení určitých podmínek. Nemá-li být toto ustanovení zbaveno veškerého užitečného účinku, musí tedy dotčená problematika do působnosti směrnice spadat.[347] Soudní dvůr pak pokračoval a uvedl, že do působnosti směrnice 2002/58 musí nutně spadat i otázka přístupu bezpečnostních složek k uchovávaným údajům. Soudní dvůr tento argumentační krok (či možná skok) odůvodnil tím, že „*[o]chrana důvěrnosti elektronických komunikací a souvisejících provozních údajů, jež je zaručena čl. 5*

[345] Srov. rozsudek *Tele2 Sverige*, bod 66.
[346] Ibidem, bod 65.
[347] To je poměrně zajímavé, jelikož obdobné podmínky v oblasti přístupu k údajům obsahoval i čl. 4 směrnice 2006/24, přesto Soudní dvůr ve věci *Irsko v. Parlament a Rada* shledal, že tuto problematiku směrnice 2006/24 neupravuje.

odst. 1 směrnice 2002/58, se totiž vztahuje na opatření, která přijímají veškeré osoby s výjimkou uživatelů, ať již se jedná o soukromé fyzické nebo právnické osoby nebo o státní subjekty. Jak potvrzuje bod 21 odůvodnění této směrnice, jejím cílem je zamezit [‚jakémukoli'] neoprávněnému ‚přístupu' ke sdělením, včetně ‚[veškerých] údajů vztahujících se k takovým sdělením', aby byla chráněna důvěrnost elektronických komunikací."[348]

Výše uvedená argumentace představuje značný posun ve srovnání s předchozí judikaturou Soudního dvora. Samozřejmě nebylo možné očekávat, že by se Soudní dvůr vrátil ke svým závěrům ve věci *Parlament v. Komise a Rada*, spokojil se s posouzením účelu zpracování a z působnosti směrnice vyloučil i činnost poskytovatelů služeb, má-li sloužit k zajištění bezpečnostních zájmů členských států. Nejen s ohledem na praktické problémy spočívající s oddělením roviny uchovávání a roviny přístupu, ale také ohledem na důvody pro zrušení směrnice 2006/24 šlo očekávat, že Soudní dvůr bude chtít problematiku přístupu k údajům do působnosti směrnice 2002/58 zahrnout. Ovšem to nic nemění na tom, že argumentace zvolená Soudním dvorem vede k zásadnímu omezení významu čl. 1 odst. 3 této směrnice a popření bodu 11 jejího odůvodnění. Nelze navíc tvrdit, že se jednalo o jediné možné řešení, nemá-li být čl. 15 odst. 1 zbaven užitečného účinku.[349] Čl. 15 odst. 1 problematiku přístupu k údajům vůbec nezmiňuje, a i kdyby do jeho působnosti problematika přístupu zahrnuta nebyla, stále by dopadal alespoň na problematiku uchovávání. V této souvislosti tak nezbývá než souhlasit s Fennellym, který uvádí, že rozsudek ve věci Tele2 Sverige „*potvrzuje křehkost zásady svěřených pravomocí v době narůstajícího soudního aktivismu v Lucemburku*."[350]

Problematičnost výše uvedeného řešení alespoň částečně zmírňuje fakt, že Lisabonskou smlouvou došlo k odstranění pilířové struktury. Čl. 16 odst. 2 SFEU tak v dnešní době zmocňuje Unii k přijímání pravidel na ochranu osobních údajů jak při běžných, tak při „policejních" činnostech, což ostatně odráží i současná směrnice 2016/680. Ačkoliv tedy výše uvedený přístup Soudního dvora neodpovídal právnímu základu směrnice 2002/58, alespoň již nevedl k tomu, že by se unijní pravidla ochrany osobních údajů použila na činnosti, které Unie dle primárního práva neměla pravomoc regulovat. Tento problém se však znovu objevil

[348] Srov. rozsudek *Tele2 Sverige*, bod 77.
[349] Srov. rozsudek *Tele2 Sverige*, bod 73.
[350] Srov. FENNELLY, David. Data retention: the life, death and afterlife of a directive. *ERA Forum*, 2019, s. 688.

v případech, ve kterých data retention sloužila nejen k potírání závažné trestné činnosti, ale také k zajišťování národní bezpečnosti.[351]

Je však třeba uvést, že v daném okamžiku ještě nebylo jisté, zda se tyto závěry Soudního dvora mají použít pouze na situace, kdy jsou údaje předávány poskytovateli služeb, či zda se vztahuje na i na situace, kdy příslušné orgány dotčené údaje získávají vlastními prostředky. Některé pasáže rozsudku hovořily obecně o „*přístupu*" příslušných orgánů,[352] z jiných by však spíše vyplývalo, že se jedná o situace, kdy jsou údaje „*zpřístupňovány*" právě poskytovateli služeb.[353] Tato otázka byla Soudním dvorem výslovně zodpovězena až ve věcech *Privacy International* a *LaQuadrature du Net.*

4.1.2.4 Privacy International a La Quadrature du Net

V navazujících případech *Privacy International* a *La Quadrature du Net* řada členských států namítala, že se Soudní dvůr v rozsudku *Tele2 Sverige* odklonil od rozsudku *Parlament v. Rada a Komise*, přičemž tento judikaturní odklon je třeba „napravit" a vrátit se ke „správnému" předchozímu přístupu.[354] Zároveň členské státy upozorňovaly na určitou odlišnost posuzovaných právních úprav oproti těm, které byly předmětem sporu ve věci *Tele2 Sverige.* Posuzované vnitrostátní právní úpravy totiž umožňovaly krom předávání provozních a lokalizačních údajů policejním orgánům za účelem boje proti trestné činnosti taktéž předávání těchto údajů zpravodajským službám za účelem zajišťování národní bezpečnosti (ve věci *Privacy International* šlo dokonce o právní úpravu týkající se výhradně činnosti zpravodajských služeb). Skutečnost, že by se unijní právní úprava ochrany osobních údajů měla dotknout činnosti zpravodajských služeb, se pro členské státy zdála být nepřijatelná, a řada z nich proto namítala, že právě z tohoto důvodu nelze předmětné vnitrostátní právní úpravy zkoumat optikou směrnice 2002/58 a Listiny. Otázka zajišťování národní bezpečnosti je totiž dle čl. 4 odst. 2 SEU výhradně v pravomoci členských států.

Generální advokát ve všech případech dospěl k závěru, že se směrnice 2002/58 na dotčené vnitrostátní právní úpravy použije.[355] Generální advokát se nejprve pokusil vysvětlit, proč Soudní dvůr zvolil v případě problematiky data retention odlišný přístup

---

[351] Viz kapitola 4.1.2.4.
[352] Rozsudek *Tele2 Sverige a Watson a další*, bod 76.
[353] Ibidem, bod 78.
[354] Srov. stanovisko generálního advokáta Campos Sánchez-Bordony ve věci *La Quadrature du Net a další*, EU:C:2020:6, bod 41 (dále jen „*stanovisko GA ve věci La Quadrature du Net*").
[355] Stanoviska generálního advokáta Campos Sánchez-Bordony ve věcech *Privacy International,* C-623/17, EU:C:2020:5; *Ordre des barreaux francophones a germanophone a další*, C-520/18, EU:C:2020:7 a *La Quadrature du Net*.

než v případě problematiky PNR. Dle generálního advokáta tento odlišný přístup vyplývá z odlišného znění čl. 3 odst. 2 první odrážky směrnice 95/46 (jejímž výkladem se Soudní dvůr zabýval ve věci *Parlament v. Rada a Komise*) a čl. 1 odst. 3 směrnice 2002/58 (jež je relevantní v případě data retention). Generální advokát v této souvislosti uvedl, že zatímco z působnosti směrnice 95/46 byla vyňata „*zpracování osobních údajů prováděná pro výkon činností, které nespadají do oblasti působnosti práva Společenství*“, z působnosti směrnice 2002/58 jsou vyňaty „*činnosti které nespadají do oblasti působnosti Smlouvy o založení Evropského společenství*“. Výše uvedené odlišné znění obou předpisů generální advokát chápal tak, že výluka z působnosti směrnice 95/46 byla širší, a tudíž zahrnovala i zpracování prováděná jednotlivci, pokud k nim dochází za účelem realizace činnosti orgánů státu. V případě směrnice 2002/58 je nicméně tato výjimka užší a dopadá pouze na činnosti samotných orgánů státu, nikoliv na činnosti jednotlivců, byť sledují tytéž cíle.[356]

Vysvětlení generálního advokáta se na první pohled jeví jako rozumná cesta, jak závěry Soudního dvora v oblasti PNR a data retention vzájemně skloubit. Ovšem nalijme si čistého vína – pokud by unijní zákonodárce skutečně zamýšlel činit mezi výlukami z působnosti těchto směrnic takto zásadní rozdíl, učinil by tak podstatně jasnějším způsobem. Mírně odlišná formulace čl. 1 odst. 3 směrnice 2002/58 tak spočívá spíše v tom, že směrnice 2002/58 upravuje o něco širší problematiku soukromí v elektronických komunikacích, nikoliv pouze pravidla pro zpracování osobních údajů. Vysvětlení generálního advokáta je také těžké skloubit s bodem 11 odůvodnění směrnice 2002/58. Ten se totiž odvolává právě na směrnici 95/46 a doslova uvádí, že směrnice 2002/58 „*nemění stávající rovnováhu*“ mezi pravidly na ochranu soukromí a osobních údajů a kompetencemi příslušných orgánů členských států. Osobně se proto domnívám, že Soudní dvůr ve věcech *Irsko v. Rada a Parlament* a *Tele2 Sverige* jednoduše změnil názor a odklonil se od svých předchozích závěrů ve věci *Parlament v. Rada a Komise*, a to ve světle rizik spojených s data retention a s ohledem na význam, který v současnosti připisuje právům na soukromí a ochranu osobních údajů.

Soudní dvůr však výše uvedené teze generálního advokáta potvrdil a vnímané rozpory mezi rozsudky *Tele2 Sverige* a *Parlament v. Rada* vysvětlil stejným způsobem.[357] Soudní dvůr dále poukázal na to, že v současnosti byla směrnice 95/46 již nahrazena GDPR, které se dle svého čl. 2 odst. 2 písm. d) nevztahuje zpracování osobních údajů prováděné „*příslušnými*

[356] Srov. stanovisko GA ve věci *La Quadrature du Net*, body 61-76.
[357] Srov. rozsudek *Privacy International*, bod 46 a rozsudek *La Quadrature du Net*, bod 101.

orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení". Z čl. 23 odst. 1 písm. d) a h) GDPR pak dle Soudního dvora vyplývá, že GDPR se na rozdíl od směrnice 95/46 již stejně jako směrnice 2002/58 vztahuje na situace, kdy zpracování za těmito účely vykonávají soukromé subjekty.[358]

Zejména argumentaci odkazem na GDPR nepovažuji za správnou. Zaprvé, jak již bylo uvedeno výše, GDPR bylo přijato podstatně později a je založeno i na podstatně odlišném právním základě (čl. 16 odst. 2 SEU ve znění Lisabonské smlouvy) než směrnice 2002/58 (ex čl. 95 SES). Argumentace Soudního dvora také nezohledňuje výjimku z působnosti v čl. 2 odst. 2 písm. a) GDPR, dle které se GDPR nepoužije na zpracování osobních údajů „*při výkonu činností, které nespadají do oblasti působnosti práva Unie*" a která výslovně není omezena pouze na příslušné orgány členských států. Čl. 2 odst. 2 písm. d) GDPR, ze kterého Soudní dvůr v této souvislosti vycházel, má přitom pouze odrážet působnost směrnice 2016/680, která ale nedopadá na činnost zpravodajských služeb a problematiku zajišťování národní bezpečnosti. Zejména pokud si uvědomíme, že se vnitrostátní právní úprava ve věci *Privacy International* týkala výhradně činnosti zpravodajských služeb, tj. problematiky národní bezpečnosti ve smyslu čl. 4 odst. 2 SEU, jeví se tedy argumentace Soudního dvora odkazem na věcnou působnost GDPR nepřípadná.

Faktem nicméně zůstává, že Soudní dvůr ve své ustálené judikatuře dlouhodobě odmítá, že by odkaz na čl. 4 odst. 2 SEU mohl členské státy vyvázat z povinností vyplývajících z unijního práva.[359] Na tuto judikaturu Soudní dvůr dle očekávání odkázal i v těchto věcech s tím, že sama skutečnost, že se dotčené vnitrostátní právní úpravy týkají také, či dokonce výhradně, národní bezpečnosti, nemůže nic změnit na působnosti směrnice 2002/58.[360] I tak se ale domnívám, že tyto rozsudky představují zatím největší ingerenci unijního práva do pravomocí členských států v oblasti národní bezpečnosti. Dopady na metody činnosti zpravodajských služeb, a tudíž způsoby zajišťování národní bezpečnosti, jsou v těchto případech nesrovnatelně bezprostřednější a intenzivnější než v předchozích případech, ve kterých Soudní dvůr zaujal tento výklad čl. 4 odst. 2 SEU, a které se týkaly

[358] Srov. rozsudek *Privacy International*, bod 47 a rozsudek *La Quadrature du Net,* bod 102.
[359] Srov. např. rozsudek Soudního dvora ze dne 4. června 2013, *ZZ*, C-300/11, EU:C:2013:363, bod 38; rozsudek Soudního dvora z 20. března 2019, *Komise v. Rakousko*, C-187/16, EU:C:2018:194, body 75 a 76 či rozsudek Soudního dvora z 2. dubna 2020, *Komise v. Polsko, Maďarsko a Česko*, spojené věci C-715/17, C-718/17 a C-719/17, EU:C:2020:257, body 143-170.
[360] Srov. rozsudek *Privacy International*, bod 44 a rozsudek *La Quadrature du Net*, bod 99.

např. problematiky veřejných zakázek na doklady totožnosti,[361] přijímání uprchlíků,[362] či práva na soudní ochranu v případě odmítnutí vstupu občana Unie na území členského státu.[363]

Mám za to, že i když podle ustálené judikatury nemůže pouhý odkaz čl. 4 odst. 2 SEU představovat *bianko šek* umožňující odchýlení se od jakýchkoliv pravidel unijního práva, s ohledem na to, jak jednoznačně je toto ustanovení formulováno („*zejména národní bezpečnost zůstává výhradní odpovědností každého členského státu*"), musí představovat alespoň významné interpretační vodítko pro výklad pravidel působnosti sekundárního práva. A to zejména v případech, kdy je vzájemné střetávání unijních pravidel a problematiky zajišťování národní bezpečnosti natolik bezprostřední a intenzivní, jak je tomu v případě data retention. Ostatně, účelem čl. 4 odst. 2 SEU bylo právě zajistit, aby v souvislosti s odstraněním pilířové struktury nedošlo k nepřiměřenému vychýlení rovnováhy pravomocí v takto citlivých oblastech ve prospěch Unie.[364] Z judikatury Soudního dvora týkající se data retention je však zjevné, že v souvislosti s data retention tohoto účelu čl. 4 odst. 2 SEU dosaženo nebylo. Při výkladu nejasných ustanovení týkajících se rozsahu působnosti směrnice 2002/58 nebyl čl. 4 odst. 2 SEU jakožto interpretační vodítko brán jakkoliv v potaz.

V rámci posuzování přiměřenosti pak Soudní dvůr sice zmínil zvláštní důležitost cíle zajišťování národní bezpečnosti, ale přesto nakonec v dané souvislosti zaujal velice striktní přezkum, vylučující až na výjimky plošné uchovávání komunikačních metadat i za účelem zajišťování národní bezpečnosti. Jedna z těchto výjimek se navíc týká existence aktuálního a závažného ohrožení národní bezpečnosti.[365] Je tedy možné, že Soudní dvůr bude brzy některým ze soudů členských států osloven, aby tato kritéria blíže rozvinul, resp. *de facto* posoudil, zda v určitém případě byly podmínky „*existujícího či hrozícího závažného ohrožení národní bezpečnosti*" splněny. Bude zajímavé sledovat, jak k takovému případu Soudní dvůr ve světle čl. 4 odst. 2 SEU přistoupí. Skutečnost, že by totiž Soudní dvůr měl *de facto* rozhodovat o tom, zda členský stát čelí ohrožení národní bezpečnosti a jak je toto ohrožení závažné, se dá se zněním a účelem čl. 4 odst. 2 SEU připomenutými výše skloubit poměrně těžko.

---

[361] Srov. rozsudek Soudního dvora z 20. března 2019, *Komise v. Rakousko*, C-187/16, EU:C:2018:194, body 75 a 76.
[362] Srov. rozsudek Soudního dvora z 2. dubna 2020, *Komise v. Polsko, Maďarsko a Česko*, spojené věci C-715/17, C-718/17 and C-719/17, EU:C:2020:257, body 143-170.
[363] Srov. rozsudek Soudního dvora ze dne 4. června 2013, ZZ, C-300/11, EU:C:2013:363.
[364] Srov. DOBBS, Mary. Sovereignty, Article 4(2) TEU and the Respect of National Identities: Swinging the Balance of Power in Favour of the Member States? *Yearbook of European Law*, 2014, s. 314, 325 a 326.
[365] Srov. rozsudek *La Quadrature du Net,* body 135 a násl.

Zatímco tedy před vynesením rozsudků Soudního dvora ve věcech *Privacy International* a *La Quadrature du Net* někteří akademici hovořili o tom, že v souvislosti s těmito případy dochází ke střetu nezastavitelné síly (v podobě práv na ochranu soukromí a osobních údajů, jak je v posledních letech vykládá Soudní dvůr) a nepohnutelného tělesa (v podobě národní bezpečnosti, jak ji vnímají členské státy),[366] nakonec se ukázalo, že národní bezpečnost představuje z pohledu Soudního dvora těleso, se kterým není problém pohnout.

Není proto divu, že aktuální mandát Rady k návrhu ePrivacy nařízení usiluje o to, aby v nařízení bylo výslovně uvedeno, že se nevztahuje na veškerá zpracování a veškeré činnosti týkající se národní bezpečnosti a obrany, bez ohledu na to, zda je vykonávají příslušné orgány členských států či soukromé subjekty na žádost orgánů státu.[367] Je otázkou, zda bude Rada schopna v legislativním procesu nakonec takto koncipovanou výjimku prosadit, jelikož Evropský parlament bude mj. ve světle stávající judikatury Soudního dvora jistě usilovat o zachování stávajícího stavu.

To, že Soudní dvůr do působnosti unijního práva vtáhl jak otázky uchovávání, tak otázky přístupu k údajům v oblasti národní bezpečnosti, jakož i fakt, že možnost plošného uchovávání závisí na posouzení existence aktuálního a reálného rizika pro národní bezpečnost, navíc vyvolává otázku, zda nemůže být v budoucnu některým z vnitrostátních soudů tento přístup Soudního dvora chápán jako jednání *ultra vires*.[368] Osobně se domnívám, že k takové situaci může velice snadno dojít, jelikož s ohledem na citlivost problematiky zajišťování národní bezpečnosti, doposud bezprecedentní míru ingerence Soudního dvora do této oblasti a v neposlední řadě odlišný pohled na věc ze strany řady ústavních soudů, nelze vyloučit, že některý z ústavních soudů členských států bude přístup Soudního dvora považovat za dostatečně zjevné a dostatečně závažné překročení pravomocí Unie. Obzvlášť v případech, kde by Soudní dvůr např. dospěl ohledně existence skutečného a aktuálního rizika pro národní

---

[366] Srov. KUNER, Christopher et. al. An unstoppable force and an immoveable object? EU data protection law and national security. *International Data Privacy Law*, 2018.

[367] Srov. *Rada Evropské unie. Návrh nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) – mandát Rady*, 2021, s. 7 a 42.

[368] Doktrína *ultra vires* vychází primárně z judikatury Spolkového ústavního soudu, ale byla přejata i ústavními soudy dalších členských států, včetně toho českého. Její podstatou je výhrada vůči absolutní přednosti unijního práva před ústavním právem členských států. Spolkový ústavní soud v této souvislosti vychází z názoru, že z titulu „pánů smluv" přísluší členským státům stanovit s konečnou platností, zda orgány Unie (včetně Soudního dvora) nepřekročily své pravomoci. Ke shledání jednání *ultra vires* by však mělo docházet jen ve zcela výjimečných případech, a proto podléhá několika přísným podmínkám. Zaprvé musí jednání unijního orgánu v tomto ohledu mít zjevné a dostatečně závažné dopady na dělbu kompetencí mezi členskými státy a Unií, zadruhé musí být umožněno, aby se k dané problematice nejprve vyjádřil Soudní dvůr. Srov. např. TOMÁŠEK, Michal a TÝČ, Vladimír et. al. *Právo Evropské unie*, 2017, s. 91 a násl.

bezpečnost k jiným závěrům než předkládající soud, se použití *ultra vires* doktríny rozhodně nedá vyloučit.

Přesto se přístup Soudního dvora jeví z hlediska systematiky směrnice 2002/58 a s ohledem na čl. 4 odst. 2 SEU rozumnější než přístup některých účastníků původních řízení ve výše uvedených věcech. Ti zastávali názor, že i v případech, kdy komunikační metadata získávají orgány státu bez spolupráce poskytovatelů služeb, bude dotčená problematika spadat do působnosti směrnice 2002/58, a to z důvodu, že i v takovém případě se členské státy odchylují od povinnosti zachovat důvěrnost sdělení.[369] Takový přístup by nutně vedl k tomu, že čl. 1 odst. 3 směrnice 2002/58 – stejně jako čl. 4 odst. 2 SEU v daném kontextu – skutečně ztratí veškerý smysl. Za hlediska rozdělení pravomocí mezi Unii a členské státy by tedy bylo neomluvitelné, pokud by Soudní dvůr takový výklad zaujal.

Pozitivní je dále i skutečnost, že bylo ze strany Soudního dvora konečně jednoznačně vymezeno, jaké situace v této souvislosti spadají do působnosti směrnice 2002/58 a jaké nikoliv. Dle Soudního dvora tak do působnosti směrnice 2002/58 spadají situace, kdy přístup příslušných orgánů ke komunikačním metadatům zajišťují poskytovatelé služeb, přičemž mimo její působnost spadají situace, kdy tento přístup zajišťují příslušné orgány členských států vlastními prostředky. Bude zajímavé sledovat, jaké praktické dopady bude toto rozlišování mít – zda např. povede ke změně vnitrostátních právních úprav, které namísto povinnosti poskytovatelů služeb uchovávat a předávat komunikační metadata orgánům státu stanoví pravomoc orgánů státu údaje získávat vlastními prostředky. Je otázkou, jak by Soudní dvůr reagoval v situaci, že by se tato praxe členských států rozmohla a Soudní dvůr tak, zejména v případě zpravodajských služeb, kdy se neuplatní směrnice 2016/680, zcela ztratil kontrolu nad tím, jakým způsobem orgány členských států zpracovávají provozní a lokalizační údaje.

Toto jasné vymezení působnosti unijních předpisů se nicméně již projevilo v rámci vyjednávání o novém režimu předávání osobních údajů do USA. Zástupci USA totiž s poukazem na rozsudky ve věcech *La Quadrature du Net* a *Privacy International* požadují, aby při posuzování otázky odpovídající úrovně ochrany v USA a stanovování příslušných záruk nebyly brány v potaz právní předpisy, které umožňují příslušným orgánům USA přistupovat k osobním údajům přímo, tedy bez pomoci poskytovatelů služeb. Činí tak právě s poukazem na to, že tato problematika dle aktuální judikatury nespadá do působnosti práva EU.[370]

[369] Šlo především o účastníky z řad nevládních organizací, které tento názor prezentovali na ústním jednání.
[370] CHRISTAKIS, Theodore. Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1). *European Law Blog*, 2021.

Argumenty USA považuji v tomto ohledu za legitimní, v praxi by však Soudní dvůr dle mého názoru takovou situaci nepřipustil. Jsem tedy přesvědčen, že by našel důvody pro zrušení rozhodnutí o adekvátní ochraně, které by tyto otázky vůbec neřešilo. Mohlo by k tomu dojít např. na základě argumentu, že všechny členské státy podléhají režimu Úmluvy, který se na tyto otázky vztahuje a který v této souvislosti stanoví určité požadavky (např. v oblasti dohledu nad činností příslušných orgánů). Pokud tedy USA v této oblasti nedodržují úroveň ochrany vyžadovanou alespoň ESLP, dochází předáním údajů k faktickému snížení jejich ochrany.[371] Proti tomu lze samozřejmě namítat, že se *stricto sensu* nejedná o ochranu poskytovanou unijním právem. Z výše uvedeného výkladu nicméně vyplývá, že Soudní dvůr je v této oblasti ochoten vykládat dosah unijního práva značně extenzivně.

4.1.3 Proporcionalita právních předpisů data retention

4.1.3.1 Proporcionalita – obecný rámec přezkumu

Jak již bylo uvedeno výše, u právních úprav data retention lze zpravidla odlišit dvě hlavní roviny – rovinu uchovávání a rovinu přístupu. Byť spolu obě tyto roviny úzce souvisí, jsou Soudním dvorem vnímány jako dva odlišné zásahy, které je třeba posuzovat odděleně.[372] Proporcionalitu opatření v rovině uchovávání tak Soudní dvůr přezkoumává především s ohledem na rozsah, množství a dobu uchovávání údajů. Posuzování proporcionality v oblasti přístupu je pak spojeno zejména se zkoumáním, jaké orgány a za jakých podmínek mají k dotčeným údajům přístup. Klíčové jsou tedy v tomto ohledu především otázky předchozího a následného soudního přezkumu a s nimi související povinnost informovat subjekty údajů o přístupu k jejich údajům. O veškerých těchto konkrétních aspektech bude podrobně pojednáno v následujících kapitolách. Základní rámec přezkumu proporcionality je však společný jak pro otázku uchovávání, tak pro otázku přístupu.

Začněme tedy u otázky, do jakých práv je prostřednictvím data retention zasahováno. Jak uchovávání provozních a lokalizačních údajů, tak následný přístup k těmto údajům jsou ze strany Soudního dvora vnímány v prvé řadě jako výjimka ze zásady důvěrnosti sdělení stanovené v sekundárním právu, konkrétně v čl. 5 směrnice 2002/58. To je z hlediska přezkumu přiměřenosti právních úprav data retention zcela klíčové, jelikož právě apel na to, aby se z data retention nestalo pravidlo, je základním stavebním kamenem striktního přístupu Soudního dvora, zejména co se týče odmítání plošné povahy povinnosti uchovávat údaje.[373]

---

[371] Srov. ibidem.
[372] Srov. rozsudek *La Quadrature du Net*, bod 116.
[373] Srov. rozsudek *Tele2 Sverige*, body 89 a 104.

Krom výjimky ze zásady důvěrnosti sdělení stanovené v sekundárním právu představuje data retention také zásah do základních práv zaručených Listinou. Vzhledem k tomu, že provozní a lokalizační údaje mohou vypovídat mnohé o soukromí dotčených osob a mohou mít charakter i citlivých údajů, představuje data retention zásah do práva na soukromí dle čl. 7 Listiny. Co se týče práva na ochranu osobních údajů ve smyslu čl. 8 Listiny, bylo v kapitole 2.4.3 vysvětleno, proč by měl být zásah do tohoto práva shledáván pouze v případě, že je porušen jeden ze základních prvků ochrany osobních údajů přímo vyjmenovaných v čl. 8 Listiny. Obdobný přístup k rozlišování práv na soukromí a ochranu osobních údajů v souvislosti s data retention navíc navrhoval, byť možná trochu nejednoznačně, generální advokát Villalón ve věci *Digital Rights Ireland*. Ten dospěl k závěru, že by směrnice 2006/24 měla být vnímána primárně jako zásah do práva na soukromí dle čl. 7 Listiny.[374] Soudní dvůr však tento přístup nepřijal a rozhodl, že jelikož představuje uchovávání provozních a lokalizačních údajů zpracování osobních údajů, jedná se také o zásah do práva na ochranu osobních údajů ve smyslu čl. 8 Listiny.[375] Tento nešťastný přístup z hlediska svébytného obsahu práva na ochranu osobních údajů, jakož i z hlediska vzájemného vztahu čl. 7 a 8 Listiny, byl následně přejat ve všech ostatních rozsudcích týkajících se data retention. Nelze tedy očekávat, že by měl být do budoucna opuštěn.

Vzhledem k tomu, že dle Soudního dvora může mít data retention dopad na to, jakým způsobem používáme prostředky elektronické komunikace, zkoumá jej i z hlediska svobody projevu ve smyslu čl. 11 Listiny. Zatímco v souvislosti s čl. 7 a 8 Listiny Soudní dvůr uvádí, že data retention představuje zvlášť závažný zásah do těchto práv, v případě čl. 11 Listiny volí mírnější formulace. Dle Soudního dvora data retention „*vyvolává otázky ohledně svobody projevu*“ a není vyloučeno, že může „*mít dopad na výkon svobody projevu*“.[376] Z hlediska svébytného obsahu zmíněných základních práv je opět nešťastné, že Soudní dvůr pak provádí test proporcionality v zásadě společně vzhledem ke všem třem těmto základním právům, nikoliv zvlášť ke každému z nich.

Posuzování proporcionality zásahu do základních práv způsobeného data retention Soudním dvorem zpravidla probíhá v několika na sebe navazujících krocích, v rámci kterých Soudní dvůr zkoumá:

a) zda existuje zásah do základních práv;

---

[374] Srov. stanovisko GA ve věci *Digital Rights Ireland*, body 55-67.
[375] Srov. rozsudek *Digital Rights Ireland*, bod 29.
[376] Srov. rozsudek *Digital Rights Ireland*, body 25 a 28.

b) zda je tento zásah stanoven zákonem;

c) zda respektuje podstatu dotčených základních práv;

d) zda skutečně odpovídá cíli obecného zájmu uznaného Unií či potřebě ochrany práv a svobod druhého;

e) zda tento zásah nejde nad rámec toho, co je naprosto nezbytné.[377]

Otázka, zda je zásah stanovený zákonem, nebyla v dosavadní judikatuře v oblasti data retention příliš řešena. Ve věci *Digital Rights Ireland* sice Soudní dvůr směrnici 2006/24 vyčetl, že nestanoví jasná a přesná pravidla pro rozsah zásahu do základních práv, avšak učinil tak v rámci posuzování nezbytnosti, nikoliv ve vztahu k požadavku zákonnosti.[378] V tom se přístup Soudního dvora odlišoval od přístupu navrhovaného generálním advokátem, který v důsledku absence úpravy dodatečných záruk dospěl s odkazem na judikaturu ESLP k závěru, že směrnice 2006/24 nesplňovala již požadavky na zákonnost zásahu, resp. potřebnou kvalitu zákona.[379] V následujících případech byl pak zásah poměrně jednoznačně vymezen v příslušných vnitrostátních právních úpravách, a touto otázkou se tedy nebylo třeba zabývat. V této souvislosti je možná na místě pouze upozornit, že dle judikatury ESLP má pojem „zákon" poměrně široký význam, jenž v obecné rovině může zahrnovat mj. nepsané právo či ustálenou judikaturu, jsou-li dostatečně přesné a předvídatelné. Požadavky na přesnost a předvídatelnost jsou nicméně tím přísnější, čím intenzivnější je zásah do základních práv.[380] V případě data retention tedy pravděpodobně lze trvat na zákonné formě. Tento požadavek ostatně vyplývá i z čl. 15 odst. 1 směrnice 2002/58, který v této souvislosti hovoří o tom, že členské státy mohou „*mohou přijmout legislativní opatření*", kterými omezí rozsah práv zaručených touto směrnicí.

Otázka, zda došlo k zásahu do podstaty základních práv, nebývá vždy výslovně posuzována. V případě data retention se však Soudní dvůr touto otázkou zabýval, když uvedl, že data retention „*nemůže zasáhnout do uvedené podstaty, neboť jak vyplývá z jejího čl. 1 odst. 2, tato směrnice [2006/24] neumožňuje seznámit se s obsahem elektronických sdělení jako takovým*."[381] Z toho lze na jedné straně vyvodit, že ať bude právní úprava data retention jakkoliv intrusivní, bude-li upravovat uchovávání a přístup pouze k provozním a lokalizačním údajům, neměla by se dotknout podstaty základních práv v čl. 7, 8 a 11 Listiny. Zároveň však z tohoto

[377] Srov. KELLERBAUER, Manuel et al. *Commentary on EU Treaties and Charter of Fundamental Rights*, 2019, s. 2248 a násl.
[378] Srov. rozsudek *Digital Rights Ireland*, bod 65.
[379] Srov. stanovisko GA ve věci *Digital Rights Ireland*, body 108-132.
[380] Viz kapitola 4.2.2.2.
[381] Rozsudek *Digital Rights Ireland*, bod 39. Srov. také rozsudek *Tele2 Sverige*, bod 101.

konstatování Soudního dvora může vyplývat, že jakékoliv hromadné uchovávání obsahu komunikace či přístup k němu je v rozporu s podstatou základních práv. Toto konstatování Soudního dvora může mít značný dopad např. na předávání údajů do USA, jelikož právní úprava USA v určitých případech umožňuje hromadnou automatickou analýzu pomocí klíčových slov. Zasahuje pak takové opatření do podstaty základních práv ve smyslu čl. 7, 8 a 11 Listiny?

Touto otázkou se zabýval generální advokát Saugmansgaard Øe ve věci *Facebook Ireland a Schrems*, a dospěl k závěru, že taková opatření nelze klást na roveň plošného přístupu k obsahu komunikace.[382] Přístup generálního advokáta považuji jednoznačně za správný. Opatření založená na hromadném filtrování komunikace sice zpracovávají velké množství sdělení, ale k přístupu k obsahu sdělení v pravém slova smyslu dochází pouze ve zlomku případů, přičemž ve zbytku případů jsou při nenalezení potřebné spojitosti s konkrétní hrozbou okamžitě mazány. Taková opatření tak jistě mohou vyvolávat zásadní otázky ohledně přiměřenosti zásahu, avšak paušálně konstatovat zásah do podstaty dotčených základních práv by dle mého názoru nebylo správné. Soudní dvůr se touto otázkou následně explicitně nezabýval, přestože konstatoval, že právní úprava USA v této souvislosti nezajišťuje adekvátní úroveň ochrany osobních údajů.[383] Tyto otázky se ještě do budoucna mohou stát relevantní, a to nejen v souvislosti s předáváním údajů do USA. Obdobné metody totiž používají i některé zpravodajské služby členských států. V každém případě pro účely této práce postačí konstatovat, že data retention nepředstavuje dle Soudního dvora zásah do podstaty základních práv ve smyslu čl. 7, 8 a 11 Listiny.

Co se týče problematiky legitimního cíle sledovaného data retention, ta také zpravidla nebude příliš kontroverzní. Je si však třeba uvědomit, že právní úpravy data retention mohou sledovat více cílů. V tomto ohledu je třeba rozlišovat mezi cílem spočívajícím v potírání „běžné“ trestné činnosti, v potírání závažné trestné činnosti a v zajišťování národní bezpečnosti. Někde na pomezí mezi potíráním závažné trestné činnosti a zajišťováním národní bezpečnosti je pak boj proti terorismu, jež může spadat do obou těchto kategorií. Soudní dvůr nedávno potvrdil, že boj proti terorismu je možné považovat za zajišťování národní bezpečnosti.[384]

---

[382] Srov. stanovisko GA Saugmansgaarda Øe ze dne 19. prosince 2019 ve věci *Facebook Ireland a Schrems*, C-311/18, EU:C:2019:1145, body 272 a násl.

[383] Srov. rozsudek *Facebook Ireland a Schrems*, bod 163 a násl. Soudní dvůr nicméně konstatoval, že k zásahu do podstaty těchto práv dochází za situace, kdy neexistuje jakákoliv možnost subjektů údajů využít právních prostředků s cílem získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu těchto údajů. Srov. ibidem, bod 187.

[384] Srov. rozsudek *Privacy International*, body 74-75.

Přestože všechny tyto cíle lze považovat za legitimní důvody pro omezení základních práv, každý z nich může odůvodňovat odlišně závažné zásahy. Zásah způsobený určitým opatřením tak může být shledán přiměřený vzhledem k cíli potírání závažné trestné činnosti, nikoliv však k cíli potírání jakékoliv trestné činnosti apod.

Na tomto místě je možná ještě vhodné zastavit se u případu *Digital Rights Ireland*, ve kterém se Soudní dvůr zabýval otázkou existence legitimního cíle při přezkumu platnosti směrnice 2006/24. Tato směrnice byla založena na tehdejším čl. 95 SES a jejím deklarovaným cílem bylo tedy odstraňování překážek vnitřního trhu vyplývajících z odlišností v úpravách data retention jednotlivých členských států. Pokud by bylo třeba přiměřenost směrnice posuzovat pouze optikou jejího harmonizačního cíle, jen stěží bychom mohli dospět k závěru, že jsou zaváděná opatření tomuto cíli přiměřená. Plošné uchovávání provozních a lokalizačních údajů téměř celé evropské populace by svou závažností bylo zjevně nepřiměřené, mělo-li by vést pouze ke zmírnění obtíží, které mohly přeshraničně působícím poskytovatelům služeb elektronických komunikací vyvstat v souvislosti s potřebou vyhovět odlišným požadavkům na data retention mezi členskými státy. To si uvědomoval i Soudní dvůr, který v této souvislosti uvedl: „*[c]o se týče otázky, zda uvedený zásah odpovídá cíli obecného zájmu, je třeba uvést, že i když má směrnice 2006/24 harmonizovat předpisy členských států týkající se povinností uvedených poskytovatelů, pokud jde o uchovávání některých údajů jimi vytvořených nebo zpracovaných, z jejího čl. 1 odst. 1 vyplývá, že hmotněprávním cílem této směrnice je zajistit dostupnost těchto údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak jsou vymezeny každým členským státem ve vnitrostátních právních předpisech. Hmotněprávním cílem této směrnice je tedy přispět k boji proti závažné trestné činnosti a v konečném důsledku také k veřejné bezpečnosti.*“[385] Ačkoliv pojem „*hmotněprávní cíl*“ použitý v českém překladu rozsudku nepovažuji za ideální,[386] jedná se samozřejmě o rozumné řešení. Potřeba zvolit toto řešení nicméně z mého pohledu dokladuje, že hlavním cílem směrnice 2006/24 bylo potírání závažné trestné činnosti, a tudíž že směrnice neměla být – přestože Soudní dvůr ve věci *Irsko v. Parlament a Rada* rozhodl odlišně – založena výhradně na tehdejším čl. 95 SES.[387]

[385] Srov. rozsudek *Digital Rights Ireland*, bod 41.
[386] Pojem „*material objective*“ použitý v anglickém jazykovém znění se v tomto ohledu jeví jako lepší.
[387] Srov. LYNSKEY, Orla. The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland. *Common Market Law Review*, 2013, s. 1790.

Poslední a klíčová část přezkumu pak spočívá v posuzování, zda dotčená právní úprava data retention nejde nad rámec toho, co je naprosto nezbytné k dosažení sledovaných cílů. V této fázi se tedy postup Soudního dvora alespoň z formálního hlediska odchyluje od typického třístupňového testu proporcionality, jak jej známe z odborné literatury,[388] stanovisek některých generálních advokátů[389] a jak ostatně vyplývá i z textu čl. 15 odst. 1 směrnice 2002/58.[390] V rámci typického třístupňového testu by mělo dojít k postupnému uplatnění tří testů – testu vhodnosti (zda dotčené opatření může dosáhnout dotčeného cíle), nezbytnosti (zda neexistuje opatření, které by stejného cíle dosáhlo při menším zásahu do základních práv) a přiměřenosti *stricto sensu*, spočívajícím ve vzájemném vážení proti sobě stojících práv a zájmů. V praxi však zkoumání, zda právní úprava data retention nepřekračuje meze naprosté nezbytnosti, které na tomto místě provádí Soudní dvůr, zahrnuje především zkoumání přiměřenosti *stricto sensu*, tedy vážení proti sobě stojících zájmů.[391] V rámci tohoto vážení je právům na soukromí a ochranu osobních údajů *de facto* připisována zvláštní důležitost oproti konkurenčním zájmům, čímž dochází ke značnému omezení prostoru pro uvážení na straně unijního zákonodárce či členského státu.

Tato zvláštní důležitost, kterou Soudní dvůr připisuje těmto základním právům, je zřetelná již z rozsudku *Digital Rights Ireland.* Když se mírou diskrece unijního zákonodárce zabýval generální advokát, měl za to, že tato diskrece má být široká. Vycházel přitom z ustálené judikatury, dle které v případech, ve kterých činnost unijního zákonodárce předpokládá volby politické, ekonomické a sociální povahy, v rámci kterých má zákonodárce provést komplexní posouzení a hodnocení, je soudní přezkum omezen a prostor pro uvážení široký.[392] V takových případech Soudní dvůr přezkoumává pouze to, zda je přijaté opatření založeno na objektivních kritériích a zda není zjevně nepřiměřené sledovanému cíli. Soudní dvůr však ve věci *Digital Rights Ireland* zaujal naprosto opačný přístup, a s odkazem na judikaturu ESLP konstatoval, že míra diskrece zákonodárce může být omezena v závislosti na řadě skutečností, mezi něž patří mimo jiné dotčená oblast, povaha dotčeného práva zaručeného Listinou, závažnost zásahu

[388] Srov. např. KELLERBAUER, Manuel et al. *Commentary on EU Treaties and Charter of Fundamental Rights*, 2019, s. 2252 a 2253.
[389] Srov. např. stanovisko generálního advokáta Cruz Villalóna ve věci Gauweiler a další, C-62/14, EU:C:2015:7, body 171 a násl.
[390] Který v této souvislosti hovoří o omezeních, která musí být „*nezbytná, přiměřená a úměrná*“, resp. „*necessary, appropriate and proportionate*“.
[391] Burda si tohoto přístupu všímá i v jiných oblastech judikatury Soudního dvora, přičemž hovoří o „*schovávání*“ třetího testu do testů přechozích. Srov. BURDA, Jan. *The Principle of Proportionality in EU Law*, 2019, s. 80.
[392] Srov. stanovisko GA ve věci *Digital Rights* Ireland, bod 96 a zde citovaná judikatura.

a jeho účel. S ohledem na významnou úlohu ochrany osobních údajů z hlediska základního práva na respektování soukromého života pak dospěl k závěru, že přezkum musí být naopak přísný.[393] Obdobně významnou pak shledal i svobodu projevu, což je v daném kontextu poměrně důležité, jelikož test proporcionality Soudní dvůr v oblasti data retention od případu *Tele2 Sverige* provádí ke všem třem dotčeným základním právům společně.[394]

S výše uvedeným do jisté míry souvisí ještě jedno specifikum přezkumu proporcionality v případě zásahu do základních práv na soukromí a ochranu osobních údajů, jež se projevilo ve věci *Digital Rights Ireland*. Když v minulosti Soudní dvůr přezkoumával platnost sekundárního práva otevírajícího prostor pro závažný zásah do základních práv, avšak zároveň umožňujícího členským státům tento zásah minimalizovat, zpravidla potvrdil platnost unijního předpisu s tím, že členské státy musí využít svou diskreci tak, aby zajistily, že výsledek bude v souladu se základními právy.[395] V případě směrnice 2006/24 však absence lidskoprávních záruk přímo ve směrnici vedla k jejímu zrušení, a to dokonce za situace, kdy zavedení těchto záruk v oblasti přístupu k údajům nebylo možné s ohledem na právní základ směrnice, což ostatně potvrdil i Soudní dvůr ve věci *Irsko v. Parlament a Rada*.

Generální advokát Villalón, který v tomto ohledu zastával stejný přístup jako Soudní dvůr, uvedl, že ponechat zajištění základních práv na vnitrostátním zákonodárci je možné pouze v případech, „*kdy Unie přijímá legislativu, která jen harmonizuje právní předpisy bezesporu přijaté všemi členskými státy, není srovnatelná se situací, kdy se Unie navíc rozhodne takovou legislativu všeobecně rozšířit.*“ Dle generálního advokáta „*v situaci, kdy omezení základních práv vyplývá ze samotné unijní právní úpravy, takže jej lze přičíst Unii, je podíl odpovědnosti připadající na unijního zákonodárce zcela jiný.*“[396] Osobně mi z předchozí judikatury Soudního dvora tato dělící linie jednoznačně nevyplývá. Např. ve věci *Hydro Seafood,* jejímž předmětem byla náhrada škody za údajné porušení základních práv, byl předmětný zásah do základních práv (povinnost usmrtit určité druhy ryb) přímým důsledkem čl. 9 bodu 1 směrnice 91/67[397], přesto Soudní dvůr poukázal na to, že „*požadavky plynoucí z ochrany základních práv v právním řádu Společenství zavazují rovněž členské státy při provádění předpisů Společenství.*

---

[393] Srov. rozsudek *Digital Rights Ireland*, body 47 a násl.
[394] Srov. rozsudek *Tele2 Sverige*, bod 93.
[395] Srov. GRANGER, Marie-Pierre. The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection. *European Law Review*, 2014, s. 844–845.
[396] Stanovisko GA ve věci *Digital Rights Ireland*, body 115-117.
[397] Směrnice Rady ze dne 28. ledna 1991 o veterinárních předpisech pro uvádění živočichů pocházejících z akvakultury a produktů akvakultury na trh.

Členské státy jsou tedy povinny provádět tyto předpisy v co největším možném rozsahu za podmínek, které neporušují tyto požadavky.“[398] Obdobně mám za to, že např. v případě evropského zatýkacího rozkazu vyplývá zásah do základních práv přímo z unijní úpravy.[399] Proto se domnívám, že přísné požadavky na unijního zákonodárce v tomto ohledu jsou jen dalším důsledkem toho, že Soudní dvůr právům na ochranu soukromí a osobních údajů připisuje zvláštní význam.

Závěrem je třeba uvést, že data retention nemusí být vždy vnímána pouze jako zásah do základních práv ve smyslu čl. 7, 8 a 11 Listiny, nýbrž také jako opatření, jež má sloužit k naplnění pozitivních povinností členských států vyplývajících z Listiny či Úmluvy. Členské státy se v této souvislosti odvolávají především na povinnost zajistit právo jednotlivců na bezpečnost ve smyslu čl. 6 Listiny.[400] Tento přístup zřejmě vychází z judikatury ESLP vážící se k čl. 3, 5 a 8 Úmluvy, která stanoví mj. povinnost států účinně potírat určité trestné činy, a to jak v rovině substantivní (z níž vyplývá např. požadavek na kriminalizaci určitých jednání), tak procedurální (z níž vyplývá požadavek na efektivní vyšetřování). ESLP v této souvislosti např. rozhodl, že Finsko porušilo své pozitivní povinnosti vyplývající z čl. 8 Úmluvy, když jím stanovené pravidlo důvěrnosti komunikace zcela vylučovalo dohledání osoby, jež se na internetu vydávala za někoho jiného, a to dokonce s úmyslem navázat intimní kontakt s nezletilými osobami.[401]

Soudní dvůr se touto otázkou zabýval ve věci *La Quadrature du Net*, přičemž dospěl k závěru, že ačkoliv z Listiny vyplývá povinnost členských států efektivně bojovat proti závažným trestným činům, čl. 6 Listiny nemůže být vykládán tak, že by členským státům ukládal povinnost přijmout určitá specifická opatření za účelem potírání určitých závažných trestných činů, jako je např. plošná data retention. Výše zmíněné pozitivní povinnosti členských států však musí dle Soudního dvora být zohledněny při posuzování přiměřenosti dotčených opatření v rámci vážení proti sobě stojících zájmů.[402] Se Soudním dvorem lze souhlasit v tom, že čl. 6 či jakýkoliv jiný článek Listiny by opravdu neměl být vykládán tak, že vyžaduje zavedení tak konkrétních a kontroverzních opatření, jako je plošná data retention. Na druhou

---

[398] Srov. rozsudek Soudního dvora ze dne 10. července 2003, *Hydro Seafood*, spojené věci C-20/00 a C-64/00, EU:C:2003:397, bod 88.
[399] Srov. rozsudek Soudního dvora ze dne 3. května 2007, *Advocaten voor de Wereld*, C-303/05, EU:C:2007:261, bod 53.
[400] Srov. rozsudek *La Quadrature du Net*, bod 123 a násl.
[401] Srov. rozsudek ESLP ze dne 2. prosince 2008, *K.U. proti Finsku*, stížnost č. 2872/02, ECHR:2008:1202JUD000287202 (dále jen „*rozsudek K.U. proti Finsku*“).
[402] Srov. rozsudek *La Quadrature du Net*, body 125 a násl.

stranu se domnívám, jak bude podrobněji popsáno níže, že Soudní dvůr bezpečnostní rovině celé problematiky nepřisuzuje takovou důležitost, jakou by si s ohledem na rozvoj technologií a závažnost některých hrozeb zasloužila.

4.1.3.2 Proporcionalita v rovině uchovávání údajů

Jak bylo uvedeno výše, Soudní dvůr považuje uchovávání provozních a lokalizačních údajů samo o sobě za zásah do základních práv dle čl. 7, 8 a 11 Listiny. Soudní dvůr v prvé řadě vychází z toho, že z provozních a lokalizačních údajů lze vyvozovat přesné závěry o soukromém životě osob.[403] S tím nelze než souhlasit.[404] Není však uchovávání jako uchovávání. Závažnost zásahu do základních práv způsobeného uchováváním údajů se neodvíjí pouze od záruk v oblasti přístupu, ale taktéž od modalit samotného uchovávání – množství uchovávaných údajů, kategorie uchovávaných údajů, délky jejich uchovávání, formy jejich uchovávání, zabezpečení jejich uchovávání apod. Tyto aspekty musí při posuzování přiměřenosti právní úpravy data retention hrát zcela klíčovou roli.

Plošné, či cílené uchovávání?

Otázka, zda sama povinnost uchovávat údaje může být uložená plošně, či zda musí být nějakým způsobem omezena, představuje zřejmě nejzásadnější právní otázku v oblasti data retention. Do popředí se však tato otázka rozhodně nedostala okamžitě. Ve věci *Digital Rights Ireland* se Soudní dvůr přípustností plošného uchovávání údajů jako takového explicitně nezabýval. Samozřejmě, Soudní dvůr při posuzování platnosti směrnice 2006/24 ve značné míře zohledňoval právě rozsah povinnosti uchovávání, tj. skutečnost, že dochází k uchovávání údajů prakticky celé evropské populace.[405] Kdyby však měl Soudní dvůr již tehdy za to, že plošný charakter data retention je sám o sobě v rozporu s čl. 7 a 8 Listiny, mohl směrnici 2006/24 zrušit již z tohoto důvodu. Nemusel by se tedy zabývat problematikou záruk v oblasti přístupu k údajům.[406] Z mého pohledu nelze pochybovat o tom, že v daném okamžiku Soudní dvůr plošné uchovávání provozních a lokalizačních údajů ještě považoval za přípustné, byť za dodržení velmi striktních podmínek v oblasti přístupu.

Tato otázka tak reálně vyvstala až ve věci *Tele2 Sverige* v návaznosti na výslovný dotaz správního odvolacího soudu ve Stockholmu. Generální advokát v souladu s názory členských států a s odkazem na podstatu data retention, která spočívá ve „čtení minulosti“, dospěl

[403] Srov. rozsudek *Digital Rights Ireland*, bod 27.
[404] Viz kapitola 3.1.1.
[405] Srov. rozsudek *Digital Rights Ireland*, body 56 a 65.
[406] Ibidem, body 60 a násl.

k závěru, že plošné uchovávání je při stanovení přísných podmínek v oblasti přístupu přípustné.[407] Soudní dvůr však zaujal odlišný postoj, když uvedl:

„97 Stran otázky, zda taková vnitrostátní právní úprava, jaká je dotčena ve věci C-203/15, splňuje tyto podmínky, je třeba uvést, že uvedená právní úprava stanoví plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, které se vztahuje na veškeré prostředky elektronické komunikace, a ukládá poskytovatelům služeb elektronických komunikací povinnost uchovávat tyto údaje systematicky a průběžně bez jakékoli výjimky. Jak vyplývá z předkládacího rozhodnutí, kategorie údajů, na které se tato právní úprava vztahuje, v podstatě odpovídají kategoriím údajů, jejichž uchovávání bylo stanoveno na základě směrnice 2006/24. [...]

104 V této souvislosti je třeba uvést, že s ohledem na své vlastnosti uvedené v bodě 97 tohoto rozsudku vede taková právní úprava k tomu, že uchovávání provozních a lokalizačních údajů je pravidlem, ačkoli režim zavedený směrnicí 2002/58 vyžaduje, aby toto uchovávání údajů bylo výjimkou.

105 Dále taková vnitrostátní právní úprava, jaká je dotčena ve věci v původním řízení, která se vztahuje obecně na všechny účastníky a registrované uživatele a týká se všech prostředků elektronické komunikace a veškerých provozních údajů, nestanovuje žádné rozlišení, omezení nebo výjimky činěné v závislosti na sledovaném cíli. Týká se globálně všech osob, které využívají služeb elektronických komunikací, avšak osoby, jejichž údaje jsou uchovávány, se nenacházejí, byť nepřímo, v situaci, která může vést k trestnímu stíhání. Vztahuje se tedy i na osoby, v jejichž případě neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset se závažnou trestnou činností. Kromě toho nestanoví žádnou výjimku, takže se vztahuje i na osoby, jejichž sdělení jsou podle pravidel vnitrostátního práva předmětem profesního tajemství (obdobně, pokud jde o směrnici 2006/24, viz rozsudek Digital Rights, body 57 a 58).

106 Taková právní úprava nevyžaduje souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti. Zejména se neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k boji proti trestné činnosti (obdobně, pokud jde o směrnici 2006/24, viz rozsudek Digital Rights, bod 59).

107 Taková vnitrostátní právní úprava, jako je právní úprava dotčená ve věci v původním řízení, proto překračuje meze toho, co je naprosto nezbytné, a nelze ji v demokratické společnosti považovat za odůvodněnou, jak vyžaduje čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny.

108 Naproti tomu čl. 15 odst. 1 směrnice 2002/58 ve spojení s články 7, 8, 11 a čl. 52 odst. 1 Listiny nebrání tomu, aby členský stát přijal právní úpravu, která preventivně umožňuje cílené uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti za podmínky, že uchovávání

[407] Srov. stanovisko GA ve věci *Tele2 Sverige*, body 192 a násl.

je omezeno na to, co je nezbytně nutné, pokud jde o kategorie údajů, které mají být uchovávány, komunikační prostředky, na něž se toto uchovávání vztahuje, dotčené osoby a dobu trvání uchovávání.

109 K tomu, aby tato vnitrostátní právní úprava splňovala požadavky uvedené v předchozím bodě tohoto rozsudku, musí tato právní úprava zaprvé stanovit jasná a přesná pravidla pro rozsah a použití takového opatření pro uchovávání údajů a stanovit minimální požadavky, tak aby osoby, jejichž údaje byly uchovány, měly dostatečné záruky umožňující účinně chránit jejich osobní údaje proti riziku zneužití. Taková právní úprava musí zejména vymezit okolnosti a podmínky, za nichž může být preventivně přijato opatření pro uchovávání údajů, čímž zaručí, že takové opatření se omezí na to, co je nezbytně nutné (obdobně stran směrnice 2006/24, viz rozsudek Digital Rights, bod 54 a citovaná judikatura).

110 Zadruhé, pokud jde o hmotněprávní podmínky, které musí splňovat vnitrostátní právní úprava, jež umožňuje v rámci boje proti trestné činnosti preventivní uchovávání provozních a lokalizačních údajů, aby byla omezena na to, co je nezbytně nutné, je třeba uvést, že i když tyto podmínky mohou být různé v závislosti na opatřeních, jež jsou přijímána pro účely předcházení, vyšetřování, odhalování a stíhání závažné trestné činnosti, uchovávání údajů musí nicméně vždy odpovídat objektivním kritériím, která vymezují vztah mezi údaji, které mají být uchovávány, a sledovaným účelem. Takové podmínky musí v praxi zejména umožňovat účinné vymezení rozsahu opatření, a v návaznosti na to i dotčené veřejnosti.

111 Pokud jde o vymezení takového opatření ve vztahu k veřejnosti a situacím, na které se může vztahovat, vnitrostátní právní úprava musí být založena na objektivních skutečnostech, na jejichž základě lze vymezit okruh osob z řad veřejnosti, jejichž údaje mohou vykázat minimálně nepřímou souvislost se závažnou trestnou činností nebo určitým způsobem přispívat k boji proti závažné trestné činnosti či k předcházení závažného ohrožení veřejné bezpečnosti. Takové vymezení lze zajistit prostřednictvím zeměpisného kritéria, jestliže příslušné vnitrostátní orgány mají na základě objektivních skutečností za to, že v jedné nebo více z územních oblastí existuje zvýšené riziko přípravy či páchání takových trestných činů.“

Z výše uvedeného v prvé řadě vyplývá, že Soudní dvůr vychází ve značné míře z toho, že plošný charakter uchovávání údajů činí z uchovávání údajů pravidlo, ačkoliv čl. 5 směrnice 2002/58 vyžaduje, aby bylo uchovávání údajů pouze výjimkou. Je však povaha uchovávání údajů jako výjimky ze zásady důvěrnosti tak jednoznačná?

V této souvislosti je vhodné opět upozornit na stanovisko generálního advokáta v dané věci, který se touto otázkou zabýval a dospěl k odlišnému závěru než Soudní dvůr. Dle generálního advokáta neznamená data retention nutně výjimku, kterou by dle ustálené judikatury bylo třeba vykládat restriktivně. Generální advokát v této souvislosti vycházel primárně z toho, že se směrnice 2002/58 dle bodu 11 svého odůvodnění „*neměla dotýkat*“ možnosti členských států přijmout opatření spočívající v uchovávání provozních a lokalizačních údajů. Generální advokát dále uvedl, že zatímco čl. 10 směrnice 2002/58 je výslovně nadepsán „Výjimky“, čl. 15 této směrnice, který obsahuje možnost členských států

zavést data retention, je nadepsán pouze jako „Použití některých ustanovení směrnice 95/46/ES“. Samo znění čl. 15 odst. 1 taktéž, přestože vyžaduje, aby přijatá opatření byla v souladu s obecnými zásadami práva Společenství, nenaznačuje nic o jejich „výjimečném charakteru“.[408]

Osobně proto souhlasím s názorem generálního advokáta. Z mého pohledu se však v této souvislosti nabízí ještě jeden argument, vyplývající přímo ze znění čl. 5 směrnice 2002/58. Čl. 5 odst. 1 směrnice totiž zní: „*členské státy zajistí prostřednictvím vnitrostátních právních předpisů důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě a veřejně dostupných služeb elektronických komunikací a s nimi souvisejících provozních údajů. Zejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1. Tento odstavec nebrání technickému uchovávání, které je nezbytné pro přenos sdělení, aniž by tím byla dotčena zásada důvěrnosti.*“ Účelem zásady důvěrnosti sdělení dle čl. 5 odst. 1 směrnice 2002/58 tak dle mého názoru bylo, aby k zachycování komunikace nedocházelo bez souhlasu či bez zákonného podkladu, nikoliv to, aby k zákonnému zachycování komunikace mohlo docházet pouze ve výjimečných případech.

Judikatura Soudního dvora neposkytuje zcela jasnou odpověď na to, zda zásada důvěrnosti sdělení tak, jak ji vykládá Soudní dvůr, vyplývá toliko ze směrnice, či zda je možné jej dovodit taktéž přímo z Listiny. Do budoucna se přitom může jednat o zcela zásadní otázku, jelikož směrnice 2002/58 bude dříve či později revidována, přičemž právě znění ustanovení nahrazujícího čl. 15 odst. 1 směrnice 2002/58 bylo jedním z klíčových sporných bodů v rámci legislativního procesu vedoucího k nové právní úpravě. Europol i řada členských států v návaznosti na rozsudek *Tele2 Sverige* zastávaly názor, že zákaz plošné data retention nevychází přímo z Listiny, nýbrž výhradně z toho, jak je formulována zásada důvěrnosti komunikace v čl. 15 odst. 1 směrnice 2002/58.[409] Nejaktuálnější judikatura Soudního dvora dle mého názoru naznačuje spíše opak, jelikož Soudní dvůr mj. uvádí, že „*[p]řijetím této směrnice tedy unijní normotvůrce konkretizoval práva zakotvená v článcích 7 a 8 Listiny, takže uživatelé prostředků elektronické komunikace mohou v zásadě právem očekávat, že jejich komunikace a s ní související údaje zůstanou anonymní a nebude možné je zaznamenat bez jejich*

[408] Srov. stanovisko GA ve věci *Tele2 Sverige*, body 109 a násl.
[409] Srov. Council of the European Union. *Working document – Data retention – Contributions by delegations*, 2017, s. 30.

souhlasu.“[410] Mám tedy za to, že samotná změna sekundárního práva ke změně názoru Soudního dvora nepostačí.

Dalším problémem konceptu cílené data retention, jak byl Soudním dvorem nastíněn ve věci *Tele2 Sverige*, je jeho obtížná realizovatelnost v praxi.[411] Jde o to, jak data retention účinně omezit jen na určité časové období, určité zeměpisné oblasti či okruh určitých osob. V současnosti asi není možné tvrdit, že by se závažná trestná činnost obecně vyskytovala pouze v určitém časovém období. Lze si sice představit, že by se k plošné data retention přistoupilo např. v případě indicií o předpokládaném teroristickém útoku. V takovém případě je ale značně omezen potenciál data retention jakožto nástroje ke čtení minulosti, jelikož k ukládání údajů bude docházet až v době po vzniku takového podezření. Zároveň se tím značně omezuje okruh trestných činů, k jejichž potírání může být data retention využita. Obdobně je to s územním zacílením. Např. hrozba teroristických činů je primárně spojena s velkými aglomeracemi, totéž ale nelze tvrdit v případě jiné závažné trestné činnosti. K přípravě a plánování těchto činů může navíc docházet ve zcela jiném místě, než ve kterém jsou následně realizovány. V případě trestných činů páchaných prostřednictvím internetu pak možnost územního omezení odpadá zcela. Zaměření na určitý okruh osob se pak z hlediska účinnosti nebude příliš lišit od *quick freeze* metody, jelikož je závislé na prvotní identifikaci souvislosti mezi těmito osobami a určitou hrozbou. Nelze také zapomínat na to, že jedním ze základních požadavků na jakoukoliv úpravu umožňující skryté zpracování osobních údajů je její předvídatelnost. Pokud by však měla být předvídatelně stanovena kritéria pro zacílení data retention, pachatelé závažných trestných činů by se mohli povinnosti uchovávat údaje poměrně snadno vyhnout. Identifikace určitých rizikových oblastí či okruhů osob by taky v mnoha případech mohla narážet na problémy spojené se zákazem diskriminace.

Žádný z členských států se z výše uvedených důvodů nepokusil požadavky Soudního dvora uvést do praxe a většina z nich své vnitrostátní právní úpravy plošné data retention ponechala v platnosti. To vedlo mj. k zahájení řízení ve věcech *La Quadrature du Net a další*, *Ordre des barreaux francophones et germanophones*, *Commissioner of the Garda Síochána, SpaceNet* a *Telekom Deutschland.* Britská právní úprava ve věci *Privacy International* pak umožňovala nejen plošné uchovávání, ale především plošné předávání provozních a lokalizačních údajů zpravodajským službám, nešlo tedy o typickou data retention úpravu.

[410] Rozsudek *La Quadrature du Net*, bod 109.
[411] Srov. Council of the European Union. *Working document – Data retention – Contributions by delegations*, 2017, s. 6.

Soudní dvůr tak měl příležitost svoje úvahy o cílené data retention upřesnit, mj. ve světle argumentace členských států. Ve věci *Tele2 Sverige* se totiž úvahy Soudního dvora ohledně zeměpisného či časového zacílení data retention objevily až v rozsudku a členské státy na ně tak neměly možnost reagovat. Argumentace členských států ve výše uvedených případech byla tedy zaměřena především na to, proč není možné účinně cílit již povinnost uchovávání, která musí být plošná, a proč je třeba adresnost opatření zajišťovat až v okamžiku přístupu. Jinými slovy, členské státy zpravidla otevřeně argumentovaly ve prospěch přehodnocení závěrů Soudního dvora ve věci *Tele2 Sverige.*

Požadavkem na přehodnocení těchto závěrů se nejprve zabýval generální advokát. Ten sice uvedl, že by Soudní dvůr měl na nepřípustnosti plošné data retention setrvat. Také však uvedl, že cílená data retention může být založena i na jiných kritériích než na těch, které zmínil Soudní dvůr ve věci *Tele2 Sverige.* Dle generálního advokáta lze cílené data retention dosáhnout i omezením kategorií uchovávaných údajů. Dle generálního advokáta by tak nebyly uchovávány veškeré provozní a lokalizační údaje, ale pouze ty nejdůležitější, jejichž souhrn však neumožní získat přesný a detailní obraz o životě dotčených osob. Generální advokát dále poukázal na dokumenty vyplývající ze zasedání pracovních skupin Rady, jež v návaznosti na vynesení rozsudku *Tele2 Sverige* uvažovaly právě např. o omezení kategorií uchovávaných údajů, pseudonymizaci údajů, stanovení kratší doby uchovávání, vyloučení určitých kategorií poskytovatelů služeb apod.[412]

Omezení uchovávaných kategorií údajů na to, co je nezbytně nutné, je bezesporu něco, co musí být od právních úprav data retention vyžadováno. Mám však za to, že i při omezení údajů na nezbytné minimum půjde v případě uchovávání údajů o všech uživatelích elektronické komunikace sice o omezenější, avšak nadále plošnou povinnost data retention. Jinými slovy – cesta nastíněná generálním advokátem je z mého pohledu rozhodně správná, ovšem jen stěží lze říci, že se jedná o cílenou data retention, jak ji měl na mysli Soudní dvůr ve věci *Tele2 Sverige*. Ostatně členské státy, když o takovém řešení hovořily, jej záměrně nazývaly omezenou data retention („*restricted data retention*"), nikoliv cílenou data retention („*targeted data retention*").[413] V neposlední řadě je třeba dodat, že členské státy nakonec dospěly k závěru, že neexistuje prostor pro zásadnější omezení kategorií uchovávaných údajů, aniž by se to významně dotklo účinnosti data retention.[414] Reálně by tak musela být zvolena cesta omezení

[412] Srov. stanovisko GA ve věci *Ordre des barreaux francophones a germanophone*, body 91 a násl.
[413] Srov. Council of the European Union. *Data retention – preparation of Council debate*, 2017.
[414] Srov. Council of the European Union. *Data retention – State of play*, 2018, s. 4.

dob uchovávání a opatření v rovině zabezpečení uchovávání (např. pseudonymizace). Šlo by tak o plošnou data retention s přísnějšími požadavky na záruky v oblasti uchovávání a přístupu.

Soudní dvůr nicméně následně potvrdil svou předchozí judikaturu v tom smyslu, že stanovení plošné povinnosti uchovávání je nepřípustné, přičemž cílené uchovávání může být dosaženo zaměřením na určitou skupinu osob či určitou oblast. Tyto oblasti musí dle Soudního dvora být určeny na základě nediskriminačních kritérií. Mělo by tak jít o oblasti, ve kterých je zvýšené riziko přípravy či páchání závažné trestné činnosti, mj. např. díky vyšší koncentraci osob (tj. např. letiště či nádraží).[415]

Soudní dvůr dále – zřejmě v reakci na argumenty vznesené členskými státy a předkládajícími soudy, které na problémy s uplatňováním kritérií stanovenými v rozsudku *Tele2 Sverige* upozorňovaly – připustil ze zákazu plošného uchovávání určité výjimky. V prvé řadě připustil plošné uchovávání některých kategorií údajů. První takovou kategorií jsou IP adresy. Soudní dvůr se nechal členskými státy přesvědčit, že některé závažné trestné činy není možné bez plošné povinnosti uchovávání IP adres spolehlivě vyšetřovat a stíhat. Půjde o trestné činy páchané téměř výhradně prostřednictvím internetu, jako např. šíření dětské pornografie. Soudní dvůr nicméně uvedl, že IP adresy mohou být použity k rekonstrukci internetové historie konkrétního uživatele a tím i k vytvoření profilu. Díky tomu představuje plošné uchovávání IP adres závažný zásah do základních práv, který je možné ospravedlnit pouze za podmínky, že uchovávání bude omezeno na nezbytně nutnou dobu a přístup k IP adresám bude možný pouze za účelem vyšetřování závažné trestné činnosti, za současného dodržení přísných záruk v oblasti přístupu. Jinými slovy, v případě IP adres Soudní dvůr zaujal přístup, který členské státy navrhovaly zaujmout obecně.[416] Toto zmírnění požadavků rozsudku *Tele2 Sverige* bylo jednoznačně na místě, jelikož nemožnost uchovávání tohoto druhu údajů by reálně znamenala, že určité trestné činy páchané výhradně prostřednictvím internetu by v praxi nebylo možné postihovat.[417]

Další výjimkou v této souvislosti jsou údaje o identitě uživatelů prostředků internetové komunikace. V návaznosti na rozsudek *Ministerio Fiscal* Soudní dvůr uvedl, že uchovávání těchto údajů nepředstavuje závažný zásah do základních práv, a může být tedy vyžadováno i za účelem potírání jiné než závažné trestné činnosti. Toto uchování navíc nemusí být omezeno na určitou dobu. Soudní dvůr vycházel z toho, že tyto údaje samy o sobě neodhalují místo, dobu

[415] Srov. rozsudek *La Quadrature du Net*, bod 150.
[416] Srov. rozsudek *La Quadrature du Net*, body 152-156.
[417] K problematice vzniku „stop“ v kyberprostoru viz kapitola 3.1.5.

a adresáty komunikace, a tudíž jen na jejich základě není možné činit přesné závěry o životě osob.[418] Poněkud zarážející je ale to, že tento mírnější přístup platí dle Soudního dvora pouze tehdy, „*nemohou-li uvedené údaje být spojeny s informacemi o uskutečněných komunikacích*“.[419] Krom toho, že v praxi budou často tyto údaje potřebné právě k identifikaci autora určitého sdělení, je otázkou, jak by tato „nemožnost spojení s dalšími údaji“ měla být v praxi zajištěna v rámci samotného uchovávání údajů. Zdá se tedy, že Soudní dvůr zamýšlel svůj požadavek směřovat spíše do roviny přístupu, v tom smyslu, že zatímco přístup např. k údaji o totožnosti majitele SIM karty, která byla vložena do odcizeného telefonu, může být umožněn i za účelem vyšetřování méně závažné trestné činnosti (krádeže), přístup k informaci o totožnosti majitele SIM karty za účelem identifikace autora určité SMS zprávy může být umožněn pouze za účelem vyšetřování závažné trestné činnosti. Způsob, jakým Soudní dvůr svůj požadavek naformuloval, je každopádně matoucí. Samotné plošné uchovávání tohoto druhu údajů v praxi jednoduše nemůže být podmíněno tím, že tyto údaje v budoucnu nebude možné spojit s jinými údaji.

Rozdíl mezi přístupem Soudního dvora k IP adresám na straně jedné a k údajům o identitě uživatelů na straně druhé tak zřejmě spočívá v tom, že na IP adresu je zpravidla prostřednictvím cookies navázána internetová historie uživatele. Ovšem i IP adresa umožňuje činit závěry o životě osob až ve spojitosti s údaji o navštívených stránkách. Zároveň se jedná pouze o adresu, jež identifikaci konkrétní osoby umožňuje právě až ve spojení s údajem o identitě uživatele. Vyčlenění právě výše uvedených druhů údajů z obecného zákazu požadavku na plošné uchovávání opět nebylo předmětem hlubší diskuze před Soudním dvorem. Je tedy otázkou, zda se ukáže v praxi funkční, či zda se proti jeho praktické využitelnosti budou členské státy vymezovat v dalších řízeních. Obdobně, jako to udělaly vůči bezvýjimečnému zákazu plošného uchovávání v návaznosti na rozsudek *Tele2 Sverige.*

Soudní dvůr připustil i plošné uchovávání všech provozních a lokalizačních údajů, ovšem pouze v době, kdy příslušný členský stát čelí „*skutečné a existující či předvídatelné hrozbě pro národní bezpečnost*“.[420] Dle Soudního dvora má jít o hrozby, které jsou schopné vážně destabilizovat základní ústavní, politické, ekonomické nebo sociální struktury státu a zejména přímo ohrožovat společnost a obyvatelstvo, např. právě o teroristické útoky. K plošnému uchovávání údajů však může být přistoupeno pouze poté, co soud či jiný nezávislý

[418] Srov. rozsudek *La Quadrature du Net*, body 156-159.
[419] Ibidem, bod 158.
[420] Ibidem, bod 137.

orgán potvrdí, že byly tyto podmínky splněny, a pouze na dohlednou dobu, byť s možností prodloužení.[421]

Bude velmi zajímavé sledovat, jak členské státy výše uvedenou možnost využijí a zda tento způsob bude odpovídat představám Soudního dvora. Ten ve svých úvahách mj. nezmínil, že by se nutně muselo jednat o hrozbu konkrétního útoku, dalo by se tedy uvažovat i o tom, že se může jednat o obecnější druh rizika. To je přinejmenším v některých členských státech (Belgie, Francie, Německo), alespoň podle konstatování jejich vlád a soudů, poměrně reálné a stálé.[422] Stejně tak Soudní dvůr výslovně nesvázal možnost plošně uchovávat údaje s vyhlášením nouzového stavu dle vnitrostátního práva, jak navrhoval generální advokát.[423] Dokážu si tedy představit, že tyto členské státy konstatují – např. na základě obecnějších informací zpravodajských služeb zabývajících se existencí těchto rizik – existující vážné ohrožení národní bezpečnosti spočívající v riziku teroristických útoků. Jelikož nelze očekávat, že by toto riziko v blízké době vymizelo, je možné, že bude následně na základě přezkoumávání situace např. v několikaměsíčních intervalech tento stav udržován. V této souvislosti je třeba upozornit na to, že vnitrostátní předkládající soudy se často přikláněly k tomu, že plošná data retention je s ohledem na bezpečnostní situaci v daném státě nezbytná. Nelze tedy vyloučit, že budou poměrně shovívavé při posuzování toho, zda jsou výše uvedené podmínky splněny. Je samozřejmě možné, že v tomto ohledu budou položeny další předběžné otázky. Jak bylo uvedeno v kapitole 4.1.2.4, s ohledem na znění čl. 4 odst. 2 SEU a zásadu svěřených pravomocí by měl být Soudní dvůr velice zdrženlivý ohledně možného přehodnocování závěrů vnitrostátních soudů v tomto ohledu.

Kategorie uchovávaných údajů

Kategorie údajů uchovávaných dle vnitrostátních právních úprav nejdou zpravidla nad rámec kategorií, jež byly uchovávány dle směrnice 2006/24.[424] Výše uvedené rozlišování mezi údaji o IP adresách, údaji o identitě uživatelů zařízení a zbylými provozními a lokalizačními údaji přitom představuje první případ, ve kterém se Soudní dvůr rozhodl z hlediska modalit uchovávání rozlišovat mezi jednotlivými druhy údajů. Zatím tedy neexistují provozní a lokalizační údaje, jejichž uchovávání by Soudní dvůr zcela zakázal, ovšem je třeba rozlišovat mezi údaji, u nichž je přípustné plošné uchovávání, a zbytkem údajů, u nichž je – alespoň tedy

[421] Ibidem, body 134-139.
[422] Srov. např. předkládající rozhodnutí ve věci *La Quadrature du Net*, bod 23. Předkládací rozhodnutí je dostupné z https://curia.europa.eu/.
[423] Srov. stanovisko GA ve věci *La Quadrature du Net*, bod 104.
[424] Pro výčet jednotlivých kategorií uchovávaných údajů dle směrnice 2006/24 viz kapitola 3.2.2.2.

mimo případy existence aktuální hrozby pro národní bezpečnost – možné pouze uchovávání cílené.

Samozřejmě je také třeba důsledně trvat na tom, aby uchovávané údaje neodhalovaly obsah komunikace. Jak již bylo uvedeno výše, v některých případech může být hranice mezi metadaty a obsahem poměrně tenká, což je zřejmé zejména v případě adres URL, které někdy mohou být, např. na rozdíl od běžné adresy či telefonního čísla, natolik specifické, že umožňují s velkou přesností předpokládat i obsah komunikace. Jelikož se však dá obsah komunikace pořád pouze předpokládat (byť s vysokou přesností), jedná se stále jen o metadata, byť taková, která si s ohledem na svou povahu jistě zaslouží zvláštní pozornost. Generální advokát v této souvislosti ve svém stanovisku ve věci *Ordre des barreaux francophones a germanophone* vyzval mj. k tomu, aby v případě uchovávání URL adres byla maximálně omezena doba uchovávání, resp. aby byla maximálně omezena potřeba tyto údaje uchovávávat.[425] Soudní dvůr však následně zvláštní požadavky směrem k adresám URL nezmínil.

Před Soudním dvorem byla dále opětovně specificky zmiňována i problematika provozních a lokalizačních údajů chráněných profesním (advokátním, lékařským) tajemstvím a otázka, zda je uchovávání těchto údajů vůbec přípustné a příp. zda má probíhat za specifických podmínek. Soudní dvůr ve věcech *Digital Rights Ireland* a následně *Tele2 Sverige* sice konstatoval, že směrnice 2006/24 nevylučuje z povinnosti uchovávání ani údaje podléhající profesnímu tajemství, avšak dále se k této otázce nevyjádřil. Zřejmě tak šlo jen o další důvod pro to, aby byl zásah do základních práv vyplývající ze směrnice 2006/24 považován za zvlášť závažný.[426] Tomu odpovídá přístup Soudního dvora ve věci *La Quadrature du Net*, kde Soudní dvůr uvedl, že skutečnost, že dotčená povinnost zahrnuje taktéž údaje podléhající profesnímu tajemství, posiluje odrazující účinky této úpravy co se využívání elektronických komunikací týče. To dle Soudního dvora platí i o údajích týkajících se komunikace *whistleblowerů,* chráněných směrnicí 2019/1937.[427] Soudní dvůr nicméně nerozhodl, že by s tímto druhem údajů z hlediska uchovávání muselo být zacházeno odlišně.

Takový přístup Soudního dvora dává smysl především z praktického hlediska. V okamžiku uchovávání je poměrně obtížné rozlišovat mezi údaji chráněnými profesním tajemstvím a ostatními údaji. To pravděpodobně nelze zajistit jinak než registrací určitých

[425] Srov. stanovisko GA Campos Sánchez-Bordony ve věci *Ordre des barreaux francophones a germanophone*, bod 99.
[426] Srov. rozsudek *Digital Rights Ireland*, bod 58 a rozsudek *Tele2 Sverige*, bod 105.
[427] Srov. rozsudek *La Quadrature du Net*, bod 118.

chráněných zařízení, u nichž by následně nemohlo k uchovávání údajů docházet. To si však lze představit asi pouze u údajů chráněných profesním tajemstvím, nikoliv u údajů *whistleblowerů.* Takové řešení by nicméně zcela jistě nebylo schopno vyloučit uchovávání u veškerých údajů chráněných profesním tajemstvím. Zároveň nelze vyloučit, že by tato zařízení byla následně záměrně užívána k páchání trestné činnosti. Je každopádně zcela na místě těmto údajům poskytovat vyšší úroveň ochrany následně – ať už v rovině přístupu (tj. nezpřístupněním údajů, u nichž je pravděpodobné, že budou obsahovat informace chráněné profesním tajemstvím) či v následných řízeních (např. stanovením nepoužitelnosti takto získaných důkazů). Ostatně, když se touto otázkou prvně zabýval generální advokát ve věci *Digital Rights Ireland*, hovořil právě o rozlišování v rovině přístupu.[428]

Povaha data retention neumožňuje z uchovávání účinně vyloučit citlivé údaje. Řada uchovávaných údajů může, ale zároveň nemusí mít povahu citlivého údaje, což v okamžiku uchovávání nelze posoudit. Soudní dvůr proto uchovávání citlivých údajů nevylučuje, byť stejně jako v případě údajů chráněných zvláštním tajemstvím představuje tato skutečnost jeden z hlavních důvodů, proč je zásah do základních práv spojený s data retention třeba považovat za zvlášť závažný.[429]

Doba uchovávání údajů

Doba uchovávání údajů představuje z hlediska posuzování přiměřenosti právní úpravy data retention stejně důležitou otázku jako rozsah kategorií uchovávaných údajů. Zatímco údaj o lokalitě mobilního zařízení v jednom okamžiku nám o životě jeho uživatele sdělí poměrně málo, budeme-li mít k dispozici údaje o lokalitě tohoto zařízení za posledních několik měsíců, potenciál činit přesné závěry o životě jeho uživatele se rapidně zvyšuje. Studie zároveň naznačují, že se užitečnost uchovávaných údajů pro účely potírání trestné činnosti po určité době snižuje, byť se názory členských států ohledně toho, jak je tato doba dlouhá, poměrně rozcházejí. Zatímco např. francouzská právní úprava stanoví jednotnou lhůtu uchovávání v délce dvou let, v případě německé právní úpravy to je 4 až 10 týdnů v závislosti na typu údajů.[430]

Směrnice 2006/24 nestanovila jednotnou dobu uchovávání údajů, ale umožňovala členským státům zvolit dobu mezi šesti měsíci a dvěma lety. Soudní dvůr při posuzování

---

[428] Stanovisko GA ve věci *Digital Rights Ireland*, bod 128.
[429] Srov. rozsudek *La Quadrature du Net*, body 117, 119, 132 a 142.
[430] Srov. stanovisko GA ve věci *Ordre des barreaux francophones a germanophone*, bod 96 a zde uvedená poznámka pod čarou.

platnosti směrnice 2006/24 ve věci *Digital Rights Ireland* směrnici vyčetl, že nepožaduje, aby doba uchovávání byla stanovena na základě objektivních kritérií, aby bylo zaručeno její omezení na nezbytné minimum, např. tím, že by bylo rozlišováno mezi jednotlivými kategoriemi údajů dle jejich užitečnosti.[431] I tyto skutečnosti představovaly důvody pro zrušení směrnice. Přístup Soudního dvora se nezměnil ani při posuzování vnitrostátních právních úprav. Ačkoliv se Soudní dvůr zatím nevyslovil k maximální přípustné délce uchovávání, stanovil požadavek, aby provozní a komunikační údaje s výjimkou údajů o identitě uživatele zařízení byly uchovávány pouze po dobu nezbytně nutnou.[432]

S požadavkem Soudního dvora na to, aby byly údaje uchovávány po dobu nezbytně nutnou, je třeba naprosto souhlasit. Členské státy by měly mít povinnost detailně zdůvodnit délku uchovávání údajů, a to ideálně pro každou kategorii údajů zvlášť. Ne všechny údaje jsou při delším uchovávání stejně rizikové pro práva jednotlivců, a ne u všech údajů je jejich delší uchovávání ve stejné míře nezbytné pro dosažení sledovaných cílů. Rovnováha mezi rizikem spojeným s uchováváním a užitečností uchovávání by proto měla být hledána a zdůvodňována vzhledem k jednotlivým kategoriím údajů. Mám za to, že právě v době uchovávání údajů leží do budoucna největší prostor pro další „smiřování" přístupu Soudního dvora a členských států. Závěry Soudního dvora o nepřípustnosti plošného uchovávání jiných metadat než IP adres a údajů o totožnosti uživatelů se v současnosti zdají být poměrně kategorické, na druhou stranu se Soudní dvůr doposud vždy zabýval právními úpravami stanovujícími doby uchovávání v řádu měsíců či let pro všechny kategorie údajů společně. Pokud by členské státy byly schopny předložit určité údaje např. na podporu tvrzení, že uchovávání údajů o adresátech sdělení či lokalizačních údajů v průběhu několika týdnů zpravidla neumožňuje činit velmi přesné závěry o životě osob, avšak je extrémně užitečné pro vyšetřování závažné trestné činnosti, mohlo by to vést k dalšímu zmírnění přístupu Soudního dvora. K tomu by mohlo dojít např. již ve věci *SpaceNet* či související věci *Telekom Deutschland*, jejichž předmětem je v tomto ohledu velmi přísná německá právní úprava data retention, která umožňuje uchovávání lokalizačních údajů pouze po dobu tří týdnů a zbylých údajů po dobu deseti týdnů.

[431] Srov. rozsudek *Digital Rights Ireland*, body 63 a 64. Generální advokát ve svém stanovisku v této věci uvedl, že dle jeho názoru nebyly v řízení předloženy přesvědčivé argumenty, jež by odůvodňovaly uchovávání údajů po dobu delší jednoho roku. Srov. stanovisko GA ve věci *Digital Rights Ireland*, bod 149.
[432] Srov. rozsudek *La Quadrature du Net*, bod 147.

Kde a za jakých podmínek mohou být údaje uchovávány?

Co se týče místa uchovávání údajů, Soudní dvůr již ve věci *Digital Rights Ireland* jednoznačně stanovil, že provozní a lokalizační údaje musí být uchovávány na území Unie. Fakt, že směrnice 2006/24 takovou povinnost nestanovila, byl jedním z důvodů pro její zrušení.[433] Stejný požadavek pak dle Soudního dvora platí i vůči vnitrostátním právním úpravám.[434]

Takový požadavek je zcela legitimní, jelikož uchovávání údajů takového rozsahu a citlivosti na území třetího státu by představovalo nejen značné riziko pro práva jednotlivců, ale i pro bezpečnostní zájmy Unie a členských států. Nejde jen o to, že v daném případě nelze účinně dohlížet na dodržování unijních pravidel na ochranu osobních údajů ze strany poskytovatele služeb, ale především o to, že nelze vyloučit, že k těmto údajům budou přistupovat orgány třetích států. Existenci takového rizika ostatně jednoznačně potvrzují již několikrát zmiňovaná odhalení Edwarda Snowdena, následně zohledněná Soudním dvorem ve věcech *Schrems* a *Facebook Ireland a Schrems.*[435]

Pokud jde o zabezpečení uchovávaných údajů, Soudní dvůr vyžaduje, aby právní úprava data retention stanovila povinnost poskytovatelů služeb zavést technická a organizační opatření zajišťující mimořádně vysokou úroveň ochrany.[436] Přestože Soudní dvůr v této souvislosti opět neposkytuje konkrétnější vodítka, lze si představit, že se musí jednat o maximální úroveň zabezpečení vůči neoprávněnému přístupu – jak z vně, tak z vnitřku organizace. Ostatně, přísné a oproti směrnici 95/46 konkrétnější požadavky na zabezpečení údajů vyplývají i z GDPR, dle kterého musí úroveň zabezpečení odpovídat mj. riziku zpracování (které je v případě uchovávání provozních a lokalizačních údajů vysoké) a možnostem správce (které jsou v případě poskytovatelů služeb elektronických komunikací také zpravidla vysoké).[437] S tímto přístupem Soudního dvora opět nelze polemizovat. Jak již bylo uvedeno, základním rizikem spojeným s data retention je riziko neoprávněného přístupu k údajům. Je naprosto logické, že bude od členských států očekáváno, aby toto riziko v co největší možné míře snížily. Toho lze docílit nejenom důkladným vynucováním povinností vyplývajících z GDPR, ale také stanovením konkrétních požadavků na uchovávání údajů. Může jít např. o pseudonymizaci či šifrování uchovávaných údajů, separátní uchovávání jednotlivých kategorií údajů, vedení *logů*, pravidelné testování zabezpečení apod.

---

[433] Srov. rozsudek *Digital Rights Ireland*, bod 68.
[434] Srov. rozsudek *Tele2 Sverige*, bod 122.
[435] Viz kapitola 2.2.2.8.
[436] Srov. rozsudek *Digital Rights Ireland*, bod 67 a rozsudek *Tele2 Sverige*, bod 122.
[437] Viz kapitola 2.2.2.7.

4.1.3.3 Proporcionalita v rovině přístupu k údajům

Při posuzování proporcionality právní úpravy přístupu k uchovávaným provozním a lokalizačním údajům jsou klíčové následující otázky – kdo, za jakým účelem a za jakých podmínek má mít možnost přístupu k preventivně uchovávaným údajům.

První dvě výše zmíněné otázky spolu samozřejmě úzce souvisí. Dle Soudního dvora data retention představuje zvlášť závažný zásah do základních práv, a proto může být odůvodněna pouze cílem boje proti závažné trestné činnosti.[438] Přístup k takto uchovávaným údajům tak může být povolen pouze tehdy, je-li jeho účelem boj proti závažné trestné činnosti. Z vymezení možných účelů přístupu tak vyplývá, jaké orgány mohou k uchovávaným údajům přistupovat. Budou to právě ty orgány, které dle vnitrostátního práva mají boj proti závažné trestné činnosti na starosti.

Krom boje proti závažné trestné činnosti může být k provozním a lokalizačním údajům přistupováno i za účelem zajišťování národní bezpečnosti, jak nedávno Soudní dvůr potvrdil ve věci *La Quadrature du Net*.[439] S ohledem na závažnost hrozeb v této oblasti i znění čl. 15 odst. 1 směrnice 2002/58 jsou tyto závěry samozřejmě logické, byť je sporné, zda mají otázky přístupu např. zpravodajských služeb vůbec spadat do působnosti unijního práva.[440]

Ve věci *La Quadrature du Net* Soudní dvůr také potvrdil své předchozí závěry z věci *Ministerio Fiscal*, když uvedl, že přístup k údajům o identitě uživatele komunikačního zařízení nepředstavuje zvlášť závažný zásah do práv jednotlivce, a může být tedy umožněn i pro účely potírání jiné než závažné trestné činnosti.[441] Jak již bylo uvedeno výše, Soudní dvůr v tomto ohledu vychází z toho, že „*[b]ez křížové kontroly údajů o komunikaci vedené z uvedených karet SIM a bez lokalizačních údajů nelze z těchto údajů zjistit datum, čas, dobu trvání ani adresáty komunikace uskutečněné prostřednictvím dotčené SIM karty či dotčených SIM karet, ani místo, kde se tato komunikace uskutečnila, či její četnost s určitými osobami v určitém období. Z uvedených údajů tedy nelze vyvodit přesné závěry o soukromí osob, o jejichž údaje se jedná*.“[442] Z těchto závěrů Soudního dvora nebylo zcela jednoznačné, zda Soudní dvůr např. i přístup k lokalizačním údajům v určitém okamžiku (např. k lokalizaci zařízení v okamžiku vraždy) považuje za vyvozování přesných závěrů o životě osob, či zda lze o takovém vyvozování hovořit až ve chvíli, kdy jsou k dispozici údaje za určité období

[438] Srov. rozsudek *Tele2 Sverige*, bod 102.
[439] Srov. rozsudek *La Quadrature du Net*, bod 110.
[440] Viz kapitola 4.1.2.4.
[441] Srov. rozsudek *La Quadrature du Net*, body 152-159.
[442] Srov. rozsudek *Ministerio Fiscal*, bod 60.

umožňující vytvoření určitého profilu jednotlivce. Formulace Soudního dvora hovořící o „*místu, kde se komunikace uskutečnila*“ v jednotném čísle však napovídala, že spíše první možnost je správná, a přístup k jakýmkoliv údajům uchovávaným poskytovateli telekomunikačních služeb odlišným od údajů o identitě uživatele zařízení tak bude možný pouze za účelem boje proti závažné trestné činnosti, resp. boje proti hrozbám v oblasti národní bezpečnosti. To bylo následně potvrzeno ve věci *Prokuratuur*, ve které Soudní dvůr rozhodl, že i v případech, kdy je žádáno o přístup k provozním a lokalizačním údajům shromážděným v průběhu velmi krátkého období (za jeden den), je zásah způsobený takovým přístupem třeba považovat za závažný a může k němu dojít pouze za účelem boje proti závažné trestné činnosti, nikoliv trestné činnosti běžné. Soudní dvůr v tomto ohledu vychází z toho, že i provozní a lokalizační údaje za takto krátké období mohou, alespoň v určitých případech, umožnit vyvozování přesných závěrů o životě osob.[443] Zároveň předtím, než je takový přístup umožněn, nelze zjistit, jak citlivé zpřístupňované údaje v tomto ohledu ve skutečnosti jsou.[444] Tato konstatování Soudního dvora nelze příliš rozporovat – byť v takovém případě zřejmě nelze uvažovat o vytváření komplexního profilu jednotlivce, i provozní a lokalizační údaje vážící se k jediné konverzaci mohou odhalit poměrně citlivé informace o životě osob. Vzhledem k existenci takového rizika by tak neměl být přístup ke komunikačním metadatům odlišným od údajů o totožnosti uživatele možný v případě méně závažných trestných činů či přestupků. Ze skutečnosti, že přístup k takovým údajům představuje kvůli riziku odhalení citlivých skutečností závažný zásah, by však z mého pohledu nemělo být automaticky dovozováno, že samotné uchovávání těchto údajů po velmi krátkou dobu je natolik závažné, že jej nemůže odůvodnit ani boj proti závažné trestné činnosti.[445]

Vzhledem k přístupu Soudního dvora k problematice plošného uchovávání nebude překvapením, že přístup k údajům nemůže mít plošný charakter. Soudní dvůr ve věci *Privacy International* jednoznačně určil, že právní úpravy, které stanoví plošné předávání provozních a lokalizačních údajů příslušným orgánům, jsou v rozporu s požadavky čl. 7, 8 a 11 Listiny, a to i za situace, kdy jsou tyto údaje předávány výhradně zpravodajským službám, tj. kdy k předávání dochází výhradně za účelem zajišťování národní bezpečnosti.[446] Soudní dvůr z tohoto zákazu explicitně nepřipustil žádné výjimky, ani pro případ závažného ohrožení

[443] Srov. rozsudek *Prokuratuur*, body 35-39.
[444] Srov. ibidem, bod 40.
[445] Blíže k této problematice viz kapitoly 4.1.3.2 a 4.3.4.3.
[446] Srov. rozsudek *Privacy International*, body 50 a násl.

národní bezpečnosti. V této souvislosti je pro úplnost třeba dodat, že hromadná automatická analýza komunikačních metadat, kterou v situaci závažného ohrožení národní bezpečnosti Soudní dvůr připustil ve věci *La Quadrature du Net*, byla prováděna na serverech poskytovatelů služeb, nikoliv až po předání údajů příslušným orgánům.[447]

Co se týče kategorií osob, k jejichž údajům může být přistupováno, je samozřejmé, že může být přistupováno k údajům osob, které jsou podezřelé z plánování nebo spáchání závažného trestného činu nebo narušení národní bezpečnosti. Nejasné ale je, jakých dalších osob se tento přístup může týkat. Z věci *Tele2 Sverige* se zdá, že se přístup může týkat také jiných osob, jsou-li dány objektivní skutečnosti, na jejich základě lze mít za to, že tyto údaje mohou v konkrétním případě účinně přispět k boji proti takovým činnostem (např. údaje oběti, osob z jejího okolí apod.). To ovšem podle daného rozsudku platí jenom v případě teroristických činů, nikoliv závažné trestné činnosti obecně.[448] Takový přístup nelze považovat za rozumný, uvědomíme-li si např. důležitost přístupu k údajům oběti únosu. Je však otázkou, zda Soudní dvůr skutečně přístup k údajům „souvisejících osob" zamýšlel takto omezit. Ve věci *La Quadrature du Net* totiž Soudní dvůr v souvislosti s *quick freeze* metodou uvedl, že uchovávání údajů těchto „souvisejících" osob může být nařízeno i v případě jiných než teroristických trestných činů. Možnost nařízení uchovávání údajů „souvisejících" osob za účelem boje proti závažné trestné činnosti obecně by nedávalo smysl, pokud by k nim mohl být umožněn přístup pouze v případě vyšetřování terorismu. Na druhou stranu je zvláštní, že ohledně podmínek přístupu Soudní dvůr opět odkázal na rozsudek *Tele2 Sverige*, který takové omezení obsahuje.[449] Nelze tedy vyloučit, že se tato otázka ještě stane předmětem rozhodovací činnosti Soudního dvora. Osobně ale nevidím důvod, proč by v případech, kdy se údaje jiných osob než podezřelého či pachatele ukážou jako naprosto nezbytné k vyšetřování jakéhokoliv závažného trestného činu, nemohl být přístup k těmto údajům soudem povolen, jsou-li uchovávány.

Co se týče podmínek přístupu, ty Soudní dvůr načrtl již v rozsudku *Digital Rights Ireland*,[450] přičemž doposud nevyvstaly další konkrétní otázky, které by jej nutily jeho závěry změnit či více specifikovat, jelikož následná řízení se s výjimkou případů *Ministerio Fiscal* a *Prokuratuur* soustředila především na problematiku plošného uchovávání. Soudní dvůr

[447] Srov. rozsudek *La Quadrature du Net*, bod 172.
[448] Srov. rozsudek *Tele2 Sverige*, bod 119.
[449] Srov. rozsudek *La Quadrature du Net*, bod 165.
[450] Srov. rozsudek *Digital Rights Ireland*, body 61-62.

každopádně vyžaduje, aby přístup k uchovávaným údajům – s výjimkou naléhavých případů – podléhal schválení soudu či jiného nezávislého orgánu.[451] Soudní dvůr blíže nestanovil, za jakých podmínek může vnitrostátní soud přístup k údajům povolit. Stranou tak zatím zůstává naprosto klíčová otázka, zda má být přístup k údajům umožněn pouze jako *ultima ratio*, tj. za situace, kdy jiné nástroje nemohou vést ke sledovanému cíli (vyšetření trestného činu, odvrácení teroristického útoku). Nicméně vzhledem k tomu, že Soudní dvůr opakovaně poukazuje na to, že k použití data retention má docházet pouze v případech, kdy je to naprosto nezbytné, lze takový požadavek dle mého názoru alespoň dovodit.[452] Soudní dvůr dále požaduje, aby ve chvíli, kdy již nemůže být ohrožen účel zpracování, byly dotčené osoby o přístupu k jejich údajům informovány a měly možnost se obrátit na soud.[453]

Ve věci *Prokuratuur* se Soudní dvůr zabýval kritérii, které by měl nezávislý orgán povolující přístup k údajům splňovat. Dle Soudního dvora je potřeba, aby takový orgán „*měl všechny pravomoci a vykazoval všechny záruky nezbytné pro sladění jednotlivých dotčených zájmů a práv. Pokud jde konkrétně o vyšetřování, takový přezkum vyžaduje, aby tento soud nebo orgán byly schopny zajistit spravedlivou rovnováhu mezi zájmy souvisejícími s potřebami vyšetřování v rámci boje proti trestné činnosti na jedné straně a základními právy na respektování soukromého života a na ochranu osobních údajů osob, jichž se přístup dotýká, na straně druhé.*“[454] Takový orgán musí „*mít postavení, které mu umožňuje jednat při plnění svých povinností objektivně a nestranně, a za tímto účelem musí být zcela mimo dosah jakýchkoli vnějších vlivů*“.[455] Dle Soudního dvora tyto podmínky nebude splňovat státní zastupitelství, které vykonává roli veřejného žalobce a je v následném řízení před soudem jednou ze stran sporu.[456] S tímto pohledem nelze než souhlasit. Z toho, jak Soudní dvůr vymezil podmínky pro nezávislost a nestrannost, vyplývá, že by schvalovacím orgánem mohly být i dozorové úřady. Jelikož však taková role vyžaduje krom znalosti problematiky ochrany osobních údajů také dobrou znalost trestního řízení, bude z mého pohledu zpravidla vhodnější tuto problematiku svěřit trestním soudům, jak ostatně bývá zvykem např. v případě povolování odposlechů.

---

[451] Srov. ibidem, bod 120.
[452] Srov. rozsudek *La Quadrature du Net*, bod 176.
[453] Srov. rozsudek *La Quadrature du Net*, body 190 a násl.
[454] Rozsudek *Prokuratuur*, bod 52.
[455] Ibidem, bod 53.
[456] Ibidem, body 55-57.

Soudní dvůr ve věci *La Quadrature du Net* také rozhodl, že přípustný není pouze jednorázový *ex post* přístup k uchovávaným údajům, ale taktéž zpřístupnění těchto údajů v reálném čase. Ovšem za velmi přísných podmínek, tj. pouze u osob, u nichž je objevena určitá spojitost s teroristickými aktivitami a na základě předchozího svolení soudu, které nelze vynechat ani ve výjimečných situacích.[457] Poté, co již nemůže být ohrožen účel zpracování, musí být dotčené osoby o zpracování jejich údajů informovány. Mám za to, že v tomto ohledu je přístup Soudního dvora extrémně restriktivní, jelikož znemožňuje zpřístupnění údajů v reálném čase například v případě vyšetřování únosů, kde však může být z povahy věci naprosto zásadní.

Soudní dvůr dále ve věci *La Quadrature du Net* rozhodl, že v okamžiku, kdy členský stát čelí „*skutečné a existující či předvídatelné*“ hrozbě pro národní bezpečnost, může na nezbytně nutnou dobu přistoupit taktéž k plošné automatické analýze provozních a lokalizačních údajů za účelem identifikace osob podezřelých z účasti na teroristických trestných činech. V této souvislosti je krom soudního přezkumu existence hrozby vyžadováno, aby kritéria, na základě kterých dochází k takovému posuzování, byla nediskriminační, a aby každý pozitivní výsledek byl následně přezkoumán neautomatickými prostředky. Opět se vyžaduje pozdější oznámení o tom, že v případě určité osoby byl nalezen pozitivní výsledek, především za účelem zajištění soudního přezkumu *ex post.*[458]

Osobně považuji přístup Soudního dvora k automatické analýze provozních a lokalizačních údajů za překvapivý. Právě v možnosti plošné automatické analýzy provozních a lokalizačních údajů spatřuji ta největší rizika spojená se zpracováním komunikačních metadat. Tato rizika jsou neporovnatelně vyšší, než je tomu v případě plošného uchovávání údajů a následného adresného přístupu, tj. data retention v pravém slova smyslu. To, že je oba tyto nástroje možné použít za stejných podmínek (tj. pouze v případě přímého ohrožení národní bezpečnosti) tedy z hlediska přiměřenosti nepovažuji za rozumné řešení. Jinými slovy, mám za to, že Soudní dvůr příliš nadhodnocuje rizika spojená s plošným uchováváním, a naopak nepřiznává dostatečnou důležitost rizikům, jež jsou spojená s automatickou analýzou těchto dat. Z mého pohledu není vhodné stejným způsobem přistupovat k opatření, jež umožňuje automatickou analýzu metadat celé populace, jako k opatření, jež ukládá povinnost tato metadata pouze ukládat za účelem adresného přístupu k nim na základě povolení soudu. Mám

[457] Srov. *La Quadrature du Net*, body 183 a násl.
[458] Srov. ibidem, body 172 a násl.

za to, že hromadné zpracování metadat vzhledem k tomu, jak snadné je tyto údaje třídit a analyzovat, představovat dokonce závažnější zásah do základních práv, než např. hromadné zachytávání obsahu komunikace prostřednictvím klíčových slov.

Soudní dvůr zároveň vyžaduje, aby nad dodržováním pravidel ochrany osobních údajů v souvislosti s data retention vykonávaly dohled nezávislé dozorové úřady. V tomto případě jde o jediný aspekt, který Soudní dvůr dovozuje přímo ze znění čl. 8 odst. 3 Listiny, a tudíž i jediný náznak vymezení svébytného obsahu práva na ochranu osobních údajů.[459] Požadavky Soudního dvora v této oblasti lze považovat za zcela legitimní, avšak musíme si uvědomit, že vyplývají již ze sekundárního práva, tj. GDPR (v případě dohledu nad uchováváním údajů poskytovateli služeb) a směrnice 2016/680 (v případě dohledu nad zpracováním prováděným příslušnými orgány a povinnosti vyrozumět subjekt údajů).

Závěrem lze uvést, že není zcela zřejmé, zda se Soudním dvorem stanovené podmínky přístupu k údajům uplatní pouze v případě údajů uchovávaných povinně na základě uložené povinnosti, či taktéž v případě údajů, které provozovatel služeb uchovává z jiného právního titulu (např. pro účely vyúčtování). Každopádně se nedomnívám, že by Soudní dvůr v takových případech zvolil odlišný přístup. Je sice pravdou, že Soudní dvůr v souvislosti s otázkou přístupu vždy hovoří o přístupu „*k takto uchovávaným údajům*“, tj. údajům uchovávaným na základě zákonné povinnosti. To však bude spíše důsledkem toho, že v případech řešených Soudním dvorem se vždy jednalo o údaje uchovávané na základě plošné povinnosti.[460] Ovšem vzhledem k tomu, že Soudní dvůr vnímá uchovávání a následný přístup jako oddělené zásahy do zásady důvěrnosti sdělení a základních práv vyplývajících z čl. 7, 8 a 11 Listiny, nelze očekávat, že by pro přístup k údajům uchovávaným z jiných důvodů přistupoval jinak.

Závěrem je třeba uvést, že ačkoliv v rámci řízení *Tele2 Sverige* některé členské státy zastávaly názor, že by na dodatečné záruky mělo být nahlíženo jako na spojené nádoby, a tudíž že by nedostatky v jedné oblasti mohly být případně vyváženy v oblasti jiné,[461] Soudní dvůr takový přístup neakceptoval. Vzhledem k tomu, jak klíčový význam tyto záruky mají pro minimalizaci rizika zneužití uchovávaných údajů, mám za to, že jiný přístup ani nepřipadá v úvahu.

---

[459] Srov. rozsudek *Tele2 Sverige*, bod 123.
[460] To platí i pro případ *Ministerio Fiscal*, ve kterém sice otázka uchovávání nebyla řešena v důsledku toho, že předkládající soud se na tuto otázku nedotazoval. I v daném případě však byly požadované údaje uchovávány na základě právní povinnosti. Srov. rozsudek *Ministerio Fiscal*, bod 12.
[461] Srov. stanovisko GA ve věci *Tele2 Sverige*, bod 220.

4.1.4 Účinky rozsudků Soudního dvora

O legitimitě a významnosti cílů sledovaných právními úpravami data retention nemůže být pochyb. Případné zrušení či nepoužití těchto právních úprav pak logicky musí mít na sledování těchto cílů negativní dopady – jak z hlediska možnosti účinně bojovat proti hrozbám do budoucna, tak z hlediska použitelnosti již nashromážděných údajů. Není proto divu, že ve sporech týkajících se data retention opakovaně vyvstaly otázky ohledně možného zachování účinků právních úprav data retention, u nichž byl shledán rozpor s unijním právem.

Obecně platí, že výklad Soudního dvora – a to včetně případů konstatování neplatnosti unijních aktů – má účinky *ex tunc*. To znamená, že Soudní dvůr vykládá pravidla unijního práva tak, jak měla být vykládána a používána již od svého počátku, nikoliv až od doby, kdy Soudní dvůr jejich výklad poskytne.[462] Neplatnost unijních aktů či požadavek na nepoužitelnost vnitrostátních předpisů, u nichž byl shledán rozpor s právem EU, tedy zpravidla platí zpětně. Z této zásady však judikatura v minulosti dovodila několik výjimek.

První, poměrně „běžnou" výjimkou je omezení účinků výkladu Soudního dvora samotným Soudním dvorem. K tomu může dojít v prvé řadě v řízení o přímé žalobě, kdy Soudní dvůr odloží konstatování neplatnosti o určitou dobu, jež považuje za nezbytnou k přijetí nového aktu, který již bude v souladu s právem EU. Soudní dvůr však také může, vyžaduje-li to zásada právní jistoty či jiné významné zájmy, omezit účinky svého výkladu v řízení o předběžné otázce. V minulosti tak Soudní dvůr např. učinil v případech, kdy by výkladem Soudního dvora bylo nepříznivě dotčeno značné množství právních vztahů založených v dobré víře.[463] S ohledem na význam cílů sledovaných právními úpravami data retention jistě nebylo možné vyloučit, že by Soudní dvůr takový přístup aplikoval i v této oblasti.

Ve zcela výjimečných situacích současná judikatura připouští, aby účinky vnitrostátní právní úpravy, jež je shledána v rozporu s právem EU, zachoval taktéž vnitrostátní soud. V tomto ohledu jde o výjimku z obecné zásady, dle které mají vnitrostátní orgány – včetně vnitrostátních soudů – obecně povinnost neaplikovat či zrušit (jsou-li k tomu dle vnitrostátního práva oprávněny) ta ustanovení vnitrostátních právních předpisů, jež jsou shledána v rozporu s unijním právem. Soudní dvůr tuto možnost doposud dovodil pouze v oblasti životního prostředí, resp. v oblasti posuzování vlivů na životní prostředí. Ve věci *Inter-Environnement*

[462] Srov. např. rozsudek Soudního dvora ze dne 24. listopadu 2020, *Openbaar Ministerie*, C-510/19, EU:C:2020:953, bod 73.
[463] Srov. ibidem, bod 74.

Wallonie a Terre wallonne[464] šlo o poměrně ojedinělou situaci, kdy byla u belgické Státní rady (jež měla pravomoc vyhlášku případně zrušit) napadena platnost vyhlášky provádějící směrnici 91/676[465] z důvodu, že při jejím přijímání nebylo provedeno posouzení vlivů na životní prostředí, přestože se jednalo o „plán" či „program" ve smyslu směrnice 2001/42[466]. V daném případě tak porušení v zásadě procesněprávních požadavků unijního práva mělo vést k tomu, že bude zrušena vnitrostátní transpozice jiného předpisu práva EU, což by nutně vedlo ke snížení úrovně ochrany životního prostředí. Soudní dvůr tak akceptoval, aby za této situace vnitrostátní soud účinky vnitrostátní právní úpravy dočasně zachoval na dobu nezbytně nutnou ke zhojení shledané protiprávnosti. Později ve věci *Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen*[467] Soudní dvůr tuto výjimku rozšířil, když předkládajícímu soudu umožnil zachovat účinky vnitrostátního opatření (v daném případě šlo o povolení prodloužení provozu jaderné elektrárny, pro nějž nebylo provedeno posouzení vlivů) za podmínky, že by v opačném případě existovala reálná hrozba přerušení dodávek elektřiny, kterou není možné řešit jiným způsobem. Zdá se tedy, že umožnění zachování účinků vnitrostátním soudem může být odůvodněno dostatečně významnými cíli veřejného zájmu, a neomezuje se tedy na specifické situace, ve kterých je sporný vnitrostátní právní předpis jinak řádným provedením unijního práva. Nelze vyloučit, že by za takto výjimečné mohly být považovány cíle sledované vnitrostátní právní úpravou data retention.

A jak tedy Soudní dvůr k otázce zachování účinků napadených právních předpisů přistoupil v případech týkajících se data retention? Ve věci *Digital Rights Ireland* měl Soudní dvůr možnost upravit časové účinky prohlášení neplatnosti směrnice 2006/24, ať už jejím konstatováním toliko *ex nunc*, či dokonce odložením zrušení směrnice do doby, než bude přijata nová směrnice obsahující soudem požadované záruky. Generální advokát měl v dané věci za to, že je na místě konstatování neplatnosti odložit na přiměřenou dobu nutnou k přijetí nové právní úpravy. Odůvodňoval to nejen důležitostí cílů sledovaných směrnicí, ale taktéž tím, že absenci záruk, v níž sám spatřoval hlavní nedostatek směrnice 2006/24, mnohdy členské státy napravily ve vnitrostátním právu.[468] Soudní dvůr však směrnici 2006/24 zrušil s účinností *ex tunc*.

---

[464] Rozsudek Soudního dvora ze dne 28. února 2012, *Inter-Environnement Wallonie a Terre wallonne*, C-41/11, EU:C:2012:103.
[465] Směrnice Rady ze dne 12. prosince 1991 o ochraně vod před znečištěním dusičnany ze zemědělských zdrojů.
[466] Směrnice Evropského parlamentu a Rady 2001/42/ES ze dne 27. června 2001 o posuzování vlivů některých plánů a programů na životní prostředí.
[467] Rozsudek Soudního dvora ze dne 29. července 2019, *Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622.
[468] Srov. stanovisko GA Villalóna ve věci *Digital Rights Ireland*, body 154-158.

Soudní dvůr se otázkou možného zachování účinků vůbec nezabýval a není tedy zřejmé, proč k odložení účinků zrušení směrnice do přijetí nové právní úpravy nepřistoupil. Možným vysvětlením se zdá být to, že s ohledem na vnímanou závažnost zásahu do základních práv způsobeného data retention Soudní dvůr nepovažoval za vhodné unijního zákonodárce tímto způsobem „popostrčit" k přijetí nové směrnice, a zamýšlel tak nechat větší prostor pro politickou diskuzi, zda je unijní právní úprava data retention vůbec třeba. Je také možné, že Soudní dvůr měl tehdy ještě za to, že právní předpisy přijaté na základě ex čl. 95 SES nemohou regulovat problematiku přístupu k údajům, a tudíž ani nemohou obsahovat záruky, které Soudní dvůr vyžadoval pro soulad směrnice s čl. 7 a 8 Listiny. Za takového předpokladu by jakákoliv unijní úprava data retention byla *a priori* odsouzena ke zrušení – buď pro nedostatečný právní základ, nebo pro rozpor s čl. 7 a 8 Listiny. Každopádně vzhledem k tomu, že následně ve věci *Tele2 Sverige* Soudní dvůr odmítl koncept plošné data retention jako takový, jakákoliv nová unijní právní úprava data retention by stejně dlouho nevydržela, resp. pravděpodobně by vůbec nestačila vstoupit v platnost.

Zrušení směrnice 2006/24 samozřejmě nemohlo mít dopady na platnost vnitrostátních transpozičních předpisů. V právu EU neexistuje pravidlo, ze kterého by vyplývala automatická neplatnost vnitrostátních transpozičních předpisů v případě konstatování neplatnosti příslušné směrnice EU.[469] Z rozsudku ve věci *Digital Rights Ireland* nutně nevyplývala ani neaplikovatelnost těchto předpisů vnitrostátními soudy či povinnost jejich zrušení či úpravy vnitrostátním zákonodárcem. Soudní dvůr ve věci *Digital Rights Ireland* neodmítl koncept data retention jako takový, ale koncept data retention bez dostatečných dodatečných záruk v rovině uchovávání a přístupu. Ostatně, přijetí data retention výslovně nadále umožňoval i čl. 15 odst. 1 směrnice 2002/58, byť tehdy ještě nebylo jasné, jaká byla povaha (*power-recognising* či *power-granting*) a rozsah (pouze uchovávání, či uchovávání i přístup) tohoto ustanovení.[470] Vnitrostátní právní úpravy data retention obsahující příslušné záruky tudíž nemusely být rozhodnutím Soudního dvora v praxi vůbec zasaženy. Tím, že tyto právní úpravy ztratily povahu transpozičních předpisů,[471] se navíc rozšířil manévrovací prostor členských států, které mohly nově např. stanovit kratší dobu uchovávání než směrnicí požadovaných šest měsíců, a tím např. vyhovět přísnějším požadavkům vnitrostátních ústavních soudů.

---

[469] Srov. KRÁL, Richard. Neplatnost směrnic EU a její důsledky pro vnitrostátní transpoziční předpisy. *Jurisprudence*, 2011.
[470] Viz kapitola 4.1.2.4.
[471] Srov. KRÁL, Richard. Neplatnost směrnic EU a její důsledky pro vnitrostátní transpoziční předpisy. *Jurisprudence*, 2011.

Otázkou omezení časových účinků svého rozhodnutí se Soudní dvůr nezabýval ani ve věci *Tele2 Sverige*, zřejmě z toho důvodu, že se na tuto problematiku předkládající soudy nedotazovaly. Ve věci *La Quadrature du Net* se Soudní dvůr zabýval možností zachování účinků vnitrostátní právní úpravy předkládajícím soudem, a to na výslovný dotaz belgické Státní rady. Generální advokát měl za to, že takové zachování účinků je možné. Vycházel jednak z toho, že pokud je takové omezení možné z důvodů ohrožení bezpečnosti v souvislosti s přerušením dodávek elektřiny, je možné i v souvislosti s data retention. Zároveň poukázal na to, že v daném případě nebylo snadné dosáhnout souladu vnitrostátní právní úpravy s rozsudkem *Tele2 Sverige*, a také, že sporná vnitrostátní právní úprava naopak odrážela závěry Soudního dvora ve věci *Digital Rights Ireland*.[472] Soudní dvůr se však s přístupem generálního advokáta neztotožnil. Soudní dvůr uvedl, že se dotčená věc svou povahou lišila od procesních porušení v oblasti životního prostředí, které byly předmětem věcí *Inter-Environnement Wallonie a Terre wallonne* a *Inter-Environnement Wallonie a Bond Beter Leefmilieu Vlaanderen*. Umožnění použití vnitrostátní právní úpravy data retention, která je v rozporu s unijním právem, by znamenalo umožnit členským státům nadále poskytovatelům služeb ukládat povinnosti, jež jsou v rozporu s právem EU, a tudíž nadále v rozporu s unijním právem zasahovat do práv subjektů údajů, což je nepřípustné.[473]

Soudní dvůr nicméně konstatoval, že otázka použitelnosti důkazů získaných na základě dotčených vnitrostátních právních předpisů spadá při dodržení zásady efektivity do působnosti vnitrostátního práva. Co se týče zásady efektivity, Soudní dvůr ze své předchozí judikatury dovodil, že právo na spravedlivý proces vyžaduje, aby nebyly akceptovány důkazy, které budou mít pravděpodobně zásadní vliv na skutková zjištění a ke kterým se dotčená osoba nemohla vyjádřit.[474]

Se striktním přístupem k možnosti zachování účinků nesouladné vnitrostátní právní úpravy ze strany předkládajícího soudu souhlasím. Nemá-li být ohrožen užitečný účinek rozhodnutí Soudního dvora, měla by tato možnost být skutečně omezena na ojedinělé případy, ideálně ty, kde sice došlo k porušení určitých procesních pravidel, avšak s ohledem na okolnosti lze předpokládat, že konečný stav je s unijním právem v souladu. Ovšem pokud Soudní dvůr dovodil, že ani boj proti závažné trestné činnosti či hrozbám v oblasti národní bezpečnosti

[472] Srov. stanovisko GA Campos Sánchez-Bordony ve věci *Ordre des barreaux francophones a germanophone*, body 144-154.
[473] Srov. rozsudek *La Quadrature du Net*, body 213-220.
[474] Srov. ibidem, body 221-228.

nemůže odůvodnit plošné uchovávání provozních a lokalizačních údajů, nedává smysl, aby z týchž důvodů toto uchovávání dočasně umožnil předkládající soud. Na druhou stranu je rozumné, že rozhodnutí Soudního dvora automaticky nezpůsobí nepoužitelnost provozních a lokalizačních údajů jakožto důkazů v soudních řízeních s výjimkou případů, kdy tak stanoví vnitrostátní právo či kdy by mělo dojít k porušení práva na spravedlivý proces.

4.1.5 Závěr

V judikatuře Soudního dvora týkající se data retention lze identifikovat tři klíčové právní otázky – otázku působnosti dotčených unijních předpisů, otázku přípustnosti plošného uchovávání údajů a otázku nezbytných dodatečných záruk v oblasti uchovávání a přístupu k údajům.

Co se týče problematiky působnosti unijních předpisů v této oblasti, byla v prvé řadě kritizována nekonzistentnost judikatury Soudního dvora. Ten totiž ve věci *Parlament v. Komise a Rada* týkající se problematiky PNR nejprve dospěl k závěru, že dotčená problematika spadá mimo působnost aktů přijatých na základě čl. 95 SES, jelikož výhradním účelem předání údajů je boj proti terorismu a závažné trestné činnosti. Stejnou optiku však následně neaplikoval ve věci *Tele2 Sverige*, ve které dospěl k závěru, že problematika data retention do působnosti předpisů přijatých na základě čl. 95 SES spadá. Soudní dvůr také nejprve posvětil právní základ směrnice 2006/24 s poukazem na to, že dotčená směrnice neupravuje otázky přístupu příslušných orgánů k uchovávaným údajům, aby následně ze stejných důvodů směrnici zrušil pro její neslučitelnost s čl. 7 a 8 Listiny.

Krom výše uvedené nekonzistentnosti byl kritizován i Soudním dvorem zastávaný extenzivní výklad působnosti směrnice 2002/58 jako takový, který nemá oporu v jejím znění ani v jejím právním základě. V tomto ohledu je nejvíce problematické, že Soudní dvůr z hlediska působnosti unijních předpisů nijak nerozlišuje mezi oblastí boje proti závažné trestné činnosti a oblastí zajišťování národní bezpečnosti, která je dle čl. 4 odst. 2 SEU výlučně záležitostí členských států. Z Radou navrhovaného znění ePrivacy nařízení je nicméně zřejmé, že členské státy ingerenci unijního práva do oblasti národní bezpečnosti nehodlají přijmout „bez boje“. Nelze ani vyloučit, že se členské státy budou působnosti unijních předpisů snažit vyhnout tak, že zakotví široké pravomoci příslušných orgánů získávat komunikační metadata bez zapojení poskytovatelů služeb, což může v konečném důsledku vést ke snížení úrovně ochrany základních práv na soukromí a ochranu osobních údajů napříč členskými státy. V neposlední řadě reálně připadá v úvahu i situace, kdy některý z vrcholných soudů členských států dospěje k závěru, že je přístup Soudního dvora k této problematice třeba považovat za jednání *ultra vires.*

Co se týče problematiky posuzování přiměřenosti data retention, bylo v prvé řadě kritizováno, že ačkoliv Soudní dvůr považuje data retention za zásah do základních práv stanovených v čl. 7, 8 a 11 Listiny, mezi jednotlivými právy významněji nerozlišuje, což je problematické především z hlediska potřeby bližšího vymezení práva na ochranu osobních údajů. Zároveň bylo kritizováno chápání data retention jako „výjimky zpravidla" důvěrnosti sdělení ve smyslu čl. 5 odst. 1 směrnice 2002/58, jelikož ze znění ani odůvodnění této směrnice nevyplývá, že by k zákonnému uchovávání údajů mělo docházet pouze výjimečně.

Výše zmíněné nedostatky ve vymezení obsahu práva na ochranu osobních údajů však Soudnímu dvoru nezabránily, aby i v souvislosti s data retention poskytoval velmi vysokou úroveň ochrany subjektům údajů, a to ve vztahu k legislativní činnosti unijního zákonodárce i členských států. Ve vztahu k unijnímu zákonodárci se to projevilo mj. tím, že Soudní dvůr unijnímu zákonodárci nepřiznal pro jiné oblasti typický široký prostor pro uvážení, ani nepřipustil, aby nedostatky unijní úpravy mohly být kompenzovány zárukami zavedenými členskými státy. Ve vztahu k členským státům vyvrcholil přísný přístup Soudního dvora ve věci *Tele2 Sverige*, kdy Soudní dvůr dospěl k závěru, že vnitrostátní právní předpisy stanovující plošné uchovávání údajů jsou *samy o sobě* neslučitelné s Listinou, bez ohledu na dodatečné záruky. Takto striktní přístup nicméně nebylo možné považovat za dosažení rozumné rovnováhy mezi základními právy a bezpečnostními zájmy členských států, a je proto jedině dobře, že byl tento přístup následně modifikován, alespoň co se týče některých kategorií údajů a v případech, kdy členský stát čelí aktuální hrozbě pro svou národní bezpečnost.

Ačkoliv umožnění výjimek ze striktního zákazu plošného uchovávání ve věci *La Quadrature du Net* je bezesporu krok správným směrem, mám za to, že judikatura Soudního dvora nadále nepředstavuje nalezení spravedlivé rovnováhy mezi právy na soukromí a ochranu osobních údajů a bezpečnostními zájmy členských států.

Zaprvé, tento přístup Soudního dvora z mého pohledu nadále dostatečně neodlišuje zásah způsobený samotným uchováváním od zásahu způsobeného přístupem k údajům, resp. dokonce jejich automatickou analýzou. To lze dobře demonstrovat právě tím, že stanovuje *de facto* stejné podmínky pro plošné uchovávání údajů jako pro jejich plošnou automatizovanou analýzu. Právě v možnosti plošné automatické analýzy provozních a lokalizačních údajů osobně spatřuji ta největší rizika spojená se zpracováním komunikačních metadat. Tato rizika jsou neporovnatelně vyšší, než je tomu v případě typických právních úprav data retention spočívajících v plošném uchovávání údajů a adresném přístupu k nim, navíc při stanovení přísných záruk v rovině přístupu. To, že je oba tyto nástroje možné použít za stejných podmínek

(tj. pouze v případě aktuálního či předvídatelného závažného ohrožení národní bezpečnosti), tedy z hlediska přiměřenosti nepovažuji za rozumné řešení. Z mého pohledu není vhodné stejným způsobem přistupovat k opatření, jež umožňuje automatickou analýzu metadat celé populace za účelem hledání potenciálních pachatelů, jako k opatření, jež ukládá povinnost tato metadata pouze ukládat za účelem individuálního přístupu k nim na základě předchozího povolení soudu, ukáže-li se takový přístup jako nezbytný v konkrétním případě.

Zadruhé, přístup Soudního dvora dostatečným způsobem nezohledňuje, že dodatečné záruky v oblasti uchovávání a přístupu mohou rizika spojená se samotným uchováváním značně minimalizovat. Zejména v případech, kdy budou doby uchovávání nastaveny tak, aby byla v maximální míře omezena možnost vytváření ucelených profilů a bude trváno na dodržení všech dodatečných záruk (skutečně maximální zabezpečení údajů, přístup pouze v nezbytných případech, přístup pouze za účelem boje proti závažné trestné činnosti a hrozbám v oblasti národní bezpečnosti, předchozí přezkum soudem, následný přezkum soudem, průběžný dohled dozorových orgánů), dojde z mého pohledu k významnému snížení zásahu do základních práv spojeného se samotným uchováváním, a tudíž i souvisejícího rizika *chilling effect.* Nelze také zapomínat, že riziko zneužití je přítomné i u ostatních nástrojů, které mají orgány státu v tomto ohledu k dispozici, a že možnost přístupu ke komunikačním metadatům může někdy vést k tomu, že nebude třeba nasadit prostředky, které nakonec povedou k většímu zásahu do základních práv.

Zatřetí, je otázkou, do jaké míry je samo plošné uchovávání údajů v praxi schopno vyvolávat v širší populaci významnější *chilling effect*, vezmeme-li v potaz masivní zpracování (nejen uchovávání) rozmanitých kategorií osobních údajů (nejen metadat), které dnes běžně provádějí soukromé subjekty (provozovatelé vyhledávačů, sociálních sítí apod.) za komerčními účely (jejichž váha je ve srovnání s cíli sledovanými data retention bezesporu nižší). Samozřejmě lze namítat, že v případě těchto komerčních zpracování má subjekt zpravidla volbu, zda s takovým zpracováním udělí souhlas. O tom, do jaké míry se však jedná o skutečnou možnost volby, by bylo nicméně možné polemizovat.[475] To, že jsou metadata ve značném rozsahu uchovávána i pro vlastní komerční účely samotných poskytovatelů telekomunikačních služeb, pak dokládají statistiky z mnoha členských států. Zdá se tedy, že „dodatečný" zásah do základních práv způsobený data retention se jen velmi málo liší od rozsahu zásahu

[475] Ke skutečné roli souhlasu se zpracováním údajů v dnešním kontextu viz např. MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*, 2014, roč. 5, č. 9, s. 3-74.

do základních práv způsobeným uchováváním údajů pro komerční účely. Tento dodatečný zásah má však vysokou přidanou hodnotu, jelikož vylučuje, aby se úspěšnost vyšetřování trestného činu či odvrácení hrozby pro národní bezpečnost odvíjela *de facto* od náhody, zda údaje nezbytné pro vyšetřování nebudou právě v tom malém procentu údajů, které se poskytovatel služeb rozhodl neuchovávat pro vlastní potřebu.

Přestože tedy umožnění výjimek ze striktního zákazu plošného uchovávání představuje krok správným směrem, mám za to, že tento zákaz měl být spíše zcela opuštěn ve prospěch tzv. omezené data retention, tj. řešení, které sice umožňuje plošné uchovávání komunikačních metadat, ovšem pouze po velmi krátkou dobu a za dodržení přísných dodatečných záruk v oblasti uchovávání i přístupu k údajům. Je však otázkou, zda Soudní dvůr bude v budoucnu ochoten přistoupit k dalšímu zmírnění svého striktního přístupu. Případy *SpaceNet* a *Telekom Deutschland*, v nichž je posuzována poměrně přísná německá úprava data retention, budou v tomto ohledu zásadní.

4.2 EVROPSKÝ SOUD PRO LIDSKÁ PRÁVA

4.2.1 Přehled

Pohled ESLP na data retention není tak jednoznačný, jak je tomu v případě pohledu Soudního dvora. Je tomu tak z důvodu, že ESLP zatím neměl možnost vyslovit se k „typickému" data retention případu, ve kterém by byla sporná otázka plošného uchovávání komunikačních metadat a adresný přístup státních orgánů k nim. Pro bližší pochopení přístupu ESLP k problematice data retention je tak na místě zkoumat jeho judikaturu týkající se ostatních režimů skrytého sledování komunikace, z níž je pak možné závěry ESLP extrapolovat i na problematiku data retention.[476] Právě to bude předmětem následujících kapitol.

Prvním případem z této oblasti, v němž ESLP stanovil základní podmínky pro přístup státních orgánů k obsahu komunikace, byl případ *Klass a další proti Německu* z roku 1978. Případ se týkal německé úpravy telefonních odposlechů a ESLP se v něm vyjádřil např. k otázce dotčených práv, otázce prokazování existence zásahu do těchto práv, otázce předvídatelnosti zásahu, otázce soudního přezkumu apod. Ačkoliv si specifické skutkové okolnosti následujících případů vyžádaly upřesnění či doplnění závěrů ESLP vyslovených v této věci,

[476] Níže zkoumané rozsudky představují výběr rozsudků, u nichž je potenciál pro takovou extrapolaci nejvyšší – ať už s ohledem na jejich význam či s ohledem na blízkost zkoumané problematiky problematice data retention. Nejedná se nicméně o úplný výčet veškeré judikatury ESLP týkající se skrytého sledování, která zahrnuje podstatně větší množství rozsudků. Pro některé další významnější případy srov. např. European Court of Human Rights. *Guide on Article 8 of the Convention – Right to respect for private and family life*, 2020, s. 49 a násl. či European Court of Human Rights. *Mass Surveillance Factsheet*, 2020.

základní podmínky pro zásah do práva na soukromý život stanovené v dotčeném rozsudku zůstaly platné dodnes.

Dalším zajímavým případem pro účely této práce je případ *Malone proti Spojenému království*[477] z roku 1984, ve kterém se ESLP zabýval problematikou přístupu státních orgánů k výpisům telefonních hovorů. ESLP dospěl k závěru, že nejen přístup k obsahu komunikace, ale i přístup ke komunikačním metadatům je třeba považovat za zásah do práva na soukromý život. Některé dříve stanovené podmínky pro přístup k obsahu komunikace proto vztáhl i na údaje o volaných číslech či trvání telefonních hovorů.

Německá právní úprava skrytého sledování komunikace byla předmětem sporu i ve věci *Weber a Saravia proti Německu*[478] z roku 2006. V důsledku technologického vývoje posledních let se v ní musel ESLP vyjádřit k novému fenoménu tzv. „*strategického sledování*", spočívajícího ve zpracovávání velkého množství údajů osob, u nichž doposud neexistuje spojitost s konkrétní hrozbou, a to právě za účelem nalezení takové spojitosti.[479] ESLP v obecné rovině akceptoval takový druh sledování, za podmínky, že je doprovázen přísnými zárukami proti zneužití.

Případ *S a Marper proti Spojenému království* z roku 2009 se od výše uvedených případů odlišuje, jelikož se netýkal otázky přístupu státních orgánů k obsahu komunikace či komunikačním metadatům, nýbrž problematiky uchovávání DNA profilů osob, jež byly zadrženy pro spáchání trestného činu, avšak nakonec osvobozeny. ESLP v tomto případě dospěl k závěru, že již pouhé uchování osobních údajů ze strany státních orgánů představuje zásah do práva na soukromý život. Tyto závěry ESLP následně převzal Soudní dvůr ve věci *Digital Rights Ireland*, když je aplikoval právě na problematiku data retention.

Jak bylo uvedeno v úvodu této práce, první desetiletí 21. století bylo v důsledku nástupu nových bezpečnostních hrozeb a nových technologií zaměřených na jejich potírání pro řadu států charakteristické přijímáním nových právních úprav umožňujících nasazení těchto technologií. V rámci posuzování těchto právních úprav pak dostal ESLP prostor nejen pro konsolidaci svojí předchozí judikatury, ale také pro její přizpůsobení novému bezpečnostnímu a technologickému kontextu. Mezi klíčové případy z této doby patří *Zakharov*

---

[477] Rozsudek ESLP ze dne 2. srpna 1984, *Malone proti Spojenému království*, stížnost č. 8691/79, CE:ECHR:1984:0802JUD000869179 (dále jen „*rozsudek Malone proti Spojenému království*").
[478] Rozhodnutí ESLP ze dne 29. června 2006, *Weber a Saravia proti Německu*, stížnost č. 54934/00, CE:ECHR:2006:0629DEC005493400 (dále jen „*rozhodnutí Weber a Saravia proti Německu*").
[479] V této souvislosti lze jen připomenout, že právě neexistence spojitosti s konkrétní hrozbou je jedním z hlavních argumentů Soudního dvora pro shledání nepřiměřenosti plošné data retention.

proti Rusku[480] z roku 2015, *Szabó a Vissy proti Maďarsku*[481] z roku 2016*, Center for Rattvisa proti Švédsku* a *Big Brother Watch proti Spojenému království* z roku 2018. Pro účely této práce jsou zajímavé především dva posledně zmíněné rozsudky. Nejen proto, že se v nich ESLP opět zabýval problematikou strategického sledování, ale především z důvodu, že tomu tak bylo již ve světle restriktivní judikatury Soudního dvora k problematice data retention. Pro oba tyto rozsudky je charakteristické, že ESLP přijal poměrně shovívavý přístup k problematice hromadného sledování, který se značně odlišuje od přístupu Soudního dvora k problematice data retention. Nutno však uvést, že oba tyto rozsudky jsou v současnosti předmětem přezkumu ze strany Velkého senátu ESLP, a některé v nich obsažené závěry tak ještě mohou být přehodnoceny.

V roce 2020 se pak ESLP zabýval několika případy (*Ringler proti Rakousku*[482], *Tretter a další proti Rakousku*[483]) týkajícími se přímo problematiky přístupu státních orgánů ke komunikačním metadatům, ovšem s tím rozdílem, že tyto údaje nebyly uchovávány na základě plošně uložené povinnosti. Stížnosti v těchto věcech však byly odmítnuty z důvodu, že nebyly shledány podmínky judikatury ESLP pro provedení přezkumu *in abstracto.* Plošné povinnosti uchovávání komunikačních metadat se naopak týkal případ *Breyer proti Německu*[484], který byl však specifický tím, že se nejednalo o širší okruh komunikačních metadat, ale pouze o údaje o totožnosti uživatelů, konkrétně jména a adresy majitelů SIM karet. ESLP v této věci dospěl k závěru, že k porušení čl. 8 Úmluvy nedošlo.

V neposlední řadě budou v následujících kapitolách zohledněny závěry ESLP ve věci *K.U. proti Finsku*[485] z roku 2009, jež se od výše uvedených věcí odlišuje tím, že v ní ESLP shledal, že Finsko nedostálo svým povinnostem chránit právo na soukromý život oběti trestného činu spáchaného na internetu, a to z důvodu, že finské právo tehdy neobsahovalo nástroj, který by umožňoval zjistit identitu pachatele. Pro účely této práce je tento případ zajímavý především tím, že členské státy i předkládající soudy před Soudním dvorem často poukazují na to, že data

---

[480] Rozsudek ESLP ze dne 4. prosince 2015, *Zakharov proti Rusku*, stížnost č. 47143/06, CE:ECHR:2015:1204JUD004714306 (dále jen „*rozsudek Zakharov proti Rusku*“).
[481] Rozsudek ESLP ze dne 12. ledna 2016, *Szabó a Vissy proti Maďarsku*, stížnost č. 37138/14, CE:ECHR:2016:0112JUD003713814 (dále jen „*rozsudek Szabó a Vissy proti Maďarsku*“).
[482] Rozhodnutí ESLP ze dne 12. května 2020, *Ringler proti Rakousku*, stížnost č. 2309/10, CE:ECHR:2020:0512DEC000230910 (dále jen „*rozhodnutí Ringler proti Rakousku*“).
[483] Rozhodnutí ESLP ze dne 29. září 2020, *Tretter a další proti Rakousku*, stížnost č. 3599/10, CE:ECHR:2020:0929DEC000359910 (dále jen „*rozhodnutí Tretter proti Rakousku*“)
[484] Rozsudek ESLP ze dne 30. ledna 2020, *Breyer proti Německu*, stížnost č. 50001/12, CE:ECHR:2020:0130JUD005000112 (dále jen „*rozsudek Breyer proti Německu*“).
[485] Rozsudek ESLP ze dne 2. prosince 2008, *K.U. proti Finsku*, stížnost č. 2872/02, CE:ECHR:2008:1202JUD000287202 (dále jen „*rozsudek K.U. proti Finsku*“) .

retention nelze vnímat jako pouhý zásah do základních práv, ale taktéž jako nástroj, kterým členské státy naplňují povinnost lidská práva chránit, mj. právě s ohledem na požadavky vznesené ESLP ve věci *K.U. proti Finsku.*

Z výše uvedeného vyplývá, že se judikatura ESLP doposud věnovala velmi široké škále metod sledování komunikace ze strany orgánů států. Byly řešeny otázky přístupu k obsahu komunikace či ke komunikačním metadatům, problematika plošného i cíleného sledování, problematika sledování za účelem potírání trestné činnosti či sledování za účelem potírání hrozeb v oblasti národní bezpečnosti apod. Sám ESLP v této souvislosti uvádí, že ačkoliv každá forma sledování vyžaduje určitý specifický přístup, existují základní zásady, které je možné extrapolovat a aplikovat v případě jakékoliv formy sledování.[486] Tyto základní zásady budou identifikovány a rozebrány níže. Následně bude popsán a analyzován přístup ESLP přímo k problematice data retention, a to jak ve světle těchto obecných zásad, tak ve světle rozsudků, ve kterých se ESLP k určitým aspektům data retention již konkrétně vyslovil.

4.2.2 Skryté sledování komunikace ze strany státních orgánů

Aby byl jakýkoliv zásah do chráněných práv shledán v souladu s Úmluvou, musí být stanoven zákonem, sledovat legitimní cíl a být nezbytný v demokratické společnosti. To samozřejmě platí i pro zásahy způsobené skrytým sledováním ze strany orgánů státu.[487]

4.2.2.1 Existence zásahu do práv chráněných Úmluvou

V prvním kroku je třeba zabývat se vůbec existencí zásahu do práv chráněných Úmluvou v daném konkrétním případě. Z čl. 34 Úmluvy a související ustálené judikatury ESLP vyplývá, že systém Úmluvy neumožňuje podávání *actio popularis*. Ochrany u ESLP se tak mohou dovolávat pouze „oběti" porušení práv přiznaných Úmluvou a Protokoly k ní. Tento v jiných oblastech nijak kontroverzní požadavek se však stává poněkud problematický v případě skrytého sledování státními orgány. Oběti takového skrytého sledování totiž ve většině případů nemusí ani tušit, že bylo do jejich práv zasaženo. Navíc, i pokud se domnívají, že k takovému zásahu došlo, často nebudou mít možnost takový zásah prokázat. ESLP se tak již od prvních případů v této oblasti musel vypořádávat se stížnostmi namířenými vůči právní úpravě umožňující skryté sledování, aniž by však stěžovatelé byli schopni prokázat, že tato opatření byla použita proti nim samotným. Přístup ESLP k této problematice se nicméně v jednotlivých případech odlišoval – zatímco někde byla existence legislativy umožňující skryté sledování

[486] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 303.
[487] Srov. ibidem, body 304 a násl.

shledána sama o sobě dostatečná k tomu, aby byl stěžovatel považován za oběť,[488] v jiných případech bylo vyžadováno prokázání dalších skutečností, které činily nasazení takových opatření vůči stěžovatelům pravděpodobnější oproti zbytku populace – např. kvůli jejich povolání či občanské angažovanosti.[489]

Ve věci *Zakharov proti Rusku* se proto ESLP rozhodl svůj přístup k otázce prokazování statusu oběti sjednotit. Dle sjednoceného přístupu je v prvé řadě třeba zkoumat, zda je stěžovatel osobou, vůči které mohou být v teoretické rovině taková opatření použita. Nejčastěji budou příslušné vnitrostátní právní úpravy formulovány obecně, umožňující použití příslušných opatření v zásadě proti jakémukoliv členu veřejnosti za splnění určitých podmínek (např. podezření z trestného činu), a první krok tak bude automaticky splněn. Lze si však představit i specifické případy, kdy budou opatření namířena např. pouze na komunikaci v zahraničí, čímž se omezí i okruh potenciálních obětí těchto opatření. Klíčový je však druhý krok testu, dle kterého je dále třeba zkoumat, zda příslušná vnitrostátní právní úprava obsahuje účinné nástroje kontroly, které mohou osoby, jež se domnívají, že se staly předmětem skrytého sledování, využít. Pokud vnitrostátní právní úprava bude obsahovat účinné nástroje k ověření, zda ke skrytému sledování došlo a zda takové sledování bylo v souladu se zákonem, ESLP shledá stížnost formulovanou *in abstracto* nepřípustnou. To však neplatí v případech, kdy stěžovatel vykazuje výše zmíněné zvláštní charakteristiky, které činí jeho sledování ze strany státních orgánů pravděpodobnější – v takových případech je ESLP ochoten shledat stížnosti formulované *in abstracto* přípustné i přesto, že vnitrostátní právní úprava obsahuje účinné nástroje kontroly.[490]

Co se dále týče otázky, do jakých práv chráněných Úmluvou bylo zasaženo, pro všechny formy skrytého sledování komunikace bude v zásadě společné, že budou představovat zásah do práv chráněných čl. 8 Úmluvy, konkrétně práva na soukromý život a nedotknutelnost korespondence,[491] případně nedotknutelnost domova.[492] V případě skrytého sledování

[488] Srov. rozsudek *Klass a další proti Německu*, body 30-38.
[489] Srov. rozsudek ESLP ze dne 22. května 2008, *Stefanov proti Bulharsku*, stížnost č. 65755/01, CE:ECHR:2008:0522JUD006575501, body 48-52 a rozsudek ESLP ze dne 10. února 2009, *Iordachii a další proti Moldavsku*, stížnost č. 25198/02, CE:ECHR:2009:0210JUD002519802, body 29-35.
[490] Srov. rozsudek *Zakharov proti Rusku*, body 171 a násl. či rozsudek *Centrum för Rättvisa proti Švédsku*, body 90-95.
[491] Srov. rozsudek *Klass a další proti Německu*, bod 41.
[492] Srov. ibidem.

komunikace ESLP také často hovoří konkrétněji o zásahu do práva na informační sebeurčení vyplývajícího z čl. 8 Úmluvy.[493]

Skryté sledování ze strany orgánů státu bude mít navíc z povahy věci povahu zpracování osobních údajů ve smyslu Úmluvy 108. V takových případech vykládá ESLP pojem soukromý život právě s ohledem na široké vymezení pojmů osobní údaj a zpracování v Úmluvě.[494] Tyto pojmy jsou přitom vymezené v podstatě stejně jako v unijní legislativě. Tím se obsah práva na soukromý život do jisté míry sbližuje s obsahem čl. 8 Listiny zakotvujícím svébytné právo na ochranu osobních údajů, jelikož také Soudní dvůr zásah do tohoto práva shledává v zásadě ve všech případech zpracování osobních údajů. Mírnou odlišností je, že ESLP bude za zásah do soukromého života v zásadě považovat pouze takové zpracování osobních údajů, které jde mírou či povahou nad rámec toho, co lze běžně očekávat.[495]

ESLP stejně jako Soudní dvůr uznává, že skryté sledování komunikace může představovat zásah do svobody projevu uživatelů elektronické komunikace garantované čl. 10 Úmluvy. V praxi však v těchto případech ESLP, alespoň tedy co se týče přezkumu *in abstracto*, nahlíží na svobodu projevu spíše jako na svobodu tisku (resp. svobodu médií). Svůj přezkum slučitelnosti opatření skrytého sledování s čl. 10 Úmluvy tak zaměřuje téměř výhradně na otázku ochrany novinářských zdrojů. To platí jak v rovině posuzování existence zásahu, tak v rovině posuzování jeho závažnosti. Ve věci *Weber a Saravia proti Německu* tak např. ESLP dospěl k závěru, že ačkoliv byly stěžovatelé novináři, nebyla sporná opatření zaměřena na odhalování jejich zdrojů, a zásah do svobody projevu ve smyslu čl. 10 Úmluvy tak nelze považovat za závažný.[496] To, že z hlediska přezkumu existuje rozdíl mezi skrytým sledováním komunikace novináře za účelem odhalit jeho zdroje, a sledováním za jiným účelem, např. vyšetřování trestného činu spáchaného bez souvislosti s novinářskou činností, potvrzuje i navazující judikatura.[497]

Ve věci *Breyer proti Německu* se pak ESLP odmítl zabývat možným porušením čl. 10 Úmluvy nikoliv z důvodu, že stěžovatel nebyl novinář, nýbrž z důvodu, že stěžovatel napadal pouze povinnost uchovávání údajů o uživatelích, aniž by tvrdil, že v jeho případě došlo k přístupu státních orgánů ke komunikaci. ESLP dospěl k závěru, že v takovém případě je třeba stížnost zkoumat pouze optikou práva na soukromý život, nikoliv optikou nedotknutelnosti

[493] Srov. rozsudek *Breyer proti Německu*, bod 75.
[494] Srov. ibidem, bod 74.
[495] Srov. ibidem, bod 75.
[496] Srov. rozhodnutí *Weber a Saravia proti Německu*, body 145 a 151.
[497] Srov. rozsudek *Big Brother Watch proti Spojenému království*, body 487-489.

korespondence či právě svobody projevu.[498] To je poměrně zvláštní přístup, pokud si uvědomíme, že v řadě případů budou údaje o uživatelích užitečné právě k identifikaci autora určitého sdělení. Samotná povinnost uchovávání tak spolu s možností pozdějšího přístupu k údajům má přitom jistě potenciál vést k *chilling effect*, jehož existenci ESLP jinak zohledňuje.[499]

Přístup ESLP ke svobodě projevu se může zdát jako příliš restriktivní, neberoucí v potaz, že riziko skrytého sledování může ovlivnit svobodu projevu i běžné populace. Na druhou stranu, v případě osob z běžné populace si lze jen obtížně představit kritéria přezkumu v režimu čl. 10 Úmluvy, které by se zásadněji odlišovala od kritérií přezkumu v režimu čl. 8 Úmluvy. Za takové situace by byl přínos zvláštního přezkumu v režimu čl. 10 Úmluvy bez větších praktických dopadů na výsledek sporu. Naopak zaměření tohoto přezkumu na specifické otázky související se svobodou tisku (samozřejmě v širším slova smyslu) mu dávají přidanou hodnotu nad rámec přezkumu v režimu čl. 8 Úmluvy, což je žádoucí.

V souvislosti se skrytým sledováním komunikace ze strany orgánů státu se stěžovatelé často dovolávají také porušení čl. 13 Úmluvy, stanovujícího právo na účinné opravné prostředky. Vzhledem k tomu, že existence účinných opravných prostředků tvoří v případě skrytého sledování klíčovou otázku i v rámci přezkumu porušení čl. 8 Úmluvy, jsou obě otázky úzce provázány. ESLP proto ohledně porušení čl. 13 Úmluvy buď dospívá ke stejným závěrům, jako v případě čl. 8 Úmluvy,[500] nebo konstatuje, že se porušením čl. 13 Úmluvy není třeba separátně zabývat.[501] Byť v praxi se dopady obou přístupů neliší, poslední zmíněný se zdá být častější, přinejmenším v aktuální judikatuře. Stejným způsobem přistupuje ESLP v relevantních případech i k namítanému porušení čl. 6 Úmluvy.[502]

V neposlední řadě je třeba uvést, že dle judikatury, kterou se následně inspiroval Soudní dvůr při formulování svého přístupu k problematice data retention, může zásah do základních práv chráněných Úmluvou představovat již samotné uchovávání údajů, bez ohledu na to, zda uchované údaje byly následně dále zpracovány ze strany státních orgánů.[503] Povahu

[498] Srov. rozsudek *Breyer*, body 60-63.
[499] Srov. rozsudek *Big Brother Watch*, bod 495.
[500] Srov. rozsudek *Klass a další proti Německu*, body 61-72 či rozhodnutí *Weber a Saravia proti Německu*, body 154-56.
[501] Srov. rozsudek *Zakharov proti Rusku*, bod 307 či rozsudek *Centrum för Rättvisa proti Švédsku*, bod 184.
[502] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, body 90-94.
[503] Srov. rozsudek *S. a Marper proti Spojenému království*, bod 67.

a podmínky možného následného zpracování je však logicky třeba vzít v potaz při posuzování závažnosti zásahu způsobeného takovým uchováváním.[504]

4.2.2.2 Zásah, který je v souladu se zákonem

Ověřování, zda zásah do základních práv chráněných Úmluvou byl stanoven zákonem ve smyslu judikatury ESLP, je v případech skrytého sledování komunikace obzvláště důležitý, jelikož riziko zneužití je v případě pravomocí, jež jsou vykonávány skrytě, zjevné.[505] K tomuto požadavku přitom nemůže být přistupováno ryze formálně, spíše naopak. Nejde pouze o formální existenci právního předpisu, ale i o jeho „kvalitu". Požadavky judikatury se tak v této souvislosti soustředí na přístupnost legislativy a předvídatelnost zásahu pro dotčené osoby.[506] Co se týče skrytého sledování, jde především o to, aby byly jasně a dostupným způsobem vymezeny pravomoci státních orgánů, zejména to, jaké orgány a za jakých podmínek mohou k takovým opatřením přistoupit.[507] Ustálená judikatura v této souvislosti vyžaduje, aby dotčená vnitrostátní právní úprava upravovala přinejmenším šest základních otázek,[508] konkrétně:

- okruh jednání, k jejichž potírání mohou být dotčená opatření použita;
- okruh osob, vůči kterým mohou být dotčená opatření použita;
- časové omezení trvání dotčených opatření;
- pravidla pro uchování a použití získaných informací;
- záruky, které se uplatní při předání získaných informací třetím osobám;
- podmínky, za niž musí být získané informace smazány.

Výše uvedené přitom platí jak pro oblast boje proti trestné činnosti, tak pro oblast boje proti hrozbám v oblasti národní bezpečnosti.[509] Míra přesnosti vnitrostátního práva nicméně nebude v každém případě stejná a bude odviset mj. od povahy dotčeného opatření, např. co se týče jeho adresátů.[510] ESLP také není při posuzování výše uvedených požadavků extrémně striktní a poukazuje na potřebu vyhnout se přílišné rigiditě takto stanovených pravidel. Proto např. okruh jednání, k jejichž potírání mohou být dotčená opatření použita, není třeba vymezit prostřednictvím taxativního výčtu skutkových podstat trestných činů.[511] Skutečnost,

---

[504] Srov. rozsudek *Breyer proti Německu*, bod 97.
[505] Srov. rozsudek *Malone proti Spojenému království*, bod 67.
[506] Srov. např. rozsudek *Big Brother Watch proti Spojenému království*, bod 305.
[507] Srov. ibidem, bod 306.
[508] Srov. např. rozsudek *Big Brother Watch proti Spojenému království*, bod 305 či *Zakharov proti Rusku*, bod 231.
[509] Srov. rozsudek *Zakharov proti Rusku*, bod 238.
[510] Srov. rozsudek *S. a Marper proti Spojenému království*, bod 96.
[511] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 64.

že příslušné orgány své pravomoci vykonávají v praxi přiměřeně, však zpravidla nebude pro posouzení zákonnosti zásahu relevantní.[512] Na druhou stranu ESLP poměrně nedávno shledal, že požadavky na kvalitu zákona byly splněny, přestože maximální doba uchovávání údajů nebyla v právní úpravě stanovena, jelikož v praxi nepřekračovala dva roky.[513]

Osobně nejsem velkým zastáncem toho, jak ESLP vykládá požadavek na zákonnost opatření skrytého sledování, jelikož dle mého názoru často vede ke směšování požadavků na zákonnost a na přiměřenost právní úpravy. To ostatně uznává i sám ESLP, když v některých případech obě otázky posuzuje společně.[514] Konstatování toho, že zásah nebyl stanoven zákonem, by podle mne mělo být omezeno na případy, kdy je příslušná právní úprava z pohledu dotčených osob nejasná, či na případy, kdy jsou omezení příslušných orgánů sice stanovena (tj. přiměřenost je v praxi zajištěna), avšak prostřednictvím předpisů, se kterými se dotčené osoby nemají možnost seznámit. Na rozdíl od ESLP se například domnívám, že nestanovení maximální lhůty pro uchování údajů ve vnitrostátním právu má vést ke shledání, že dotčená právní úprava není v souladu s požadavkem přiměřenosti, nikoliv ke shledání, že by zásah nebyl stanoven zákonem.

Z hlediska toho, co lze v případě členských států EU považovat za zásah, který je v souladu se zákonem, je klíčový poměrně aktuální rozsudek *Big Brother Watch proti Spojenému království*. V něm ESLP shledal porušení čl. 8 Úmluvy z důvodu, že se přístup státních orgánů k provozním a lokalizačním údajům neomezoval na účely boje proti závažné trestné činnosti a že nepodléhal předchozímu souhlasu soudu. K tomuto závěru však ESLP dospěl výhradně na základě toho, že se jednalo o právní úpravu spadající do působnosti směrnice 2002/58, tj. úpravu, u níž dříve ve věcech *Digital Rights Ireland* a *Tele2 Sverige a další* vznesl tyto požadavky Soudní dvůr. ESLP shledal, že dotčená právní úprava není v souladu s judikaturou Soudního dvora, která je pro členské státy EU závazná, a zásah tudíž není v souladu se zákonem ve smyslu čl. 8 a 10 Úmluvy.[515]

Přestože je tedy přístup ESLP k problematice skrytého sledování velice odlišný od přístupu Soudního dvora, přinejmenším v případech, kdy se Soudní dvůr k určité problematice jednoznačně vyjádřil, je ESLP ochoten shledávat porušení Úmluvy již z důvodu, že zásah neodpovídal požadavkům judikatury Soudního dvora. Je nicméně otázkou, do jaké

[512] Srov. rozsudek *Malone proti Spojenému království*, bod 79.
[513] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 372.
[514] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 58.
[515] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 467.

míry bylo toto konstatování důsledkem specifické situace v dané věci, tj. skutečnosti, že sama vláda Spojeného království i vnitrostátní soudy konstatovaly, že sporná vnitrostátní právní úprava nevyhovovala požadavkům unijního práva, a musela být v návaznosti na to změněna. Za těchto okolností tedy přístup ESLP nebyl příliš překvapivý. Tento aspekt rozsudku *Big Brother Watch proti Spojenému království* by proto sám o sobě neměl být považován za důkaz obecného sbližování judikatury ESLP a Soudního dvora týkající se skrytého sledování komunikace. Musíme si totiž uvědomit, že striktní přístup Soudního dvora nebyl aplikován na ostatní posuzované aspekty sporu (např. možnost hromadného zpracování obsahu komunikace). Spíše naopak – rozsudek *Big Brother Watch proti Spojenému království* je vnímán jako důkaz toho, že se přístup ESLP k této problematice od přístupu Soudního dvora vzdaluje.[516] Dobře přístup ESLP shrnuje Celeste, když uvádí, že ESLP v dané věci „*vyzval Spojené království k respektování rozhodnutí Soudního dvora, aniž by však převzal závěry Soudního dvora ohledně plošné data retention*“.[517]

4.2.2.3 Zásah, který sleduje legitimní cíl

Jak čl. 8 Úmluvy, tak její čl. 10 obsahují taxativní výčet legitimních cílů, za jejichž účelem může dojít k zásahu do chráněných práv. Právo na soukromý život je možné omezit „*v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných*“, svobodu projevu pak „*v zájmu národní bezpečnosti, územní celistvosti nebo veřejné bezpečnosti, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky, ochrany pověsti nebo práv jiných, zabránění úniku důvěrných informací nebo zachování autority a nestrannosti soudní moci*“. Právní úpravy skrytého sledování komunikace budou sledovat některý či častěji dokonce více z výše uvedených cílů (zejména zajištění národní bezpečnosti, veřejné bezpečnost a předcházení zločinnosti). Této otázce proto nebývá v případech řešených ESLP věnována zásadní pozornost, např. ve srovnání s otázkou zákonnosti zásahu či nezbytnosti zásahu v demokratické společnosti.

Někteří autoři sice uvádějí, že opatření, jejichž podstatou je vyšetřování trestné činnosti, nemohou k omezení čl. 8 Úmluvy sloužit, nemají-li zároveň prokazatelný dopad na předcházení

---

[516] Srov. FIEDOROWICZ, Michael. Overview of European State-Sanctioned Mass Surveillance Law. *Chicago Unbound: International Immersion Program Papers*, 2019, s. 12 a 13 či CHRISTAKIS, Theodore. A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial thoughts on the Big Brother Watch Judgment. *European Law Blog*, 2018.

[517] CELESTE, Edoardo. The Court of Justice and the Ban on Bulk Data Retention. *European Constitutional Law Review*, 2019, s. 154.

trestné činnosti.[518] Tento názor však není správný. ESLP totiž obecně akceptuje, že opatření umožňující vyšetřování trestné činnosti zároveň přispívají k její prevenci, aniž by v této souvislosti vyžadoval jakékoliv specifické prokazování.[519] Opatření umožňující identifikaci pachatelů trestné činnosti je navíc dle ESLP možné zařadit i pod šířeji vymezené legitimní cíle zajišťování veřejné bezpečnosti a ochrany práv druhých, např. obětí trestných činů.[520] To jednoznačně potvrzuje i rozsudek *K.U. proti Finsku*, ve kterém byla dotčená otázka řešena právě z pohledu oběti trestného činu. V dané věci stěžovatel spatřoval zásah do svého práva na soukromý život v tom, že dotčená vnitrostátní právní úprava neumožňovala, aby poskytovatel služeb zpřístupnil policii údaje o identitě osoby, která se na internetu vydávala za (tehdy nezletilého) stěžovatele, a to za účelem navázání vztahů s jinými nezletilými chlapci. ESLP v daném případě dospěl k závěru, že Finsko nesplnilo své pozitivní povinnosti vyplývající z čl. 8 Úmluvy, jelikož sporná vnitrostátní právní úprava poskytovala absolutní přednost anonymitě autora sdělení před právy dotčených osob.[521]

Rozsudek *K.U. proti Finsku* bývá často používán jako argument ve prospěch vnímání data retention nikoliv pouze jako střetu základního práva subjektu údajů a veřejného zájmu, ale v určitém smyslu spíše jako střetu základních práv, zejména práv subjektu údajů na soukromí a pozitivní obligace státu chránit základní právo ostatních osob na bezpečnost.[522] Mám za to, že v případech, kdy hovoříme o pozitivní povinnosti státu zajišťovat bezpečnost obecně a nikoliv ve vztahu ke konkrétnímu jednotlivci, je na místě se na věc dívat optikou ochrany veřejného zájmu. V opačném případě by bylo téměř každý střet veřejného statku a základního práva vnímat také optikou střetu dvou základních práv. To však neznamená, že by v rámci testu proporcionality měla být pozitivní povinnost států chránit bezpečnost svých občanů ignorována. V rámci vážení protichůdných zájmů musí být zajištěno, že jeho výsledek nepovede k tomu, že by bylo v určitých případech zcela vyloučeno účinné vyšetřování určitých trestných činů.

4.2.2.4 Zásah, který je nezbytný v demokratické společnosti

Klíčovou roli při posuzování, zda byl určitý zásah do základních práv nezbytný v demokratické společnosti, hraje prostor pro uvážení, který judikatura ESLP přiznává členským státům. Šíře

---

[518] Srov. BREYER, Patrick. Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*, 2005, s. 368.
[519] Srov. např. *rozsudek S. a Marper proti Spojenému království*, bod 100.
[520] Srov. např. rozsudek *Breyer proti Německu*, bod 86.
[521] Srov. rozsudek *K.U. proti Finsku*, bod 49.
[522] Srov. např. rozsudek *La Quadrature du Net a další*, bod 126 a násl.

tohoto prostoru není univerzální pro všechny druhy zásahů. Odvíjí se mj. od povahy práva, do kterého je zasahováno, i povahy samotného zásahu, např. z hlediska sledovaných cílů. Jde-li o zásah, který jednotlivci významně stěžuje výkon „klíčových práv" chráněných Úmluvou (za které bylo označeno i právo na soukromý život dle čl. 8 Úmluvy), je prostor pro uvážení států zpravidla užší. Prostor pro uvážení bude naopak širší v případech, kdy neexistuje jednoznačný konsensus mezi státy ohledně významu sledovaných cílů či způsobů jejich dosahování (což v případě skrytého sledování komunikace nebude neobvyklé).[523]

Přístup ESLP k šíři prostoru pro uvážení v oblasti skrytého sledování komunikace není zcela jednoznačný. ESLP někdy hovoří o „*určitém prostoru pro uvážení*"[524], někdy o „*poměrně širokém prostoru pro uvážení*"[525] či jindy dokonce „*širokém prostoru pro uvážení*". [526] Na druhé straně požaduje, aby byl zásah nikoliv pouze nezbytný v demokratické společnosti, ale „*striktně nezbytný*" v demokratické společnosti, což by naznačovalo poměrně úzký manévrovací prostor pro členské státy.[527] Ohledně požadavku na „*striktní nezbytnost*" je navíc v novějších rozsudcích odkazováno i na judikaturu Soudního dvora, která je v tomto ohledu velmi přísná.[528] Tato nejednoznačnost do jisté míry potvrzuje kritiku doktríny prostoru pro uvážení, která byla zmíněna v kapitole 2.4.1.

Nejrozumnější intepretací výše uvedených úvah se zdá být, že ačkoliv ESLP vyžaduje „striktní nezbytnost" v případě zásahů způsobených skrytým sledováním komunikace, ohledně toho, co lze v daném kontextu považovat za „striktně nezbytné", mají státy určitý prostor pro uvážení. Šíře prostoru pro uvážení závisí mj. na účelu zásahu, přičemž zejména v tak citlivé oblasti, jako je zajišťování národní bezpečnosti či boj proti závažné trestné činnosti, bude prostor pro uvážení spíše široký, mj. vzhledem k rozvoji moderních technologií a s ním souvisejícími možnostmi pachatelů těchto činů unikat odhalení. Širší prostor pro uvážení v této oblasti je proto často zdůvodňován nejen existencí „nových" hrozeb, jako je např. terorismus, ale i rozvojem technologií, které poskytují pachatelům těchto činů nové možnosti jak unikat odhalení.[529] To, že se za takové situace státy uchylují k používání nejmodernějších technologií spočívajících v masivním monitoringu komunikace, ESLP označil dokonce za „*přirozený*

[523] Srov. rozsudek *Breyer proti Německu*, bod 80.
[524] Srov. rozsudek *Klass a další proti Německu*, bod 49 či rozsudek *Breyer proti Německu*, bod 79.
[525] Srov. rozhodnutí *Weber a Saravia proti Německu*, bod 137.
[526] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 314.
[527] Srov. rozsudek *Klass a další proti Německu*, bod 42 či rozsudek *Szabó a Vissy proti Maďarsku*, bod 73.
[528] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 73.
[529] Srov. rozhodnutí *Weber a Saravia proti Německu*, bod 73, rozsudek *Centrum för Rättvisa proti Švédsku*, bod 112 či rozsudek *Big Brother Watch proti Spojenému království*, bod 314.

důsledek podoby dnešního terorismu“.[530] Rozvoj technologií dostupných členským státům za účelem skrytého sledování komunikace ESLP naopak neshledal za důvod, proč by měl být prostor pro uvážení členských států omezen.[531]

Široký prostor pro uvážení mají členské státy zejména ohledně volby režimu skrytého sledování (např. zda půjde o režim plošného či adresného sledování), a to zřejmě právě z důvodu, že v této oblasti doposud mezi členskými státy neexistuje jednoznačná shoda.[532] Ovšem v rámci zvoleného režimu je pak jejich prostor pro uvážení omezen v tom smyslu, že jsou povinny přijmout záruky, jež omezí zásah na potřebné striktní minimum, zejména co se týče prostoru pro zneužití ze strany státních orgánů.[533] Problém s výše uvedeným přístupem nicméně spočívá v tom, že členské státy *de facto* motivuje k tomu, aby si zvolily režimy sledování, které jsou ze své podstaty nejvíce intrusivní.

Právě záruky proti zneužití, jež mají zajistit, aby nedošlo „*ke zničení demokracie ve jménu její ochrany*“, tvoří již od počátku judikatury ESLP k problematice skrytého sledování komunikace jádro přezkumu nezbytnosti zásahu.[534] ESLP vychází z toho, že ačkoliv nelze riziko zneužití opatření tohoto typu nikdy zcela vyloučit, je třeba jej alespoň minimalizovat.[535] Klíčové dle ESLP je, aby sporná vnitrostátní úprava nepřiznávala příslušným orgánům prakticky neomezenou diskreci, která by otevírala prostor pro zneužití jejich pravomocí.[536] Přestože se nejedná o okolnost, která by mohla sama o sobě ovlivnit výsledek posouzení, ESLP bere v potaz i to, zda ke zneužití v praxi dochází, či nikoliv.[537] Při posuzování, zda jsou záruky dostatečné, se ESLP soustředí zejména na následující aspekty vnitrostátní právní úpravy:

- povaha opatření;
- rozsah opatření;
- důvody, na základě kterých mohou být opatření použita;
- orgány, které mohou opatření realizovat;
- orgány, které na realizaci opatření dohlíží;
- prostředky nápravy pro dotčené osoby.[538]

---

[530] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 68.
[531] Srov. rozsudek rozsudek *Big Brother Watch proti Spojenému království*, bod 316.
[532] Srov. rozsudek *Centrum för Rättvisa proti Švédsku*, bod 112.
[533] Srov. ibidem, 114 či rozsudek *Szabó a Vissy proti Maďarsku*, bod 68.
[534] Srov. rozsudek *Klass a další proti Německu*, bod 49 či rozsudek *Centrum för Rättvisa proti Švédsku*, bod 104.
[535] Srov. rozsudek *Big Brother Watch proti Spojenému království,* bod 319.
[536] Srov. rozsudek *Zakharov proti Rusku*, bod 248.
[537] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 377.
[538] Srov. rozsudek *Centrum för Rättvisa proti Švédsku*, bod 104.

Ne v každé výše uvedené oblasti stanovuje judikatura ESLP jasné požadavky na vnitrostátní právní úpravu a ne v každém rozhodnutí se ESLP ke všem výše uvedeným oblastem vyjádří. Ve většině případů se ESLP soustředí především na otázku nezávislého dohledu nad použitím opatření, ať už před jejich použitím, či alespoň následně. Klíčovou je také otázka notifikace dotčených osob, která úzce souvisí s prostředky nápravy, které mají dotčené osoby k dispozici. Důležité je, že ESLP na rozdíl od Soudního dvora k požadavkům na vnitrostátní úpravu v jednotlivých výše uvedených aspektech nepřistupuje zcela rigidně, a *a priori* neodmítá „tezi spojených nádob", resp. provádění „celkového posouzení", dle kterého mohou být nedostatky v jedné oblasti zhojeny kvalitou záruk v oblasti jiné, nejsou-li zcela zásadního charakteru.[539] Takový přístup ESLP se nejeví jako *a priori* problematický, ovšem pouze za podmínky, že bude umožněna kompenzace pouze mírných nedostatků, nikoliv např. kompletní absence určité záruky, která by mohla vést k tomu, že se celý systém záruk zbortí jako domeček z karet. Mám však za to, že ESLP umožňuje „napravit" i poměrně zásadní nedostatky, když např. absenci předchozího povolování použití opatření umožňuje zhojit robustní *ex post* kontrolou.[540]

Problematika povahy a rozsahu opatření v prvé řadě úzce souvisí s jejich cílenou či plošnou povahou. V případě režimů cíleného sledování klade ESLP důraz právě na zacílení zásahu na osoby, u nichž existuje alespoň rozumné podezření na spojitost s určitou hrozbou.[541] Totéž však nevyžaduje od režimů hromadného sledování. Dle ESLP ani režimy strategického sledování umožňující hromadně prohledávat obsah komunikace pomocí určitých selektorů (např. v podobě klíčových slov) samy o sobě nevybočují z prostoru pro uvážení, kterým státy disponují. ESLP výslovně odmítl, že by taková opatření měla být aplikována pouze na osoby, u nichž existuje předchozí podezření na souvislost s určitou hrozbou. To by totiž dle ESLP bylo v rozporu se samotnou podstatou těchto režimů sledování, která spočívá ve vyhledávání takové souvislosti pro účely další analýzy. Předchozí souvislost s konkrétní hrozbou je tak vyloučena „z povahy věci".[542] Nelze tedy než souhlasit Christakisem v tom smyslu, že v současné judikatuře ESLP existují dva odlišné režimy přezkumu – jeden pro cílené a jeden pro hromadné režimy sledování.[543]

---

[539] Srov. ibidem, bod 181.
[540] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 77.
[541] Srov. rozsudek *Klass a další proti Německu*, bod 51 či rozsudek *Zakharov proti Rusku*, bod 260.
[542] Srov. rozsudek *Big Brother Watch a další proti Spojenému království*, body 314 a násl.
[543] CHRISTAKIS, Theodore. A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial thoughts on the Big Brother Watch Judgment. *European Law Blog*, 2018.

Každopádně je třeba uvést, že i ESLP považuje zásah do práva na soukromý život způsobený tímto druhem sledování za velmi vážný.[544] Zároveň platí, že případy, ve kterých ESLP „posvětil" hromadné režimy sledování, se doposud týkaly monitoringu extrateritoriální komunikace, v čemž ESLP spatřuje alespoň určité zaměření na segment komunikace, u níž lze očekávat vyšší přínos z hlediska sledovaných cílů.[545] V případě režimů založených na hromadném automatizovaném zpracování komunikace také ESLP vyžaduje, aby existovaly dostatečné záruky v oblasti výběru, která sdělení budou vybrána k následnému zpracování, tak, aby byl zásah do soukromého života omezen na nezbytné minimum. V tomto ohledu však ESLP není příliš přísný, jelikož nevyžaduje, aby příslušná kritéria byla vyjmenována v zákoně či v příkazu k hromadnému sledování.[546] Porušení práva na soukromý život tak shledává až v případě, kdy se k absenci takového výčtu přidává i nedostatečný dohled nad procesem selekce.[547] Z výše uvedeného je zřejmé, že je současný přístup ESLP k hromadným režimům sledování poměrně shovívavý. Přístup ESLP se tak zásadně odlišuje od velmi striktního přístupu Soudního dvora k problematice data retention. Hlubší analýza těchto rozdílů bude předmětem kapitoly 4.3.

Rozsah opatření se v prvé řadě odvíjí od vymezení činů, k jejichž potírání má příslušné opatření sloužit. ESLP se v tomto ohledu soustředí především na aspekt předvídatelnosti, tj. jasné vymezení alespoň typů takových jednání ve vnitrostátním právu.[548] Je pravdou, že ESLP v minulosti kritizoval, když příslušná legislativa umožňovala použít opatření skrytého sledování komunikace i v případech méně závažných trestných činů (např. kapsářství)[549] či u většiny trestných činů v trestním zákoníku.[550] Nicméně vzhledem k tomu, že dotčené právní úpravy vykazovaly řadu dalších nedostatků, je poměrně obtížné určit, jakou váhu v konečném důsledku hrály tyto skutečnosti při konstatování porušení čl. 8 Úmluvy. Naopak v případech, kde byla dotčená opatření omezena pouze na závažné trestné činy či jednání ohrožující národní bezpečnost, se z pohledu ESLP jednalo o skutečnost svědčící ve prospěch přiměřenosti dotčené právní úpravy.[551] Jasné je to, že z judikatury ESLP doposud nevyplývá jednoznačný požadavek na to, aby byla opatření skrytého sledování komunikace (ať už

[544] Srov. rozhodnutí *Weber a Saravia proti Německu*, bod 125 či rozsudek *Szabó a Vissy proti Maďarsku*, bod 69.
[545] Srov. rozsudek *Big Brother Watch a další proti Spojenému království*, body 337 a 343.
[546] Srov. ibidem, bod 340.
[547] Srov. ibidem, body 346-347.
[548] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 64,
[549] Srov. rozsudek *Zakharov proti Rusku*, body 182 a 244.
[550] Srov. rozsudek *Iordachi a další proti Rumunsku*, body 43 a 44.
[551] Srov. rozhodnutí *Weber a Saravia proti Německu*, body 115 a 126

hromadného či cíleného) omezena pouze na závažné trestné činy či jednání ohrožující národní bezpečnost. Jak bylo uvedeno výše, to neplatí v případech, ve kterých tento požadavek předtím stanovil Soudní dvůr.[552]

Co se týče rozsahu opatření z časového hlediska, zastává ESLP obdobný přístup. Jeho judikatura tak striktně nepředepisuje, jak dlouhé trvání by měla mít opatření různého typu (odposlech, hromadné zpracování obsahu komunikace, uchovávání metadat apod.), ale opět se soustředí na otázku záruk proti zneužití. Důležité tedy je, aby trvání opatření bylo upraveno vnitrostátním právem, a to včetně podmínek pro případné prodloužení této doby.[553]

Jádrem judikatury ESLP k problematice skrytého sledování komunikace je pak otázka nezávislého dohledu. O něm lze uvažovat celkem ve třech okamžicích – před nasazením opatření (tj. v rámci *ex ante* autorizace jejich použití), v jejich průběhu, a nakonec i poté, co jsou opatření realizována (tj. v rámci *ex post* přezkumu legality). Zatímco v prvních dvou fázích musí případný dohled z povahy věci probíhat bez zapojení a bez vědomosti dotčených osob, otázka následného přezkumu je naopak úzce spojena s prostředky nápravy, které má dotčená osoba k dispozici, a tudíž i s vyrozuměním této osoby.[554]

Dle judikatury ESLP by měl být dohled nad skrytým sledováním komunikace ze strany orgánů státu – ať už *ex ante* či *ex post* – především nezávislý na exekutivě. V této souvislosti není vyžadováno, aby dohled vykonávaly soudní orgány. Jedná se však o velmi preferovanou variantu, jelikož soudní dohled poskytuje nejvyšší záruky nezávislosti, nestrannosti a řádné procedury.[555] Akceptovány byly nicméně i režimy kontroly jinými nezávislými tělesy, např. nezávislými komisemi pro kontrolu tajných služeb či unijními dozorovými úřady pro ochranu osobních údajů, včetně kontroly parlamentními tělesy. Nutno však dodat, že ve většině těchto případů existovalo více druhů dohledu najednou.[556] U dohledu ze strany státních zástupců či ministra spravedlnosti naopak z logických důvodů potřebná míra nezávislosti shledána nebyla.[557] Pro účinnost dohledu je klíčové, aby měly příslušné orgány přístup ke všem

[552] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 467.
[553] Srov. rozsudek *Centrum för Rättvisa proti Švédsku*, bod 127.
[554] Srov. ibidem, body 105 a 106 či rozsudek *Big Brother Watch proti Spojenému království*, body 309 a 310.
[555] Srov. rozsudek *Klass a další proti Německu*, body 55-56 či rozsudek *Zakharov proti Rusku*, bod 233.
[556] Srov. rozhodnutí *Weber a Saravia proti Německu*, body 108-118 či rozsudek *Centrum för Rättvisa proti Švédsku*, bod 176.
[557] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 77 či rozsudek *Zakharov proti Rusku*, bod 280.

relevantním dokumentům, včetně těch utajovaných.[558] Informace o činnosti dohlížejících orgánů by také měly být – alespoň v určité míře – dostupné veřejnosti.[559]

Co se týče konkrétně autorizace použití opatření, tj. *ex ante* přezkumu, ten je ze strany ESLP považován za klíčovou záruku proti zneužití systému skrytého sledování komunikace.[560] Ani v tomto případě se však nejedná o nezbytnou podmínku slučitelnosti systému skrytého sledování komunikace s Úmluvou, jelikož i z požadavku na předchozí přezkum připustil ESLP v minulosti určité výjimky. První, zcela logickou výjimku představují naléhavé situace, kdy by zpoždění v důsledku potřeby autorizace mohlo nepříznivě ovlivnit cíle sledovaného opatření.[561] Podmínkou však je, aby existovaly záruky toho, že se taková urgentní procedura omezí na odůvodněné případy a nebude zneužívána.[562] Druhou výjimku, která je důsledkem již výše uvedeného holistického přístupu ESLP, jsou situace, kdy je absence či praktická neúčinnost systému předchozí kontroly nahrazena robustním a efektivním přezkumem *ex post*.[563] Předchozí soudní či alespoň kvazisoudní přezkum je však nezbytný v případě opatření namířených proti médiím.[564]

Cílem *ex post* přezkumu je především ověřit, zda byla příslušná opatření nasazena v souladu se zákonem či předchozím povolením. V případě shledání porušení by měla vést k přijetí nápravných opatření (např. ke zničení ilegálně získaných informací) a příp. potrestání osob, které se dopustily pochybení.[565] Jak již bylo uvedeno výše, jelikož v případě *ex post* přezkumu již není vyloučeno zapojení dotčených osob, je tato otázka úzce spojená právě s prostředky nápravy, které mají k dispozici dotčené osoby. Otázka efektivity prostředků nápravy pak úzce souvisí s problematikou informování dotčených osob.[566] Ani povinnost následného informování však není dle judikatury požadavkem, přes který by za každých okolností „nejel vlak", přestože jde o něco, co by v příslušné vnitrostátní právní úpravě zakotveno být „*mělo*".[567] ESLP v prvé řadě uznává, že v řadě případů může taková pozdější notifikace vést k odhalení metod příslušných orgánů, a umožňuje tedy její odložení

[558] Srov. rozsudek *Centrum för Rättvisa proti Švédsku*, bod 155,
[559] Srov. rozsudek *Zakhraov proti Rusku*, bod 283.
[560] Srov. ibidem, bod 249.
[561] Srov. rozhodnutí *Weber a Saravia proti Německu*, bod 115 či rozsudek *Centrum för Rättvisa proti Švédsku*, bod 140.
[562] Srov. rozsudek *Zakharov proti Rusku*, bod 266.
[563] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 77.
[564] Srov ibidem.
[565] Srov. rozsudek *Zakharov proti Rusku*, bod 282.
[566] Srov. ibidem, bod 286.
[567] Srov. rozhodnutí *Weber a Saravia proti Německu*, bod 135 či rozsudek C*entrum för Rättvisa proti Švédsku*, bod 164.

až do okamžiku, kdy takové riziko pomine. I když se takový přístup jeví jako naprosto logický, je třeba jej vnímat v kontextu toho, že např. v případě činnosti zpravodajských služeb se dle ESLP může jednat o roky či dokonce desetiletí, díky čemuž v mnoha případech ztratí notifikace veškerou účinnost.[568]

ESLP dále na následném oznámení netrvá v případech, kdy příslušná vnitrostátní právní úprava umožňuje jednotlivcům se z vlastní iniciativy obrátit na příslušné orgány za účelem ověření, zda byly předmětem opatření skrytého sledování komunikace ze strany státních orgánů, resp. zda tato opatření byla nasazena v souladu se zákonem.[569] Ve věci C*entrum för Rättvisa proti Švédsku* ESLP zaujal v této souvislosti doposud zřejmě nejshovívavější přístup. ESLP sice konstatoval, že v praxi nemají příslušné orgány povinnost dotčené osoby sami notifikovat či jim na jejich žádost poskytnout informace o nasazení opatření skrytého sledování komunikace, nicméně ve světle *ex ante* soudního přezkumu a obecným mechanismům stálého dohledu nad příslušnými orgány (např. ze strany ombudsmana či dozorového úřadu zřízeného na základě obecné unijní právní úpravy) porušení čl. 8 Úmluvy neshledal.[570] Pozdější notifikaci také ESLP nevyžaduje u opatření hromadného sledování, u kterých z povahy věci – hovoříme-li pouze o prvotním třídění údajů za účelem dalšího zpracování – nelze hovořit o konkrétní osobě, která by byla cílem těchto opatření a měla být tedy notifikována.[571]

4.2.3 Data retention

Ačkoliv ESLP neměl doposud příležitost adresně se vyjádřit ke všem sporným otázkám týkajícím se problematiky data retention, zejména k přiměřenosti plošné povinnosti uchovávání údajů, problematika komunikačních metadat není jeho judikatuře zcela cizí. Z původní judikatury ESLP týkající se získávání výpisů telefonních hovorů vyplývalo, že ačkoliv přístup ke komunikačním metadatům představuje zásah do práva na soukromý život, je tento zásah méně závažný než zásah způsobený odposlechem telefonních hovorů, ke kterému by příslušné orgány měly přistupovat pouze výjimečně a za striktních podmínek.[572] Tento přístup byl nicméně formulován v roce 1984 a odpovídal tomu, jakou tehdy tyto údaje měly vypovídající hodnotu. Ve světle nástupu mobilních telefonů a internetu však byly tyto závěry přehodnoceny. Z dnešní judikatury naopak vyplývá, že zásah způsobený zpracováním tohoto typu údajů není

[568] Srov. rozsudek *Klass a další proti Německu*, bod 58.
[569] Srov. rozsudek *Kennedy proti Spojenému království*, bod 167 a rozsudek C*entrum för Rättvisa proti Švédsku*, bod 166.
[570] Srov. rozsudek *Centrum för Rättvisa proti Švédsku*, bod 178.
[571] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 317.
[572] Srov. rozsudek *Malone proti Spojenému království*, bod 84.

nutně méně závažný než zpracování obsahu komunikace např. prostřednictvím odposlechů telefonních hovorů.[573] Právě naopak, díky snadné zpracovatelnosti těchto údajů je z nich možné vyvodit velmi přesné závěry o soukromém životě osob.[574] S tím nelze než souhlasit. Především pokud jde o hromadnou analýzu velkého množství dat, mají metadata v praxi podstatně větší vypovídací hodnotu než obsah komunikace.

Nicméně nejsou metadata jako metadata. ESLP – stejně jako v současnosti Soudní dvůr – považuje zásah spojený se zpracováním údajů o totožnosti uživatelů za méně závažný ve srovnání se zpracováním ostatních provozních či lokalizačních údajů. Ve věci *Breyer proti Německu* tak ESLP shledal, že zásah způsobený povinným uchováváním údajů o identitě uživatelů předplacených SIM karet, aniž by byly zároveň uchovávány provozní údaje týkající se jednotlivých sdělení či lokalizační údaje, není sice triviální, ale je poměrně omezený.[575] ESLP v daném případě vycházel z rozsudku *Ministerio Fiscal*, v němž Soudní dvůr dospěl k závěru, že přístup k údajům o uživatelích nepředstavuje závažný zásah do práv na soukromí a ochranu osobních údajů. Dle názoru ESLP se případ *Ministerio Fiscal* podobal věci *Breyer proti Německu* více než případy *Digital Rights Ireland* a *Tele2 Sverige.* To bylo kritizováno, mj. v disentním stanovisku soudce Ranzoniho, který z tehdejšího pohledu zcela oprávněně rozporoval podobnost dotčeného případu s věcí *Ministerio Fiscal*. Poukazoval na to, že věc *Ministerio Fiscal* se netýkala plošného uchovávání údajů o všech majitelích SIM karet, ale jednorázového přístupu k údajům o identitě majitele SIM karty, jež byla vložena do mobilního telefonu odcizeného při loupeži.[576] Ovšem jak bylo uvedeno v kapitole 4.1.3.2, Soudní dvůr ve svých posledních rozsudcích z této oblasti dospěl taktéž k závěru, že je plošné uchovávání údajů o totožnosti uživatelů přípustné, jelikož díky nižší vypovídací hodnotě těchto údajů představuje oproti uchovávání ostatních provozních a lokalizačních údajů menší zásah do práv na soukromí a ochranu osobních údajů.

ESLP ve světle nižší závažnosti zásahu do práva na soukromý život v případě uchovávání a přístupu k údajům o uživatelích značně slevil ze svých standardních požadavků v oblasti skrytého sledování komunikace. ESLP tak neshledal porušení práva na soukromý život navzdory tomu, že případy, ve kterých byl možný přístup k těmto údajům, nebyly ve vnitrostátním právu vymezeny zcela konkrétně.[577] Přístup byl navíc možný bez předchozího

[573] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 356.
[574] Srov. ibidem.
[575] Srov. rozsudek *Breyer proti Německu*, bod 95.
[576] Srov. disentní stanovisko soudce Ranzoniho ve věci *Breyer proti Německu*, bod 14.
[577] Srov. rozsudek *Breyer proti Německu*, bod 100.

povolení nezávislého orgánu i bez povinnosti následné notifikace.[578] ESLP se tak spokojil s existencí obecného dohledu ze strany dozorových úřadů pro ochranu osobních údajů a možností dotčených osob namítat nezákonnost zpracování v rámci opravných prostředků proti konečným rozhodnutím příslušných orgánů. Nicméně ve světle toho, že k přístupu v praxi docházelo v desítkách milionů případů ročně, mají tyto způsoby *ex post* kontroly zjevné limity. Zaprvé nelze očekávat, že by dozorové úřady byly schopny ověřit legalitu přístupu v takovém množství případů. Zadruhé, „konečné rozhodnutí příslušných orgánů" bude přijato jen ve zlomku případů. Ve zbylých případech žádné takové konečné rozhodnutí, které by mohl dotčený jednotlivec napadat, existovat nebude.

I když lze s ESLP souhlasit v tom smyslu, že vypovídací hodnota údajů o uživatelích je nižší ve srovnání s provozními a lokalizačními údaji sesbíranými za určité delší období, je třeba si uvědomit, že v praxi budou údaje o uživatelích sloužit spíše jako jakýsi „klíč" k propojení identity uživatele s dalšími, z povahy věci podstatně citlivějšími údaji. Mohou tak např. umožnit spojit obsah zprávy na mobilním telefonu oběti s jejím autorem apod. Ačkoliv se tedy jedná o zásah méně závažný, je otázkou, zda je míra této závažnosti tak nízká, aby nebylo vyžadováno dodržení téměř žádných požadavků vyplývajících z judikatury ESLP týkající se skrytého sledování komunikace. I z tohoto důvodu byly závěry ESLP ve věci *Breyer proti Německu* kritizovány v disentním stanovisku soudce Ranzoniho, který poukazoval mj. na to, že v případě *Benedik proti Slovinsku* ESLP kladl důraz právě na aspekt souvislosti údajů o uživatelích a dalších, potenciálně citlivějších údajů, včetně obsahu komunikace.[579] Vůči tomuto argumentu soudce Ranzoniho však lze namítat, že ve věci *Benedik proti Slovinsku* vedly tyto úvahy toliko ke konstatování, že přístupem k údajům o uživatelích došlo k zásahu do práva na soukromý život.[580] Ve věci *Benedik proti Slovinsku* se ESLP otázkou intenzity zásahu či konkrétními požadavky na přístup k těmto údajům blíže nezabýval, jelikož shledal porušení čl. 8 Úmluvy již na základě toho, že vnitrostátní soudy nesprávně dospěly k závěru, že zpracováním těchto údajů vůbec nedochází k zásahu do čl. 8 Úmluvy.[581]

Přístupu k údajům o uživatelích se v neposlední řadě týkal i již zmiňovaný rozsudek *K.U. proti Finsku*, ve kterém dospěl k závěru, že Finsko nesplnilo své pozitivní povinnosti vyplývající z čl. 8 Úmluvy, když jeho vnitrostátní právní úprava poskytovala absolutní přednost

[578] Srov. ibidem, bod 107.
[579] Srov. rozsudek ESLP ze dne 24. července 2018, *Benedik proti Slovinsku*, stížnost č. 62357/14, CE:ECHR:2018:0424JUD006235714, bod 109 (dále jen „rozsudek *Benedik proti Slovinsku*").
[580] Srov. ibidem.
[581] Srov. ibidem, body 129-130.

anonymitě autora sdělení na internetu před právy obětí trestného činu páchaného prostřednictvím internetu. Ačkoliv z tohoto rozsudku skutečně vyplývá, že členské státy nemohou plošně znemožnit identifikaci osob páchajících trestnou činnost na internetu, a tudíž i účinné vyšetřování takových činů, jen stěží může být rozsudek *K.U. proti Finsku* vykládán způsobem, že *de facto* ukládá členským státům povinnost přijmout systém plošného uchovávání komunikačních metadat. Dotčený případ se totiž týkal výhradně problematiky přístupu k údajům, které měl poskytovatel služeb k dispozici, navíc v situaci, kdy o přiměřenosti takového přístupu nemohly panovat zásadní pochyby. Problém tak spočíval jen v tom, že příslušná vnitrostátní právní úprava neobsahovala pro poskytnutí takových údajů žádný právní „podvozek". Příslušná vnitrostátní právní úprava tak de facto poskytovala absolutní přednost anonymitě uživatele internetu za všech okolností, což shledal ESLP jako problematické. ESLP nicméně v žádném případě členským státům nepředepsal výsledek vážení protichůdných zájmů ani neuložil, aby přijaly takové režimy data retention, které umožní identifikaci pachatele za každých okolností.

Otázka záruk proti zneužití, které ESLP vyžaduje v případě přístupu k širšímu okruhu komunikačních metadat, byla řešena ve věcech *Tretter proti Rakousku* a *Ringler proti Rakousku*, byť pouze v kontextu posuzování přípustnosti stížnosti. ESLP shledal obě stížnosti usilující o přezkum *in abstracto* nepřípustné z důvodu, že rakouské právo obsahovalo dostatečné prostředky nápravy pro osoby, které se domnívají, že jejich údaje byly zpřístupněny příslušným orgánům. K tomuto závěru dospěl ESLP navzdory tomu, že příslušná vnitrostátní právní úprava v praxi nevyžadovala notifikaci osob, jejichž údaje byly zpřístupněny. ESLP za dostačující prostředek nápravy vylučující *in abstracto* přezkum považoval především možnost obrátit se na příslušné orgány s žádostí o informace, zda k takovému přístupu došlo. ESLP dále shledal systém záruk za dostačující díky následné možnosti subjektu údajů obrátit se na dozorové úřady, které legalitu postupu příslušných orgánů musely přezkoumat, a možnost subjektu údajů podat žalobu proti rozhodnutí dozorového úřadu. Jelikož žadatelé tyto nástroje nevyužili, nepřistoupil ESLP k přezkumu *in abstracto*.[582]

Je zjevné, že ESLP přisuzuje velkou váhu dohledu ze strany dozorových orgánů. Právě ten je v takových případech klíčový, jelikož je-li ze strany dozorového úřadu shledáno, že příslušné orgány při plnění své informační povinnosti nepochybily, jen stěží bude mít subjekt údajů k dispozici informace, prostřednictvím kterých by pak názor dozorového úřadu mohl

[582] Srov. rozhodnutí *Ringler proti Rakousku*, body 69-81 a rozhodnutí *Tretter proti Rakousku*, body 67-70.

zpochybnit u soudu. Na druhou stranu je třeba uvést, že s ohledem na to, jakou mírou nezávislosti dozorové úřady v rámci EU disponují, není takový přístup v rozporu s judikaturou ESLP týkající se nezávislého dohledu. Přesto se jedná o velmi mírné požadavky, obzvlášť pokud si uvědomíme, že by se subjekt údajů nejprve zřejmě musel preventivně obrátit se žádostí o informace na všechny příslušné orgány v Německu zvlášť, a následně pak na dozorový úřad ve vztahu ke všem poskytnutým odpovědím.

Byť výše uvedené závěry byly vysloveny v rámci přezkumu přípustnosti stížnosti, ani z výše uvedené judikatury týkající se jiných druhů skrytého sledování komunikace nevyplývá, že by byl v případě přístupu ke komunikačním metadatům za každých okolností vyžadován *ex ante* souhlas soudu či *ex post* notifikace dotčených osob. Zdá se, že ESLP se do značné míry spokojí s možností osob, které mají za to, že jejích provozní a lokalizační údaje byly zpřístupněny příslušným orgánům, obrátit se na nezávislý dozorový orgán, např. právě dozorový úřad dle unijní legislativy na ochranu osobních údajů či následně na soud, nesouhlasí-li s rozhodnutím dozorového úřadu.

Z výše analyzovaných případů tedy vyplývá, že v judikatuře ESLP doposud nebyla řešena zásadní otázka přípustnosti plošné povinnosti uchovávání údajů. Z judikatury týkající se jiných druhů skrytého sledování komunikace lze nicméně dovozovat, jakým způsobem by se k této otázce ESLP postavil. ESLP v prvé řadě *a priori* neodmítá režimy hromadného sledování, a tudíž nevyžaduje, aby zpracování údajů určitých osob bylo podmíněno předchozí identifikací souvislosti mezi osobou, jejíž údaje jsou zpracovávány, a konkrétní hrozbou. ESLP navíc v minulosti akceptoval i takové režimy, které umožňovaly hromadné automatické zpracování obsahu komunikace. Je však otázkou, zda z této skutečnosti můžeme jednoduše *maiori ad minus* dovodit, že by ESLP posvětil plošné uchovávání metadat. Zaprvé, jak již bylo uvedeno výše, je dichotomie obsah (větší zásah) a metadata (menší zásah) v kontextu dnešních technologií spíše zastaralá. Naopak lze tvrdit, že jakmile máme k dispozici určité množství metadat, umožňuje jejich automatizovaná analýza mnohdy mnohem intenzivnější zásah do soukromého života jednotlivce, než automatizovaná analýza (byť také třeba většího množství) obsahu komunikace. Zároveň je si třeba uvědomit, že režimy automatizovaného zpracování obsahu komunikace, ač byly svou povahou hromadné, cílily zpravidla na určitý segment komunikace, nikoliv na veškerá sdělení na daném území. V případě data retention se však uchovávají provozní a lokalizační údaje týkající se veškerých uživatelů prostředků elektronické komunikace na daném území. Nelze tak jednoduše říci, že ESLP již posvětil

režimy, které měly v zásadě stejnou povahu jako plošná data retention, resp. které byly více intrusivní.

To však nic nemění na tom, že ESLP poskytuje státům široký prostor pro uvážení ohledně volby režimu skrytého sledování komunikace. Pravděpodobně tedy nelze očekávat, že by ESLP shledal, že plošné uchovávání komunikačních metadat spadá *a priori* mimo tento prostor pro uvážení. Data retention sleduje, stejně jako ESLP posuzované režimy hromadného sledování, cíl boje proti těm nejzávažnějším hrozbám pro moderní stát. Závažnost zásahu je dále z celkového hlediska snižována tím, že v případě klasické plošné data retention je sice uchováváno značné množství údajů, avšak ve skutečnosti je přistupováno pouze ke zlomku uchovávaných údajů. Míra prostoru pro uvážení ohledně volby režimu skrytého sledování komunikace dále vychází i z konsensu mezi státy, přičemž v případě data retention tento konsensus svědčí rozhodně ve prospěch plošné povinnosti uchovávání údajů. Zároveň platí, jak již bylo rozebráno výše, že požadavky ESLP na slučitelnost režimu skrytého sledování s čl. 8 Úmluvy nejsou pro všechny režimy stejné, ale přizpůsobují se povaze fungování konkrétního režimu. Jelikož plošnost uchovávání je základní podmínkou efektivity data retention, nelze očekávat, že by ESLP na jedné straně členským státům umožnil tento nástroj využívat, na druhé straně na jeho použití pak kladl takové požadavky, které by v praxi vylučovaly jeho efektivitu. Lze tedy konstatovat, že ačkoliv se ESLP k problematice plošné data retention doposud jednoznačně nevyjádřil, jeho dosavadní judikatura jednoznačně směřuje k tomu, že by plošnou data retention jako takovou neshledal automaticky v rozporu s čl. 8 Úmluvy.

Co se týče dalších požadavků na režim data retention, nelze předpokládat, že by ESLP kladl zásadní hmotněprávní požadavky na dobu uchovávání či vymezení jednání, k jejichž potírání by měl umožněn přístup k údajům. Požadavky ESLP na režimy skrytého sledování komunikace jsou ostatně především procesního charakteru. Nelze tedy očekávat, že by ESLP jako např. Soudní dvůr vyžadoval, aby byl přístup k údajům možný pouze pro boj proti závažné trestné činnosti, či aby doba uchovávání nepřesáhla několik měsíců apod. Procesní požadavky by se pak jistě týkaly zejména problematiky nezávislého dohledu. Úpravy členských států EU by je z výše uvedených důvodů (tj. zejména s ohledem na existenci nezávislých dozorových úřadů, jejichž rozhodnutí podléhají soudnímu přezkumu) zpravidla splnily. To samozřejmě nutně neplatí pro oblast národní bezpečnosti, ve které dozorové úřady budou zpravidla disponovat menšími, či dokonce žádnými pravomocemi. Judikatura ESLP nicméně v oblasti národní bezpečnosti poskytuje členským státům ještě větší prostor pro uvážení.

4.2.4 Závěr

Co se týče problematiky skrytého sledování komunikace obecně, z výše uvedeného vyplývá, že přístup ESLP se soustředí téměř výhradně na procedurální aspekty takového sledování, zejména na oblast dohledu. Judikatura ESLP nepředepisuje, jakou podobu by měly mít systémy skrytého sledování používané členskými státy, a zpravidla neklade konkrétní či přísné hmotněprávní požadavky pro nasazení jednotlivých opatření. Takový přístup poskytuje členským státům poměrně široký prostor pro to, aby si samy zvolily, jakým způsobem budou závažnou trestnou činnost a hrozby v oblasti národní bezpečnosti potírat, což odpovídá politické citlivosti této oblasti.

Na druhou stranu je třeba uvést, že obavy ohledně toho, zda takový přístup – zejména ve světle podstatně restriktivnější judikatury Soudního dvora – klade dostatečný důraz na ochranu práv jednotlivců chráněných Úmluvou, jsou taktéž oprávněné. To je dáno tím, že judikatura ESLP nestanoví téměř žádné požadavky, jejichž dodržení by bylo opravdu nezbytné za každých okolností. Díky tomu byly ze strany ESLP akceptovány i takové režimy skrytého sledování komunikace, které v určitých ohledech (jako např. *ex post* notifikace) vykazují poměrně významné nedostatky. Obzvláště problematické se jeví to, že ESLP své požadavky upravuje s ohledem na to, jaký režim skrytého sledování komunikace státy zvolí. Takový přístup přitom může vést k tomu, že režimy neadresného sledování, které jsou z hlediska dopadů na širokou populaci rozsahem obvykle závažnější než režimy cíleného sledování, paradoxně v konečném důsledku podléhají volnějším podmínkám.

Co se týče konkrétně problematiky data retention, současná judikatura ESLP uznává, že zásah do soukromého života způsobený zpracováním provozních a lokalizačních údajů může být závažný. To však neplatí pro údaje o uživatelích, v případě kterých nepovažoval ESLP za závažný zásah do soukromého života ani plošnou povinnost jejich uchovávání v případě všech majitelů předplacených SIM karet. Vzhledem k přístupu ESLP k jiným režimům skrytého sledování komunikace nelze očekávat, že by ESLP v této souvislosti stanovoval přísné požadavky hmotněprávního charakteru, např. co se plošnosti uchovávání či účelů, pro které mohou být uchované údaje použity. Jádro přezkumu tak bude jako v jiných případech tvořit otázka nezávislého dohledu. To však zřejmě nebude platit pro právní úpravy data retention členských států EU, u kterých ESLP bude pro účely slučitelnosti zásahu s Úmluvou vyžadovat, aby dotčená vnitrostátní právní úprava odpovídala požadavkům Soudního dvora.

4.3 KOMPARACE PŘÍSTUPU SOUDNÍHO DVORA A EVROPSKÉHO SOUDU PRO LIDSKÁ PRÁVA

4.3.1 Dotčená práva

Z judikatury Soudního dvora i ESLP dle očekávání vyplývá, že data retention je třeba vnímat jako zásah do základních práv. Konkrétní vymezení práv, do nichž je prostřednictvím data retention zasahováno, se pak logicky mírně odlišuje s ohledem na odlišné znění lidskoprávních katalogů, které příslušné soudy vykládají. Soudní dvůr proto hovoří primárně o právu na respektování soukromého života, právu na ochranu osobních údajů, svobodě projevu a zásadě důvěrnosti komunikace vyplývající ze sekundárního práva.[583] ESLP hlavně o právu na respektování soukromého života (ve smyslu informačního sebeurčení) a taktéž důvěrnosti komunikace (resp. korespondence) ve smyslu čl. 8 Úmluvy.[584] V praxi však nemůže být pochyb o tom, že otázky informačního sebeurčení a důvěrnosti komunikace jsou v argumentaci obou soudů klíčové, bez ohledu na to, jak je v konkrétním lidskoprávním katalogu pojmenováno právo, jehož jsou součástí.

Poměrně překvapivé je, jak malou přidanou hodnotu z hlediska přezkumu těchto otázek se zdá mít samostatné zakotvení práva na ochranu osobních údajů v čl. 8 Listiny. Přestože Soudní dvůr vždy hovoří o tom, že data retention představuje zásah jak do práva na soukromí, tak do práva na ochranu osobních údajů, v rámci přezkumu přiměřenosti postupuje tak, jakoby byl obsah obou práv totožný.[585] Na druhou stranu nelze s jistotou tvrdit, že samostatné zakotvení práva na ochranu osobních údajů nemá vůbec žádné dopady. Z výše uvedené analýzy judikatury vyplývá, že Soudní dvůr je co se týče přístupu k data retention podstatně přísnější než ESLP. Míra této přísnosti by klidně mohla být důsledkem toho, že zakotvení práva na ochranu osobních údajů jako samostatného práva do jisté míry motivuje, nebo alespoň ospravedlňuje, vysokou úroveň ochrany poskytovanou Soudním dvorem v těchto případech. Soudní dvůr nicméně takové úvahy nikdy explicitně nepotvrdil.

Spíše než samostatné právo na ochranu osobních údajů hraje v judikatuře Soudního dvora klíčovou roli zásada důvěrnosti komunikace, jak je zakotvena v čl. 15 odst. 1 směrnice 2002/58. Právě tato zásada se zdá být hlavním argumentačním nástrojem Soudního dvora v oblasti data retention, umožňující Soudnímu dvoru přistupovat k uchovávání údajů jako k výjimce z pravidla, která nemůže mít plošnou povahu.[586] Dle aktuální judikatury se navíc zdá,

[583] Srov. rozsudek *Tele2 Sverige*, body 95 a 104.
[584] Srov. rozsudek *Klass proti Německu*, bod 41 či rozsudek *Zakharov proti Rusku*, bod 173.
[585] Srov. rozsudek *Tele2 Sverige*, body 94 a násl.
[586] Srov. rozsudek *Tele2 Sverige*, bod 104.

že z pohledu Soudního dvora vyplývá tato zásada přímo z Listiny, a změna sekundárního práva tak sama o sobě zřejmě ke zmírnění přístupu Soudního dvora nepovede. ESLP ve své judikatuře se zásadou důvěrnosti komunikace tímto způsobem nepracuje, a nevylučuje tedy režimy hromadného zpracování údajů pouze s poukazem na to, že by se v takovém případě stala výjimka pravidlem.[587]

Podstatnější rozdíly mezi oběma soudy lze nalézt u problematiky svobody projevu. To, jak Soudní dvůr v praxi při posuzování přiměřenosti nerozlišuje mezi čl. 7 a 8 Listiny, platí i pro její čl. 11 zakotvující svobodu projevu. Soudní dvůr tedy při posuzování přiměřenosti nejenže významněji nerozlišuje vzájemně mezi čl. 7 a 8 Listiny, ale ani mezi čl. 7 a 8 na straně jedné, a čl. 11 Listiny na straně druhé.[588] Přístup ESLP je odlišný, jelikož se při přezkumu opatření skrytého sledování komunikace optikou čl. 10 Úmluvy soustředí téměř výhradně na otázku ochrany novinářských zdrojů. Kritéria posuzování přiměřenosti jsou proto jiná, než je tomu v případě posuzování zásahu do práva na soukromí, a to zejména co se týče přísnějších požadavků na přístup k údajům, na něž by se měla vztahovat ochrana novinářských zdrojů.[589] To, že ESLP zkoumá tato opatření optikou svobody projevu pouze u určitých kvalifikovaných stěžovatelů, by mohlo vyvolávat dojem, že takový přístup vede k nižší úrovni ochrany zbytku populace. Mám však za to, že tomu tak není. V případě běžné populace totiž optika svobody projevu nebude přinášet specifické otázky nad rámec důvěrnosti komunikace ve smyslu čl. 8 Úmluvy, resp. čl. 7 Listiny. Proto se domnívám, že je přístup ESLP k otázce svobody projevu vhodnější.

4.3.2 Legitimní cíle

Právní úpravy data retention (resp. skrytého sledování komunikace orgány státu) jsou zpravidla odůvodněny bojem proti trestné činnosti (ve smyslu předcházení, vyšetřování, odhalování a stíhání trestné činnosti) a proti hrozbám v oblasti národní bezpečnosti. Jde o poměrně standardně uznávané legitimní cíle, pro které mohou být omezena základní práva – ať už v režimu Listiny či Úmluvy.[590] Proto nemůže být větším překvapením, že problematika legitimity těchto cílů není v příslušné judikatuře natolik zásadní a kontroverzní jako problematika přiměřenosti. V judikatuře obou zkoumaných soudů taktéž, alespoň co se týče uznání legitimity těchto cílů, neexistují zásadnější rozdíly, které by bylo na tomto místě třeba

[587] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 317.
[588] Srov. rozsudek *Tele2 Sverige*, body 94 a násl.
[589] Srov. rozsudek *Big Brother Watch proti Spojenému království*, body 487-489.
[590] Srov. rozsudek *La Quadrature du Net*, bod 110 či rozsudek *Klass proti Německu*, bod 46.

rozebírat. Přesto je však k otázce cílů sledovaných právními úpravami data retention, resp. skrytého sledování komunikace obecně, třeba uvést pár poznámek.

V prvé řadě je třeba uvést, že uznání legitimity výše uvedených cílů v obecné rovině nutně neznamená, že data retention může být odůvodněna bojem proti jakékoliv trestné činnosti. Klíčové v tomto ohledu bylo zejména konstatování Soudního dvora v rozsudku *Tele2 Sverige*, dle kterého „*vzhledem k závažnosti zásahu do dotčených základních práv, který představuje vnitrostátní právní úprava, která stanoví uchovávání provozních a lokalizačních údajů pro účely boje proti trestné činnosti, může být takové opatření odůvodněno pouze bojem proti závažné trestné činnosti.*“[591] Soudní dvůr od té doby svůj velmi striktní postoj zmírnil, přičemž dle jeho aktuální judikatury může být nejen přístup k údajům o uživatelích, ale taktéž jejich plošné uchovávání, odůvodněno i bojem proti jiným než závažným trestným činům. V případě ostatních údajů (včetně IP adres) však z judikatury Soudního dvora vyplývá nutnost omezit povinnost uchovávání a přístupu pouze na účel boje proti závažné trestné činnosti a zajišťování národní bezpečnosti.[592] Otázka míry volnosti členských států ohledně definice toho, co je pro tyto účely závažným trestným činem, zůstává doposud nezodpovězena

Judikatura ESLP je ohledně omezení tohoto druhu volnější, možná až příliš. Co se týče údajů o totožnosti uživatelů, ESLP neshledal porušení čl. 8 Úmluvy ani v případě úpravy, která umožnila jejich uchovávání a přístup k nim za účelem řešení přestupků.[593] K problematice ostatních provozních a lokalizačních údajů se ESLP v této souvislosti nevyslovil, byť v případě režimu skrytého sledování komunikace posuzovaného v případě *Zakharov proti Rusku* ESLP vyslovil „znepokojení“ nad tím, že příslušná právní úprava umožňovala odposlech hovoru v případě drtivé většiny trestných činů, včetně např. kapsářství.[594] I když si uvědomuji, že rolí ESLP je především stanovovat minimální standard v rámci Rady Evropy, mám za to, že jeho přístup je možná až příliš benevolentní.

Co se pak týče problematiky zajišťování národní bezpečnosti, ta je oběma soudy uznána nejen za legitimní cíl, nýbrž za cíl, který může odůvodnit větší zásahy do dotčených základních práv než cíl boje proti závažné trestné činnosti.[595] O konkrétních podobách těchto zásahů pak bude hovořeno dále v kapitole věnující se blíže posuzování přiměřenosti. I když je takový

[591] Rozsudek *Tele2 Sverige*, bod 102.
[592] Srov. rozsudek *La Quadrature du Net*, bod 140.
[593] Srov. rozsudek *Breyer proti Německu*, bod 21.
[594] Srov. rozsudek *Zakharov proti Rusku*, bod 244.
[595] Srov. rozsudek *La Quadrature du Net*, body 146 a 177 či rozsudek *Big Brother Watch proti Spojenému království*, bod 314.

přístup zcela na místě (nejen z důvodu vyšší závažnosti těchto hrozeb, ale i odlišných metod práce příslušných orgánů), v případě Soudního dvora vyvolává jeho preskriptivní judikatura v této oblasti z mého pohledu oprávněné výtky stran popírání významu čl. 4 odst. 2 SEU a zasahování unijního práva do takto citlivé oblasti.

4.3.3 Zákonnost

Soudní dvůr se v souvislosti s požadavkem na to, aby byl zásah do základních práv stanoven zákonem, hlásí k ustálené judikatuře ESLP, jejímž jádrem jsou požadavky na zákonnost v materiálním smyslu, tedy především na jasnost a předvídatelnost právní úpravy.[596] V případě opatření skrytého sledování komunikace ESLP vyžaduje, aby příslušná vnitrostátní právní úprava stanovující zásah do základního práva sama definovala rozsah omezení výkonu dotyčného práva, a tudíž dotčeným osobám umožňovala předvídat, v jakých situacích může k uchovávání údajů či k jejich zpřístupnění příslušným orgánům dojít. ESLP v této souvislosti stanovil šest otázek, které mají být ve vnitrostátní právní úpravě obsaženy.[597]

Přestože se Soudní dvůr formálně hlásí ke stejnému přístupu jako ESLP, v tomto ohledu nekopíruje přístup ESLP zcela a např. nekontroluje, zda je opravdu všech šest uvedených otázek ve vnitrostátní právní úpravě obsaženo. Některé nedostatky, které by ESLP posoudil tak, že zásah nebyl stanoven zákonem, Soudní dvůr chápe spíše jako důkaz o nepřiměřenosti zásahu. To je však třeba vnímat pozitivně, jelikož otázky spojené s absencí některých záruk ve vnitrostátním právu je třeba chápat primárně jako nedostatek v rovině přiměřenosti, nikoliv jako nedostatek jasnosti a předvídatelnosti zákona. Konstatování toho, že zásah nebyl stanoven zákonem, by tak mělo být omezeno spíše na případy, kdy je příslušná právní úprava z pohledu dotčených osob nejasná či v případech, kdy jsou omezení příslušných orgánů sice stanovena (tj. přiměřenost je v praxi zajištěna), avšak prostřednictvím předpisů, se kterými se dotčené osoby nemají možnost seznámit. Tomuto přístupu má v současnosti rozhodně blíže Soudní dvůr.

4.3.4 Proporcionalita

4.3.4.1 Obecné poznámky

Základní deklarovaná východiska pro přezkum přiměřenosti jsou v případě Soudního dvora i ESLP podobná, zejména co se týče požadavku na striktní přezkum. Dle obou soudů musí být výjimky z dotčených základních práv činěny pouze v rozsahu, v jakém je to „naprosto

[596] Srov. rozsudek *Digital Rights Ireland*, bod 54.
[597] Srov. rozsudek *Big Brother Watch proti Spojenému království*, body 304-307.

nezbytné“.[598] V praxi se nicméně pohled těchto soudů na to, co je možné považovat za naprosto nezbytné, značně liší.

V případě ESLP je požadavek na striktní nezbytnost třeba vnímat v kontextu toho, že ESLP členským státům zároveň přiznává široký prostor pro uvážení ohledně volby režimu skrytého sledování komunikace, přičemž tuto skutečnost následně zohledňuje při posuzování přiměřenosti jednotlivých aspektů tohoto režimu.[599] ESLP tedy od států vyžaduje, aby zásah do základních práv minimalizovaly, ovšem nikoliv na úkor samotné podstaty zvoleného režimu. Proto např. v případě režimů hromadného sledování nevyžaduje existenci souvislosti mezi zpracovávanými údaji a konkrétní hrozbou.[600] Požadavky ESLP proto nejsou takové povahy, aby státy *de facto* donutily změnit zvolený režim, avšak soustředí se na to, aby v rámci tohoto režimu byly dodrženy minimální záruky proti zneužití. To ostatně odpovídá citlivosti dotčené oblasti z pohledu členských států a již několikrát zmíněné funkci ESLP, kterou je stanovit toliko minimální standard ochrany lidských práv. S tím ostatně souvisí, že posuzování přiměřenosti ze strany ESLP se dále soustředí především na otázky procesních záruk proti zneužití, přičemž nedostatky v případě jednoho druhu záruk mohou být do jisté míry kompenzovány jinde.

Přístup Soudního dvora je v praxi nesrovnatelně přísnější a s prostorem pro uvážení členských států příliš nepočítá, a to ani v rovině volby režimu, ani v rámci jeho realizace. Požadavky na jednotlivé záruky jsou pevně stanoveny, s tím, že jejich absence nemůže být kompenzována jinde. Jsou jak procesního (např. co se týče autorizace přístupu či soudního přezkumu), tak hmotněprávního charakteru (např. co se týče požadavků na dobu uchovávání či vymezení trestných činů, k jejichž potírání může data retention sloužit). Klíčovou roli v argumentaci Soudního dvora hraje také sekundární právo, konkrétně čl. 5 odst. 1 směrnice 2002/58, ze kterého Soudní dvůr dovozuje zásadu důvěrnosti komunikace, z níž dotčená opatření představují výjimku, která nemůže mít plošnou povahu.[601]

Rozsudky Soudního dvora jsou dále podstatně více preskriptivní, což je vidět zejména na rozsudku *La Quadrature du Net*, kde Soudní dvůr předepsal odlišné náležitosti data retention z hlediska jednotlivých druhů údajů (provozní a lokalizační údaje obecně, IP adresy, údaje o totožnosti uživatelů), resp. účelů (zajišťování národní bezpečnosti, boj proti závažné trestné činnosti, boj proti ostatní trestné činnosti) a stavu bezpečnosti v členském státě.[602] Některé

[598] Srov. rozsudek *Digital Rights Ireland*, bod 52 či rozsudek *Klass proti Německu*, bod 42.
[599] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 314.
[600] Srov. ibidem, bod 317.
[601] Srov. rozsudek *Tele2 Sverige*, body 95 a 104.
[602] Srov. rozsudek *La Quadrature du Net*, bod 168.

klíčové úvahy Soudního dvora či jím načrtnutá řešení se navíc často objevují až v rozsudcích, aniž by byly diskutovány v rámci písemné či ústní fáze řízení. V minulosti se obdobně formulované požadavky, např. co se týče požadavku na cílenou data retention, ukázaly jako v praxi zcela nefunkční, což nakonec vedlo Soudní dvůr k jejich následnému zmírňování.

Ve srovnání s argumentací Soudního dvora je v argumentaci ESLP věnován zpravidla větší prostor „pohledu států" v tom smyslu, že se příslušné rozsudky důsledněji věnují i povaze hrozeb, kterým musí státy čelit, a to nejen z hlediska jejich závažnosti, ale také toho, že jsou tyto hrozby čím dál tím více realizovány pomocí prostředků elektronické komunikace.[603] Judikatura Soudního dvora se soustředí podstatně více na pohled dotčených osob, což bylo následně Soudnímu dvoru určitým způsobem vyčítáno ze strany předkládajících soudů, které Soudní dvůr upozorňovaly na nutnost více zohledňovat i bezpečnostní rovinu celého problému, mj. s ohledem na pozitivní závazky členských států zajišťovat bezpečnost. Zatímco ESLP chápe alespoň do určité míry rozvoj technologií jako důvod pro poskytnutí více prostoru členským státům, v případě Soudního dvora je evidentní důraz spíše na zajištění vysoké úrovně ochrany dotčených práv. Tento poměrně zásadní rozdíl v přístupu se dle mého názoru následně projevuje ve všech zásadních otázkách týkajících se přiměřenosti data retention.

4.3.4.2 Vypovídací hodnota komunikačních metadat

Vysokou závažnost zásahu do základních práv způsobenou zpracováním komunikačních metadat, vyplývající z jejich vysoké vypovídací hodnoty i snadné zpracovatelnosti, konstatuje jak Soudní dvůr, tak ESLP. S tím nelze než souhlasit.

Výhradu lze nicméně vznést k přístupu Soudního dvora, který ve své judikatuře nadále zastává názor, že plošné uchovávání komunikačních metadat představuje menší zásah do dotčených základních práv než obdobné uchovávání obsahu komunikace, které by dle Soudního dvora představovalo zásah do samotné podstaty dotčených základních práv.[604] Je otázkou, zda za současného stavu technologií je takový přístup skutečně správný, jelikož právě díky snadné zpracovatelnosti komunikačních metadat mají v případě hromadných režimů sledování tyto údaje větší vypovídací hodnotu než obsah komunikace. Závažnost zásahu by proto měla být posuzována spíš s ohledem na celkové fungování daného režimu skrytého sledování, a nelze proto vycházet pouze z dichotomie „metadata v. obsah".[605] Jde o to, jakým způsobem je s údaji nakládáno – třídění obsahu komunikace prostřednictvím klíčových slov

[603] Srov. rozsudek *Big Brother Watch proti Spojenému království*, body 384-386.
[604] Srov. rozsudek *Tele2 Sverige*, bod 101.
[605] Viz kapitola 3.1.2.

v reálném čase může dle mého názoru vyvolávat menší rizika než hromadné zpracování metadat umožňující vytváření profilů. Konstatování Soudního dvora ohledně zásahu do podstaty základních práv v případě hromadného zpracování obsahu je dle mého názoru příliš zjednodušující a bylo v kontextu rozsudků zabývajících se výhradně zpracováním metadat naprosto nadbytečné. Zároveň je politováníhodné, že takto zásadní závěry ohledně podstaty práv na soukromý život a ochranu osobních údajů jsou vysloveny v jednom bodě rozsudku bez jakéhokoliv dalšího odůvodnění. Díky tomu např. nevíme, zda tyto úvahy Soudního dvora platí jen pro skutečně plošné zpracování obsahu komunikace, nebo obecně pro režimy, které umožní jakékoliv zpracování obsahu komunikace bez předchozí souvislosti s konkrétní hrozbou.[606]

4.3.4.3 Plošné uchovávání komunikačních metadat

I v tomto případě je základní východisko obou soudů stejné – samo uchovávání údajů představuje zásah do dotčených základních práv, bez ohledu na to, zda následně dojde k přístupu k uchovávaným údajům či zda v souvislosti s tímto uchováváním vznikne dotčeným osobám nějaká újma. Jde o přístup, který byl prvně formulován ze strany ESLP v souvislosti s uchováváním údajů o DNA v policejních databázích a který byl následně převzat Soudním dvorem a aplikován na problematiku data retention.[607] Jde o přístup zcela logický, kterému nelze nic vytknout.

Přesto se domnívám, že podstatou zásahu do základních práv způsobeného samotným uchováváním údajů není jejich uchování jako takové, ale skutečnost, že takové uchování představuje nezbytný předpoklad následného přístupu k těmto údajům, a tudíž i riziko neoprávněného přístupu k těmto údajům, které není možné zcela vyloučit. Právě v hodnocení intenzity zásahu způsobeného samotným uchováváním údajů vidím zřejmě nejzásadnější odlišnost mezi Soudním dvorem na straně jedné, a ESLP na straně druhé. Soudní dvůr plošné uchovávání údajů zakazuje, byť nově s určitými výjimkami. ESLP se sice k této konkrétní otázce nevyjádřil, avšak z jeho judikatury týkající se jiných režimů skrytého sledování komunikace lze dovozovat, že předchozí spojitost s konkrétní hrozbou pro účely uchovávání také nebude požadavkem, přes který by v režimu Úmluvy nejel vlak.[608]

V kapitole zabývající se judikaturou Soudního dvora bylo podrobněji vysvětleno, proč jeho přístup považuji za příliš striktní. Je tomu tak zejména z následujících důvodů:

---

[606] K tomuto aspektu viz stanovisko GA ve věci *Facebook Ireland a Schrems*, body 272 a násl.
[607] Srov. rozsudek *S. a Marper proti Spojenému království* a rozsudek *Digital Rights Ireland*, body 32-35.
[608] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 317.

1) Tento přístup nadhodnocuje rizika spojená s uchováváním údajů a dostatečně neodlišuje rovinu uchovávání od roviny přístupu, resp. dokonce automatizované analýzy dat.
2) Tento přístup dostatečně nepřihlíží k tomu, že dodatečné záruky v oblasti uchovávání a přístupu mohou tato rizika značně minimalizovat.
3) Tento přístup dostatečným způsobem nezohledňuje, že ke zpracování osobních údajů v masivním měřítku dochází v současné době naprosto běžně za komerčními účely, mj. také samotnými poskytovateli služeb.
4) Tento přístup dostatečně nepřihlíží k tomu, že v současné době je řada závažných trestných činů či činů ohrožujících národní bezpečnost páchána výhradně pomocí prostředků elektronické komunikace, přičemž v případě neexistence plošné povinnosti uchovávat komunikační metadata se možnost vyšetření těchto činů stává ve značné míře závislá na tom, zda je poskytovatel služeb uchovával z komerčních důvodů.
5) Tento přístup dostatečným způsobem nezohledňuje, že absence plošné data retention může vést k používání opatření, které budou v konečném důsledku v jednotlivých případech podstatně invazivnější (např. nasazení odposlechů, sledování apod.).

To, že se Soudní dvůr svůj značně striktní přístup z rozsudku *Tele2 Sverige* rozhodl ve věci *La Quadrature du Net* upřesnit či spíše modifikovat tím, že plošné uchovávání připustil v běžném režimu alespoň v případě údajů o totožnosti uživatelů a IP adres, je rozhodně krok správným směrem. Mám však za to, že by do budoucna bylo vhodné tímto způsobem umožnit plošné uchovávání i ostatních provozních a lokalizačních údajů. Přístup ESLP, který plošné uchovávání *a priori* nevylučuje, se tedy zdá být vhodnější. Ruku v ruce s plošným uchováváním však musí jít naprosto striktní hmotněprávní i procesní záruky v oblasti uchovávání a přístupu, což je oblast, kde z mého pohledu vykazuje určité nedostatky naopak judikatura ESLP.

4.3.4.4 Dodatečné záruky v oblasti uchovávání a přístupu

Klíčovými zárukami, o kterých je v příslušné judikatuře hovořeno, jsou především doba uchovávání údajů a povinnost jejich následného zničení, zabezpečení údajů proti neoprávněnému přístupu, otázky předchozí a následné kontroly přístupu k údajům a v neposlední řadě povinnost informovat dotčené osoby. Mám za to, že každá z těchto oblastí tvoří klíčový stavební díl přiměřené právní úpravy data retention, a proto nedostatky byť

i v jedné oblasti mohou značně ovlivnit přiměřenost celého režimu.[609] Proto by nemělo být možné nedostatky v jedné oblasti kompenzovat v oblasti jiné, jak např. ve své judikatuře týkající se skrytého sledování komunikace obecně připouští ESLP.[610]

Co se týče požadavků na zabezpečení údajů, je za zcela správný třeba považovat požadavek Soudního dvora na jejich uložení na území EU, a to nejen z hlediska toho, že v případě uložení mimo EU nelze nikdy zcela vyloučit, že se k nim dostanou orgány třetího státu. Důležité také je, že v případě uložení dat na území EU se na jejich uložení uplatní pravidla GDPR a dohled ze strany dozorových úřadů. Zkoumaná judikatura se naproti tomu příliš nevěnuje požadavkům na konkrétní technická opatření k zajištění důvěrnosti a integrity uchovávaných údajů. ESLP sice požaduje, aby tyto otázky byly určitým způsobem upraveny, ovšem opět s ohledem na svou funkci nepředepisuje konkrétní řešení. Překvapivější je však absence takových konkrétních požadavků v případě Soudního dvora, jehož judikatura je v jiných oblastech značně preskriptivní. Nedostatky v této oblasti sice Soudní dvůr vyčetl směrnici 2006/24,[611] v pozdější judikatuře se ale věnoval spíše jiným otázkám.

Osobně se domnívám, že by v tomto ohledu bylo vhodné od právní úpravy data retention vyžadovat, aby stanovila vysoké a konkrétní požadavky na zabezpečení údajů, např. stran certifikace používaných zařízení, vedení *logů*, pseudonymizace apod. Je sice pravdou, že tyto povinnosti bude možné v mnoha případech dovodit i výkladem GDPR (především díky požadavku na přístup založený na riziku), přesto by však s ohledem na citlivost uchovávaných údajů měly být ve vnitrostátní úpravě vymezeny explicitně. Obzvlášť uvědomíme-li si, že jejich zakotvení prakticky nemůže být na újmu cílům sledovaným dotčenou vnitrostátní právní úpravou. Je politováníhodné, že drtivá většina členských států, přestože před Soudním dvorem usilovně bojují za umožnění plošné data retention, nestanovuje konkrétnější povinnosti týkající se zabezpečení těchto údajů.[612] V této souvislosti také nelze zapomínat na to, že zajištění mimořádně vysoké úrovně ochrany by se mohlo pro některé, zejména menší poskytovatele služeb ukázat jako příliš nákladné. V takovém případě by alespoň část těchto nákladů měl dle mého názoru být připraven nést členský stát. V neposlední řadě je třeba uvést, že z hlediska bezpečnosti nejsou důležité jen požadavky na poskytovatele služeb, dostatečně konkrétní povinnosti zabezpečení by měly být upraveny i pro případy, kdy se zpřístupněnými údaji pracují

[609] Srov. stanovisko GA ve věci *Tele2 Sverige*, body 220 a násl.
[610] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 77.
[611] Srov. rozsudek *Digital Rights Ireland*, bod 66.
[612] Srov. Council of the European Union. *Data retention – State of play*, 2018, s. 9.

příslušné orgány členských států. K výraznému posunu v této oblasti by nicméně v současnosti měla přispět směrnice 2016/680.[613]

Co se týče doby uchovávání údajů, oba soudy vyžadují, aby byla omezena na to, co je skutečně nebytné. Z příslušné judikatury Soudního dvora dále vyplývá, že půjde spíš o dobu počítanou v týdnech či měsících než letech. Dle mého názoru by – opět za účelem zajištění maximální možné ochrany základních práv za současného co nejmenšího omezení účelu daného opatření – bylo na místě, aby příslušná vnitrostátní právní úprava diferenciovala doby uchovávání s ohledem na citlivost jednotlivých typů údajů a jejich užitečnost pro sledované účely. Tím by pak bylo na místě klást přísnější požadavky např. na lokalizační údaje, se kterými jsou spojena značná rizika, avšak jejichž využitelnost značně klesá v čase.[614] U těchto údajů by možná bylo vhodné trvat na kratších lhůtách pro uchovávání. To neznamená, že by taková lhůta měla být jasně předepsána v judikatuře, dle mého názoru by však mělo být po zákonodárci požadováno alespoň provedení takového posouzení, což zatím judikatura žádného ze zkoumaných soudů explicitně nevyžaduje, byť Soudní dvůr hovoří o nutnosti uchovávat údaje jen po nezbytně nutnou dobu.[615] Některé současné právní úpravy data retention však takovou diferenciaci obsahují.[616]

Požadavek na předchozí soudní souhlas potřebný k přístupu k údajům obsahuje již původní judikatura ESLP týkající se skrytého sledování, byť v určitých případech umožňuje ESLP jeho nahrazení *ex post* přezkumem.[617] Požadavek na předchozí souhlas soudu či jiného nezávislého orgánu před přístupem k údajům obsahuje i judikatura Soudního dvora, a to již od případu *Digital Rights Ireland.*[618] Z mého pohledu se opět jedná o standardní a nenahraditelný požadavek v oblasti data retention. Aby však měl skutečnou přidanou hodnotu, je nezbytné, aby ruku v ruce s ním šla i povinnost příslušných orgánů důkladně odůvodnit své žádosti o přístup k údajům, tak aby byl příslušný soud vždy schopen posoudit skutečnou nezbytnost přístupu k údajům v daném konkrétním případě. Mám za to, že požadavek na předchozí soudní souhlas je klíčový nejen z hlediska vyloučení zneužití přístupu k údajům, ale zejména proti systematickému nadužívání tohoto nástroje v případech, kdy by sledovaných cílů bylo možné dosáhnout prostřednictvím metod a nástrojů, které jsou k dotčeným osobám šetrnější.

---

[613] Srov. kapitola 2.2.3.
[614] Srov. kapitola 3.2.2.2.
[615] Srov. rozsudek *La Quadrature du Net*, bod 138.
[616] Jde např. o německou právní úpravu posuzovanou ve věcech *SpaceNet* a *Telekom Deutschland.*
[617] Srov. rozsudek *Szabó a Vissy proti Maďarsku*, bod 77.
[618] Srov. rozsudek *Digital Rights Ireland*, bod 62.

Samozřejmě si lze představit i případy, kdy není vhodné na *ex ante* přezkumu trvat. V prvé řadě půjde o naléhavé případy, ve kterých by prodleva způsobená čekáním na soudní souhlas mohla vést k závažným následkům. Možnost v takových případech nahradit *ex ante* přezkum *ex post* přezkumem umožňuje judikatura obou zkoumaných soudů.[619] Dále by to mělo být možné v situacích, ve kterých není možné očekávat, že bude mít přístup k údajům negativní dopady na dotčené osoby – např. v případě pátrání po pohřešovaných osobách.

Klíčovou otázkou z hlediska požadavku na předchozí soudní přezkum přístupu k údajům je, do jaké míry má být tento požadavek aplikován na činnost zpravodajských služeb. V této souvislosti je nejprve třeba předeslat, že oba soudy akceptují, že závažnost hrozeb v oblasti národní bezpečnosti může odůvodnit větší zásahy do dotčených základních práv, než je tomu v případě boji proti trestné činnosti. To však nutně neznamená popření požadavků na nezávislý dohled. Judikatura Soudního dvora nijak nenaznačuje, že by v oblasti národní bezpečnosti bylo možné na požadavek předchozího povolení přístupu ze strany soudu či jiného nezávislého orgánu rezignovat.[620] Dohled ze strany soudního či nezávislého správního orgánu je dále vyžadován např. při konstatování existence hrozby odůvodňující dočasné plošné uchovávání, v případě nařízení sběru provozních a lokalizačních údajů v reálném čase či v případě jejich automatické analýzy.[621] Ani v případě ESLP se zvláštní charakter činnosti zpravodajských služeb neprojevuje tak, že by byl požadavek na předchozí nezávislý přezkum zcela vypuštěn. To platí i pro režimy hromadného sledování, v případě kterých je nezávislý dohled vyžadován např. nad nastavením kritérií, na základě kterých dochází k další analýze.[622] Prostor pro uvážení členských států ohledně způsobů naplnění tohoto požadavku nicméně bude širší než v případě boje proti trestné činnosti.

Osobně se domnívám, že by přístup zpravodajských služeb ke komunikačním metadatům měl podléhat nezávislému, ideálně předchozímu přezkumu, který by byl schopen účinně dohlížet na to, aby nedocházelo ke zneužívání či zjevnému nadužívání takového opatření. Zároveň mám za to, že obecný dohled vykonávaný např. parlamentními orgány by neměl být považován za dostačující. Konkrétní modality nezávislého přezkumu jsou s ohledem na specifika činnosti zpravodajských služeb (závažnost hrozeb v této oblasti, preventivní a v zásadě utajovaný charakter jejich činnosti, nepoužitelnost shromážděných

[619] Srov. rozsudek *Tele2 Sverige*, bod 120 či rozsudek *Szabó a Vissy proti Maďarsku*, bod 77.
[620] Srov. rozsudek *Privacy International*, bod 52.
[621] Srov. rozsudek *La Quadrature du Net*, bod 139.
[622] Srov. rozsudek *Big Brother Watch proti Spojenému království*, bod 340.

informací v trestním řízení apod.) k diskusi. Může jít o nezávislé komise zabývající se konkrétními případy či specializované soudy, které budou odrážet specifika dané oblasti (např. neveřejnost, neúčast dotčených osob apod.). Ve chvíli, kdy však přístup zpravodajských služeb v konkrétních případech nebude podléhat žádnému dohledu, je zřejmé, že rizika zneužití a s nimi související *chilling effect* mohou být značná. Za zcela nežádoucí naopak považuji, aby bylo možné informace získané zpravodajskými službami v rámci „volnějšího režimu" následně použít v trestním řízení. Má-li dojít k vzájemnému propojení zpravodajské a trestněprávní roviny, které se s ohledem na specifika moderních hrozeb zdá v určitých situacích nevyhnutelné, musí dojít i k určitému sblížení nároků na ochranu základních práv v rámci obou režimů.

Oba soudy taktéž vyžadují *ex post* informování dotčených osob za účelem umožnění soudního přezkumu legality opatření, s čímž lze opět zcela souhlasit. Je však samozřejmé, že by mělo toto informování být nutné až v okamžiku, kdy již nemůže ohrozit probíhající vyšetřování.[623] Mám za to, že povinnost takového informování by nemělo být možné nahradit pouze tím, že dotčeným osobám bude umožněno obracet se na příslušné orgány preventivně s žádostí o informace, zda jejich údaje byly zpracovány, k čemuž v současnosti směřuje judikatura ESLP. Pokud tyto údaje mohou být sděleny bez toho, aby došlo k ohrožení sledovaných cílů, měly by tak příslušné orgány činit z vlastní iniciativy. Na druhou stranu mám za to, že je možné od tohoto požadavku upustit (z výše připomenutých důvodů) v případě činnosti zpravodajských služeb, tak, aby bylo vyloučeno riziko odhalení metod jejich práce. Samozřejmě za podmínky, že jinak existuje nezávislý dohled nad jejich činností, a to nejen obecně, ale také co se konkrétních případů zpracování údajů týče.

V neposlední řadě je třeba zabývat se otázkou, zda by kategorie určitých osob (advokátů, lékařů, novinářů) neměly podléhat vyšší úrovni ochrany, tj. přísnějším zárukám. Jedná se o problematiku, která je dlouhodobě zmiňována odpůrci data retention, kteří často požadují, aby údaje tohoto typu vůbec nebylo možné uchovávat. Jak již bylo uvedeno výše, ESLP požadavky na specifickou úroveň ochrany vznáší v souvislosti s problematikou ochrany novinářských zdrojů. Soudní dvůr ve své judikatuře sice zmiňuje, že v případě těchto osob je posílen *chilling effect* spojený s data retention, avšak výslovně specifické požadavky

[623] Srov. rozsudek *Tele2 Sverige*, bod 121 či Big *Brother Watch proti Spojenému království*, bod 310.

nestanovuje.[624] Mám za to, že těmto údajům by měla být v určitých případech přiznána vyšší ochrana, avšak tyto aspekty mají být zohledněny až v rovině přístupu.

4.3.5 Závěr

Přestože se ESLP doposud nezabýval „typickým" data retention případem, v rámci kterého by byla řešena plošná povinnost uchovávání provozních a lokalizačních údajů a adresného přístupu k nim, lze z jeho judikatury týkající se ostatních režimů skrytého sledování komunikace vyčíst, jak by k problematice data retention přistupoval, a tento přístup porovnat s judikaturou Soudního dvora.

Co se týče aspektů dotčených práv, legitimních cílů i zákonnosti opatření data retention, je judikatura obou soudů velice podobná. Hlavní rozdíly lze spatřovat až v rámci posuzování přiměřenosti. Přístup ESLP do jisté míry odpovídá hlavnímu úkolu tohoto soudu, kterým je zajistit minimální standard ochrany základních práv v rámci Rady Evropy.[625] Jeho přístup se tak soustředí především na otázky dodatečných záruk, které mají spíše procedurální povahu. ESLP však lze vyčítat, že ohledně dodržování těchto záruk není vždy zcela důsledný. Oproti Soudnímu dvoru ESLP vykazuje větší pochopení pro argumenty států týkající se nezbytnosti nasazování moderních metod v boji proti závažné trestné činnosti a terorismu. I proto *a priori* neodmítá, aby docházelo ke zpracování osobních údajů osob, u nichž doposud nebyla odhalena souvislost s konkrétní hrozbou. Tento přístup ESLP bývá označován za pragmatický,[626] zohledňující skutečnost, že rozsáhlá zpracování osobních údajů nejen komerčními subjekty, ale i orgány státu, představují do jisté míry neoddělitelnou součást moderního způsobu života.[627]

Přístup Soudního dvora je podstatně přísnější, a to jak v rovině hmotněprávních, tak procesněprávních požadavků na právní úpravy data retention. Klíčové je v tomto ohledu především odmítání plošné data retention, které však z mého pohledu nepředstavuje správnou cestu. Je tedy jedině správně, že Soudní dvůr svůj pohled na plošnou data retention nedávno alespoň částečně modifikoval. Na druhou stranu lze za pozitivní považovat trvání Soudního dvora na určitých přísnějších zárukách v oblasti přístupu, byť je otázkou, zda by tyto neměly být zmírněny alespoň pro oblast národní bezpečnosti.

---

[624] Srov. rozsudek *La Quadrature du Net*, bod 118.
[625] Srov. např. O'LEARY, Síofra. A Tale of Two Cities: Fundamental Rights Protection in Strasbourg and Luxembourg. *Cambridge Yearbook of European Legal Studies*, 2018, s. 8.
[626] Srov. CELESTE, Edoardo. The Court of Justice and the Ban on Bulk Data Retention. *European Constitutional Law Review*, 2019, s. 156.
[627] Srov. WALKER, Claire. Data retention in the UK: Pragmatic and proportionate, or a step too far? *Computer Law & Security Review*, 2009, s. 333.

To, že Soudní dvůr poskytuje vyšší úroveň ochrany než ESLP, v daném kontextu nepředstavuje rozpor v judikatuře mezi oběma soudy. Právě naopak, jedná se o stav odpovídající funkci obou soudů, který je předvídaný čl. 52 odst. 3 Listiny. Na tomto konstatování nemůže nic změnit ani skutečnost, že z judikatury ESLP vyplývá pozitivní povinnost stanovit pravidla umožňující identifikaci osob páchajících trestnou činnost prostřednictvím internetu.[628] Tuto judikaturu totiž není možné vykládat tak, že by smluvním stranám ukládala povinnost zavedení plošné data retention umožňující identifikaci takových osob za každých okolností. Jde spíše o to, aby dotčená vnitrostátní právní úprava vyšetřování takových činů nepřiměřeně neznemožňovala. S takovým požadavkem však judikatura Soudního dvora v rozporu není.

ESLP zároveň v případech, ve kterých je jím posuzovaná právní úprava ve zjevném rozporu s judikaturou Soudního dvora, dospívá k závěru, že zásah do práv chráněný Úmluvou nebyl v souladu se zákonem, čímž dochází k významnému sblížení úrovně ochrany poskytované oběma soudy v případě členských států EU.[629] Pro členské státy tento stav znamená povinnost zajistit úroveň ochrany práva na soukromí a osobních údajů vyžadovanou Soudním dvorem, s tím, že nedodržení požadavků unijního práva může v některých případech znamenat i shledání porušení Úmluvy, přestože je standard ochrany vyžadovaný ESLP jinak nižší. Jednotlivci z členských států EU se tak v určitých případech mohou úspěšně dovolat vyššího standardu ochrany základních práv vyžadovaného Soudním dvorem i před ESLP, kde – na rozdíl od řízení o předběžné otázce před Soudním dvorem – mohou v praxi řízení zahájit i sami, vyčerpají-li předtím vnitrostátní prostředky nápravy.

[628] Srov. rozsudek *K.U. proti Finsku.*
[629] Srov. rozsudek *Big Brother Watch proti Spojenému království*, body 465-468.

ZÁVĚR

Data retention v EU opakovaně přežila svou smrt. Zrušení směrnice 2006/24 Soudním dvorem ve věci *Digital Rights Ireland* ani následné odmítnutí konceptu plošné data retention jako takového ve věci *Tele2 Sverige* totiž nevedlo k tomu, že by se z data retention stal problém minulosti. Právě naopak – vnitrostátní právní předpisy data retention jsou nadále platné v mnoha členských státech, přičemž řada z nich je v současnosti předmětem řízení před vnitrostátními soudy či Soudním dvorem.[630] Hledání kompromisu mezi schopností členských států účinně reagovat na současné bezpečnostní hrozby na straně jedné, a zajištěním vysoké úrovně ochrany soukromí a osobních údajů na straně druhé, je proto aktuálnější než kdy dříve.

Jádrem této práce byla analýza a kritické zhodnocení judikatury Soudního dvora týkající se ochrany soukromí a osobních údajů v souvislosti s data retention a její komparace s judikaturou ESLP. V tomto ohledu jsem dospěl k závěru, že kritika této judikatury, zaznívající především od členských států, je z velké části oprávněná, a to nejen co se týče posuzování působnosti unijních předpisů v této oblasti, ale i co se týče posuzování proporcionality. Problémem je v tomto ohledu především odmítání plošného uchovávání *per se*, a to přesto, že se jedná o nepostradatelný prvek data retention, v případě jehož absence nemůže data retention plnit svou hlavní funkci spočívající v umožnění „nahlížení do minulosti". Přestože byl původně velice striktní přístup Soudního dvora v současnosti zmírněn, mám za to, že nadále existuje prostor pro jeho modifikaci. Soudní dvůr zcela legitimně usiluje o zajištění vysoké úrovně ochrany základních práv v souvislosti s data retention, jelikož zásah do základních práv způsobený tímto nástrojem je z hlediska počtu dotčených osob bezesporu obrovský, zcela nevídaný v případě jiných nástrojů. Na druhou stranu je však třeba zohlednit nižší intenzitu tohoto zásahu, která je dána tím, že k těmto údajům je povolen pouze adresný přístup, a v drtivé většině případů jsou tyto údaje tedy pouze uchovány a následně smazány. Klíčovým nástrojem pro zajištění přiměřenosti jsou tak dle mého názoru robustní záruky, které v maximální míře vyloučí riziko nejen zneužití, ale také nadužívání tohoto nástroje v případech, kdy to není ke sledovaným účelům nezbytné.

Ani přístup ESLP však nelze považovat za ideální v tom smyslu, že by jej mohl Soudní dvůr jednoduše převzít a začít aplikovat. Přístup ESLP lze ocenit v tom, že nástroje hromadného

[630] Srov. European Commission. *Data Retention for law enforcement purposes – Final report*, 2020, s. 15 či Eurojust. *Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report*, 2017, s. 13.

zpracování osobních údajů *a priori* nedémonizuje a uznává, že spolu s tím, jak se náš život přesouvá do kyberprostoru, přesouvá se tam i závažná trestná činnost a jiné hrozby, a stát proto musí mít efektivní nástroje k jejich potírání. Judikatura ESLP se tak správně soustředí především na problematiku záruk proti zneužití, avšak není v tomto ohledu tak přísná a důsledná, jak by bylo v souvislosti s data retention potřebné. To souvisí s tím, že funkcí ESLP je především zajištění minimální společné úrovně ochrany základních práv v rámci Rady Evropy. Je tedy žádoucí, aby Soudní dvůr aspiroval na vyšší úroveň ochrany.

Jaké podmínky by tedy měl Soudní dvůr pro vnitrostátní právní úpravy data retention stanovit? Vyvážená právní úprava data retention by měla umožňovat účinné potírání trestné činnosti a hrozeb v oblasti národní bezpečnosti za současné minimalizace zásahů do základních práv. Jelikož je plošné uchovávání základním předpokladem účinnosti data retention, mělo by být takové plošné uchovávání možné. Jelikož rozsah uchovávaných údajů vyvolává oprávněné obavy ohledně zneužití takto uchovávaných údajů, je naprosto nezbytné, aby bylo plošné uchovávání doprovázeno opravdu robustním systémem záruk, a to jak v oblasti uchovávání, tak v oblasti přístupu.

Co se týče oblasti uchovávání, představuje klíčovou otázku doba uchovávání jednotlivých údajů. Jelikož všechny kategorie provozních a lokalizačních údajů nejsou při jejich uchovávání v čase stejně užitečné ani stejně rizikové, měla by být doba uchovávání stanovena zvlášť pro jednotlivé kategorie údajů. V případě údajů, u kterých je riziko sestavení podrobných profilů o životě osob nejvyšší, by se mělo jednat o velmi krátké doby uchovávání. Takový přístup by na jedné straně minimalizoval riziko vytváření přesných závěrů o životě osob, aniž by však vyloučil možnost policie dostat se ke komunikačním metadatům alespoň z období těsně před spácháním trestného činu, v případě kterých lze dle dostupných údajů beztak očekávat nejvyšší užitečnost. Některé méně citlivé údaje, jako např. údaje o totožnosti uživatelů, by mělo být možné uchovávat po delší dobu, což ostatně judikatura uznává již dnes. Konkrétní doby uchovávání by měly pokud možno vycházet z dostupných statistických údajů. Pokud takové údaje nejsou k dispozici, měla by příslušná právní úprava vyžadovat jejich sběr za účelem budoucího (ideálně pravidelného) přehodnocení dob uchovávání.

Další zásadní otázku představuje zabezpečení uchovávaných údajů, které musí být zajištěno ve všech stádiích – při uchovávání údajů poskytovateli služeb, při jejich předávání i při jejich následném zpracování příslušnými orgány. Požadavky na bezpečnost přitom musí být konkrétní a vysoké. Ačkoliv v obecné rovině požadavek na vysokou úroveň zabezpečení vyplývá z GDPR i směrnice 2016/680, v souvislosti s data retention by měly být požadavky

stanoveny konkrétně v příslušných zákonech. Základem musí být maximální dodržení principu *privacy by design* a využití maximálního počtu nástrojů jako např. šifrování, pseudonymizace, vedení logů, oddělení povinně uchovávaných údajů od ostatních údajů, pravidlo čtyř očí, pravidelné testování zabezpečení apod. Povinnost uchovávání údajů na území EU je pak samozřejmostí. Co se týče mechanismu předávání, nabízí se např. inspirace rakouským předávacím systémem *durchlaufstelle*, který umožňuje zabezpečenou a oboustranně zašifrovanou komunikaci mezi příslušnými orgány a poskytovateli služeb, sbírá a generuje statistiky o počtu podaných a vyřízených žádostí, aniž by však údaje centrálně uchovával či umožňoval centralizovaný přístup k nim. Je samozřejmě naprosto správné, aby náklady na takto robustní systém hradil stát, má-li o tyto údaje kvůli jejich nepostradatelnosti zájem.

Co se týče záruk v oblasti přístupu, ten musí být s výjimkou případů, kdy členské státy čelí závažné, naléhavé a konkrétní hrozbě pro národní bezpečnost, adresný. V případě potírání trestné činnosti by měl být přístup umožněn pouze v případě závažných trestných činů a činů páchaných téměř výhradně prostřednictvím prostředků elektronické komunikace, které pomocí standardních metod vyšetřování není možné účinně vyšetřovat. Dále by měl být přístup umožněn za účelem boje proti hrozbám v oblasti národní bezpečnosti, samozřejmě včetně situací, kdy je o přístup žádáno za účelem zabránění hrozícího budoucího útoku.

Co se týče problematiky boje proti trestné činnosti, klíčovou záruku představuje požadavek na předchozí schválení soudem, na kterém je třeba trvat ve všech případech krom naléhavých situací, v nichž by čekání na souhlas soudu mohlo ohrozit zdraví či život osob. V takových případech však musí být absence předchozího soudního přezkumu vyvážena *ex post* přezkumem. Přístup k údajům by měl být používán pouze v případech, kdy sledovaného účelu nelze dosáhnout jinak či pokud by bylo dosahování tohoto účelu podstatně ztížené. Je nezbytné klást přísné požadavky na odůvodňování žádostí, aby soudy mohly vykonávat skutečně účinný přezkum a schvalování nebylo pouze formální. V případech, kdy je žádáno o údaje osoby, jejíž jméno je známé, musí být vyžadováno jeho uvedení v žádosti. Samozřejmě je třeba trvat na vyrozumění dotčených osob ihned, jakmile to nemůže ohrozit účel zpracování. Kritéria, na základě kterých je existence takového ohrožení konstatována, by také měla být stanovena v zákoně.

Co se týče problematiky zajišťování národní bezpečnosti, lze si s ohledem na preventivní a v zásadě skrytou povahu činnosti zpravodajských služeb představit volnější podmínky. I v těchto případech je však dle mého názoru třeba trvat na existenci soudního či jiného nezávislého dohledu, a to i nad konkrétními případy, byť samozřejmě není vyloučeno,

aby dohled v těchto oblastech vykonávaly specializované soudy či jiné nezávislé orgány na základě speciálních procesních pravidel, např. vylučujících účast veřejnosti či dokonce dotčených osob. Takové režimy ostatně v některých členských státech fungují. Není ale možné, aby byla plošnost uchovávání ospravedlněna robustními zárukami pro činnost orgánů v oblasti trestního práva, pokud by současně existoval široký prostor pro zneužití těchto údajů zpravodajskými službami.

Závěrem lze uvést, že ze zkoumání dotčené problematiky vyplývá potřeba neustálého dialogu o parametrech data retention mezi příslušnými orgány členských států, soudy, dozorovými úřady i nevládními organizacemi. Když se data retention v EU objevila poprvé, šlo o extrémně intrusivní nástroj z hlediska šíře i intenzity dopadů, jelikož rozsah uchovávaných údajů nebyl kompenzován dostatečně přísnými zárukami proti zneužití. Tato podoba data retention se zcela oprávněně potkala s odporem nevládních organizací, dozorových úřadů, ústavních soudů členských států i Soudního dvora. Do jisté míry opačným extrémem však byl striktní přístup Soudního dvora k data retention ve věci *Tele2 Sverige*, který zase nepřiměřeně zasáhl do možnosti členských států zajišťovat bezpečnost v moderním kontextu. Současná judikatura Soudního dvora, zejména rozsudek *La Quadrature du Net* a v něm vyslovený poněkud shovívavější pohled na plošné uchovávání, dokazuje, že zde nadále existuje prostor pro dialog, v rámci kterého budou veškeré dotčené zájmy vyvažovány. K vytvoření alespoň rámcové představy ohledně základních otázek, kterých by se tento dialog měl týkat, snad dopomůže i tato práce. Právě v tom by měla spočívat její přidaná hodnota, bez ohledu na to, zda se čtenář ohledně přípustnosti plošné data retention i po přečtení práce kloní spíše k názoru Soudního dvora než k mému. Jedná se ostatně o otázku, která je bytostně spjata především s tím, kde jsou soukromí a bezpečnost umístěny v hodnotovém žebříčku každého z nás.

SHRNUTÍ

Práce se zabývala ochranou soukromí a osobních údajů v souvislosti s problematikou data retention, tj. v souvislosti povinným uchováváním komunikačních metadat poskytovateli telekomunikačních služeb za účelem případného pozdějšího adresného přístupu k těmto údajům ze strany orgánů členských států činných v oblasti trestního práva a v oblasti zajišťování národní bezpečnosti.

V tomto ohledu si práce kladla tři dílčí cíle. Prvním dílčím cílem bylo posouzení oprávněnosti kritiky, kterou členské státy ve značném počtu a dlouhodobě vznáší vůči velmi striktní judikatuře Soudního dvora v této oblasti a která v poslední době rezonuje také u řady vnitrostátních soudů. Druhým dílčím cílem bylo srovnání přístupu Soudního dvora a ESLP k problematice data retention a posouzení, zda judikatura ESLP nevede z hlediska nalezení rovnováhy mezi ochranou soukromí a osobních údajů a zájmy sledovanými data retention k vyváženějším výsledkům než judikatura Soudního dvora. Pro případ, že by přístup ani jednoho z těchto soudů nebyl shledán ideálním, kladla si práce jako třetí dílčí cíl navrhnout vlastní požadavky na právní úpravy data retention, které by bylo možné považovat za vyvážené, a to jak z hlediska práv na soukromí a ochranu osobních údajů, tak z hlediska veřejného zájmu na potírání trestné činnosti a zajišťování národní bezpečnosti.

Za výše uvedeným účelem byla práce členěna do tří substantivních částí. V první části práce byl popsán a analyzován právní rámec ochrany soukromí a osobních údajů v Evropské unii. Ve vztahu k problematice data retention bylo konstatováno, že povinně uchovávaná komunikační metadata je třeba považovat za osobní údaje ve smyslu příslušné unijní legislativy. Bylo vysvětleno, že tyto údaje vypovídají mnohé o soukromí jednotlivců a v určitých případech mohou mít dokonce povahu citlivých osobních údajů. Již samotné uchovávání údajů je přitom třeba považovat za jejich zpracování, a tudíž i za zásah do práva na soukromí i práva na ochranu osobních údajů. Dále bylo popsáno, jak plošné uchovávání komunikačních metadat naráží na některé základní zásady unijní úpravy ochrany osobních údajů, byť dotčené předpisy zároveň umožňují odchylky ve prospěch cílů, které data retention sleduje. V neposlední řadě byl nastíněn poměrně robustní systém povinností správců, práv subjektů údajů a nezávislého dohledu, který vyplývá z příslušných unijních předpisů a který v souvislosti s data retention dopadá jak na poskytovatele služeb elektronické komunikace, tak na orgány působící v oblasti trestního práva.

Druhá část práce se pak věnovala bližšímu popisu a analýze data retention jakožto účinného nástroje pro zajišťování bezpečnostních zájmů členských států na straně jedné, ale také rozsáhlého zásahu do práva na soukromí a ochranu osobních údajů na straně druhé. V tomto ohledu byly shrnuty a analyzovány hlavní argumenty jejích kritiků i zastánců. Jako klíčová právní otázka z hlediska posuzování přiměřenosti data retention byla určena problematika plošného uchovávání. Ta je nejen podmínkou účinnosti tohoto nástroje, jelikož umožňuje příslušným orgánům „nahlížet do minulosti“, ale také hlavním kamenem úrazu z hlediska jeho proporcionality, jelikož z povahy věci vyžaduje preventivní uchovávání osobních údajů celé evropské populace. Tato část práce se zabývala také směrnicí 2006/24, jejím obsahem i legislativním procesem vedoucím k jejímu přijetí. Přestože tato směrnice byla zrušena Soudním dvorem, zůstávají její pravidla nadále relevantní, jelikož vnitrostátní právní úpravy data retention jsou dodnes vystaveny právě na jejich základě. V tomto ohledu byly popsány a analyzovány hlavní problémy této směrnice, které je z velké míry možné přičíst právě kompromisům v legislativním procesu.

V rámci třetí části práce pak byla analyzována a porovnána judikatura Soudního dvora a ESLP v této oblasti. Co se týče analýzy judikatury Soudního dvora, ta se soustředila na dvě hlavní oblasti – problematiku působnosti unijních předpisů v oblasti data retention a problematiku posuzování proporcionality právních úprav data retention. V rovině působnosti unijních předpisů bylo shledáno, že problematika data retention jako celek neměla spadat do působnosti unijních předpisů přijatých výhradně na základě tehdejšího čl. 95 SES, a tudíž, že mělo být vyhověno žalobě Irska na neplatnost směrnice 2006/24. Jako ještě problematičtější pak bylo shledáno rozšíření působnosti unijního práva i na otázku přístupu příslušných orgánů členských států k uchovávaným údajům, a to včetně orgánů působících v oblasti zajišťování národní bezpečnosti. I když šlo ve značné míře toliko o důsledek zahrnutí problematiky uchovávání do působnosti směrnice 2002/58 (jelikož roviny uchovávání a přístupu je v praxi těžké oddělit), přesto měly být dotčené otázky dle mého názoru spíše ponechány na posouzení ústavních soudů členských států. Ty ostatně v minulosti svou ochotu dohlížet na dodržování základních práv v souvislosti s data retention deklarovaly poměrně jednoznačně.

Co se týče posuzování proporcionality, se Soudním dvorem je třeba souhlasit v tom, že v souvislosti s problematikou data retention je třeba zajistit vysokou úroveň ochrany práv na soukromí a ochranu osobních údajů. Stejně tak nelze namítat nic proti konstatování, že data retention představuje z hlediska počtu dotčených osob výjimečně rozsáhlý zásah do základních práv. Na druhou stranu bylo se Soudním dvorem polemizováno ohledně intenzity tohoto zásahu

co se samotného uchovávání týče, která je dle mého názoru nižší, než jak ji vnímá judikatura Soudního dvora. V práci proto bylo argumentováno ve prospěch přípustnosti tzv. omezené data retention, spočívající v plošném uchovávání údajů, ovšem při zajištění skutečně robustních záruk proti zneužití.

V případě judikatury ESLP je na jedné straně třeba vyzdvihnout, že hromadné uchovávání údajů *a priori* nedémonizuje a soustředí se právě na problematiku záruk proti zneužití. Na druhou stranu, požadavky na tyto záruky však odpovídají funkci ESLP, kterou je zajištění minimálního společného standardu ochrany základních práv v rámci Rady Evropy, a Soudní dvůr by proto měl aspirovat na stanovení standardu vyššího.

V závěru práce proto byly představeny základní parametry z mého pohledu vyvážené právní úpravy data retention. Dle mého názoru by nemělo být vyloučeno plošné uchovávání komunikačních metadat, avšak v případě údajů, jejichž vypovídací hodnota o soukromí osob je vyšší, by měly být lhůty pro uchovávání velmi krátké. Zároveň by měly být stanoveny vysoké požadavky na zabezpečení údajů, zahrnující taktéž povinnost přijmout konkrétní opatření jako např. vedení *logů*. Povolení soudu by mělo být vyžadováno vždy s výjimkou naléhavých případů, přičemž ruku v ruce s tímto požadavkem jde požadavek na důkladné zdůvodňování žádostí o přístup, aby byl *ex ante* soudní přezkum skutečně účinný. Konkrétní by měla být i pravidla pro *ex post* notifikaci dotčených osob. Klíčovým aspektem, který však současná judikatura prakticky vůbec neřeší, by měla být povinnost vést co možná nejpřesnější anonymní statistiky o podaných a vyřízených žádostech, ze kterých by měla být zřejmá povaha a stáří zpřístupněných údajů, povaha vyšetřovaného trestného činu a ideálně i následná úspěšnost vyšetřování. Většina těchto požadavků, zejména požadavek na nezávislý dohled (ideálně v podobě *ex ante* povolování přístupu k údajům), by se dle mého názoru měla uplatnit taktéž v případě přístupu k údajům ze strany zpravodajských služeb.

SUMMARY

This thesis deals with privacy and personal data protection with regards to data retention, i.e. with regards to the obligatory retention of communications metadata by providers of electronic communications services and public communications networks in order to ensure possible future access to such data by the authorities of Member States active in the fields of criminal law and national security.

The thesis set three objectives in this regard. The first objective was to assess the reasonableness of the critique which many of the Member States raised towards the very strict case-law of CJEU in this area and which also resonated with several national courts. The second objective was to compare the case law of CJEU and ECHR with regards to data retention and to assess which provides for better balance between the protection of privacy and personal data and the relevant security interests of the Member States. In the event that the approach of neither of these courts turned out to be ideal, the third objective was to propose a new and better-balanced approach.

To reach these objectives, the thesis is divided into three substantive parts. The first part of the thesis describes and analyzes the legal framework for the privacy and personal data protection in the EU. Several observations with regards to data retention are made in this regard. Firstly, it is shown that the communications metadata are personal data according to EU secondary legislation and may even have the nature of sensitive personal data. Secondly, it is observed that mere retention of such data must be regarded as processing of personal data and therefore as an interference with the right to private life and the right to the protection of personal data. Thirdly, the tensions between the blanket retention of metadata and some basic principles of EU data protection legislation are demonstrated, although it is shown that these principles are not absolute and can be restricted for the purposes of fighting crime and safeguarding national security. Last but not least, it is shown that the EU law provides for rather robust system of controller obligations, data subject rights and independent oversight with regards to storage, transmission and further use of communications metadata.

The second part of the thesis provides for more in-depth description and analysis of data retention concept. Data retention is described as an effective tool for safeguarding the security interests of the Member States, but also as a wide-ranging interference with the privacy and data protection rights. The main arguments of its critics and supporters are then summarized and analyzed. The blanket and indiscriminate nature of the data retention is presented as a key legal

issue, since it is not only a prerequisite for the effectiveness of this instrument (as it allows the competent authorities to 'look into the past'), but also the main problem in terms of its proportionality. The chapter also deals with Directive 2006/24, both its content and the legislative process leading to its adoption. Although the directive has been annulled by CJEU, it is still very much relevant since the data retention legislation of majority of the Member States is still based on it. It is argued that the main issues of the directive are attributable to the compromises in the legislative process.

In the third part of the thesis, the case law of the CJEU and the ECHR is analyzed and compared. Analysis of the CJEU case law focuses on two main areas – the issue of the scope of EU legislation in the field of data retention and the issue of proportionality of blanket data retention.

With regards to the first issue, it is argued that it was wrong to regulate data retention through the secondary law based solely on the former Article 95 of the EC Treaty. Therefore, it is argued that Ireland's action for annulment of Directive 2006/24 should have been successful. The extension of the scope of such legislation to the issue of access to the data by the competent authorities (including in the area of national security) is then considered to be even more problematic. Therefore, it is argued the issue of access should have been left outside of the scope of relevant EC legislation and for the assessment of the constitutional courts of the Member States, which in the past clearly declared their willingness to ensure the protection of fundamental rights in this area.

With regards to the issue of proportionality, there is no arguing with CJEU that high level of protection of privacy and personal data must be ensured with regards to data retention. Similarly, there is no objection to the finding that data retention constitutes an exceptionally wide-ranging interference with fundamental rights, especially in terms of the number of persons concerned. On the other hand, it is argued that the intensity of this interference is in fact lower than CJEU observes. Therefore, the thesis argues in favor of the admissibility blanket retention if genuinely robust guarantees against abuse are provided.

With regards to ECHR case law, it is appreciated that the blanket retention is not *a priori* demonized, and that ECHR focuses on the issue of safeguards against abuse. However, it is shown that the requirements for these safeguards correspond to the main function of the ECHR, which is to ensure a minimum common standard of protection of fundamental rights in the Council of Europe, and therefore it is argued that CJEU should aspire to establish a higher standard.

Since neither the approach of CJEU nor ECHR seems to be ideal, the thesis puts forward its own set of requirements for proportionate data retention. It is argued that the blanket retention should be in principle possible. However, the retention periods must be very short and ideally differentiated for different categories of data based on their predictive value. At the same time, high data security requirements should be laid down, including the obligation to take specific *privacy by design* measures. The prior court authorization should always be required prior to the access to the retained data, except in cases of urgency. Requests for access must be thoroughly reasoned to ensure that the prior judicial review is effective. The rules for *ex post* notification of the persons concerned should also be specific. A key aspect, which the current case law does not address, is the obligation to keep accurate anonymous statistics on submitted and processed requests. These statistics should show the nature and length of retention of the data requested, the nature of the crime under investigation and ideally the success of the investigation. Most of these requirements, in particular the requirement for independent oversight (ideally in the form of *ex ante* authorization of access), should also apply to access to data by intelligence services.

SEZNAM ZKRATEK

BTS	Base Transceiver Station (základnová stanice)
CIA	Central Intelligence Agency (Ústřední zpravodajská služba USA)
GDPR	Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
EU	Evropská unie
ESLP	Evropský soud pro lidská práva
Listina	Listina základních práv Evropské unie
NSA	National Security Agency (Národní bezpečnostní agentura USA)
OECD	Organisation for Economic Co-operation and Development (Organizace pro hospodářskou spolupráci a rozvoj)
PNR	Passenger Name Records (Údaje jmenné evidence cestujících)
SEU	Smlouva o Evropské unii
SES	Smlouva o založení Evropského společenství
SFEU	Smlouva o fungování Evropské unie
SRN	Spolková republika Německo
USA	United States of America (Spojené státy americké)
Úmluva	Úmluva o ochraně lidských práv a základních svobod
Úmluva 108	Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network (Virtuální privátní síť)

SEZNAM POUŽITÝCH ZDROJŮ

MONOGRAFIE A ZÁVĚREČNÉ PRÁCE

GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. New York: Springer International Publishing, 2014. ISBN 978-3-319-05022-5.

FILIPOVÁ, Paula. *The impact of the CJEU case law on the interpretation of the fundamental rights to privacy and data protection*. Diplomová práce. Praha: Karlova univerzita, 2015.

FIODOROVA, Anna. *Information Exchange and EU Law Enforcement*. Oxfordshire: Routledge, 2018. ISBN: 978-0-367-59039-0.

JIROVSKÝ, Lukáš. *Data retention – ukládání provozních a lokalizačních údajů*. Diplomová práce. Praha: Karlova Univerzita, 2015.

KASNECI, Dede. *Data Protection Law: Recent Developments*. Diploma Thesis. Trieste: Università degli studi di Trieste, 2010.

KELLERBAUER, Manuel et. al. *Commentary on EU Treaties and Charter of Fundamental Rights*. Oxford: Oxford University Press, 2019. ISBN: 978-0198794561.

KRÁL, Richard. *Nařízení ES z pohledu jejich vnitrostátní aplikace a implementace*, 2006. Praha: C. H. Beck, 2006. ISBN 80-7179-548-8.

KRÁL, Richard et. al. *Zbytečně zatěžující transpozice – neodůvodněný gold-plating směrnic EU v České republice*. Praha: Univerzita Karlova, 2015. ISBN 978-80-87975-18-3.

LYNSKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015. ISBN 978-019-8718-239.

MÁDR, Petr. *Právo na ochranu osobních údajů dle článku 8 Listiny základních práv Evropské unie*. Diplomová práce. Praha: Karlova univerzita, 2015.

MIKOLASCH, Felix. *Data Retention in the European Union.* Bachelor thesis. Barcelona: Universitat Autònoma de Barcelona, 2019.

NULÍČEK, Michal et al. *GDPR / Obecné nařízení o ochraně osobních údajů – Praktický komentář*. Praha: Wolters Kluwer, 2017. ISBN: 978-80-7552-765-3.

NUTILOVÁ, Helena. *Ochrana osobních údajů*. Disertační práce. Praha: Karlova univerzita, 2012.

PAJUNOJA, Lauri. *The Data Protection Directive on Police Matters 2016/680 protects privacy – The evolution of EU´s data protection law and its compatibility with the right to privacy*. Master Thesis. Helsinky: University of Helsinki, 2017.

RIJPMA, Jorrit J. et al. *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection*. Hague: Eleven International Publishing, 2020. ISBN 978-94-6236-129-4.

STAMPFEL, Gerald. et al. *Data Retention: The EU Directive 2006/24/EC from a Technological Perspective*. Vienna: Medien und Recht Publishing, 2008. ISBN 978-3-900741-53-2.

SENDEN, Hanneke. *Interpretation of Fundamental Rights in a Multilevel Legal System An analysis of the European Court of Human Rights and the Court of Justice of the European Union*. Antwerp: Intersentia, 2011. ISBN 978-17-806-8027-9.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008. ISBN 978-0-674-02772-5.

ŠIMÍČEK, Vojtěch. *Právo na soukromí*. Brno: Mezinárodní politologický ústav Masarykovy univerzity, 2011. ISBN 978-80-210-5449-3.

ZUBIK, Marek et al. *European Constitutional Courts towards Data Retention Laws*. Cham: Springer, 2021. ISSN 2352-1910.

PŘÍSPĚVKY VE SBORNÍCÍCH

BLAS, Diana A. First Pillar and Third Pillar: Need for a Common Approach on Data Protection? In: GUTWIRTH, Serge et al. *Reinventing Data Protection?* Springer, 2009, s. 225-237. ISBN 978-1-4020-9497-2.

DE HERT, Paul a Serge GUTWIRTH. Privacy, data protection and law enforcement: Opacity of the individual and transparency of power. In: CLAES Erik et al. *Privacy and the Criminal Law*. Antwerpen-Oxford: Intersenti, 2006, s. 61-104. ISBN 978-9-05095-545-4.

FURA, Elisabet. The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA. In: CASADEVALL, Joseph et al. *Freedom of Expression – Essays in honour of Nicolas Bratza – President of the European Court of Human Rights*. Tilburg: Wolf Legal Publishers, 2012, s. 463-481. ISBN 978-92-871-7424-6.

KRÁL, Richard. On the Consequences of the Annulment of EU Directives for their Incompability with the EU Charter of Fundamental Rights. In: PÍTROVÁ et al. *Rule of Law and Mechanisms of its Protection Czech Perspective*. Rw&w Science & New Media Passau-Berlin-Prague, 2015, s. 144-151. ISBN 978-3-9816855-4-1.

KOSTA, Eleni. The Retention of Communications Data in Europe and the UK. In: EDWARDS, Lilian et al. *Law, Policy and the Internet*. London: Hart Publishing, 2018, s. 204-207. ISBN 978-18-4946-703-2.

ROBERTS, Hal. The EU Data Retention Directive in an Era of Internet Surveillance. In: DEIBERT, Ronald et al. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge: MIT Press, 2010, s. 35-55. ISBN 978-0-26251-435-4.

VOBOŘIL, Jan. Využívání provozních a lokalizačních údajů ze strany oprávněných orgánů, zejména Policie ČR. In: MYŠKA, Matěj et al. *Data Retention Reloaded: zkušenosti, problémy a aplikační praxe*. Brno: Masaryk Univesity Press, 2013, s. 9-40. ISBN 978-80-210-6722-6.

ČLÁNKY

AZOULAI, Loic a VAN DER SLUIS, Marijn. Institutionalizing personal data protection in times of global institutional distrusts: Schrems. *Common Market Law Review.* 2016, vol. 53, no. 5.

BIGNAMI, Francesca. Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law* [on-line]. 2007, vol. 8, no. 1 [cit. 2021-02-20]. Dostupné z: https://chicagounbound.uchicago.edu/cjil/vol8/iss1/13/

BEDI, Suneal. The Myth of the Chilling Effect. *Kelley School of Business Research Paper* [on-line]. 2021 [cit. 2021-04-19]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3794037

BEIJER, Malu. Active Guidance of Fundamental Rights Protection by the Court of Justice of the European Union: Exploring the Possibilities of a Positive Obligations Doctrine. *Review of European Administrative Law* [on-line]. 2015, vol. 8, no. 2 [cit. 2021-02-20]. Dostupné z: https://www.uitgeverijparis.nl/nl/reader/197175/1001245527

BERNAL, Paul. Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy* [on-line]. 2016, vol. 1, no. 2 [cit. 2021-02-20]. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/23738871.2016.1228990

BIRNHACK, Michael D. The EU Data Protection Directive: An Engine of a Global Regime. *Computer Law & Security Report* [on-line]. 2008, vol. 24, no. 6 [cit. 2020-08-19]. Dostupné z: https://law.bepress.com/cgi/viewcontent.cgi?article=1102&context=taulwps

BREYER, Patrick. Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR. *European Law Journal*. 2005, vol. 11, no. 3.

BROWN, Ian. Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology* [on-line]. 2010, vol. 19, no. 2 [cit. 2021-02-20]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1683284

CAMPBELL, Louise. Judicial Co-operation and Human Rights in Europe after the Treaty of Lisbon: A Twist in the Tale of Two Courts. *Southampton Student Law Review* [on-line]. 2012, vol. 2, no. 2 [cit. 2021-02-20]. Dostupné z: https://www.southampton.ac.uk/~assets/doc/SSLR%20volume%202%20issue%202.pdf

CARUANA, Mireille. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology* [on-line]. 2019, vol. 33, no. 3 [cit. 2020-08-19]. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/13600869.2017.1370224

CELESTE, Edoardo. The Court of Justice and the Ban on Bulk Data Retention. *European Constitutional Law Review* [on-line]. 2019, vol. 15, no. 1 [cit. 2021-02-22]. Dostupné z: http://doras.dcu.ie/24695/

CLARK, Ian. The digital divide in the post-Snowden era. *Journal of Radical Librarianship* [on-line]. 2016, vol. 2 [cit. 2020-08-12]. Dostupné z: https://journal.radicallibrarianship.org/index.php/journal/article/view/12/26

CLARKE, Roger. Data retention as mass surveillance: the need for an evaluative framework. *International Data Privacy Law* [on-line]. 2015, vol. 5, no. 2 [cit. 2020-08-12]. Dostupné z: https://doi.org/10.1093/idpl/ipu036

DEEKS, Ashley. An International Legal Framework for Surveillance. *Virginia Journal of International Law* [on-line]. 2014, vol. 55, no. 2 [cit. 2020-08-12]. Dostupné z: https://www.cs.yale.edu/homes/jf/Deeks.pdf

DE HERT, Paul et. al. The Proposed ePrivacy Regulation: The Commission's and the Parliament's Draft s at a Crossroads? *Brussels Privacy Hub Working Paper* [on-line]. 2020, vol. 6, no. 20 [cit. 2021-02-20]. Dostupné z: https://research.tilburguniversity.edu/en/publications/the-proposed-e-privacy-regulation-the-commissions-and-the-parliam

DOBBS, Mary. Sovereignty, Article 4(2) TEU and the Respect of National Identities: Swinging the Balance of Power in Favour of the Member States? *Yearbook of European Law* [on-line]. 2014, vol. 33, no. 1 [cit. 2021-03-27]. Dostupné z: https://academic.oup.com/yel/article/33/1/298/1683959

CHRISTAKIS, Theodore. A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial thoughts on the Big Brother Watch Judgment. *European Law Blog* [on-line]. 2018 [cit. 2020-12-21]. Dostupné z: https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/

DOUGLAS-SCOTT, Sindhaid. The European Union and Human Rights after the Treaty of Lisbon. *Human Rights Law Review* [on-line]. 2011, vol. 11, no. 1 [cit. 2021-02-20]. Dostupné z: https://www.corteidh.or.cr/tablas/r27635.pdf

FABBRINI, Federico. Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S. *Harvard Human Rights Journal* [on-line]. 2015, vol. 28, no. 1 [cit. 2021-02-20]. Dostupné z: https://heinonline.org/HOL/LandingPage?handle=hein.journals/hhrj28&div=5&id=&page=

FEILER, Lukas. The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection. *European Journal of Law and Technology* [on-line]. 2010, vol. 1, no. 3 [cit. 2021-02-21]. Dostupné z: https://ejlt.org/index.php/ejlt/article/view/29

FENNELLY, David. Data retention: the life, death and afterlife of a directive. *ERA Forum* [on-line]. 2019, vol. 19, no. 5 [cit. 2021-02-21]. Dostupné z: https://link.springer.com/article/10.1007/s12027-018-0516-5

FIEDOROWICZ, Michael. Overview of European State-Sanctioned Mass Surveillance Law. *Chicago Unbound: International Immersion Program Papers* [on-line]. 2019 [cit. 2020-12-15]. Dostupné z: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1104&context=international_immersion_program_papers

GRANGER, Marie-Pierre. The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection. *European Law Review*. 2014, vol. 39, no. 6.

GUILD, Elspeth a CARRERA, Sergio. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. *CEPS Liberty and Security in Europe Papers* [on-line]. 2014, no. 65 [cit. 2020-12-15]. Dostupné z: https://www.ceps.eu/ceps-publications/political-and-judicial-life-metadata-digital-rights-ireland-and-trail-data-retention/

HARAŠTA, Jakub a MÍŠEK Jakub. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie* [on-line]. 2015, vol. 6, no. 12 [cit. 2020-12-15]. Dostupné z: https://journals.muni.cz/revue/article/view/4091/pdf

HUDOBNIK, Matthias. Data protection and the law enforcement directive: a procrustean bed across Europe? *ERA Forum* [on-line]. 2020, no. 21 [cit. 2020-12-15]. Dostupné z: https://link.springer.com/article/10.1007/s12027-020-00645-3

HUSTINX, Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* [on-line]. 2013 [cit. 2020-08-15]. Dostupné z: https://gegevensbeschermingsrecht.nl/onewebmedia/peter.pdf

CHRISTAKIS, Theodore. Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1). *European Law Blog* [on-line], 2021 [cit. 2021-04-15]. Dostupné z: https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/

KOSTA, Eleni. The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection. *SCRIPTed-A Journal of Law, Technology and Society* [on-line]. 2013, vol. 10, no. 3 [cit. 2020-08-12]. Dostupné z: https://script-ed.org/article/luxemburg-national-court-decisions-compatibility-data-retention-directive-rights-privacy-data-protection/

KOPEČKOVÁ, Andrea. Právní povaha cookies. *Epravo.cz* [on-line]. 2015 [cit. 2020-08-12]. Dostupné z: https://www.epravo.cz/top/clanky/pravni-povaha-cookies-98982.html

KRÁL, Richard. Neplatnost směrnic EU a její důsledky pro vnitrostátní transpoziční předpisy. *Jurisprudence*. 2011, č. 1.

KRÁL, Richard a MÁDR, Petr. On the (In)Applicability of the EU Charter of Fundamental Rights to National Measures Exceeding the Requirements of Minimum Harmonisation Directives. *European Law Review.* 2021, vol. 46, no. 1.

KUIJER, Martin. The challenging relationship between the European Convention on Human Rights and the EU legal order: consequences of a delayed accession. *The International Journal of Human Rights* [on-line]. 2020, vol. 24, no. 7 [cit. 2020-02-20]. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/13642987.2018.1535433

KUNER, Christopher et. al. An unstoppable force and an immoveable object? EU data protection law and national security. *International Data Privacy Law* [on-line]. 2018, vol. 8, no. 1 [cit. 2021-03-27]. Dostupné z: https://academic.oup.com/idpl/article/8/1/1/4980995?login=true

LEISER, Mark a CUSTERS, Bart. The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680. *European Data Protection Law Review* [on-line]. 2019, vol. 5, no. 3 [cit. 2020-08-12]. Dostupné z: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl5&div=55&id=&page

LENAERTS, Koen a GUTIÉREZ-FONS, José A. The constitutional allocation of powers and general principles of EU law. *Common Market Law Review*. 2010, vol. 47, no. 6.

LETSAS, George. *The ECHR as a Living Instrument: Its Meaning and its Legitimacy* [on-line]. 2012. [cit. 2020-08-15]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2021836

LYNSKEY, Orla. The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland. *Common Market Law Review* [on-line]. 2013, vol. 51, no. 6 [cit. 2021-02-20]. Dostupné z: https://heinonline.org/HOL/LandingPage?handle=hein.kluwer/cmlr0051&div=150&id=&page=

McGOLDRICK, Dominic. A defence of the margin of appreciation and an argument for its application by the human rights committee. *International & Comparative Law Quarterly* [on-line]. 2016, vol. 65, no. 1 [cit. 2020-08-15]. Dostupné z: https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/a-defence-of-the-margin-of-appreciation-and-an-argument-for-its-application-by-the-human-rights-committee/6A693A1ED9BEF835D17E5B90747F5353

MURRAY, Daragh. Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review* [on-line]. 2019, vol. 52, no. 6 [cit. 2020-09-19]. Dostupné z: https://www.hrbdt.ac.uk/download/bulk-surveillance-in-the-digital-age-rethinking-the-human-rights-law-approach-to-bulk-monitoring-of-communications-data/

MYŠKA, Matěj. Aktuální otázky data retention. *Revue pro právo a technologie* [Online]. 2010, roč. 1, č. 1. [cit. 2020-09-19]. Dostupné z: https://journals.muni.cz/revue/article/view/3976

NI LOIDEAIN, Nora. EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era. *Media and Communication* [Online]. 2015, vol. 3, no. 2. Dostupné z: https://www.cogitatiopress.com/mediaandcommunication/article/view/297

NIMMER, Melville B. The Right of Publicity. *Law and Contemporary Problems* [on-line]. 1954, vol. 19, no. 2. Dostupné z: https://www.tandfonline.com/doi/abs/10.1080/10811680.2020.1805957?journalCode=hclw20

O'LEARY, Síofra. A Tale of Two Cities: Fundamental Rights Protection in Strasbourg and Luxembourg. *Cambridge Yearbook of European Legal Studies* [on-line]. vol. 20 [cit. 2021-02-22]. Dostupné z: https://www.cambridge.org/core/journals/cambridge-yearbook-of-european-legal-studies/article/abs/tale-of-two-cities-fundamental-rights-protection-in-strasbourg-and-luxembourg/9C1ED7519B72024CF07EF0433A104808

PAPAKONSTANTINOU, Vagelis a DE HERT, Paul. The amended EU law on eprivacy and electronic communications after its 2011 implementation; new rules on data protection, spam, data breaches and protection of intellectual property rights. *Marshall Journal of Computer and Information Law* [on-line]. 2011, vol. 21, no. 1 [cit. 2021-02-20]. Dostupné z: https://repository.law.uic.edu/jitpl/vol29/iss1/2/

PEERS, Steve. The European Parliament and data retention: Chronicle of a 'sell-out' foretold? *Statewatch* [on-line]. 2005 [cit. 2021-02-21]. Dostupné z: https://www.statewatch.org/media/documents/news/2005/dec/sp_dataret_dec05.pdf

PENNEY, W. Internet surveillance, regulation, and chilling effects online: a comparative case study. *Internet Policy Review* [on-line]. 2017, vol. 6, no. 2 [cit. 2021-02-19]. Dostupné z: https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case

QUINTEL, Teresa. Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive. *European Data Protection Law Review* [on-line]. 2018, vol. 4, no. 1 [cit. 2021-02-19]. Dostupné z: https://edpl.lexxion.eu/article/EDPL/2018/1/15

RAUHOFER, Judith. Just Because You're Paranoid, Doesn't Mean They're Not after You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union. *SCRIPTed: Journal of Law, Technology and Society* [on-line]. 2006, vol. 3, no. 4 [cit. 2021-02-20]. Dostupné z: https://www.research.ed.ac.uk/portal/files/18457455/Rauhofer_Just_Because_You_re_Paranoid.pdf

ROBERTS, Andrew. Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications. *Modern Law Review* [on-line]. 2015, vol. 78, no. 3. Dostupné z: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2230.12127

ROBINSON, Neil et. al. *Review of EU Data Protection Directive: Summary* [on-line]. 2009 [cit. 2021-02-19]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf

SAJFERT, Juraj a QUINTEL, Teresa. *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities* [on-line]. 2017 [cit. 2021-02-19]. Dostupné z: https://doi.org/10.1080/13600869.2017.1370224

SARRE, Rick. Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia. *Asian Journal of Criminology* [on-line]. 2017, no. 12 [cit. 2021-02-19]. Dostupné z: https://link.springer.com/article/10.1007/s11417-017-9256-7

SERVENT, Ariadna Ripoll. Holding the European Parliament responsible: policy shift in the Data Retention Directive from consultation to codecision. *Journal of European Public Policy* [on-line]. 2013, vol. 20, no. 7 [cit. 2021-02-21]. Dostupné z: https://www.tandfonline.com/doi/abs/10.1080/13501763.2013.795380?journalCode=rjpp2

SPINA, Alessandro. Risk Regulation of Big Data: Has the Time Arrived for a paradigm Shift in EU Data Protection Law? *European Journal of Risk Regulation* [on-line]. 2014, vol. 5, no. 2 [cit. 2021-02-21]. Dostupné z: https://doi.org/10.1017/S1867299X0000369X

WARREN, Samuel D. a BRANDEIS, Luis. Right to Privacy. *Harvard Law Review* [on-line]. 1890, vol. 4, no. 5 [cit. 2020-08-15]. Dostupné z: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

WHITLEY, Edgar a HOSEIN, Ian. Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy* [on-line]. 2005, vol. 29, no. 11 [cit. 2020-08-15]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0308596105000923

VAINIO, Niklas. Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States. *International Journal of Law and Information Technology* [on-line]. 2015, vol. 23, no. 3 [cit. 2020-08-15]. Dostupné z: https://academic.oup.com/ijlit/article/23/3/290/783843

VAN EIJK, Rob. Schrems II: Article 49 derogations may not be so narrow and restrictive after all? *Future of Privacy Forum* [on-line]. 2021 [cit. 2021-03-27]. Dostupné z: https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all/

VOBOŘIL, J. Ústavní soud posvětil plošné sledování elektronické komunikace. *Lupa.cz* [on-line]. 2019 [cit. 2021-03-27]. Dostupné z: https://www.lupa.cz/clanky/ustavni-soud-posvetil-plosne-sledovani-elektronicke-komunikace/

WAHL, Thomas. CJEU: Data Retention Allowed in Exceptional Cases. *Eucrim* [on-line]. 2020, no. 3 [cit. 2021-02-21]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2020-03.pdf

WALKER, Claire. Data retention in the UK: Pragmatic and proportionate, or a step too far? *Computer Law & Security Review* [on-line]. 2009, vol. 25, no. 4 [cit. 2021-02-21]. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0267364909001009

WHELANOVÁ, Markéta. Implementace přímo použitelných nařízení Evropské unie do českého právního řádu. *Správní právo* [on-line]. 2019, roč. LII, č. 6 [cit. 2021-03-27]. Dostupné z: https://www.mvcr.cz/soubor/sp-6-19-whelanova-pdf.aspx

ZELGER, Bernadette. EU Competition law and extraterritorial jurisdiction – a critical analysis of the ECJ's judgement in Intel. *European Competition Journal* [on-line]. 2020, vol. 16, no. 2-3

[cit. 2021-03-27]. Dostupné z: https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1840844

JUDIKATURA

Evropský soud pro lidská práva

Rozsudek ESLP ze dne 6. září 1978, *Klass a další proti Německu*, stížnost č. 5029/71, CE:ECHR:1978:0906JUD000502971.

Rozsudek ESLP ze dne 22. října 1981, *Dudgeon v. Spojené království*, stížnost č. 7525/76, CE:ECHR:1981:1022JUD000752576.

Rozsudek ESLP ze dne 25. března 1983, *Silver a další v. Spojené království*, stížnosti č. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, CE:ECHR:1983:0325JUD000594772.

Rozsudek ESLP ze dne 2. srpna 1984, *Malone proti Spojenému království*, stížnost č. 8691/79, CE:ECHR:1984:0802JUD000869179.

Rozsudek ESLP ze dne 16. prosince 1992, *Niemetz v. Německo*, stížnost č. 13710/88, CE:ECHR:1992:1216JUD001371088.

Rozsudek ESLP ze dne 28. ledna 2003, *Peck proti Spojenému království*, stížnost č. 44647/98, CE:ECHR:2003:0128JUD004464798.

Rozhodnutí ESLP ze dne 29. června 2006, *Weber a Saravia proti Německu*, stížnost č. 54934/00, CE:ECHR:2006:0629DEC005493400.

Rozsudek ESLP ze dne 22. května 2008, *Stefanov proti Bulharsku*, stížnost č. 65755/01, CE:ECHR:2008:0522JUD006575501.

Rozsudek ESLP ze dne 2. prosince 2008, *K.U. proti Finsku*, stížnost č. 2872/02, CE:ECHR:2008:1202JUD000287202.

Rozsudek ESLP ze dne 4. prosince 2008, *S. a Marper proti Spojenému království*, stížnosti č. 30562/04 a 30566/04, CE:ECHR:2008:1204JUD003056204.

Rozsudek ESLP ze dne 10. února 2009, *Iordachii a další proti Moldavsku*, stížnost č. 25198/02, CE:ECHR:2009:0210JUD002519802.

Rozsudek ESLP ze dne 1. července 2014, *S.A.S. v. Francie*, stížnost. č. 43835/11, CE:ECHR:2014:0701JUD004383511.

Rozsudek ESLP ze dne 4. prosince 2015, *Zakharov proti Rusku*, stížnost č. 47143/06, CE:ECHR:2015:1204JUD004714306.

Rozsudek ESLP ze dne 12. ledna 2016, *Szabó a Vissy proti Maďarsku*, stížnost č. 37138/14, CE:ECHR:2016:0112JUD003713814.

Rozsudek ESLP ze dne 5. září 2017, *Bărbulescu v. Rumunsko,* stížnost č. 61496/08, CE:ECHR:2017:0905JUD006149608.

Rozsudek ESLP ze dne 19. října 2017, *Lebois v. Bulharsko*, stížnost č. 67482/14, CE:ECHR:2017:1019JUD006748214.

Rozsudek ESLP ze dne 19. června 2018 ve věci *Centrum för Rättvisa v. Švédsko*, stížnost č. 35252/08, CE:ECHR:2018:0619JUD003525208.

Rozsudek ESLP ze dne 24. července 2018, *Benedik proti Slovinsku*, stížnost č. 62357/14, CE:ECHR:2018:0424JUD006235714.

Rozsudek ESLP ze dne 13. září 2018 ve věci *Big Brother Watch v. Spojené království*, stížnosti č. 58170/13, 62322/14, a 24960/15, CE:ECHR:2018:0913JUD005817013.

Rozsudek ESLP ze dne 25. června 2019, *Nicolae Virgiliu Tănase v. Rumunsko*, stížnost č. 41720/13, CE:ECHR:2019:0625JUD004172013.

Rozsudek ESLP ze dne 31. října 2019, *Vučina v. Chorvatsko*, stížnost č. 58955/13, CE:ECHR:2019:0924DEC005895513.

Rozsudek ESLP ze dne 14. ledna 2020, *Beizaras and Levickas v. Litva*, stížnost č. 41288/15, CE:ECHR:2020:0114JUD004128815.

Rozsudek ESLP ze dne 30. ledna 2020, *Breyer proti Německu*, stížnost č. 50001/12, CE:ECHR:2020:0130JUD005000112.

Rozhodnutí ESLP ze dne 12. května 2020, *Ringler proti Rakousku*, stížnost č. 2309/10, CE:ECHR:2020:0512DEC000230910.

Rozhodnutí ESLP ze dne 29. září 2020, *Tretter a další proti Rakousku*, stížnost č. 3599/10, CE:ECHR:2020:0929DEC000359910.

Soudní dvůr Evropské unie

Rozsudky a posudky

Posudek Soudního dvora ze dne 18. prosince 2014, 2/13, EU:C:2014:2454.

Rozsudek Soudního dvora ze dne 23. května 2003, *Österreichischer Rundfunk a další*, spojené věci C 465/00, C-138/01 a C-139/01, EU:C:2003:294.

Rozsudek Soudního dvora ze dne 12. června 2003, *Schmidberger*, C-112/00, EU:C:2003:333.

Rozsudek Soudního dvora ze dne 10. července 2003, *Hydro Seafood*, spojené věci C-20/00 a C-64/00, EU:C:2003:397.

Rozsudek Soudního dvora ze dne 6. listopadu 2003, *Lindqvist*, C-101/01, EU:C:2003:596.

Rozsudek Soudního dvora ze dne 30. května 2006, *Parlament v. Rada a Komise*, C-317/04 a C-318/04, EU:C:2006:34.

Rozsudek Soudního dvora ze dne 3. května 2007, *Advocaten voor de Wereld*, C-303/05, EU:C:2007:261.

Rozsudek Soudního dvora ze dne 29. ledna 2008, *Promusicae*, C-275/06, EU:C:2008:54.

Rozsudek Soudního dvora ze dne 16. prosince 2008, *Satakunnan Markkinapörssi a Satamedia*, C-73/07, EU:C:2008:727.

Rozsudek Soudního dvora ze dne 10. února 2009, *Irsko v. Parlament a Rada*, C-301/06, EU:C:2009:6.

Rozsudek Soudního dvora ze dne 26. listopadu 2009, *Komise v. Irsko*, C-202/09, EU:C:2009:736.

Rozsudek Soudního dvora ze dne 26. listopadu 2009, *Komise v. Řecko*, C-211/09, EU:C:2009:7.

Rozsudek Soudního dvora ze dne 4. února 2010, *Komise v. Švédsko*, C-185/09, EU:C:2010:59.

Rozsudek Soudního dvora ze dne 29. června 2010, *Bavarian Lager*, C-28/08 P, EU:C:2010:378.

Rozsudek Soudního dvora ze dne 29. července 2010, *Komise v. Rakousko*, C-189/09, EU:C:2010:455.

Rozsudek Soudního dvora ze dne 28. února 2012, *Inter-Environnement Wallonie a Terre wallonne*, C-41/11, EU:C:2012:103.

Rozsudek Soudního dvora ze dne 30. května 2013, *Komise v. Švédsko*, C-270/11, EU:C:2013:339.

Rozsudek Soudního dvora ze dne 4. června 2013, *ZZ*, C-300/11, EU:C:2013:363.

Rozsudek Soudního dvora ze dne 8. dubna 2014, *Digital Rights Ireland a Seitlinger a další*, spojené věci C-293/12 a C-594/12, EU:C:2014:238.

Rozsudek Soudního dvora ze dne 30. dubna 2014, *UPC DTH*, C-475/12, EU:C:2014:285.

Rozsudek Soudního dvora ze dne 13. května 2014, *Google Spain a Google*, C-131/12, EU:C:2014:317.

Rozsudek Soudního dvora ze dne 6. října 2015, *Schrems*, C-362/14, EU:C:2015:650.

Rozsudek Soudního dvora ze dne 19. října 2016, *Breyer*, C-582/14, EU:C:2016:779.

Rozsudek Soudního dvora ze dne 21. prosince 2016, *Tele2 Sverige a Watson a další*, spojené věci C-203/15 a C-698/15, EU:C:2016:970.

Posudek Soudního dvora ze dne 26. července 2017, 1/15, EU:C:2017:592.

Rozsudek Soudního dvora ze dne 20. prosince 2017, *Nowak*, C-434/16, EU:C:2017:994.

Rozsudek Soudního dvora ze dne 5. června 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388.

Rozsudek Soudního dvora ze dne 10. července 2018, *Jehovan Todistajat*, C-25/17, EU:C:2018:551.

Rozsudek Soudního dvora ze dne 2. října 2018, *Ministerio Fiscal*, EU:C:2018:788.

Rozsudek Soudního dvora ze dne 14. února 2019, *Buivids*, C-345/17, EU:C:2019:122

Rozsudek Soudního dvora z 20. března 2019, *Komise v. Rakousko*, C-187/16, EU:C:2018:194

Rozsudek Soudního dvora ze dne 29. července 2019, *Fashion ID*, C-40/17, EU:C:2019:629.

Rozsudek Soudního dvora ze dne 11. prosince 2019, *Asociaiția de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064.

Rozsudek Soudního dvora ze dne 9. července 2020, *Land Hessen*, C-272/19, EU:C:2020:535.

Rozsudek Soudního dvora ze dne 2. dubna 2020, *Komise v. Polsko, Maďarsko a Česká republika*, spojené věci C-715/17, C-718/17 and C-719/17, EU:C:2020:257.

Rozsudek Soudního dvora ze dne 16. července 2020, *Facebook Ireland a Schrems*, C-311/18, EU:C:2020:559.

Rozsudek Soudního dvora ze dne 6. října 2020, *Privacy International*, EU:C:2020:790.

Rozsudek Soudního dvora ze dne 6. října 2020, *La Quadrature du Net a další*, spojené věci C-511/18, C-512/18 a C-520/18, EU:C:2020:791.

Rozsudek Soudního dvora ze dne 11. listopadu 2020, *Orange Romania*, C-61/19, EU:C:2020:90.

Rozsudek Soudního dvora ze dne 2. března 2021, *Prokuratuur*, C-746/18, EU:C:2021:152.

Stanoviska generálních advokátů

Stanovisko generálního advokáta Tizzana ze dne 14. listopadu 2002 ve spojených věcech *Österreichischer Rundfunk a další*, C-465/00, C-138/01 a C-139/01, EU:C:2002:662.

Stanovisko generálního advokáta Tizzana ze dne 19. září 2002 ve věci *Lindqvist*, C-101/01, C:2002:513.

Stanovisko generálního advokáta Légera ze dne 22. listopadu 2005 ve spojených věcech *Parlament v. Rada a Komise*, C-317/04 a C-318/04, EU:C:2005:710.

Stanovisko generálního advokáta Cruze Villalóna ze dne 12. prosince 2013 ve spojených věcech *Digital Rights Ireland a Seitlinger a další*, C-293/12 a C-594/12, EU:C:2013:845.

Stanovisko generálního advokáta Saaugmansgaarda Øe ze dne 19. července 2016 ve spojených věcech *Tele2 Sverige a Watson a další*, C-203/15 a C-698/15, EU:C:2016:572.

Stanovisko generálního advokáta Saaugmansgaarda Øe ze dne 19. prosince 2019 ve věci *Facebook Ireland a Schrems*, C-311/18, EU:C:2019:1145.

Stanovisko generálního advokáta Campos Sánchez-Bordony ze dne 15. ledna 2020 ve věci *Privacy International,* C-623/17, EU:C:2020:5.

Stanovisko generálního advokáta Campos Sánchez-Bordony ze dne 15. ledna 2020 ve spojených věcech *La Quadrature du Net a další*, C-511/18 a C-512/18, EU:C:2020:6.

Stanovisko generálního advokáta Campos Sánchez-Bordony ze dne 15. ledna 2020 věci *Ordre des barreaux francophones a germanophone a další*, C-520/18, EU:C:2020:7.

Ústavní soud České republiky

Nález Ústavního soudu ze dne 22. března 2011, Pl. ÚS 24/10

Nález Ústavního soudu ze dne 14. května 2019, sp. zn. Pl. ÚS 45/17

OSTATNÍ ZDROJE

Commission of the European Communities. *Community Policy on Data Processing*, 1973. SEC(73)4300 final.

Council of Europe. *Council of Europe Committee of Ministers Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector*, 1987.

Council of the European Union. *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Progress report*, 2019, 9351/19.

Council of the European Union. *Retention of electronic communication data - next steps* [on-line]. 2017, 6713/17 [cit. 2021-02-25]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-6713-2017-INIT/en/pdf

Council of the European Union. *Data retention – State of play* [on-line]. 2018, 14319/18 [cit. 2021-02-25]. Dostupné z: https://www.statewatch.org/media/documents/news/2018/dec/eu-council-data-ret-state-of-play-14319-18.pdf

Council of the European Union. *Working document – Data retention – Contributions by delegations* [on-line]. 2017, 9374/2017 REV 1 [cit. 2021-02-25]. Dostupné z: https://www.statewatch.org/media/documents/news/2017/dec/eu-council-ms-papers-data-retention-eprivacy-reg-wk-9374-17-rev1.pdf

Council of the European Union. *Data retention – preparation of Council debate* [on-line]. 2017, 14068/17 [cit. 2021-02-25]. Dostupné z: https://www.statewatch.org/media/documents/news/2017/nov/eu-council-data-retention-14068-17.pdf

Eurojust. *Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15 – Report* [on-line]. 2017, 10098/17 [cit. 2021-02-25]. Dostupné z: https://www.statewatch.org/media/documents/news/2017/nov/eu-eurojust-data-retention-MS-report-10098-17.pdf

European Commission. *Commission communication on the protection of individuals in relation to the processing of personal data in the Community and information security*, 1990. COM/90/314FINAL.

European Commission. *Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data – Explanatory memorandum*, 1990, SYN 287.

European Commission. *Proposal for a Council directive concerning the protection of personal data and privacy in the context of public digital telecomunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks – Explanatory memorandum*, 1990, SYN 288.

European Commission. *Opinion of the Commission pursuant to Article 251 (2), third subparagraph, point (c) of the EC Treaty, on the European Parliament's amendments to the Council's common position regarding the proposal for a Directive of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector amending the proposal of the Commission pursuant to Article 250 (2) of the EC Treaty* [on-line]. 2002, 52002PC0338 [cit. 2021-02-25]. Dostupné z: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002PC0338:EN:HTML

European Commission. *Data Retention for law enforcement purposes – Final report* [on-line] 2020 [cit. 2021-02-20]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1

European Court of Human Rights. *Guide on Article 8 of the Convention – Right to respect for private and family life*. Strasbourg: Council of Europe, 2020.

European Court of Human Rights. *Mass Surveillance Factsheet*, 2020.

European Data Protection Board. *Guidelines 05/2020 on consent under Regulation 2016/679* 2020.

European Data Protection Board. *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, 2020.

European Digital Rights. *Shadow evaluation report on the Data Retention Directive (2006/24/EC)* [on-line], 2011 [cit. 2021-02-25]. Dostupné z: https://edri.org/files/shadow_drd_report_110417.pdf

European Parliament. *Resolution of the European Parliament on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing*, 1975. OJ C100/27.

European Parliament. *Resolution of the European Parliament of 8 April 1976 on the protection of the right of the individual in the face of developing technical progress in the field of automatic data processing*, 1976. OJ C140/34.

European Parliament, *Resolution of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing*, 1979.

Europol. *Data categories to be retained for law enforcement purposes – Working paper* [on-line]. 2017, WK 5380/2017 INIT [cit. 2021-02-25]. Dostupné z: https://www.statewatch.org/media/documents/news/2018/feb/eu-council-data-retention-europol-data-to-be-retained-wk-5380-17-censored.pdf

European Union Agency for Fundamental Rights and Council of Europe. *Handbook on European data protection law 2018 edition* [on-line]. 2018 [cit. 2021-02-25]. Dostupné z: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

Evropská komise. *Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)*, 2017. COM/2017/010 final.

Evropská komise. *Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) – důvodová zpráva*, 2012. COM/2012/011 final.

Fundamental Rights Agency. *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*. Luxembourg: Publications Office of the European Union, 2017.

OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

OECD. *Revised OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013.

Office of the High Commissioner for Human Rights. *The right to privacy in the digital age: report*, 2018. A/HRC/39/29.

Pracovní skupina pro ochranu údajů zřízená podle čl. 29 směrnice 95/46. *Stanovisko č. 4/2007 k pojmu osobní údaje*, 2007. 01248/07/CS.

Rada Evropské unie. *Návrh nařízení o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích*) – *mandát Rady*, 2021. 6087/21.

OCHRANA SOUKROMÍ A OSOBNÍCH ÚDAJŮ V PRÁVU EVROPSKÉ UNIE S OHLEDEM NA PROBLEMATIKU DATA RETENTION

ABSTRAKT

Práce se zabývá ochranou soukromí a osobních údajů v právu Evropské unie s ohledem na problematiku data retention, tedy problematiku uchovávání komunikačních metadat poskytovateli telekomunikačních služeb za účelem případného pozdějšího adresného přístupu k těmto údajům ze strany orgánů státu. Práce se věnuje nejen rozboru unijních právních předpisů v této oblasti, ale především analýze související judikatury Soudního dvora, která tato pravidla významným způsobem dotváří. V rámci této analýzy se autor soustředí na dvě zásadní právní otázky v této judikatuře řešené – problematiku působnosti unijních právních předpisů v této oblasti a problematiku posuzování proporcionality právních úprav data retention. Co se týče první zmiňované otázky, poukazuje autor na z jeho pohledu příliš extenzivní výklad působnosti relevantních unijních předpisů zastávaný Soudním dvorem. Nejvíce problematickou shledává autor skutečnost, že Soudní dvůr vztáhl předpisy přijaté na tehdejším článku 95 SES také na problematiku přístupu orgánů členských států k uchovávaným údajům, a to včetně orgánů členských států působících v oblasti zajišťování národní bezpečnosti. Co se týče otázky posuzování proporcionality, kritizuje autor především skutečnost, že Soudní dvůr považuje za neslučitelné s unijním právem plošné uchovávání komunikačních metadat jako takové, bez ohledu na to, jak přísné záruky proti zneužití členské státy stanoví. Tento z pohledu autora příliš striktní přístup Soudního dvora je následně porovnáván s přístupem Evropského soudu pro lidská práva, který je v daném ohledu shovívavější. Avšak ani přístup Evropského soudu pro lidská práva není hodnocen jako ideální, zejména vzhledem k nižším požadavkům na záruky proti zneužití. Autor proto v závěru práce představuje vlastní požadavky na právní úpravy data retention, které dle jeho názoru vedou k nalezení odpovídající rovnováhy mezi právy na soukromí a ochranu osobních údajů na straně jedné, a bezpečnostními zájmy členských států na straně druhé.

KLÍČOVÁ SLOVA

Data retention; komunikační metadata; provozní a lokalizační údaje; ochrana soukromí; ochrana osobních údajů; GDPR; směrnice 2002/58; směrnice 2016/680.

PROTECTION OF PRIVACY AND PERSONAL DATA IN EUROPEAN UNION LAW WITH REGARDS TO DATA RETENTION

ABSTRACT

The thesis deals with the issue of data retention, i.e. the issue of storing communications metadata by telecommunications service providers for the purpose of possible later access to this data by state authorities. The thesis focuses not only on the relevant EU legislation, but also on the related case law of the Court of Justice, which plays crucial role in determining the standard of protection offered by EU law. This analysis focuses on two main legal issues – the issue of scope of the EU legislation in this area and the issue of proportionality. With regards to the first issue, the author is of the opinion that the Court of Justice interprets the scope of the relevant EU legislation overly broadly. Author criticizes the fact that the Court of Justice applied secondary law adopted on the basis of Article 95 TEC on the issue of access to the retained data by the Member States authorities, including the authorities of Member States which are active in the field of national security. Regarding the issue of proportionality, author criticizes the fact that the Court of Justice perceives the blanket retention of communications metadata to be incompatible with EU law as such, no matter how strict the safeguards against abuse the Member States lay down. This too strict of an approach of the Court of Justice is then compared with the approach of the European Court of Human Rights, which is more lenient in this respect. However, neither the approach of the European Court of Human Rights is considered ideal, mostly due to the lower requirements for safeguards against abuse. Therefore, the author presents his own requirements for data retention legislation, which in his opinion lead to finding a better balance between the rights to privacy and personal data protection on the one hand and the security interests of Member States on the other.

KEY WORDS

Data retention; communications metadata; traffic and location data; privacy; personal data protection, GDPR, directive 2002/58; directive 2016/680.