



**RADA  
EVROPSKÉ UNIE**

**Brusel 19. dubna 2011 (02.05)  
(OR. en)**

**9324/11**

**DAPIX 38  
TELECOM 47  
COPEN 85**

**PRŮVODNÍ POZNÁMKA**

---

Odesílatel: Jordi AYET PUIGARNAU, ředitel,  
za generální tajemnici Evropské komise  
Datum přijetí: 18. dubna 2011  
Příjemce: Pierre de BOISSIEU, generální tajemník Rady Evropské unie  
Č. dok. Komise: KOM(2011) 225 v konečném znění  
Předmět: Zpráva Komise Radě a Evropskému parlamentu  
Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)

---

Delegace naleznou v příloze dokument Komise KOM(2011) 225 v konečném znění.

---

Příloha: KOM(2011) 225 v konečném znění



EVROPSKÁ KOMISE

V Bruselu dne 18.4.2011  
KOM(2011) 225 v konečném znění

**ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU**

**Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)**

# ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU

## Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES)

### 1. ÚVOD

Směrnice o uchovávání údajů<sup>1</sup> (dále jen „směrnice“) vyžaduje, aby členské státy uložily povinnost poskytovatelům veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (dále jen „poskytovatelé“) uchovávat provozní a lokalizační údaje po dobu šesti měsíců až dvou let pro účely vyšetřování, odhalování a stíhání závažných trestných činů.

Tato zpráva Komise hodnotí v souladu s článkem 14 směrnice, jak je směrnice uplatňována členskými státy a její dopad na hospodářské subjekty a spotřebitele, přičemž se bere v potaz další vývoj elektronických komunikačních technologií a statistické údaje dodané Komisí, přičemž cílem je určit, zda je nutné změnit ustanovení této směrnice, zejména co se týče údajů, na které se vztahuje, a dob uchovávání. Tato zpráva vzhledem ke kritice, které je obecně uchovávání údajů podrobováno, rovněž posuzuje dopady směrnice na základní práva a otázku, zda je nutné reagovat opatřeními na problémy související s používáním anonymních SIM karet pro účely trestné činnosti<sup>2</sup>.

Hodnocení celkově prokázalo, že v EU je uchovávání údajů hodnotným nástrojem pro systémy trestního soudnictví a pro prosazování práva. Směrnice přinesla omezený příspěvek k harmonizaci uchovávání údajů, pokud jde například o účelové omezení, doby uchovávání a rovněž i o oblast náhrad nákladů, jež vznikají poskytovatelům, která nespadá do působnosti směrnice. EU by i nadále měla pomocí společných pravidel zajišťovat, aby byly soustavně dodržovány přísné normy pro ukládání, vyhledávání a používání provozních a lokalizačních údajů vzhledem k dopadům a rizikům, která z těchto činností vyplývají pro vnitřní trh a respektování práva na soukromí a ochranu osobních údajů. S ohledem na tyto závěry zamýšlí Komise navrhnout změny směrnice, které budou vycházet z hodnocení dopadů.

### 2. ZÁKLADY PRO HODNOCENÍ

Údaje pro tuto hodnotící zprávu pochází z rozsáhlých diskuzí s členskými státy, odborníky a zúčastněnými stranami a jimi poskytnutých příspěvků.

---

<sup>1</sup> 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, Úř. věst. L 105, 13.4.2006, s. 54-63.

<sup>2</sup> Závěry Rady Evropské unie o boji proti zneužívání elektronických komunikací a jejich anonymity pro účely trestné činnosti, 2908. zasedání Rady ve složení pro spravedlnost a vnitřní věci – Brusel, 27—28. listopadu 2008.

V květnu 2009 pořádala Komise konferenci na téma blížího hodnocení směrnice o uchování údajů (s názvem Towards the Evaluation of the Data Retention Directive), které se účastnili zástupci orgánů na ochranu údajů, soukromého sektoru, občanské společnosti a akademických kruhů. V září 2009 zaslala Komise dotazník zúčastněným osobám z těchto skupin, na který obdržela zhruba 70 odpovědí<sup>3</sup>. S cílem sdílet předběžná hodnocení směrnice a diskutovat o budoucích úkolech v této oblasti pořádala Komise v prosinci 2010 druhou konferenci týkající se směrnice (s názvem Taking on the Data Retention Directive), které se účastnil obdobný vzorek zúčastněných osob.

V období mezi říjnem 2009 a březnem 2010 měla Komise schůzku se zástupci všech členských států a přidružených zemí Evropského hospodářského prostoru k detailnímu projednání otázek uvedených v dotazníku, které se dotýkaly uplatňování směrnice. Členské státy započaly s uplatňováním směrnice později, než se očekávalo, a to zejména pokud jde o údaje týkající se internetu. Zpoždění při provádění směrnice do vnitrostátního práva zapříčinila, že úplné statistické údaje buď za rok 2008 nebo 2009, vyžadované článkem 10 směrnice mohlo Komisi dodat devět členských států, ačkoliv celkově devatenáct členských států dodalo částečné statistické údaje (viz oddíl 4.7). Komise si v červenci 2010 písemně od členských států vyžádala další kvalitativní a kvantitativní informace ohledně nezbytnosti uchovávaných údajů pro dosažení výsledků v oblasti prosazování práva. Deset členských států v odpovědi poskytlo podrobnosti týkající se konkrétních případů, u kterých se prokázalo nezbytné uchovávat údaje<sup>4</sup>.

Tato zpráva čerpá ze stanovisek přijatých v rámci Platformy pro elektronické uchování dat za účelem vyšetřování, odhalování a stíhání závažných trestných činů od jejího vytvoření v roce 2008<sup>5</sup>. Komise zohlednila zprávy pracovní skupiny pro ochranu údajů zřízené podle článku 29<sup>6</sup>, zejména zprávu o druhé donucovací akci, tj. její hodnocení, jak členské státy dodržují požadavky na ochranu a bezpečnost údajů stanovené ve směrnici<sup>7</sup>.

---

<sup>3</sup> Odpovědi jsou zveřejněny na internetové stránce Komise ([http://ec.europa.eu/home-affairs/news/consulting\\_public/consulting\\_0008\\_en.htm](http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm)).

<sup>4</sup> Belgie, Česká republika, Kypr, Litva, Maďarsko, Nizozemsko, Polsko, Slovinsko a Spojené království. Švédsko také dodalo údaje o několika případech konkrétní závažné trestné činnosti, u kterých byly historické provozní údaje zásadní pro odsouzení, ačkoliv neexistovala povinnost uchovávat údaje.

<sup>5</sup> Tato expertní skupina byla vytvořena podle rozhodnutí Komise 2008/324/ES, Úř. věst. L 111, 23. 4.2008, s. 11-14. Komise se pravidelně schází s touto skupinou. Její stanoviska jsou zveřejněna na internetové stránce [http://ec.europa.eu/justice\\_home/doc\\_centre/police/doc\\_police\\_intro\\_en.htm](http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm)

<sup>6</sup> Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená článkem 29 směrnice o ochraně údajů (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, Úř. věst. L 281, 23.11.1995, s. 31).

<sup>7</sup> Zpráva 01/2010 o druhé společné donucovací akci: Dodržování povinností stanovených vnitrostátními předpisy v oblasti uchování provozních údajů na právním základě článku 6 a 9 směrnice o soukromí a elektronických komunikacích a směrnice o uchování údajů 2006/24/ES, která mění směrnici o soukromí a elektronických komunikacích, ze strany poskytovatelů telekomunikačních či internetových služeb na vnitrostátní úrovni (WP 172), 13.7.2010, k dispozici na internetové stránce (viz [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm)).

### 3. UCHOVÁVÁNÍ ÚDAJŮ V EVROPSKÉ UNII

#### 3.1. Uchovávání údajů pro účely trestního soudnictví a prosazování práva

Poskytovatelé služeb a sítí (dále jen „poskytovatelé“) zpracovávají v rámci svých aktivit osobní údaje, a to pro účely předávání sdělení, vyúčtování, plateb za propojení, marketingu a dalších služeb s přidanou hodnotou. Toto zpracovávání zahrnuje údaje uvádějící zdroj, určení, datum, čas, dobu trvání a druh komunikace a rovněž uživatelské komunikační zařízení a v případě mobilního telefonu i polohu zařízení. Podle směrnice 2002/58/ES o soukromí a elektronických komunikacích (dále jen „směrnice o e-soukromí“)<sup>8</sup> tyto provozní údaje generované při využívání služeb elektronické komunikace musí být vymazány nebo anonymizovány, pokud již nejsou potřeba pro přenos sdělení s výjimkou údajů nadále potřebných pro účely účtování, marketingu nebo údajů, s jejichž uchováváním vyjádřil souhlas účastník nebo uživatel. Lokalizační údaje lze zpracovávat, pouze pokud jsou anonymizovány, anebo se souhlasem uživatelů nebo účastníků v nezbytném rozsahu a po nezbytnou dobu pro poskytování služeb s přidanou hodnotou.

Před vstupem směrnice v platnost vnitrostátní orgány za použití zvláštních podmínek po provozovatelích vyžadovaly přístup k těmto údajům, aby mohly například identifikovat účastníka používající určitou IP adresu, prostudovat komunikační aktivity a zjistit polohu mobilního telefonu.

Na úrovni EU bylo uchovávání a využití údajů pro účely prosazování práva poprvé řešeno směrnicí 97/66/ES o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací. Tato směrnice poprvé stanovila možnost, aby členské státy přijaly legislativní opatření, jestliže je to nutné pro ochranu veřejné bezpečnosti, obrany, bezpečnosti státu, včetně hospodářské prosperity státu, pokud byly tyto činnosti spojeny s otázkami bezpečnosti státu, a pro prosazování trestního práva<sup>9</sup>.

Toto ustanovení bylo dále rozvedeno směrnicí o e-soukromí, která přiznala členským státům možnost, aby přijaly legislativní opatření odchylná od zásady důvěrnosti sdělení, a to včetně možnosti za určitých podmínek uchovávat a zpřístupňovat a využívat údaje pro účely prosazování práva. Ustanovení čl. 15 odst. 1 umožňuje, aby členské státy omezily rozsah práv a povinností, a to včetně prostřednictvím uchovávání údajů po omezenou dobu, 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“.

Role uchovávaných údajů pro systémy trestního soudnictví a pro prosazování práva je dále rozvedena v oddíle 5.

---

<sup>8</sup> 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) (Úř. věst. L, 31.7.2002, s. 37-47).

<sup>9</sup> Ustanovení čl. 14 odst. 1 směrnice Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací (Úř. věst. L 24, 30.1.1998, s. 1-8).

### 3.2. Cíl směrnice o uchovávání údajů a její právní základ

V důsledku ustanovení směrnice 97/66/ES a směrnice o e-soukromí, která povolují přijmout členským státům právní předpisy v oblasti uchovávání údajů, měli poskytovatelé v některých členských státech povinnost nakoupit vybavení pro uchovávání údajů a zaměstnat pracovníky pro vyhledávání údajů pro donucovací orgány, zatímco neexistovala stejná povinnost pro poskytovatele v jiných členských státech, což vedlo k narušením vnitřního trhu. Navíc trendy u obchodních modelů a poskytování služeb, jako např. nárůst paušálních tarifů, předplacené a bezplatné služby elektronických komunikací způsobily, že poskytovatelé postupně přestávali ukládat provozní a lokalizační údaje pro účely účtování, a tudíž se snižovala dostupnost těchto údajů pro účely trestního soudnictví a prosazování práva. Teroristické útoky v Madridu v roce 2004 a v Londýně v roce 2005 zvýšily naléhavost diskuzí, jak tyto otázky řešit na úrovni EU.

V této souvislosti uložila směrnice o uchovávání údajů členským státům povinnost zajistit, aby poskytovatelé veřejně dostupných služeb elektronických komunikací a veřejných komunikačních sítí uchovávali komunikační údaje pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak jsou vymezeny každým členským státem v jeho vnitrostátních právních předpisech, a usilovala o harmonizaci určitých souvisejících otázek v rámci EU.

Směrnice změnila čl. 15 odst. 1 směrnice o e-soukromí vložení odstavce, který stanovuje, že se čl. 15 odst. 1 nevztahuje na údaje, které se mají uchovávat podle směrnice o uchovávání údajů<sup>10</sup>. Členské státy se proto (jak uvádí 12. bod odůvodnění směrnice) i nadále mohou odchýlit od zásady důvěrnosti sdělení. Směrnice (o uchovávání údajů) upravuje pouze uchovávání údajů po omezenější dobu, pro účely vyšetřování, odhalování a stíhání závažných trestných činů.

Tento komplexní právní vztah mezi směrnicí a směrnicí o e-soukromí v kombinaci s neexistencí definice „závažného trestného činu“ ani v jedné z těchto směrnicí způsobuje, že je složité odlišit opatření přijatá členskými státy k provedení povinností uchovávat údaje, které jsou stanoveny ve směrnici, na straně jedné a obecné postupy v členských státech pro uchovávání údajů, které je umožněno podle čl. 15 odst. 1 směrnice o e-soukromí na straně druhé<sup>11</sup>. Tato otázka je dále rozebrána v oddíle 4.

Právním základem směrnice je článek 95 Smlouvy o založení Evropského společenství (nahrazený článkem 114 Smlouvy o fungování Evropské unie) upravující vytvoření a fungování vnitřního trhu. Následně po přijetí směrnice byl její právní základ napadnut před Evropským soudním dvorem s tvrzením, že jejím primárním cílem je vyšetřování, odhalování a stíhání závažných trestných činů. Soudní dvůr rozhodl, že směrnice upravuje činnosti, které jsou nezávislé na provádění jakékoliv policejní nebo justiční spolupráce v trestních věcech a že neharmonizuje přístup k údajům ze strany příslušných vnitrostátních orgánů ani použití či

---

<sup>10</sup> Článek 11 směrnice uvádí: Ve směrnici 2002/58/ES se v článku 15 vkládá nový odstavec 1a., který zní: „Odstavec 1 se nevztahuje na údaje, které se podle 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 mají uchovávat pro účely stanovené v čl. 1 odst. 1 uvedené směrnice.“

<sup>11</sup> Pracovní skupina pro ochranu údajů zřízená podle článku 29 sporuje, zda cílem směrnice (o uchovávání údajů) byla odchylka z obecné povinnosti vymazávat provozní údaje po ukončení elektronické komunikace nebo pověřit uchováváním všechny ty poskytovatele, kteří již měli zmocnění uchovávat je pro své vlastní obchodní účely.“

výměnu těchto údajů mezi těmito orgány. Soudní dvůr proto shledal, že směrnice se v zásadě zaměřuje na činnosti poskytovatelů v relevantním odvětví vnitřního trhu. Soudní dvůr proto potvrdil volbu právního základu<sup>12</sup>.

### 3.3. Zajišťování údajů

Uchovávání údajů se liší od zajišťování údajů (známého také jako „quick freeze“), při kterém mají poskytovatelé, kterým je doručen soudní příkaz, povinnost uchovávat údaje týkající se pouze konkrétních osob podezřelých z trestné činnosti od data uvedeného v soudním příkazu. Zajišťování údajů je jedním z vyšetřovacích nástrojů, o kterém uvažovaly státy účastníci se Úmluvy Rady Evropy o kyberkriminalitě<sup>13</sup>, a používají jej. Téměř všechny účastníci se státy zřídily kontaktní místo, jehož rolí je zajistit, aby byla poskytnuta bezprostřední součinnost při vyšetřování kyberkriminality nebo v trestních řízeních. Avšak zdá se, že ne všechny strany úmluvy upravily ve svých právních předpisech toto zajišťování údajů, a neproběhlo ještě hodnocení účinnosti tohoto modelu pro potírání kyberkriminality<sup>14</sup>. V nedávné době byl vyvinut druh zajišťování údajů známý pod označením „quick freeze plus“. Tento model jde dál, než je zajišťování údajů, jelikož soudce může udělit přístup i k údajům, které poskytovatelé dosud nevyřadili. Existovala by rovněž velmi omezená zákonná výjimka z povinnosti vymazávat, po krátkou dobu, určité komunikační údaje, které se normálně ukládají, jako jsou lokalizační údaje, údaje o připojení k internetu a dynamické IP adresy v případě uživatelů, kteří mají paušální připojení a u kterých není potřeba ukládat údaje pro účely účtování.

Zastánci zajišťování údajů jsou toho názoru, že méně zasahuje do soukromí ve srovnání s uchováváním údajů. Většina členských států však nesouhlasí s tím, že by jakákoliv varianta zajišťování údajů mohla odpovídajícím způsobem nahradit uchovávání údajů, přičemž argumentují, že zatímco výsledkem uchovávání údajů je dostupnost historických údajů, zajišťování údajů nezaručuje schopnost vytvořit důkazní materiál před soudním příkazem ani neumožňuje vyšetřování v případě, kdy osoba není známa, a neumožňuje, aby byly shromažďovány důkazy o pohybu osob, například obětí nebo svědků trestné činnosti<sup>15</sup>.

## 4. PROVEDENÍ SMĚRNICE O UCHOVÁVÁNÍ ÚDAJŮ

Členské státy měly směrnici provést do 15. září 2007, s výjimkou povinností týkajících se uchovávání údajů o připojení k internetu, internetové elektronické poště a internetové telefonii, u kterých bylo možné odložit provedení do 15. března 2009.

---

<sup>12</sup> Rozsudek Soudního dvora (velkého senátu) ze dne 10. února 2009, C-301/6 ve věci Irsko v. Evropský parlament, Rada Evropské unie, Sb. rozh. [2009] I-00593.

<sup>13</sup> Článek 16 Úmluvy Rady Evropy o kyberkriminalitě (<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>).

<sup>14</sup> Zdroj: Rada Evropy.

<sup>15</sup> Toto rovněž uznal Německý ústavní soud ve svém rozhodnutí, kterým zrušil německý zákon provádějící směrnici (viz oddíl 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 ze dne 2. března 2010, bod 208).

Následující analýza vychází z oznámení o provedení, která Komise obdržela od 25 členských států, včetně Belgie, která směrnici provedla pouze částečně<sup>16</sup>. V Rakousku a Švédsku jsou legislativní návrhy v projednávání. V těchto dvou členských státech neexistuje povinnost uchovávat údaje, avšak donucovací orgány mohou požadovat a požadují a získávají provozní údaje od poskytovatelů v rozsahu, v jakém jsou k dispozici. Po úvodním oznámení o provedení Českou republikou, Německem a Rumunskem ústavní soudy těchto členských států zrušily vnitrostátní právní předpisy provádějící směrnici<sup>17</sup> a tyto státy nyní zvažují, jak ji znovu provést.

Tento oddíl analyzuje, nakolik členské státy provedly příslušná ustanovení směrnice. Přezkoumává rovněž, zda členské státy zvolily, že budou nahrazovat poskytovatelům náklady vzniklé v souvislosti s uchováváním údajů a s možností jejich vyhledávání, což směrnice nijak neupravuje a rovněž se zabývá otázkou, jaký význam mají pro směrnici rozhodnutí ústavních soudů v Německu, Rumunsku a České republice.

#### 4.1. Účel uchovávání údajů (článek 1)

Směrnice ukládá členským státům přijmout opatření zajišťující, že jsou uchovávány údaje a že jsou údaje dostupné pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak si je každý členský stát vymezuje ve svých vnitrostátních právních předpisech. Účel uvedený ve vnitrostátních právních předpisech pro uchovávání údajů a/nebo pro přístup k nim se však i nadále liší v EU. Deset členských států (Bulharsko, Estonsko, Irsko, Řecko, Španělsko, Litva, Lucembursko, Maďarsko, Nizozemsko, Finsko) vymezilo „závažný trestný čin“ odkazem na minimální dobu odnětí svobody, možnost uložit trest odnětí svobody nebo na seznam trestných činů definovaný jinde ve vnitrostátních předpisech. Osm členských států (Belgie, Dánsko, Francie, Itálie, Lotyšsko, Polsko, Slovensko, Slovinsko) vyžaduje, aby údaje byly uchovávány nejen pro vyšetřování, odhalování a stíhání závažných trestných činů, nýbrž pro všechny trestné činy a rovněž pro prevenci trestné činnosti nebo obecněji pro účely národní bezpečnosti, bezpečnosti státu nebo veřejné bezpečnosti. Právní předpisy čtyř členských států (Kypr, Malta, Portugalsko, Spojené království) odkazují na „závažný trestný čin“ nebo „závažnou trestnou činnost“, aniž by je blíže vymezovaly. Podrobnosti uvádí tabulka č. 1.

**Tabulka č. 1: Účelové omezení pro uchovávání údajů uvedené ve vnitrostátní právních předpisech**

<sup>16</sup> Dvacet pět členských států, které oznámily Komisi provedení, tvoří Belgie, Bulharsko, Česká republika, Dánsko, Německo, Řecko, Estonsko, Irsko, Španělsko, Francie, Itálie, Kypr, Lotyšsko, Litva, Lucembursko, Maďarsko, Malta, Nizozemsko, Polsko, Portugalsko, Rumunsko, Slovinsko, Slovensko, Finsko, Spojené království. Belgie Komisi oznámila, že předloha právní předpisu kompletující provedení je stále v legislativním procesu v parlamentu.

<sup>17</sup> Rozhodnutí č. 1258 ze dne 8. října 2009 Rumunského ústavního soudu, rumunský úřední věstník č 789, 23. listopadu 2009; rozhodnutí Bundesverfassungsgericht, 1 BvR 256/08 z 2. března 2010; úřední věstník z 1. dubna 2011, nález Ústavního soudu ČR ze dne 22. března 2011 k ustanovení § 97 odst. 3 a 4 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů a vyhláše 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.

Tabulka č. 1: Účelové omezení pro uchovávání údajů uvedené ve vnitrostátní právních předpisech	
Belgie	Pro účely vyšetřování a stíhání trestných činů, vyšetřování případů zneužívání tísňových telefonních linek, vyšetřování úmyslného zneužití sítí nebo služeb elektronických komunikací, pro účely zpravodajských misí prováděných zpravodajskými a bezpečnostními službami <sup>18</sup> .
Bulharsko	Pro „odhalování a vyšetřování závažných trestných činů a trestných činů podle článku 319a-319f trestního zákoníku a pro vyhledávání osob“ <sup>19</sup> .
Česká republika	Neprovedeno.
Dánsko	Pro účely vyšetřování a stíhání trestných činů <sup>20</sup> .
Německo	Neprovedeno.
Estonsko	Lze využít, jestliže je shromažďování důkazů jinými procesními úkony vyloučeno nebo zvláště obtížné a předmětem trestního řízení je trestný čin [prvního stupně nebo úmyslný trestný čin druhého stupně s trestem odnětí svobody nejméně tři roky] <sup>21</sup> .
Irsko	Pro účely prevence před závažnými trestnými činy [tj. trestných činů trestaných trestem odnětí svobody nejméně 5 let a více, nebo trestných činů uvedených v příloze transpozičního právního předpisu], pro účely ochrany bezpečnosti státu a lidského života <sup>22</sup> .
Řecko	Pro účely odhalování zvláště závažných trestných činů <sup>23</sup> .
Španělsko	Pro účely odhalování, vyšetřování a stíhání závažných trestných činů uvedených v trestním zákoníku nebo ve zvláštních trestních zákonech <sup>24</sup> .
Francie	Pro odhalování, vyšetřování a stíhání trestných činů a za výlučným účelem poskytnout orgánům činným v trestním řízení potřebné informace a pro prevenci teroristických útoků a ochranu duševního vlastnictví <sup>25</sup> .
Itálie	Pro účely odhalování a potlačování trestných činů <sup>26</sup> .
Kypr	Pro účely vyšetřování závažných trestných činů <sup>27</sup> .
Lotyšsko	Na ochranu státní a veřejné bezpečnosti a pro účely vyšetřování trestných činů, trestního stíhání a trestního řízení <sup>28</sup> .

<sup>18</sup> Ustanovení čl. 126 odst. 1 zákona ze dne 13. června 2005 o elektronických komunikacích. .

<sup>19</sup> Ustanovení čl. 250a odst. 2 zákona o elektronických komunikacích (v platném znění) z roku 2010.

<sup>20</sup> Ustanovení článku 1 nařízení o ochraně údajů.

<sup>21</sup> Ustanovení čl. 110 odst. 1 trestního řádu.

<sup>22</sup> Ustanovení článku 6 zákona z roku 2011 o komunikacích (Retention of Data Act).

<sup>23</sup> Tyto trestné činy jsou vymezeny v článku 4 zákona č. 2225/1994; článku 1 zákona č. 3917/2011.

<sup>24</sup> Ustanovení čl. 1 odst. 1 zákona č. 25/2007.

<sup>25</sup> Zákony, které upravují použití uchovávaných údajů pro trestní stíhání, prevenci teroristických útoků a ochranu duševního vlastnictví jsou tyto: článek L.34-1(II), CPCE, zákon č.° 2006-64 ze dne 23. ledna 2006 a zákon č.° 2009-669 ze dne 12. června 2009.

<sup>26</sup> Ustanovení čl. 132 odst. 1 zákona o ochraně údajů.

<sup>27</sup> Ustanovení čl. 4 odst.1 zákona č. 183(I)/2007.

<sup>28</sup> Ustanovení čl. 71 odst.1 zákona o elektronických komunikacích.

<b>Tabulka č. 1: Účelové omezení pro uchovávání údajů uvedené ve vnitrostátní právních předpisech</b>	
Litva	Pro účely vyšetřování, odhalování a stíhání závažných a velmi závažných trestných činů, jak jsou vymezeny litevským trestním zákoníkem <sup>29</sup> .
Lucembursko	Pro účely vyšetřování, odhalování a stíhání trestných činů s trestem odnětí svobody nejméně jeden rok <sup>30</sup> .
Maďarsko	S cílem umožnit vyšetřujícím orgánům, státnímu zástupci, soudům a národním bezpečnostním orgánům výkon jejich povinností, a s cílem umožnit policii a celní a daňové správě vyšetřovat úmyslné trestné činy s trestem odnětí svobody minimálně dva roky <sup>31</sup> .
Malta	Pro účely vyšetřování, odhalování a stíhání závažných trestných činů <sup>32</sup> .
Nizozemsko	Pro účely vyšetřování a stíhání závažných trestných činů, za které lze uložit trest odnětí svobody <sup>33</sup> .
Rakousko	Neprovedeno.
Polsko	Pro prevenci nebo odhalování trestných činů, pro prevenci a odhalování krádeží daní a jiných poplatků, pro využití státním zástupcem či soudem při probíhajících trestních řízeních, pro účely Národní bezpečnostní agentury, Bezpečnosti a informační služby, Protikorupční agentury, Vojenské kontrarozvědky a rozvědky s cílem umožnit plnění jejich úkolů <sup>34</sup> .
Portugalsko	Pro účely vyšetřování, odhalování a stíhání závažných trestných činů <sup>35</sup> .
Rumunsko	Neprovedeno.
Slovinsko	Pro zajištění národní bezpečnosti, ústavního pořádku a bezpečnosti politických a hospodářských zájmů státu... a pro účely národní obrany <sup>36</sup> .
Slovensko	Pro prevenci, vyšetřování, odhalování a stíhání trestných činů <sup>37</sup> .
Finsko	Pro vyšetřování, odhalování a stíhání závažných trestných činů uvedených v hlavě 5a, čl. 3 odst. 1 zákona o trestních opatřeních <sup>38</sup> .
Švédsko	Neprovedeno.
Spojené království	Pro účely vyšetřování, odhalování a stíhání závažných trestných činů <sup>39</sup> .

<sup>29</sup> Ustanovení článku 65 zákona X-1835.

<sup>30</sup> Ustanovení čl. 1 odst. 1 zákona ze dne 24. července 2010.

<sup>31</sup> Obecný účel uchovávání údajů viz článek 159/A zákona C/2003, ve znění zákona CLXXIV/2007; účel u policejního přístupu viz článek 68 zákona XXXIV/1994; účel přístupu daňové a celní správy viz článek 59, zákon CXXII/2010.

<sup>32</sup> Ustanovení čl. 20 odst. 1 zákona č. 198/2008 (Legal Notice).

<sup>33</sup> Ustanovení článku 126 trestního řádu.

<sup>34</sup> Ustanovení článku 180a zákona o telekomunikacích ze dne 16. července 2004 ve znění článku 1 zákona ze dne 24. dubna 2009.

<sup>35</sup> Ustanovení článku 1 a čl. 3 odst. 1 zákona č. 32/2008.

<sup>36</sup> Ustanovení čl. 170a odst. 1 zákona o elektronických komunikacích.

<sup>37</sup> Ustanovení § 59a odst. 6 zákona o elektronických komunikacích.

<sup>38</sup> Ustanovení § 14a odst. 1 zákona o elektronických komunikacích.

Většina členských států, které směrnici provedly, umožňuje v souladu s vnitrostátními právními předpisy přístup k uchovávaným údajům a jejich využití pro účely, které překračují účely uvedené ve směrnici, včetně prevence a boje proti trestné činnosti obecně a ohrožení života a zdraví. Přestože je to podle směrnice o e-soukromí povoleno, je omezená míra harmonizace, kterou dosáhly právní předpisy EU v této oblasti. Rozdíly u účelů, pro které jsou údaje uchovávány, pravděpodobně ovlivňují objem a četnost žádostí o ně a v návaznosti na to i náklady vyplývající z dodržování povinností, které stanoví směrnice. Tento stav navíc nemusí vytvářet dostatečnou předvídatelnost, což je podmínka každého legislativního opatření, které omezuje právo na soukromí<sup>40</sup>. Komise zvažuje potřebu dosažení větší míry harmonizace v této oblasti a varianty pro její dosažení<sup>41</sup>.

#### **4.2. Povinnost poskytovatelů uchovávat údaje (článek 1)**

Směrnice se vztahuje na „poskytovatele veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí“ (čl. 1 odst. 1). Dva členské státy (Finsko a Spojené království) nevyžadují po malých provozovatelích, aby uchovávali údaje, protože, dle jejich tvrzení, náklady pro poskytovatele i pro stát by převážily výhody vyplývající pro systémy trestního soudnictví a pro prosazování práva. Čtyři členské státy (Lotyšsko, Lucembursko, Nizozemsko, Polsko) oznámily, že zavedly alternativní úpravu správními předpisy. Zatímco velcí poskytovatelé působící v několika členských státech těží z úspor z rozsahu, pokud jde o náklady, malí poskytovatelé v některých členských státech mají tendenci zakládat společné podniky pro uchovávání údajů a vyhledávání v nich nebo tyto služby externě zajišťovat společnostmi, které se na tuto činnost specializují, aby snížili své náklady. Externí zajišťování technických funkcí tímto způsobem nemá vliv na povinnost poskytovatelů řádně dohlížet na zpracovávání a zajistit, že jsou zavedena požadovaná bezpečnostní opatření, což může problematické zejména pro menší poskytovatele. Komise přezkoumá otázky týkající se bezpečnosti údajů a dopadu variant novely rámce pro uchovávání údajů na malé a střední podniky.

#### **4.3. Přístup k údajům: orgány a postupy a podmínky (článek 4)**

Členské státy musí přijmout opatření pro zajištění toho, „že (údaje uchovávané v souladu s touto směrnicí) jsou poskytovány pouze příslušným vnitrostátním orgánům v konkrétních případech a v souladu s vnitrostátními právními předpisy“. Je věcí členských států, jak vymezí „postupy pro získání přístupu k uchovávaným údajům v souladu s požadavky nezbytnosti a přiměřenosti a podmínky, jež mají být za tím účelem splněny, stanoví jednotlivé členské státy ve svých vnitrostátních právních předpisech, s výhradou příslušných ustanovení práva

---

<sup>39</sup> Nařízení o uchovávání údajů (směrnice ES) z roku 2009 (2009 č. 859).

<sup>40</sup> Rozsudek Evropského soudního dvora ze dne 20. května 2003 ve spojených věcech C-465/00, C-138/01 a C-139/01 (žádost o rozhodnutí o předběžné otázce podaná Verfassungsgesichtshof a Oberster Gerichtshof): Rechnungshof (C-465/00) v Österreichischer Rundfunk a další a mezi Christa Neukomm (C-138/01), Joseph Laueremann (C-139/01) a Österreichischer Rundfunk (o ochraně fyzických osob v souvislosti se zpracováním osobních údajů — směrnice 95/46/ES — ochrana soukromí — zpřístupnění údajů o příjmu zaměstnanců pod kontrolou Rechnungshof).

<sup>41</sup> Při přijetí směrnice vydala Komise prohlášení, které navrhovalo uvážit seznam trestných činů uvedený u evropského zatýkacího rozkazu. (Rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy).

Evropské unie nebo mezinárodního práva veřejného, zejména Evropské úmluvy o ochraně lidských práv a základních svobod, jak ji vykládá Evropský soud pro lidská práva“.

Přístup k uchovávaným údajům může ve všech členských státech získat policie a vyjma jurisdikcí obyčejového práva (Irsko a Spojené království) i státní zástupci. Čtrnáct členských států uvádí mezi příslušné orgány, které mohou získat přístup, bezpečnostní a informační služby nebo vojenské úřady. Šest členských států mezi tyto orgány zařazuje daňovou a/nebo celní správu a tři rovněž pohraniční orgány. Jeden členský stát umožňuje dalším orgánům veřejné správy, aby získaly přístup k údajům, pokud jim to pro zvláštní účely povoluje sekundární právo. Jedenáct členských států vyžaduje soudní povolení pro každý přístup k uchovávaným údajům. Ve třech členských státech je soudní povolení vyžadováno ve většině případů. Pět dalších členských států vyžaduje povolení vyššího orgánu, nikoliv však soudce. Ve dvou členských státech se zdá, že jedinou podmínkou je písemná žádost.

<b>Tabulka č. 2: Přístup k uchovávaným telekomunikačním údajům:</b>		
	<i>Příslušné vnitrostátní orgány</i>	<i>Postupy a podmínky</i>
Belgie	Oddělení justiční spolupráce, vyšetřující soudci, státní zástupce, kriminální policie.	Přístup musí povolit soudce nebo státní zástupce. Poskytovatelé musí na žádost v „reálném čase“ dodat údaje o účastníkovi a provozní a lokalizační údaje u telefonních hovorů za poslední měsíc. Údaje o starších hovorech musí být poskytnuty co nejdříve.
Bulharsko <sup>42</sup>	Zvláštní ředitelství a oddělení Státního úřadu pro národní bezpečnost, ministerstvo vnitra, Vojenská zpravodajská služba, vojenská policie, ministr obrany, Národní vyšetřovací služba; soud a orgány činné v přípravném řízení za určitých podmínek.	Přístup je možný, pouze povolí-li ho předseda krajského soudu.
Česká republika	Neprovedeno.	
Dánsko <sup>43</sup>	Policie.	Pro přístup je nutné soudní povolení; soud nařídí přístup, pokud žádost splňuje přísné podmínky ohledně podezření, nezbytnosti a přiměřenosti.
Německo	Neprovedeno.	
Estonsko <sup>44</sup>	Rada policie a pohraniční stráž, Rada bezpečnostní policie a pro předměty a elektronickou komunikaci Rada pro daně a cla.	Pro přístup je nutné předchozí povolení vyšetřujícího soudce. Poskytovatelé musí „poskytnout (uchovávané údaje) do 10 hodin a v ostatních případech do deseti pracovních dnů (od doručení žádosti)“.
Irsko <sup>45</sup>	Členové Garda Síochána (policie) v hodnosti Chief Superintendent a vyšší; příslušníci trvalých armádních sil v hodnosti plukovníka a vyšší; Úředníci orgánu Revenue Commissioners v hodnosti vedoucího a vyšší	Žádost musí být písemná.

<sup>42</sup> Ustanovení čl. 250b odst. 1 zákona o elektronických komunikacích (v platném znění) z roku 2010 (orgány). Ustanovení čl. 250b odst. 2 a čl. 250c odst. 1 zákona o elektronických komunikacích (v platném znění) z roku 2010 (přístup).

<sup>43</sup> Ustanovení článku 71 zákona o výkonu justice.

<sup>44</sup> Ustanovení čl. 112 odst. 2 a 3 trestního řádu (orgány a postupy); Ustanovení čl. 111 odst. 9 (podmínky) zákona o elektronických komunikacích.

<sup>45</sup> Ustanovení článku 6 návrhu zákona o komunikacích z roku 2009 (Retention of Data).

Tabulka č. 2: Přístup k uchovávaným telekomunikačním údajům:		
	<i>Příslušné vnitrostátní orgány</i>	<i>Postupy a podmínky</i>
Řecko <sup>46</sup>	Justiční, vojenské a policejní orgány.	Pro přístup je nutné soudní rozhodnutí uvádějící, že vyšetřování jinými prostředky není možné nebo je zvláště obtížné.
Španělsko <sup>47</sup>	Policejní síly pověřené odhalováním, vyšetřováním a stíháním závažných trestných činů, Národní zpravodajské středisko a Celní správa.	Pro přístup k těmto údajům potřebují příslušné vnitrostátní orgány předchozí soudní povolení.
Francie <sup>48</sup>	Státní zástupce, určení příslušníci policie a četnictva.	Police musí každou žádost o přístup k uchovávaným údajům odůvodnit a musí požádat o povolení příslušnou osobu na ministerstvu vnitra pověřenou orgánem Commission nationale de contrôle des interceptions de sécurité. Žádost o přístup vyřizuje pověřená osoba pracující pro poskytovatele.
Itálie <sup>49</sup>	Státní zástupce; policie; obhájce osoby stíhané či vyšetřované.	Pro přístup je nutný „odůvodněný příkaz“ vydaný státním zástupcem.
Kypr <sup>50</sup>	Soudy, státní zástupce, policie.	Přístup musí schválit státní zástupce, má-li za to, že může přinést důkazy o spáchání závažného trestného činu. Soudce může vydat povolení, pokud existuje důvodné podezření ze spáchání závažného trestného činu a pokud je pravděpodobné, že dané údaje s tímto činem souvisejí.
Lotyšsko <sup>51</sup>	Pověření úředníci orgánů vedoucích přípravné řízení; vyšetřovatelé; pověření úředníci orgánů státní bezpečnosti; úřad státního zastupitelství; soudy.	Pověření úředníci, úřad státního zastupitelství a soudy musí posoudit „přiměřenost a účelnost“ žádosti, zaprotokolovat žádost a zajistit ochranu získaných údajů. Pověřené orgány mohou uzavřít dohodu s poskytovatelem, např. o šifrování dodávaných údajů.
Litva <sup>52</sup>	Orgány v přípravném řízení, státní zástupce, soud (soudci) a úředníci zpravodajské služby.	Pověřené orgány musí o uchovávané údaje požádat písemně. Při vyšetřování v rámci přípravného řízení je nutné soudní povolení.
Lucembursko <sup>53</sup>	Justiční orgány (vyšetřující soudci, státní zástupce), orgány státní bezpečnosti, obrany, veřejné bezpečnosti a orgány prevence, vyšetřování, odhalování a stíhání trestných činů.	Pro přístup je nutné soudní povolení.
Maďarsko <sup>54</sup>	Police, Úřad pro cla a daně, národní bezpečnostní agentury, státní zástupce, soudy.	Police a Úřad pro cla a daně potřebují povolení od státního zástupce. Státní zástupce a národní bezpečnostní agentury mohou získat přístup k těmto údajům bez soudního povolení.

<sup>46</sup> Články 3 a 4 zákona č. 2225/94.

<sup>47</sup> Články 6 a 7 zákona č. 25/2007.

<sup>48</sup> Ustanovení článku 60-1 a 60-2, trestního řádu (orgány); ustanovení L.31-1-1 (podmínky).

<sup>49</sup> Ustanovení čl. 132 odst. 3 zákona o ochraně údajů.

<sup>50</sup> Ustanovení čl. 4 odst. 2 a 4 zákona č. 183(I)/2007

<sup>51</sup> Ustanovení čl. 71 odst.1 zákona o elektronických komunikacích (orgány); nařízení vlády č. 820 (postupy).

<sup>52</sup> Ustanovení čl. 77 odst.1 a 2 zákona X-1835; ústní oznámení Komisi.

<sup>53</sup> Ustanovení čl. 5-2 odst. 1 čl. 9 odst. 2 zákona ze dne 24. července 2010 (orgány); článek 67-1, trestního řádu (podmínky).

Tabulka č. 2: Přístup k uchovávaným telekomunikačním údajům:		
	<i>Příslušné vnitrostátní orgány</i>	<i>Postupy a podmínky</i>
Malta <sup>55</sup>	Policejní síly; Bezpečnostní služba	Žádost musí být písemná.
Nizozemsko <sup>56</sup>	Vyšetřovatel policie	Přístup musí povolit státní zástupce nebo vyšetřující soudce.
Rakousko	Neprovedeno.	
Polsko <sup>57</sup>	Policie, pohraniční služba, inspektoři finančního úřadu, rozvědka a kontrarozvědka, zahraniční rozvědka, vojenská kontrarozvědka, vojenská rozvědka, soudy a státní zástupce.	Žádost musí být písemná a v případě, kdy žádost podává policie, pohraniční služba, inspektoři finančního úřadu, musí být schválena vedoucím úředníkem v organizaci.
Portugalsko <sup>58</sup>	Kriminální policie, Republikánská národní garda, Úřad pro veřejnou bezpečnost, Vojenská kriminální policie, Cizinecký a pohraniční úřad, Námořní policie.	Pro předání údajů je nutné soudní povolení odůvodněné skutečností, že přístup je zásadní pro odhalení pravdy nebo důkazů, což by jiným způsobem a prostředky bylo nemožné nebo velmi obtížné. Soud ověřuje požadavky nezbytnosti a proporcionality.
Rumunsko	Neprovedeno.	
Slovinsko <sup>59</sup>	Policie, zpravodajské a bezpečnostní agentury, vojenské agentury odpovědné za rozvědku a kontrarozvědku a bezpečnostní mise.	Pro přístup je nutné soudní povolení.
Slovensko <sup>60</sup>	Donucovací orgány, soudy.	Žádost musí být písemná.
Finsko <sup>61</sup>	Policie, pohraniční služba, celní orgány (pro uchovávané údaje o účastnících, provozní a lokalizační údaje). Středisko reakce na mimořádné situace, Středisko pro záchranu na moři, podřízená střediska pro záchranu na moři (pro identifikaci a lokalizační údaje při mimořádných situacích).	Údaje o účastnících jsou pro všechny příslušné orgány přístupné bez soudního povolení. Pro přístup k jiným údajům je zapotřebí soudního příkazu.
Švédsko	Neprovedeno.	
Spojené království <sup>62</sup>	Police, zpravodajské služby, daňové a celní orgány, další orgány státní správy uvedené v sekundárních právních předpisech.	Přístup je povolen, je-li schválen „pověřenou osobou“ a jsou-li splněny podmínky nezbytnosti a přiměřenosti ve zvláštních případech a za okolností, kdy je zpřístupnění údajů povoleno nebo vyžadováno zákonem. S poskytovateli byly dohodnuty zvláštní postupy.

<sup>54</sup> Ustanovení čl. 68 odst. 1 a čl. 69 odst. 1 písm. c) a d), zákona XXXIV 1994; ustanovení 9/A odst. 1 zákona V 1972; ustanovení čl. 71 odst. 1, 3, a 4, čl. 178/A odst. 4, článku 200, 201, čl. 268 odst. 2 zákona XIX 1998; ustanovení čl. 40 odst. 1, čl. 40 odst. 2, čl. 53 odst. 1, čl. 54 odst. 1 písm. j) zákona CXXV 1995.

<sup>55</sup> Ustanovení čl. 20 odst. 1 a 3 zákona č. 198/2008 (Legal Notice).

<sup>56</sup> Ustanovení článku 126ni trestního řádu.

<sup>57</sup> Ustanovení čl. 179 odst. 3 zákona o telekomunikacích ze dne 16. července 2004 ve znění článku 1 zákona ze dne 24. dubna 2009.

<sup>58</sup> Ustanovení čl. 2 odst. 1, čl. 3 odst. 2 a článku 9 zákona č. 32/2008.

<sup>59</sup> Článek 107c zákona o elektronických komunikacích; článek 149b trestního řádu; článek 24(b) zákona a zpravodajských službách a bezpečnostních agenturách; článek 32 zákona o obraně.

<sup>60</sup> Ustanovení § 59a odst. 8 zákona o elektronických komunikacích.

<sup>61</sup> Ustanovení čl. 35 odst. 1 a článku 9 zákona o elektronických komunikacích; články 31 až 33 zákona o policii; článek 41 zákona o pohraniční službě.

<sup>62</sup> Ustanovení článku 25 příloha 1 zákona o vyšetřujících pravomocích z roku 2000 (zákon RIPA); Ustanovení článku 7 nařízení o uchovávání údajů. Ustanovení čl. 22 odst. 2 zákona RIPA stanoví, za jakým účelem mohou tyto orgány požadovat údaje.

Komise posoudí, zda existuje potřeba dosáhnout větší míry harmonizace ohledně orgánů s přístupem k uchovávaným údajům a postupy pro jejich získání, a varianty pro dosažení této harmonizace. Varianty mohou zahrnovat jasně vymezený seznam příslušných orgánů, nezávislý a/nebo soudní dohled týkající se žádostí o údaje a minimální standardní postupy pro poskytovatele ohledně udělování přístupu příslušným orgánům.

#### **4.4. Rozsah povinnosti uchovávat údaje a kategorie údajů, na které se povinnost vztahuje (čl. 1 odst. 2, čl. 3 odst. 2 a článek 5)**

Tato směrnice se vztahuje na oblast telefonie v rámci pevné a mobilní sítě, připojení k internetu, internetovou elektronickou poštu a internetovou telefonii. Specifikuje (v článku 5) kategorie uchovávaných údajů, konkrétně údaje nutné k identifikaci:

- (a) zdroje sdělení;
- (b) adresáta sdělení;
- (c) data, času a doby trvání komunikace;
- (d) typu sdělení;
- (e) komunikačního vybavení uživatelů nebo údajného komunikačního vybavení; a
- (f) polohy mobilního komunikačního zařízení.

Vztahuje se rovněž (čl. 3 odst. 2) na údaje o neúspěšných pokusech o volání, tj. o komunikaci, během které bylo telefonní volání úspěšně spojeno, ale zůstalo bez odezvy nebo došlo k zásahu správce sítě, pokud jsou takové údaje vytvářeny nebo zpracovávány a uchovávány či zaznamenávány poskytovateli. Podle směrnice nesmí být uchovávány žádné údaje odhalující obsah sdělení. Následně bylo objasněno, že se směrnice taktéž nevztahuje na dotazy použité ve vyhledávání, tj. záznamy ze serverů generované prostřednictvím služeb vyhledávače, protože ty se považují za obsah spíše než za provozní údaje<sup>63</sup>.

Dvacet jedna členských států upravuje uchovávání pro každou z těchto kategorií údajů ve svých právních předpisech provádějících směrnici. Belgie neupravila uchovávání pro údajů o telefonii, ani nemá žádná ustanovení týkající internetových údajů. Respondenti na dotazník Komise nepovažovali za nutné, aby se změnila kategorie uchovávaných údajů, ačkoliv Evropský parlament vydal Komisi písemné prohlášení, které nabádá k rozšíření působnosti směrnice na vyhledávače „aby bylo možné rychle a účinně potírat dětskou pornografii a sexuální obtěžování on-line“<sup>64</sup>. Ve své zprávě o druhé donucovací akci pracovní skupina pro ochranu údajů zřízená podle článku 29 argumentovala, že kategorie stanovené směrnicí by měly být považovány za vyčerpávající a poskytovatelům by neměly být ukládány žádné další povinnosti. Komise posoudí nezbytnost všech těchto kategorií údajů.

---

<sup>63</sup> Stanovisko pracovní skupiny pro ochranu údajů zřízené podle článku 29 ohledně otázek ochrany údajů týkajících se vyhledávačů, 4. dubna 2008.

<sup>64</sup> Písemné prohlášení podle pravidla 123 jednacího řádu o vytvoření evropského systému včasného varování (EWS) proti pedofilům a osobám sexuálně obtěžujícím jiné osoby, 19.4.2010, 0029/2010.

#### 4.5. Doby uchovávání (článek 6 a 12)

Členské státy jsou povinny zajistit, aby se kategorie údajů uvedené v článku 5 uchovávaly po dobu nejméně šesti měsíců a nejvýše dvou let. Maximální doba uchovávání může být prodloužena členským státem, který „se nachází ve zvláštní situaci ospravedlňující prodloužení maximální doby uchovávání uvedené v článku 6 o omezenou dobu“; takové prodloužení musí být neprodleně oznámeno Komisi, která ve lhůtě šesti měsíců od oznámení rozhodne, zda prodloužení schválí nebo zamítne. Jestliže je možné prodloužit maximální dobu uchovávání, tak žádné ustanovení nestanoví, že je možné tuto dobu zkrátit pod šest měsíců. Až na jeden členský stát všechny členské státy, které oznámily provedení směrnice, uplatňují dobu nebo doby uchovávání v rámci těchto limitů, a Komisi nebylo oznámeno žádné prodloužení. V rámci EU však neexistuje soudržný přístup.

Patnáct členských států stanovuje jedinou dobu pro všechny kategorie údajů: jeden členský stát (Polsko) stanovuje dvouletou dobu uchovávání, jeden stanovuje dobu 1,5 roku (Lotyšsko), deset jich stanovuje dobu jednoho roku (Bulharsko, Dánsko, Estonsko, Řecko, Španělsko, Francie, Nizozemsko, Portugalsko, Finsko, Spojené království) a tři stanovují dobu šesti měsíců (Kypr, Lucembursko, Litva). Pět členských států stanovilo různé doby uchovávání pro různé kategorie údajů: dva členské státy (Irsko, Itálie) stanovují dva roky pro údaje o telefonii v rámci pevné a mobilní sítě a jeden rok pro údaje o připojení k internetu, internetové elektronické poště a internetové telefonii; jeden členský stát (Slovinsko) stanovuje 14 měsíců pro údaje o telefonii a osm měsíců pro údaje týkající se internetu; jeden členský stát (Slovensko) stanovuje jeden rok pro údaje o telefonii v rámci pevné a mobilní sítě a šest měsíců pro údaje týkající se internetu; jeden členský stát (Malta) stanovuje jeden rok pro údaje o telefonii v rámci pevné a mobilní sítě a internetové telefonii a šest měsíců pro údaje týkající se připojení k internetu a internetové elektronické pošty. Jeden členský stát (Maďarsko) uchovává veškeré údaje po dobu jednoho roku vyjma údajů o neúspěšných pokusech o volání, které jsou uchovávány pouze po dobu šesti měsíců. Jeden členský stát (Belgie) nestanoví žádnou dobu uchovávání pro kategorie údajů uvedené ve směrnici. Podrobnosti uvádí tabulka č. 3.

Belgie <sup>65</sup>	Mezi 1 rokem a 36 měsíci pro „veřejně dostupné“ telefonní služby. Žádná úprava pro údaje týkající se internetu.
Bulharsko	1 rok, údaje, které byly zpřístupněny, mohou být na žádost uchovávány po dobu dalších 6 měsíců.
Česká republika	Neprovedeno.
Dánsko	1 rok
Německo	Neprovedeno.
Estonsko	1 rok
Irsko	2 roky pro údaje o telefonii v rámci pevné a mobilní sítě, a 1 rok pro údaje o připojení k internetu, internetové elektronické poště a internetové telefonii.
Řecko	1 rok
Španělsko	1 rok
Francie	1 rok
Itálie	2 roky pro údaje o telefonii v rámci pevné a mobilní sítě, a 1 rok pro údaje o připojení k internetu, internetové elektronické poště a internetové

<sup>65</sup> Ustanovení čl. 126 odst. 2 zákona ze dne 13. června 2005 o elektronických komunikacích.

<b>Tabulka č. 3: Doba uchovávání stanovená ve vnitrostátním právu</b>	
	telefonii.
Kypr	6 měsíců
Lotyšsko	18 měsíců
Litva	6 měsíců
Lucembursko	6 měsíců
Maďarsko	6 měsíců pro neúspěšné pokusy o volání a 1 rok pro všechny ostatní údaje.
Malta	1 rok pro údaje o telefonii v rámci pevné a mobilní sítě a internetové telefonii a 6 měsíců pro údaje týkající se připojení k internetu a internetové elektronické pošty.
Nizozemsko	1 rok
Rakousko	Neprovedeno.
Polsko	2 roky
Portugalsko	1 rok
Rumunsko	Neprovedeno (6 měsíců podle předchozího transpozičního právního předpisu, který byl zrušen).
Slovinsko	14 měsíců pro údaje o telefonii a 8 měsíců pro údaje týkající se internetu.
Slovensko	1 rok pro údaje o telefonii v rámci pevné a mobilní sítě, 6 měsíců pro údaje o připojení k internetu, internetové elektronické poště a internetové telefonii.
Finsko	1 rok
Švédsko	Neprovedeno.
Spojené království	1 rok

Přestože rozdílnost přístupu povoluje směrnice, z této rozdílnosti vyplývá, že směrnice přináší pouze omezenou právní jistotu a předvídatelnost napříč EU poskytovatelům, kteří podnikají ve více než jednom členském státě, a občanům, jejichž komunikační údaje mohou být ukládány v různých členských státech. Měly by se zvážit možnosti další harmonizace doby uchovávání v EU vzhledem ke vzrůstající internalizaci zpracovávání údajů a externímu zajišťování služeb uchovávání údajů. S cílem naplnit zásadu proporcionality a ve světle kvantitativních a kvalitativních důkazů o hodnotě uchovávaných údajů v členských státech, a trendů v komunikacích a technologiích a v trestné činnosti a terorismu zváží Komise používání různých dob pro různé kategorie údajů i vhodnost používání různých dob pro různé kategorie závažných trestných činů, případně kombinace obojího<sup>66</sup>. Kvantitativní důkazy předložené dosud členskými státy ohledně stáří uchovávaných údajů naznačují, že v okamžiku podání (prvotní) žádosti o přístup donucovacími orgány je kolem devadesáti procent údajů starých šest či méně měsíců a kolem sedmdesáti procent tří či méně měsíců (viz oddíl 5.2).

#### **4.6. Ochrana a bezpečnost údajů a orgány dozoru (články 7 a 9)**

Směrnice po členských státech požaduje, aby zajistily, že poskytovatelé dodržují alespoň tyto čtyři zásady bezpečnosti údajů, jmenovitě, že:

- (a) uchovávané údaje mají stejnou kvalitu a podléhají stejnému zabezpečení a ochraně jako údaje na (veřejné komunikační) síti;

<sup>66</sup> Návrh Komise směrnice o uchovávání údajů v roce 2005 stanovoval dobu uchovávání jeden rok pro údaje o telefonii a šest měsíců pro údaje o internetu.

- (b) se na údaje vztahují 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;
- (c) údaje podléhají příslušným technickým a organizačním opatřením pro zajištění toho, aby k nim mohly přistupovat pouze zvláště zmocněné osoby; a
- (d) na konci doby uchovávání údajů se všechny tyto údaje zničí, a to vyjma údajů, k nimž bylo přistoupeno a byly zajištěny (pro účely stanovené směrnicí).

V souladu se směrnicí o ochraně údajů a směrnicí o e-soukromí nesmí provozovatelé zpracovávat údaje uchovávané podle směrnice pro jiné účely, pokud by stejné údaje jinak nebyly uchovávány<sup>67</sup>. Členské státy musí určit orgán veřejné moci na svém území pověřený dohledem nad dodržováním těchto zásad, který jedná „zcela nezávisle“ a který může být totožný s orgánem uvedeným ve směrnici o ochraně údajů<sup>68</sup>.

Patnáct členských států provedlo všechny tyto zásady do příslušných právních předpisů. Čtyři členské státy (Belgie, Estonsko, Španělsko, Lotyšsko) provedly dvě nebo tři z těchto zásad, avšak výslovně neukládají, aby byly údaje na konci doby uchovávání zničeny. Dva členské státy (Itálie, Finsko) stanoví, aby údaje byly zničeny. Není zjevné, jaká konkrétní technická a organizační opatření k ochraně údajů, jako je například důkladné ověřování a podrobná evidence přístupu<sup>69</sup>, byla zavedena. Dvacet dva členských států má orgán dozoru pověřený dohledem nad dodržováním těchto zásad. Ve většině případů je tímto orgánem orgán na ochranu údajů. Podrobnosti uvádí tabulka č. 4.

Tabulka č. 4: Ochrana a bezpečnost údajů a orgány dozoru		
Členský stát	Vnitrostátní právní úprava ochrany a bezpečnosti údajů	Orgán dozoru
Belgie	Poskytovatelé musí zajistit, aby předávání údajů nemohlo být zachyceno třetí stranou a aby byly splněny normy pro bezpečnost telekomunikací a zákonného zachycování stanovené Evropským ústavem pro telekomunikační normy <sup>70</sup> . Nezdá se, že by byla upravena zásada povinného zničení údajů na konci doby uchovávání.	Institut pro poštovní služby a telekomunikace
Bulharsko	Transpoziční právní úprava obsahuje požadavek zavést čtyři zásady <sup>71</sup> .	Komise pro ochranu osobních údajů dohlíží na zpracovávání a ukládání údajů s cílem zajistit dodržování zákonných povinností; parlamentní komise v zákonodárném sboru dohlíží na postupy pro ověřování a přístup k údajům

<sup>67</sup> Ustanovení čl. 13 odst. 1 směrnice 95/46/ES.

<sup>68</sup> Článek 28 směrnice 95/46/ES.

<sup>69</sup> Důkladné ověření zahrnuje mechanismus dvojího ověření, jako např. heslo plus biometrické údaje nebo heslo plus token, aby byla zajištěna fyzická přítomnost osoby, která je zodpovědná za zpracování provozních údajů. Podrobná evidence přístupu zahrnuje podrobné sledování přístupu a zpracovávání operací prostřednictvím uchovávání záznamů o totožnosti uživatele, době připojení a prohlížených souborech.

<sup>70</sup> Článek 6, královského výnosu ze dne 9. ledna 2003.

<sup>71</sup> Ustanovení čl. 4 odst. 1 zákona o elektronických komunikacích (v platném znění) z roku 2010.

Tabulka č. 4: Ochrana a bezpečnost údajů a orgány dozoru		
Členský stát	Vnitrostátní právní úprava ochrany a bezpečnosti údajů	Orgán dozoru
Česká republika <sup>72</sup>	Neprovedeno.	
Dánsko	Právní úprava obsahuje čtyři zásady. <sup>73</sup>	Národní IT a telekomunikační úřad dohlíží na dodržování povinností provozovatelů sítí elektronických komunikací a služeb s cílem zajistit, aby technické vybavení a systémy umožňovaly přístup policie k informacím o telekomunikačním provozu.
Německo	Neprovedeno.	
Estonsko	Transpoziční právní úprava pokrývá tři ze čtyř zásad. Žádné výslovné ustanovení ohledně čtvrté zásady, avšak každá osoba, jejíž soukromí bylo narušeno aktivitami souvisejícími se sledováním, může požadovat, aby soud rozhodnutím nařídil zničení údajů <sup>74</sup> .	Příslušným orgánem je orgán technického dozoru.
Irsko <sup>75</sup>	Transpoziční právní úprava obsahuje požadavek zavést čtyři zásady.	Pověřený soudce má pravomoc prošetřit skutečnost, zda příslušné vnitrostátní orgány dodržují povinnosti stanovené v transpozičním právním předpisu, a podávat o tom zprávy.
Řecko <sup>76</sup>	Transpoziční právní úprava obsahuje požadavek zavést čtyři zásady, poskytovatelé mají dále povinnost sestavit a plnit plán zajišťující dodržování povinností pod dohledem pověřeného pracovníka Úřadu pro ochranu osobních údajů.	Úřad pro ochranu osobních údajů a Úřad pro dohled na soukromím při komunikaci.
Španělsko <sup>77</sup>	Ustanovení o bezpečnosti údajů upravují tři ze čtyř zásad (kvalitu a ochranu uchovávaných údajů, přístup oprávněných osob k těmto údajům a ochranu proti neoprávněnému zpracovávání).	Příslušným orgánem je Úřad pro ochranu údajů.
Francie <sup>78</sup>	Transpoziční právní úprava obsahuje požadavek zavést čtyři zásady.	Národní komise pro informační technologie a svobody dohlíží nad dodržováním povinností.

<sup>72</sup> Ustanovení § 87 odst. 3 a § 88 zákona č. 127/2005 ve znění zákona 247/2008; ustanovení § 2 zákona č. 336/2005; ustanovení § 3 odst. 4 vyhlášky č. 485/2005; ustanovení § 28 odst. 1 zákona č. 101/2000.

<sup>73</sup> Zákon o zpracování osobních údajů; nařízení vlády č. 714 ze dne 26. června 2008 o poskytování sítí a služeb elektronických komunikací.

<sup>74</sup> Ustanovení čl. 111 odst. 9 zákona o elektronických komunikacích; ustanovení čl. 122 odst. 2 trestního řádu.

<sup>75</sup> Ustanovení článků 4, 11 a 12, návrhu zákona o komunikacích z roku 2009 (Retention of Data Act).

<sup>76</sup> Článek 6 zákona č. 3917/2011.

<sup>77</sup> Článek 8 zákona 25/2007, čl. 38 odst. 3 zákona o telekomunikacích. Zákon (v článku 9) odkazuje na výjimku pro přístup a zrušení práv stanovených v základním zákoně č. 15/1999 o ochraně osobních údajů (článek 22 a 23).

<sup>78</sup> Ustanovení článku D.98-5, CPCE; ustanovení L-34-1(V), CPCE; článek 34 zákona č. 78-17; ustanovení článku 34-1, CPCE; článek 11 zákona č. 78-17 ze dne 6. ledna 1978.

Tabulka č. 4: Ochrana a bezpečnost údajů a orgány dozoru		
Členský stát	Vnitrostátní právní úprava ochrany a bezpečnosti údajů	Orgán dozoru
Itálie	Právní úprava neobsahuje žádné výslovné ustanovení o bezpečnosti uchovávaných údajů, avšak existuje obecná povinnost zničit nebo anonymizovat provozní údaje a konsensuální zpracování lokalizačních údajů <sup>79</sup> .	Orgán pro ochranu údajů dohlíží na to, zda poskytovatelé dodržují povinnosti uložené směrnicí.
Kypr <sup>80</sup>	Transpoziční právní úprava stanoví každou ze čtyř zásad.	Komisař pro ochranu osobních údajů dohlíží na uplatňování transpoziční právní úpravy.
Lotyšsko <sup>81</sup>	Transpoziční právní úprava stanoví dvě ze zásad: důvěrnost oprávněného přístupu k uchovávaným údajům a zničení údajů na konci doby uchovávání.	Na ochranu osobních údajů v odvětví elektronických komunikací dohlíží úřad státního správce údajů, nedohlíží však na přístup k uchovávaným údajům a na jejich zpracování.
Litva <sup>82</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Státní úřad pro ochranu údajů dohlíží na provádění transpozičního právního předpisu a je zodpovědný za dodávání statistických údajů Evropské komisi.
Lucembursko <sup>83</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Úřad pro ochranu údajů
Maďarsko <sup>84</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Parlamentní komisař pro ochranu údajů a svobodu informací.
Malta <sup>85</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Komisař pro ochranu údajů
Nizozemsko <sup>86</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Agentura pro radiové komunikace dohlíží na dodržování povinnosti ze strany poskytovatelů připojení k internetu a telekomunikací; Úřad pro ochranu údajů dohlíží na všeobecné zpracovávání osobních údajů; spolupráce těchto úřadů je podrobně rozvedena v protokolu.
Rakousko	Neprovedeno.	
Polsko	Transpoziční právní úprava stanoví čtyři zásady <sup>87</sup> .	Úřad pro ochranu údajů
Portugalsko	Transpoziční právní úprava stanoví čtyři zásady <sup>88</sup> .	Portugalský úřad pro ochranu údajů.
Rumunsko	Neprovedeno.	
Slovinsko <sup>89</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Komisař pro informace.

<sup>79</sup> Článek 123 a 126 zákona o ochraně údajů.

<sup>80</sup> Články 14 a 15 zákona č. 183(I)/2007.

<sup>81</sup> Ustanovení čl. 4 odst. 4 a čl. 71 odst. 6 až 8 zákona o elektronických komunikacích.

<sup>82</sup> Ustanovení čl. 12 odst. 5, čl. 66 odst. 8 a 9 zákona o elektronických komunikacích ve znění ze dne 14. listopadu 2009.

<sup>83</sup> Ustanovení čl. 1 odst. 5 zákona ze dne 24. července 2010.

<sup>84</sup> Článek 157 zákona č. C/2003, ve znění zákona č. CLXXIV/2007; článek 2 vyhlášky č. 226/2003; a zákon č. LXIII/1992 o ochraně údajů.

<sup>85</sup> Ustanovení článku 24 A 25 zákona č. 198/2008 (Legal Note); Ustanovení čl. 40(b) zákona o ochraně údajů (Cap. 440).

<sup>86</sup> Ustanovení čl. 13 odst. 5 zákona o telekomunikacích; Plný název protokolu zní: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

<sup>87</sup> Články 180a a 180e zákona o telekomunikacích.

<sup>88</sup> Ustanovení čl. 7 odst. 1 a článku 11 zákona č. 32/2008; články 53 a 54 zákona o ochraně osobních údajů.

<sup>89</sup> Ustanovení čl. 107a odst. 6 a článek 107c zákona o elektronických komunikacích.

Tabulka č. 4: Ochrana a bezpečnost údajů a orgány dozoru		
Členský stát	Vnitrostátní právní úprava ochrany a bezpečnosti údajů	Orgán dozoru
Slovensko <sup>90</sup>	Transpoziční právní úprava stanoví čtyři zásady.	Vnitrostátní regulační a cenový úřad pro oblast elektronických komunikací dohlíží na ochranu osobních údajů.
Finsko	Transpoziční právní úprava stanoví výslovně pouze požadavek zničit údaje na konci doby uchovávání <sup>91</sup> .	Finský regulační orgán pro komunikace dohlíží na to, aby poskytovatelé dodržovali právní úpravu v oblasti uchovávání údajů. Veřejný ochránce práv v oblasti ochrany údajů dohlíží na dodržování zákonnosti při zpracovávání osobních údajů.
Švédsko	Neprovedeno.	
Spojené království	Transpoziční právní úprava stanoví čtyři zásady <sup>92</sup> .	Komisař pro informace dohlíží na uchovávání a/nebo zpracovávání údajů o komunikaci (a jakýchkoliv jiných osobních údajů) a vhodným způsobem ověřuje ochranu osobních údajů. Komisař pro odposlech (soudce v aktivní službě či penzionovaný soudce) dohlíží na získávání komunikačních údajů podle RIPA ze strany státních orgánů. Vyšetřující orgán prošetřuje stížnosti na zneužití údajů, získaných podle transpozičních právních předpisů (RIPA).

Provedení článku 7 není konzistentní. Uchovávané údaje mohou být potenciálně velmi osobní či choulostivé povahy a v rámci celého procesu uchovávání, vyhledávání a používání je nutné soustavě uplatňovat přísné normy ochrany a bezpečnosti těchto údajů, aby se minimalizovalo nebezpečí, že dojde k narušení soukromí, a zachovala důvěra občanů. Komise zváží varianty, jak posílit bezpečnost a ochranu údajů, a to včetně představením konstrukčních řešení, která nenarušují soukromí, aby zajistila, že jsou tyto normy dodržovány jak při uchovávání, tak při předávání. Komise rovněž zohlední doporučení týkající se minimálních pojistek a technických a organizačních bezpečnostních opatření, která navrhla pracovní skupina pro ochranu údajů zřízená podle článku 29 ve zprávě o druhé donucovací akci<sup>93</sup>.

#### 4.7. Statistika (článek 10)

Členské státy mají povinnost poskytovat Komisi výroční statistiky o uchovávání údajů zahrnující:

- případy, kdy byly příslušným orgánům poskytnuty informace v souladu s platnými vnitrostátními právními předpisy,
- dobu, která uplynula ode dne uchování údajů do dne, kdy příslušný orgán požádal o postoupení údajů (tj. stáří údajů); a

<sup>90</sup> Ustanovení § 59a zákona o elektronických komunikacích; ustanovení § S33 zákona č. 428/2002 o ochraně osobních údajů.

<sup>91</sup> Ustanovení čl. 16 odst. 3 zákona o elektronických komunikacích;

<sup>92</sup> Článek 6 nařízení o uchovávání údajů.

<sup>93</sup> Stanovisko č. 3/2006 pracovní skupiny pro ochranu údajů zřízené podle článku 29 f (WP119); Report 01/2010.

– případy, kdy nebylo možné žádosti o poskytnutí údajů vyhovět.

Komise požádala členské státy, aby ve statistice vyžadované podle tohoto ustanovení uvedly podrobnosti o případech individuálních „žádostí“ o údaje. Dodaná statistika se však lišila v rozsahu i v míře podrobnosti: některé členské státy ve svých odpovědích rozlišovaly mezi různými druhy komunikace, některé uváděly stáří údajů v okamžiku podání žádosti, zatímco jiné členské státy uvedly pouze roční statistiku bez jakéhokoliv podrobného rozpisu. Devatenáct členských států<sup>94</sup> dodalo statistiku o počtu žádostí o údaje za rok 2009 a/nebo 2008; patří mezi ně Irsko, Řecko a Rakousko, kde se o údaje žádalo, i když neexistovaly transpoziční právní předpisy v dané době, a Česká republika a Německo, kde byly právní úpravy uchovávání údajů zrušeny. Sedm členských států, které provedly směrnici, nedodalo Komisi statistiku, i když Belgie dodala odhad ročního počtu žádosti pro údaje o telefonii (300 000).

Spolehlivé kvantitativní a kvalitativní údaje jsou klíčové pro prokázání, že existuje nezbytnost a hodnota bezpečnostních opatření, jakým je uchovávání údajů. Akční plán z roku 2006 o opatřeních k mapování trestné činnosti a trestního soudnictví<sup>95</sup> obsahoval cíl vytvořit metodologii pro pravidelný sběr údajů v souladu se směrnicí a pro společné ukazatele a zahrnovat statistiku do databáze Eurostat (pod podmínkou, že údaje splňují kvalitativní normy). Tento cíl nebylo možné naplnit, protože většina členských států provedla plně směrnici až v posledních dvou letech a pro zdroj statistiky použila různé výklady. Komise se bude zaměřovat ve svém budoucím návrhu na novelizaci rámce pro uchovávání údajů, spolu s přezkumem akčního plánu pro statistiku, na vytvoření použitelných postupů pro měření a vykazování, které umožní transparentní a smysluplný dohled nad uchováváním údajů a které nezatíží systémy trestního soudnictví a donucovací orgány nepřiměřenou zátěží.

#### **4.8. Provedení v zemích EHP**

Právní úprava v oblasti uchovávání údajů je v platnosti na Islandu, v Lichtenštejnsku a Norsku<sup>96</sup>.

#### **4.9. Rozhodnutí ústavních soudů týkající se transpozičních právních předpisů**

Rumunský ústavní soud v říjnu 2009 a Německý spolkový ústavní soud v březnu 2010 a Ústavní soud České republiky v březnu 2011 zrušily právní předpisy provádějící směrnici v rámci svých jurisdikcí, protože je shledaly protiústavní. Rumunský soud přijal<sup>97</sup>, že zásah do základních práv je povolený, jestliže jsou dodržena určitá pravidla a stanoveny odpovídající a dostatečné záruky proti svévolnému státnímu zásahu. Nicméně shledal, že s ohledem na judikaturu Evropského soudu pro lidská práva<sup>98</sup> nebyl transpoziční právní předpis jednoznačný ve svém předmětu působnosti a účelu a neměl dostatečné záruky, a rozhodl, že

<sup>94</sup> Česká republika, Dánsko, Německo, Estonsko, Irsko, Řecko, Španělsko, Francie, Kypr, Lotyšsko, Litva, Malta, Nizozemsko, Rakousko, Polsko, Slovinsko, Slovensko, Finsko, Spojené království.

<sup>95</sup> Sdělení Komise (2006) 437, „Rozvoj komplexní a soudržné strategie EU k mapování trestné činnosti a trestního soudnictví: Akční plán EU na období let 2006 – 2010“.

<sup>96</sup> Zákonem provádějícím směrnicí je na Islandu zákon o telekomunikacích č. 81/2003 (ve znění z dubna 2005); v Lichtenštejnsku zákon o telekomunikacích z roku 2006. V Norsku byl transpoziční zákon schválen 5. dubna 2011 a čeká se na vyslovení královského souhlasu.

<sup>97</sup> Rozhodnutí č. 1258 ze dne 8. října 2009 Rumunského ústavního soudu.

<sup>98</sup> Evropský soud pro lidská práva, věc Rotaru v. Rumunsko z roku 2000, Sunday Times v. Spojené království z roku 1979 a Fürst Hans-Adam von Liechtenstein v. Rumunsko z roku 2001.

„trvalá právní povinnost“ uchovávat veškeré provozní údaje po dobu šesti měsíců je neslučitelná s právem na soukromí a svobodu projevu, která zakotvuje článek 8 Evropské úmluvy o lidských právech.

Německý ústavní soud<sup>99</sup> uvedl, že uchovávání údajů vytváří dojem sledování, který může narušit svobodný výkon základních práv. Výslovně uznal, že uchovávání údajů pro úzce vymezené použití s dostatečně vysokou mírou bezpečnosti údajů by nutně nemuselo být v rozporu s německým Základním zákonem. Nicméně soud zdůraznil, že uchovávání takových údajů je vážným omezením práva na soukromí, a tudíž by mělo být přípustné za zvláště omezených okolností, a že doba uchovávání šest měsíců představuje horní limit („*an der Obergrenze*“) toho, co lze považovat za proporcionální (bod 215). O údaje by mělo žádat, pouze pokud již existuje podezření ze spáchání závažného trestného činu nebo důkazy o ohrožení veřejné bezpečnosti, a vyhledávání údajů by mělo být pro určité druhy právem chráněné komunikace zakázáno (tj. komunikace spojené s citovými nebo sociálními potřebami), které jsou založeny na důvěrnosti. Údaje by měly být kódovány s transparentním dohledem nad jejich používáním.

Český ústavní soud<sup>100</sup> zrušil transpoziční právní předpisy na základě toho, že opatření umožňovalo masivní zásah do základních práv a nesplňovalo požadavky kladené na určitost a jasnost z pohledu právního státu. Soud kritizoval účelové omezení jako nedostatečné, úzce vymezené vzhledem k rozsahu a působnosti povinnosti uchovávat údaje. Shledal, že vymezení orgánů oprávněných k přístupu a využití uchovávaných údajů a postupy pro jejich předávání a využití není dostatečně určité v transpozičních právních předpisech, aby byla zajištěna jejich celistvost a důvěrnost. Jednotlivec neměl tudíž dostatečně garantovány adekvátní a efektivní záruky proti riziku zneužití ze strany orgánů veřejné moci. Ústavní soud nepodrobil kritice samotnou směrnicí a uvedl, že obsah samotné směrnice ponechává České republice dostatečný prostor pro její ústavně konformní transpozici do domácího právního řádu. Ústavní soud však v části *obiter dictum* vyjádřil své obavy, zda je preventivního uchovávání provozních a lokalizačních údajů nástrojem nezbytným, efektivním a vhodným, a to zejména při existenci nových metod trestné činnosti páchané za pomoci anonymních SIM karet.

Tyto tři členské státy nyní zvažují, jak opětovně provést směrnicí do právního řádu. Uchovávání údajů bylo rovněž předmětem projednání u ústavního soudu v Bulharsku, kde výsledkem byla novelizace transpozičního práva, na Kypru, kde byly soudní příkazy vydané podle transpozičního práva prohlášeny za protiústavní, a v Maďarsku, kde stále probíhá soudní řízení, které se týká opomenutí uvést v transpozičním zákoně právní účely zpracovávání údajů<sup>101</sup>.

Komise ve svém budoucím návrhu na revizi rámce pro uchovávání údajů zvažuje otázky zmíněné ve vnitrostátní judikatuře.

---

<sup>99</sup> Bundesverfassungsgericht, 1 BvR 256/08, body 1 – 345.

<sup>100</sup> Nález Ústavního soudu ČR ze dne 22. března 2011 k zákonu č. 127/2005 Sb. a vyhlášce 485/2005 Sb., viz zejména body 45-48, 50-51 a 56.

<sup>101</sup> Nejvyšší správní soud Bulharska, rozhodnutí č. 13627, 11. prosince 2008; Nejvyšší soud Kypru, řízení o opravném prostředku ve věci č. 65/2009, 78/2009, 82/2009 a 15/2010-22/2010, 1. února 2011; Stížnost podaná k Ústavnímu soudu Maďarska spolkem pro občanské svobody dne 2. června 2008.

#### 4.10. Probíhající prosazování směrnice

Komise očekává, že členské státy, které dosud ne zcela provedly směrnici, nebo nepřijaly nové právní předpisy nahrazující předpisy, které zrušily vnitrostátní soudy, tak učiní co nejdříve. Pokud se tak nestane, vyhrazuje si Komise použít své pravomoci svěřené jí Smlouvami EU. Soudní dvůr shledal, že v současnosti dva členské státy, které dosud neprovedly směrnici (Rakousko a Švédsko), nesplnily své povinnosti podle práva EU<sup>102</sup>. V dubnu 2011 se Komise rozhodla podruhé obrátit na Soud z důvodu nesplnění povinností vyplývajících z rozsudku ve věci C-185/09 ze strany Švédska a žádala o uložení finančních sankcí podle článku 260 Smlouvy o fungování Evropské unie v návaznosti na rozhodnutí švédského parlamentu, kterým bylo odloženo přijetí transpozičního právního předpisu o 12 měsíců. Komise bude i nadále bedlivě sledovat situaci v Rakousku, které předložilo časový plán pro bezprostřední přijetí transpozičních právních předpisů.

### 5. ROLE UCHOVÁVANÝCH ÚDAJŮ V TRESTNÍM SOUDNICTVÍ A V PROSAZOVÁNÍ PRÁVA

Tento oddíl shrnuje, jaké funkce plní uchovávané údaje podle příspěvků členských států k tomuto hodnocení.

#### 5.1. Objem uchovávaných údajů, ke kterému získaly přístup příslušné vnitrostátní orgány

Objem jak telekomunikačního provozu, tak i žádostí o přístup k provozním údajům roste. Statistika dodaná 19 členskými státy za rok 2008 a/nebo za rok 2009 naznačuje, že celkově v EU bylo každým rokem podáno více než 2 miliony žádostí o údaje, přičemž počet značně kolísá mezi členskými státy, a to od méně než 100 žádostí za rok (Kypr) až k více než 1 milionu (Polsko). Podle údajů dodaných dvanácti členskými státy za roky 2008 a 2009 nejčastěji požadovaným druhem údajů byly údaje o telefonii v mobilních sítích (viz tabulka č. 5, 8 a 12). Statistika neuvádí přesný účel, pro který byla podaná každá jednotlivá žádost. Česká republika, Lotyšsko a Polsko uvedly, že v případě údajů o telefonii v mobilních sítích musí příslušné orgány předložit stejnou žádost každému z hlavních telefonních operátorů, a tudíž skutečný počet žádostí u každého případu je podstatně nižší, než naznačují statistické údaje.

Neexistuje zjevné vysvětlení pro tyto rozdíly, ačkoliv počet obyvatel, převažující trendy trestné činnosti, účelová omezení a podmínky pro přístup k údajům a náklady na získání údajů jsou celkově relevantními faktory.

#### 5.2. Stáří uchovávaných údajů, které byly předmětem přístupu

Na základě statistického rozpisu, který dodalo devět členských států<sup>103</sup> pro rok 2008 (viz shrnutí v tabulce č. 5 a další podrobnosti v příloze) zhruba devadesát procent údajů, které byly předmětem přístupu ze strany příslušných orgánů v daném roce, nebylo starší šesti měsíců a kolem sedmdesáti procent nebylo starší tří měsíců v okamžiku podání (původní) žádosti o přístup k údajům.

<sup>102</sup> Rozhodnutí ve věci C-189/09 a C-185/09.

<sup>103</sup> Česká republika, Dánsko, Estonsko, Irsko, Španělsko, Kypr, Lotyšsko, Malta a Spojené království.

**Tabulka č. 5: Přehled stáří uchovávaných údajů, které byly předmětem přístupu v devíti členských státech, jež dodaly podrobnou statistiku za rok 2008**

<i>Stáří</i>	<i>Telefonie v pevné síti</i>	<i>Telefonie v mobilní síti</i>	<i>Údaje o internetu</i>	<i>Souhrn</i>
Mladší 3 měsíců	61%	70%	56%	67%
Stáří 3 až 6 měsíců	28%	18%	19%	19%
Stáří 6 až 12 měsíců	8%	11%	18%	12%
Starší 1 roku	3%	1%	7%	2%

Podle většiny členských států je využití uchovávaných údajů, které jsou starší tři nebo dokonce šesti měsíců méně časté avšak může být zásadní; jejich využití mělo tendenci se členit do tří kategorií. Zaprvé, o údaje týkající se internetu je tendence žádat později během vyšetřování trestných činů než o jiné druhy důkazů. Analýza údajů o pevných a mobilních telefonních sítích často přináší potenciální stopy, jejichž výsledkem jsou žádosti o starší údaje. Například, pokud se během vyšetřování objeví jméno na základě údajů o telefonii v pevné či mobilní síti, vyšetřovatelé mohou chtít zjistit adresu internetového protokolu (IP), kterou tato osoba používá a mohou chtít zjistit, s kým byla tato osoba v kontaktu z této adresy v určitém časovém období. Za takové situace vyšetřovatelé budou pravděpodobně žádat o údaje, které jim umožní odhalit další IP adresy a zjistit osoby, které používaly tyto IP adresy.

Zadruhé, vyšetřování zvláště závažných trestných činů, sériové trestné činnosti, organizované trestné činnosti a teroristických útoků má tendenci spoléhat se na starší uchovávané údaje zachycující dobu potřebnou k naplánování těchto deliktů, aby se zjistily způsoby trestné činnosti a vztahy mezi pachateli, spolupachateli a účastníky a prokázal úmysl. Aktivitě související se složitými finančními zločiny jsou často odhaleny až po několika měsících. Zatřetí, a výjimečně, si členské státy vyžádaly provozní údaje držené v jiném členském státě, který obvykle může uvolnit tyto údaje na základě soudního povolení v návaznosti na žádost o právní pomoc soudce v dožadujícím členském státě. Tento druh vzájemné právní pomoci může být zdoluhavý, což vysvětluje, proč některé požadované údaje byly starší šesti měsíců.

### **5.3. Přeshraniční žádosti o uchovávané údaje**

Vyšetřování a stíhání trestných činů mohou zahrnovat důkazy či svědectví nebo události z více než jednoho členského státu. Podle statistických údajů dodaných členskými státy méně než 1 % všech žádostí o uchovávané údaje se týkalo údajů držených v jiném členském státě. Donucovací orgány uvedly, že upřednostňují, když o údaje žádají domácí poskytovatele, kteří možná příslušné údaje uchovávají, spíše než zahajovat proceduru vzájemné právní pomoci, které může být zdoluhavá a nijak nezaručuje, že k požadovaným údajům bude poskytnut přístup. Rámcové rozhodnutí 2006/960/SVV o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států<sup>104</sup>, které stanoví lhůty pro poskytování informací na žádost jiného členského státu, se nepoužije, protože uchovávané údaje se považují za informace získané pomocí donucovacích opatření, která nespádají do působnosti tohoto nástroje. Žádný členský stát nebo donucovací orgán nicméně nevyzývá k tomu, aby došlo k většímu usnadnění přeshraniční výměny informací.

<sup>104</sup> Rámcové rozhodnutí Rady 2006/960/SVV ze dne 18. prosince 2006 o zjednodušení výměny operativních a jiných informací mezi donucovacími orgány členských států Evropské unie, Úř. věst. L 386, 29.12.2006. s. 89-100 a Úř. věst. L 200, 1.8.2007, s. 637-648.

#### 5.4. Hodnota uchovávaných údajů pro vyšetřování a stíhání trestných činů

Přestože absolutní počet žádostí o údaje nemusí nutně vyjadřovat, jako mají hodnotu pro jednotlivá vyšetřování trestných činů, uvedly obecně členské státy, že uchovávání údajů je přinejmenším hodnotné a v některých případech nezbytné<sup>105</sup> pro účely prevence trestné činnosti a boje proti ní, včetně ochrany obětí a osvobození nevinných v trestních řízeních. Pro úspěšné odsouzení je třeba vycházet z uznání viny, svědeckých výpovědí nebo forenzních důkazů. Členské státy nahlásily, že byla prokázána nezbytnost uchovávaných provozních údajů pro kontaktování svědků událostí, kteří by jinak nebyli identifikovatelní, a pro získávání důkazů nebo stop dokládajících účast na trestném činu. Některé členské státy<sup>106</sup> dále namítaly, že využití uchovávaných údajů pomohlo zbavit podezření ze spáchání trestného činu, aniž by bylo nutné přistoupit k metodám sledování, např. odposlechu nebo domovním prohlídkám, které lze považovat za více nešetrné.

V EU neexistuje žádná obecná definice „závažného trestného činu“, a proto neexistuje statistika EU o výskytu závažné trestné činnosti nebo o vyšetřování a stíhání závažných trestných činů, i když jsou pravidelně zveřejňovány údaje o trestné činnosti a trestním soudnictví. Souhrnný počet žádostí o uchovávané údaje podle údajů dodaných 19 členskými státy, které poskytly nějaké údaje za rok 2009 a/nebo 2008, byl okolo 2,6 milionu. K této poslední statistice o trestné činnosti a trestním soudnictví, která je k dispozici pro těchto 19 členských států a která se týká všech trestných činů, nikoliv pouze závažných trestných činů, lze uvést, že na každého policejního úředníka vychází pouze více než dvě žádosti za rok, nebo okolo 11 žádostí na každých 100 zaznamenaných trestných činů<sup>107</sup>.

Na základě statistiky a poskytnutých ilustrativních příkladů, které spojují využití historických uchovávaných komunikačních údajů s počtem odsouzení, osvobození, zastavení řízení a zabránění trestné činnosti lze vyvodit řadu závěrů ohledně role a hodnoty uchovávaných údajů pro vyšetřování trestných činů.

##### *Shromáždování důkazního materiálu*

Zprvém, uchovávané údaje umožňují shromáždit soubor důkazů vedoucích k trestnému činu. Jejich pomocí se rozeznávají nebo potvrzují další formy důkazů o aktivitách a vazbách mezi podezřelými. Lokalizační údaje jsou konkrétně používány jak donucovacími orgány, tak obžalovanými, aby se vyloučila přítomnost podezřelých na místě činu nebo potvrdilo alibi. Tyto důkazy mohou tedy zbavit osoby trestního stíhání, a tudíž odstranit nutnost použít více invazivní vyšetřovací metody, nebo vést k osvobození obžalovaného při soudním řízení. Belgie uvedla příklad odsouzení pachatelů, kteří unesli rukojmí s cílem vyvíjet nátlak (tzv.

---

<sup>105</sup> Česká republika považuje uchovávání „zcela nezbytné pro velký počet případů“; Maďarsko uvedlo, že bylo „nezbytné pro pravidelné činnosti (donucovacích orgánů)“; Slovinsko uvedlo, že bez uchovávaných údajů by byly „paralyzovány operace donucovacích orgánů“; Policejní orgány Spojeného království popsaly dostupnost provozních údajů za „zcela zásadní... pro vyšetřování hrozeb terorismu a závažných trestných činů.“

<sup>106</sup> Německo, Polsko, Slovinsko, Spojené království.

<sup>107</sup> V roce 2007 bylo 1,7 mil. policejních úředníků v EU-27, ze kterých 1,2 mil. bylo ve 19 členských státech, které dodaly statistiku o počtu žádostí o uchovávané údaje; v 2007 bylo zaznamenáno 29,2 mil. trestných činů policií v EU, ze kterých 24 mil. bylo zaznamenáno ve 19 členských státech, které dodaly statistiku. (Zdroj: Eurostat 2009).

„tiger kidnapping“) na zaměstnance trestního soudu v Antverpách z roku 2008, při kterém lokalizační údaje spojující aktivity pachatelů s třemi samostatnými městy byly rozhodující pro přesvědčení poroty, že jde o spolupachatele. V jiném případě u vraždy v roce 2007 související s motorkářským gangem lokalizační údaje mobilních telefonů pachatelů prokazovaly, že se tyto osoby nacházely na místě činu v době spáchání vraždy a vedly částečnému doznání<sup>108</sup>. Podle Belgie, Irska a Spojeného království některé trestné činy zahrnující komunikaci přes internet lze vyšetřit *pouze* prostřednictvím uchovávání údajů: například jedinou stopou po vyhrožování v diskusních skupinách na internetu (chat rooms) jsou provozní údaje v kyberprostoru. Podobné platí u trestných činů spáchaných prostřednictvím telefonu. Maďarsko a Polsko uvedly případ podvodu na starých lidech z konce roku 2009 / počátku 2010 spáchaného telefonními hovory, ve kterých pachatelé předstírali, že jsou rodinnými příslušníky, kteří si naléhavě potřebují vypůjčit peníze, přičemž tyto pachatele se podařilo odhalit pomocí uchovávaných údajů.

### *Zahajování vyšetřování*

Zadruhé, byly případy, ve kterých bylo při absenci forenzních důkazů či očitých svědků jedinou možností, jak zahájit vyšetřování, konzultovat uchovávané údaje. Německo uvedlo příklad vraždy policejního úředníka, kdy násilník uprchl ve vozidle oběti, které následně opustil. Bylo možné prokázat, že si následně telefonicky zajišťoval alternativní dopravní prostředek. Nebyly k dispozici forenzní důkazy ani očití svědci k identifikaci vraha a vyšetřující orgán se pro další postup musel spolehnout na dostupnost těchto provozních údajů. V případech sexuálního zneužívání dětí v souvislosti s internetem je uchovávání údajů nezbytným předpokladem pro úspěšné vyšetřování. Vedle dalších vyšetřovacích metod umožňují uchovávané údaje identifikovat uživatele vyobrazení pohlavního zneužívání dítěte<sup>109</sup> a usnadňují identifikaci a vysvobození dětských obětí. Česká republika uvedla, že bez přístupu k uchovávaným údajům týkajícím se internetu by nebylo možné spustit vyšetřování sítě uživatelů a šířitelů dětské pornografie, které bylo součástí „Operace Vilma“. Na úrovni celé EU byla účinnost Operace Rescue (při které pomáhal Europol) na ochranu dětí proti zneužívání podkopávána, protože neexistence transpozičních předpisů v oblasti uchovávání údajů bránila některým členským státům vyšetřovat členy rozsáhlé mezinárodní sítě pedofilů, jež využívali IP adresy, které mohly být až jeden rok staré.

Při vyšetřování kyberkriminality je IP adresa obvykle první stopou. Prosazování práva skrze vyhledávání provozních údajů může identifikovat uživatele skrývajícího se za IP adresou před určením, zda lze zahájit vyšetřování. Může rovněž umožnit policii varovat potenciální oběti kyberútoků: když se policii podaří zabavit řídicí a ovládací server používaný provozovateli botnetu, může pouze vidět IP adresy spojené s tímto serverem; avšak prostřednictvím přístupu k uchovávaným údajům může policie identifikovat a varovat možné oběti, kterým patří tyto IP adresy.

### *Uchovávané údaje jako součást vyšetřování trestných činů*

---

<sup>108</sup> Vnitrostátní úřad ve Spojeném království – *National Policing Improvement Agency, The Journal of Homicide and Major Incident Investigation*, ročník 5, vydání 1, jaro 2009, s. 39-51.

<sup>109</sup> Projekt „Měření a analýza aktivit p2p proti pedofilnímu obsahu“ podporovaný v rámci programu pro bezpečnější internet poskytl přesné informace o pedofilních aktivitách v systému eDonkey peer-to-peer, které umožnily identifikaci 178 000 uživatelů (z 89 milionů prověřovaných uživatelů), kteří požadovali pedofilní obsah.

Zatřetí, přestože donucovací orgány a soudy ve většině členských států nevytváří statistiku uvádějící, jaký druh důkazu se ukázal zásadním pro odsouzení nebo zproštění viny, jsou uchovávané údaje nedílnou součástí vyšetřování a stíhání trestných činů v EU. Některé členské státy uvedly, že nelze vždy oddělit vliv uchovávaných údajů na úspěch vyšetřování a trestního stíhání, protože soudy hodnotí všechny předložené důkazy a zřídka shledají jediný důkaz za rozhodující<sup>110</sup>. Nizozemsko uvedlo, že od ledna do července 2010 byly historické provozní údaje rozhodujícím faktorem ve 24 soudních rozhodnutích. Finsko uvedlo, že v 56 % z 3405 žádostí se potvrdilo, že uchovávané údaje byly buďto „důležité“ nebo „podstatné“ pro odhalení a/nebo stíhání trestných činů. Spojené království dodalo údaje, které se snaží kvantifikovat vliv uchovávaných údajů na trestní stíhání; uvedlo, že u tří jeho donucovacích orgánů byly uchovávané údaje použity ve většině nebo ve všech vyšetřováních, jejichž výsledkem bylo trestní stíhání nebo odsouzení.

## **5.5. Technologický vývoj a používání předplacených SIM karet**

Začtvrté, prosazování práva potřebuje udržovat krok s technologickým vývojem, jehož výtěžky jsou používány pro páchání trestné činnosti či jejímu napomáhání. Uchovávaní údajů patří mezi vyšetřovací nástroje, které jsou nezbytné k tomu, aby donucovací orgány mohly řešit aktuální výzvy týkající se trestné činnosti, co se týče její různorodosti, rozsahu a nápadu, a to zvládnutelným a nákladově efektivním způsobem. Řadu stále běžnějších forem komunikace směrnice nepokrývá. Virtuální soukromé sítě (VPN), například univerzitní nebo větších podniků, umožňují, aby se několik uživatelů připojilo k internetu za pomoci jednoho přístupového portálu ze stejné IP adresy. Nyní však přicházejí nové technologie, které umožňují přidělit adresy individuální uživatelům sítí VPN.

V rámci EU se podíly uživatelů mobilních telefonů s předplacenými kartami různí. Některé členské státy tvrdily, že anonymní předplacené SIM karty, zejména pokud jsou zakoupeny v jiném členské státě, mohou být rovněž využity osobami účastnicími se trestné činnosti jako prostředek, který brání identifikaci při vyšetřování<sup>111</sup>. Šest členských států (Dánsko, Španělsko, Itálie, Řecko, Slovensko, Bulharsko) přijalo opatření, která stanoví povinnou registraci předplacených SIM karet. Tyto a další členské státy (Polsko, Kypr, Litva) argumentovaly ve prospěch opatření pro celou EU, které by nařídilo povinnou registraci totožnosti uživatelů předplacených služeb. Nebyly předloženy žádné důkazy o účinnosti těchto vnitrostátních opatření. Zdůrazněna byla možná omezení, například v případě odcizení totožnosti nebo když je SIM karta zakoupena třetí osobou nebo uživatel využívá roamingu u karty zakoupené v třetí zemi. Celkově není v dané fázi Komise přesvědčena o potřebě reagovat v této oblasti na úrovni EU.

## **6. DOPAD UCHOVÁVÁNÍ ÚDAJŮ NA POSKYTOVATELE A SPOTŘEBITELE**

### **6.1. Poskytovatelé a spotřebitelé**

Ve společném prohlášení pro Komisi pět hlavních průmyslových svazů uvedlo, že hospodářský dopad směrnice je „podstatný“ nebo „enormní na malé provozovatele“, protože

---

<sup>110</sup> Belgie, Česká republika a Litva

<sup>111</sup> Závěry Rady Evropské unie o boji proti zneužívání elektronických komunikací a jejich anonymity pro účely trestné činnosti.

směrnice ponechává „značný manévrovací prostor“<sup>112</sup>. Osm poskytovatelů předložilo široce se rozcházející odhady nákladů, pokud jde o kapitálové a provozní výdaje na dosažení souladu se směrnicí. Tato tvrzení mohou podpořit ukazatele míry náhrad nákladů vzniklých poskytovatelům, které dodaly čtyři členské státy (viz tabulka č. 6).

Studie realizovaná před provedením směrnice ve většině členských státech odhadla náklady na vytvoření systému pro uchovávání údajů v případě poskytovatele internetu, který obsluhuje půl milionu zákazníků, na okolo 375 240 EUR v prvním roce a 9 870 EUR na provozní náklady v každém následujícím měsíci<sup>113</sup>, náklady na vytvoření systému na vyhledávání údajů na 131 190 EUR a jeho provozní náklady na 28 960 EUR měsíčně. Německý ústavní soud však ve svém rozhodnutí ze dne 2. března 2010 shledal, že uložení povinnosti uchovávat údaje „nebylo pro dotčené poskytovatele služby nadměrně zatěžující (ani) nepřiměřené s ohledem na finanční zátěž vzniklou podnikům v důsledku povinnosti uchovávat údaje“<sup>114</sup>. Náklady na uchovávání údajů v přepočtu na jednotku jsou v obráceném poměru k velikosti poskytovatele a míře standardizace přijaté členským státem pro vzájemnou interakci s poskytovateli<sup>115</sup>.

Většina poskytovatelů ve svých odpovědích na dotazník Komise uvedla, že směrnice neměla větší dopad na hospodářskou soutěž, maloobchodní spotřebitelské ceny nebo investice do nové infrastruktury a služeb.

Nejsou důkazy žádného vyčíslitelného nebo podstatného vlivu směrnice na spotřebitelské ceny za služby elektronických komunikací; spotřebitelské organizace nepřispěly do veřejné konzultace v roce 2009 žádným příspěvkem. Průzkum provedený v Německu pro organizaci občanské společnosti naznačil, že spotřebitelé zamýšlí změnit své komunikační návyky a v některých situacích nepoužívat služeb elektronických komunikací, avšak neexistují podpůrné důkazy, že by k takové změně chování docházelo buď v dotčeném členském státě nebo obecně jinde v EU<sup>116</sup>.

Komise hodlá posoudit dopad budoucích změn směrnice na průmysl a spotřebitele, a to možná i za pomoci zvláštního průzkumu agentury Eurobarometer, který by změnil postoj veřejnosti.

## 6.2. Náhrada nákladů

Směrnice neupravuje náhradu nákladů vzniklých poskytovatelům v důsledku povinnosti uchovávat údaje. Za náklady se mohou považovat:

- (a) *provozní výdaje*, tj. provozní náklady nebo opakované výdaje, které souvisí s hospodářskou činností, nástroji, komponenty, zařízením nebo vybavením; a

---

<sup>112</sup> [http://www.gsmeurope.org/documents/Joint\\_Industry\\_Statement\\_on\\_DRD.PDF](http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF)

<sup>113</sup> Wilfried Gansterer & Michael Ilger, *Data retention – The EU Directive 2006/24/EC from a Technological Perspective*, Vídeň: Verlag Medien und Recht, 2008

<sup>114</sup> Bundesverfassungsgericht, 1 BvR 256/08 z 2. března 2010, bod 299.

<sup>115</sup> <http://www.etsi.org/website/technologies/lawfulinterception.aspx>

<sup>116</sup> Průzkum provedla organizace Forsa pro AK Vorratsdatenspeicherung; [http://www.vorratsdatenspeicherung.de/images/forsa\\_2008-06-03.pdf](http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf)

- (b) *kapitálové výdaje*, tj. výdaje vytvářející budoucí zisky, nebo náklady na vývoj či vytvoření nespotebitelných částí výrobku nebo systému, mezi které mohou patřit náklady na zaměstnance a výdaje na vybavení, např. nájem, služby a energie.

Každý členský stát má nějakou formu náhrady nákladů, pokud jsou údaje požadovány v rámci trestního řízení u soudu. Dva členské státy uvedly, že nahrazují jak provozní, tak kapitálové výdaje. Šest členských států nahrazuje pouze provozní výdaje. Žádný jiný režim náhrady nákladů nebyl Komisi oznámen. Podrobnosti uvádí tabulka č. 6.

<b>Tabulka č. 6: Členské státy, které nahrazují náklady</b>			
<b>Členský stát</b>	<b>Provozní výdaje</b>	<b>Kapitálové výdaje</b>	<b>Roční výdaje na náhradu nákladů (miliony EUR)</b>
Belgie	Ano	Ne	22 (2008)
Bulharsko	Ne	Ne	-
Česká republika	Neprovedeno <sup>117</sup> .		
Dánsko	Ano	Ne	-
Německo	Neprovedeno.		
Estonsko	Ano	Ne	-
Irsko	Ne	Ne	-
Řecko	Ne	Ne	-
Španělsko	Ne	Ne	-
Francie	Ano	Ne	-
Itálie	-	-	-
Kypr	Ne	Ne	-
Lotyšsko	Ne	Ne	-
Litva	Ano, na základě odůvodněné žádosti.	Ne	-
Lucembursko	Ne	Ne	-
Maďarsko	Ne	Ne	-
Malta	Ne	Ne	-
Nizozemsko	Ano	Ne	-
Rakousko	Neprovedeno.		
Polsko	Ne	Ne	-
Portugalsko	Ne	Ne	-
Rumunsko	Neprovedeno.		
Slovinsko	Ne	Ne	-
Slovensko	Ne	Ne	-
Finsko	Ano	Ano	1
Švédsko	Neprovedeno.		
Spojené království	Ano	Ano	55 (celkové náhrady vzniklé za tři roky).

Z výše uvedeného lze uzavřít, že směrnice nedosáhla zcela svého cíle, kterým bylo zavést rovné podmínky pro poskytovatele v EU. Komise zváží varianty, jak minimalizovat překážky fungování vnitřního trhu tím, že zajistí, aby poskytovatelům byly jejich náklady vzniklé

<sup>117</sup> Před zrušením zákona, který prováděl směrnici, Česká republika nahrazovala jak provozní, tak kapitálové výdaje a oznámila, že náhrady nákladů činily 6,8 mil. EUR v roce 2009.

v souvislosti s dodržováním povinností uchovávat údaje konzistentně nahrazovány, se zvláštní pozorností věnovanou malým a středním podnikům.

## 7. DOPADY UCHOVÁVÁNÍ ÚDAJŮ NA ZÁKLADNÍ PRÁVA

### 7.1. Základní právo na soukromí a ochranu osobních údajů

Uchovávaní údajů představuje omezení práva na soukromý život a ochranu osobních údajů, která jsou základními právy v EU<sup>118</sup>. Tato omezení musí být, podle čl. 52 odst. 1 Listiny základních práv, „stanovena zákonem a respektovat podstatu těchto práva a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práva a svobod druhého“. To v praxi znamená, že jakékoliv omezení musí<sup>119</sup>:

- (a) být formulováno přesným a předvídatelným způsobem;
- (b) být nutné pro realizaci cíle obecného zájmu nebo pro ochranu práv a svobod druhého;
- (c) být přiměřené sledovanému cíli; a
- (d) respektovat podstatu dotyčných základních práv.

Ustanovení čl. 8 odst. 2 Evropské úmluvy o lidských právech rovněž uznává, že zásah státního orgánu do práva na soukromí musí být odůvodněn nezbytností v zájmu národní bezpečnosti, veřejné bezpečnosti a předcházení zločinnosti<sup>120</sup>. Ustanovení čl. 15 odst. 1 směrnice o e-soukromí a body odůvodnění směrnice o uchovávaní údajů zdůrazňují tyto zásady, na kterých je založen přístup EU k uchovávaní údajů.

V následné judikatuře Evropského soudního dvora a Evropského soudu pro lidská práva byly stanoveny podmínky, které musí každé omezení práva na soukromí splňovat. Bude-li směrnice měněna, jsou tato soudní rozhodnutí relevantní, zejména pokud jde o podmínky pro přístup a využití uchovávaných údajů.

*Každé omezení práva na soukromí musí být přesně vymezené a umožňovat předvídatelnost*

Ve věci *Österreichischer Rundfunk* Evropský soudní dvůr rozhodl, že jakýkoliv zákonný zásah do práva na soukromí musí být „vymezen v souladu požadavkem předvídatelnosti tak přesně, aby adresáti zákonné normy podle toho mohli uzpůsobit své chování“.

*Každé omezení práva na soukromí musí nezbytné a obsahovat minimální záruky*

---

<sup>118</sup> Článek 7 a článek 8 Listiny základních práv Evropské unie (Úř. věst. C 83, 30.3.2010, s. 389) zaručují, že každý má právo „na ochranu osobních údajů, které se ho týkají“. Článek 16 Smlouvy o fungování Evropské unie (Úř. věst. C 83, 30.3.2010, s. 1) také zakotvuje právo každého na „ochranu osobních údajů, které se ho týkají“.

<sup>119</sup> Viz Kontrolní seznam základních práv pro všechny legislativní návrhy ve Sdělení Komise KOM(2010) 573/4, „Strategie účinného uplatňování Listiny základních práv Evropskou unií“.

<sup>120</sup> Článek 8 Úmluvy o ochraně lidských práv a základních svobod (ETS č. 5), Rada Evropy, 4.11.1950

Ve věci Copland v. Spojené království, která se týkala monitorování soukromých telefonních hovorů, e-mailové korespondence a používání internetu ze strany státu, rozhodl Evropský soud pro lidská práva, že takové omezení práva na soukromí je možné považovat za nezbytné, pouze pokud je založeno na příslušných vnitrostátních právních předpisech<sup>121</sup>. Ve věci S. a Marper v. Spojené království, která se týkala uchovávání profilů DNA a otisků prstů každé osoby zproštěné obvinění z trestného činu nebo jejíž stíhání bylo zastaveno před odsouzením, rozhodl Evropský soud pro lidská práva, že takové omezení práva na soukromí je ospravedlnitelné sledovanému cíli, pouze pokud reaguje na palčivou sociální potřebu, je přiměřené sledovanému cíli a důvody uváděné státním orgánem pro jeho zavedení jsou relevantní a dostačující<sup>122</sup>. Základní zásady ochrany údajů vyžadují, aby uchovávání údajů bylo přiměřené účelu jejich sběru a aby byla omezena doba jejich uchovávání<sup>123</sup>. V případě telefonních odposlechů, tajného sledování a skrytého shromažďování informací zpravodajskými metodami „bylo zásadním... mít jasnou, podrobnou úpravu působnosti a použití opatření, jakož i minimální záruky týkající mimo jiné trvání, ukládání, použití, přístupu třetích osob, postupů zabezpečujícím celistvost a důvěrnost údajů a postupů jejich ničení, a tudíž poskytovat dostatečné záruky proti nebezpečí zneužití údajů a svévolnosti.“

*Každé omezení práva na soukromí musí být přiměřené obecnému zájmu*

Evropský soudní dvůr obdobně ve svém rozhodnutí ve věci Schecke a Eifert týkajícím se zveřejnění jmen všech příjemců zemědělských dotací na internetu<sup>124</sup> shledal, že zpracovávání těchto osobních údajů nebylo založeno na souhlasu uživatelů a že tvůrci zákona podle všeho nepřijali vhodné kroky k tomu, aby uvedli do rovnováhy dodržování podstaty práva na soukromí a obecný zájem (transparentnost), jak je uznává EU. Soud zejména shledal, že zákonodárci nevezali v úvahu další metody, které by odpovídaly cíli a méně by zasahovaly do práva příjemců dotací na respektování jejich soukromí a ochranu osobních údajů. V důsledku toho Soud rozhodl, že zákonodárci překročili limity proporcionality, protože omezení týkající se ochrany osobních údajů musí být provedeno v mezích toho, co je naprosto nezbytné“.

## **7.2. Kritika zásady uchovávat údaje**

Na Komisi se písemně obrátilo mnoho skupin občanské společnosti s tvrzením, že uchovávání údajů je v zásadě neopodstatněným a zbytečným omezením práva na soukromí. Považují „všeobecné a nerozlišující“ uchovávání údajů o telekomunikačním provozu jednotlivců, lokalizačních a uživatelských údajů, se kterým nebyl vysloven souhlas, za nezákonné omezení základních práv. Poté, co byla otázka legality směrnice předložena soudu v jednom členském státě (Irsko) sdružením občanské společnosti, se očekává, že bude věc postoupena Evropskému soudnímu dvoru k rozhodnutí<sup>125</sup>. Rovněž evropský inspektor ochrany údajů vyjádřil své obavy ohledně nezbytnosti opatření.

---

<sup>121</sup> Rozsudek Evropského soudu pro lidská práva ve věci Copland v. Spojené království, Štrasburk, 3.4.2007, s. 9.

<sup>122</sup> Rozsudek Evropského soudu pro lidská práva ve věci Marper v. Spojené království, Štrasburk, 4.12.2008, s. 31.

<sup>123</sup> Rozsudek Evropského soudu pro lidská práva ve věci Marper v. Spojené království, Štrasburk, 4.12.2008, s. 30.

<sup>124</sup> Rozhodnutí ve věci C-92/09 Volker a Markus Schecke GbR v. Hesensko a C-93/09 Eifert v. Hesensko a Bundesanstalt für Landwirtschaft und Ernährung, ze dne 9. listopadu 2010.

<sup>125</sup> Dne 5. května 2010 přijal irský vrchní soud návrh organizace Digital Rights Ireland Limited na vznesení předběžné otázky Evropskému soudnímu dvoru podle článku 267 Smlouvy o fungování Evropské unie (předběžná otázka).

### 7.3. Volání po přísnějších pravidlech pro bezpečnost a ochranu údajů

Zpráva Pracovní skupiny pro ochranu údajů zřízené podle článku 29 o druhé donucovací akci namítala, že rizika porušení důvěrnosti sdělení a svobody projevu jsou inherentní u každého uchovávání provozních údajů. Kritizovala některé aspekty vnitrostátních transpozičních právních předpisů, konkrétně zápis údajů, doby uchovávání, druhy uchovávaných údajů a opatření pro zajištění bezpečnosti údajů. Pracovní skupina uvedla případy, ve kterých byl uchováván *obsah* sdělení na internetu, což nespadá do působnosti směrnice, včetně IP adresy adresáta sdělení, URL internetových stránek, nadpisy e-mailů a seznam adresátů v položce „cc“. Vyzvala proto k objasnění, že kategorie jsou vyčerpávající a že by poskytovatelům neměly být na ukládány žádné další povinnosti v souvislosti s uchováváním údajů.

Evropský inspektor ochrany údajů uvedl, že směrnice „neharmonizovala vnitrostátní právní předpisy“ a že použití uchovávaných údajů není přísně omezeno účelem boje proti závažné trestné činnosti<sup>126</sup>. Zmínil, že nástroj EU obsahující pravidla pro povinné uchovávání údajů by měl, v případě prokázání nezbytnosti, obsahovat rovněž pravidla týkající se přístupu donucovacích orgánů k údajům a dalšího použití uchovávaných údajů. Vyzval EU, aby přijala komplexní legislativní rámec, který nejen uloží poskytovatelům povinnosti uchovávat údaje, ale rovněž upraví způsoby, jakými mohou členské státy využít údaje pro účely prosazování práva tak, aby vznikla „právní jistota pro občany“.

Orgány pro ochranu údajů obecně tvrdily, že ze samotného uchovávání údajů vyplývá riziko možného narušení soukromí, které směrnice na úrovni EU neřeší, přičemž namísto tohoto ukládá členským státům, aby zajistily, že jsou dodržována vnitrostátní pravidla pro ochranu údajů. Přestože neexistují konkrétní příklady závažného narušení soukromí, riziko, že bez zavedení dalších pojištění dojde k porušení bezpečnosti údajů, bude přetrvávat, a může narůstat v souvislosti s technologickým vývojem a trendy v oblasti komunikací, ať již jde o uchovávání údajů pro obchodní nebo bezpečnostní účely, uvnitř či vně EU.

## 8. ZÁVĚRY A DOPORUČENÍ

Tato zpráva zdůraznila řadu výhod stávajícího režimu uchovávání údajů v EU i oblasti, kde je vhodné tento režim zdokonalit. EU přijala směrnici v době, kdy existovalo zvýšené riziko bezprostředních teroristických útoků. Posouzení dopadů, které Komise hodlá provést, přinese příležitost posoudit uchovávání údajů v EU, pokud jde o jeho nezbytnost a přiměřenost, s ohledem na vnitřní bezpečnost, hladké fungování vnitřního trhu, posílení úcty k soukromí a základnímu právu na ochranu osobních údajů a v jejich zájmu. Návrh Komise na revizi rámce pro uchovávání údajů by měl vycházet z následujících závěrů a doporučení.

### 8.1. EU by měla podpořit a regulovat uchovávání údajů jako nezbytné bezpečnostní opatření

Většina členských států zastává stanovisko, že pravidla EU pro uchovávání údajů jsou i nadále nezbytným nástrojem pro prosazování práva, ochranu obětí a systémy trestního soudnictví. Důkazy ve formě statistických údajů a příkladů dodaných členskými státy jsou

---

<sup>126</sup> Projev pana Petera Hustinxe na konferenci s názvem Taking on the Data Retention Directive ze dne 3. prosince 2010

určítým způsobem omezené, avšak přesto dokládají velmi důležitou roli, jakou hrají uchovávané údaje při vyšetřování trestných činů. Uchovávané údaje poskytují hodnotná vodítka a důkazy pro prevenci a stíhání trestných činů a zajišťují výkon trestní spravedlnosti. Výsledkem jejich využití byla odsouzení za trestné činy, která by bez uchovávaných údajů možná nebyla nikdy vynesena. Jejich výsledkem byla i osvobození nevinných osob. Harmonizovaná pravidla v této oblasti by měla zajistit, aby uchovávání údajů bylo účinným nástrojem při boji proti trestné činnosti, aby pro průmysl existovala právní jistota hladkého fungování vnitřního trhu a aby se dodržovala vysoká míra respektování soukromí a ochrany osobních údajů soudržné napříč celou EU.

## **8.2. Provedení nebylo rovnoměrné**

Právní předpisy prováděcí směrnici platí ve 22 členských státech. Značný prostor, který byl ponechán členským státům pro přijetí opatření v oblasti uchovávání údajů podle čl. 15 odst. 1 směrnice o e-soukromí, činí posouzení směrnice o uchovávání údajů značně problematickým. Existují značné rozdíly mezi transpozičními právními předpisy v oblasti účelového omezení, přístupu k údajům, doby uchovávání, ochrany a bezpečnosti údajů a statistiky. Tři členské státy neplní povinnosti stanovené směrnicí, protože jejich právní předpisy provádějící směrnici byly zrušeny ústavními soudy. Další dva členské státy musí směrnici ještě provést. Komise bude i nadále pracovat se všemi členskými státy na tom, aby jim pomohla zajistit účinné provedení směrnice. Komise bude rovněž i nadále plnit svou roli strážkyně povinností stanovených v právu EU, a to případně i použitím řízení pro nesplnění povinnosti.

## **8.3. Směrnice neúplně harmonizovala přístup k uchovávání údajů a nevytvořila rovné podmínky pro poskytovatele**

Směrnice zajistila, že se údaje nyní uchovávají ve většině členských států. Směrnice sama o sobě nezaručuje, že uchovávané údaje jsou ukládány, vyhledávány a používány zcela v souladu s právem na soukromí a ochranu osobních údajů. Odpovědnost zajistit, aby byla tato práva dodržována, leží na členských státech. Směrnice usilovala pouze o částečnou harmonizaci přístupu k uchovávání údajů; není proto překvapivé, že neexistuje společný přístup, pokud jde o zvláštní ustanovení směrnice, jako jsou účelová omezení nebo doby uchovávání, nebo pokud jde o aspekty, na které se nevztahuje, jako je náhrada nákladů. Nad míru rozdílnosti, kterou výslovně stanovuje směrnice, však rozdíly ve vnitrostátním úpravě uchovávání údajů představují pro poskytovatele značné komplikace.

## **8.4. Systematičtěji nahrazovat náklady vzniklé poskytovatelům**

I nadále přetrvává nedostatek právní jistoty pro průmysl. Povinnost uchovávat a vyhledávat údaje představuje pro poskytovatele, zejména menší podnikatele, podstatné náklady, přičemž provozovatelé jsou jimi zasaženi různou měrou a různě jsou jim nahrazovány v různých členských státech, i když nejsou důkazy, že by byl v důsledku směrnice negativně zasažen celý sektor telekomunikací. Komise zváží způsoby poskytování konzistentních náhrad nákladů poskytovatelům.

## **8.5. Zajistit přiměřenost v celém procesu ukládání, vyhledávání a použití údajů**

Komise zajistí, aby každý budoucí návrh týkající se uchovávání údajů respektoval zásadu proporcionality a byl přiměřený cíli, kterým je boj proti závažné trestné činnosti a terorismu, a nepřekračoval rámec toho, co je nezbytné k dosažení tohoto cíle. Uzná, že jakákoliv výjimka nebo omezení ochrany osobních údajů se provede pouze v mezích toho, co je nezbytné.

Důkladně posoudí dopady přísnější regulace ukládání a využití údajů a přístupu k nim na účinnost a účelnost systémů trestního soudnictví a pro prosazování práva, na soukromí a na náklady veřejné správy a poskytovatelů. Tyto oblasti by se měly v posouzení dopadů zvláště prozkoumat:

- soudržnost u účelových omezení pro uchovávání údajů a druhy trestných činů, u kterých lze k údajům získat přístup a využít je;
- větší harmonizace u dob povinného uchovávání a případně jejich zkrácení;
- zajištění nezávislého dohledu nad žádostmi o přístupu k údajům a celkovým uchováváním údajů a režimy pro přístup k nim, které existují ve všech členských státech;
- omezení počtu orgánů, které mají oprávnění přístupu k údajům;
- snížení kategorií údajů, které se mají uchovávat;
- vodítka pro technická a organizační bezpečnostní opatření týkající se přístupu k údajům, včetně postupů pro předávání agendy;
- vodítka pro využití údajů, včetně prevence vytěžování údajů; a
- vytvoření použitelných postupů pro metodiku měření a vykazování s cílem usnadnit porovnávání budoucího nástroje ve vztahu k jeho uplatňování a hodnocení.

Komise rovněž zváží, zda a případně jak přístup EU k zajišťování údajů může doplnit jejich uchovávání.

S odkazem na „kontrolní seznam“ v oblasti lidských práv a přístup ke správě informací v prostoru svobody, bezpečnosti a práva<sup>127</sup> zváží každou z těchto oblastí Komise podle zásad proporcionality a požadavku předvídatelnosti. Komise rovněž zajistí soudržnost s probíhajícím přezkumem rámce EU pro ochranu údajů<sup>128</sup>.

## 8.6. Další postup

Ve světle tohoto posouzení navrhne Komise revizi stávajícího rámce pro uchovávání údajů. V konzultaci se zájmovými skupinami z oblasti prosazování práva, soudnictví, průmyslu a spotřebitelů, orgány pro ochranu údajů a organizacemi občanské společnosti navrhne řadu variant. Dále prozkoumá, jak veřejnost vnímá uchovávání údajů a jeho dopad na chování lidí. Tato zjištění budou představovat vstupy pro posouzení dopadů navrhovaných politických variant, které budou základem pro návrh Komise.

---

<sup>127</sup> Viz výše sdělení o provádění Listiny základních práv, „Přehled o správě informací v prostoru svobody, bezpečnosti a práva“, KOM(2010)385, 20.7.2010.

<sup>128</sup> KOM(2010) 609, 4.11.2010.

## Příloha: Doplňující statistika týkající se uchování provozních údajů

### Poznámky:

1. Stářím údajů se myslí doba, která uplynula ode dne uchování údaje do dne, kdy příslušný orgán požádal o předání údaje.
2. Internetovými údaji se myslí údaje týkající se připojení k internetu, internetové elektronické pošty a internetové telefonie.
3. Statistické údaje pro Česko republiku, Lotyšsko a Polsko podléhají upřesnění (viz oddíl 5.1).

### Statistické údaje dodané členskými státy za rok 2008

<b>Tabulka č. 7: Žádosti o uchovávané údaje podle stáří v roce 2008</b>									
Stáří požadovaných údajů (v měsících) / členský stát	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Celkem
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	102691	18440	10110	319	0	0	0	0	131560
Dánsko	2669	672	185	37	23	2	7	4	3599
Německo	9363	2336	985	0	0	0	0	0	12684
Estonsko	2773	733	157	827	0	0	0	0	4490
Irsko	8981	2016	936	1855	90	85	78	54	14095
Řecko	Nerozčleněno podle stáří								
Španělsko	22629	15868	10298	4783	0	0	0	0	53578
Francie	Nerozčleněno podle stáří								
Itálie	Nedodáno								
Kypr	30	4	0	0	0	0	0	0	34
Lotyšsko	10539	2739	1368	1211	597	438	0	0	16892
Litva	55735	23817	5251	512	0	0	0	0	85315
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	810	59	0	0	0	0	0	0	869
Nizozemsko	Nerozčleněno podle stáří								
Rakousko	Nerozčleněno podle stáří								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nerozčleněno podle stáří								
Slovensko	Nedodáno								
Finsko	9134	1144	448	214	268				4008
Švédsko	Nedodáno								
Spojené království	315350	88339	34665	19398	6385	2973	1536	1576	470222
<b>Celkem</b>	<b>533504</b>	<b>156167</b>	<b>64403</b>	<b>29156</b>	<b>7095*</b>	<b>3230*</b>	<b>1353*</b>	<b>1366*</b>	<b>1392281</b>

\* Vyjma Finska

<b>Tabulka č. 8: Žádosti o uchovávané provozní údaje podle druhu údaje v roce 2008 (v závorkách případný počet případů, u kterých nebylo možné žádosti vyhovět)</b>				
<b>Druh údajů / členský stát</b>	<b>Telefonie v pevné síti</b>	<b>Telefonie v mobilní síti</b>	<b>Internetové údaje</b>	<b>Celkem</b>
Belgie	Nedodáno			
Bulharsko	Nedodáno			
Česká republika	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Dánsko	192 (0)	3273 (5)	134 (0)	3599 (5)
Německo	Nerozčleněno podle druhu			12684 (931)
Estonsko	4114 (1519)	376 (7)	Nedodáno	4490 (1526)
Irsko	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Řecko	Nerozčleněno podle druhu			584
Španělsko	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Francie	Nerozčleněno podle druhu			503437
Itálie	Nedodáno			
Kypr	3 (0)	31 (5)	0 (0)	34 (5)
Lotyšsko	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Litva	765 (72)	84550 (5657)	Nedodáno	85315 (5729)
Lucembursko	Nedodáno			
Maďarsko	Nedodáno			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Nizozemsko	Nerozčleněno podle druhu			85000
Rakousko	Nerozčleněno podle druhu			3093
Polsko	Nedodáno			
Portugalsko	Nedodáno			
Rumunsko	Nedodáno			
Slovinsko	Nerozčleněno podle druhu			2821
Slovensko	Nedodáno			
Finsko	Nerozčleněno podle druhu			4008
Švédsko	Nedodáno			
Spojené království	90747 (0)	329421 (0)	50054 (0)	470222 (0)
<b>Celkem</b>				1392281

<b>Tabulka č. 9: Žádosti o uchovávané provozní údaje o telefonii v pevné síti, kde údaje byly předány, podle stáří, v roce 2008</b>									
<b>Stáří požadovaných údajů (v měsících) / členský stát</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Celkem</b>
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	3669	916	143	124	0	0	0	0	4852
Dánsko	133	28	31	0	0	0	0	0	192
Německo	Nedodáno								
Estonsko	1876	161	74	484	0	0	0	0	2595
Irsko	4118	712	197	182	32	21	23	16	5301
Řecko	Nedodáno								
Španělsko	1948	1431	741	328	0	0	0	0	4448
Francie	Nedodáno								
Itálie	Nedodáno								
Kypr	3	0	0	0	0	0	0	0	3
Lotyšsko	698	213	167	193	104	137	0	0	1512
Litva	251	442	0	0	0	0	0	0	693
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	28	1	0	0	0	0	0	0	29
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nedodáno								
Slovensko	Nedodáno								
Finsko	Nedodáno								
Švédsko	Nedodáno								
Spojené království	54805	27052	5340	753	1135	437	1050	175	90747
<b>Celkem</b>	<b>67529</b>	<b>30956</b>	<b>6693</b>	<b>2064</b>	<b>1271</b>	<b>595</b>	<b>1073</b>	<b>191</b>	<b>110372</b>

<b>Tabulka č. 10: Žádosti o uchovávané provozní údaje o telefonii v mobilní síti, kde údaje byly předány, podle stáří, v roce 2008</b>									
<b>Stáří požadovaných údajů (v měsících) / členský stát</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Celkem</b>
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	98232	17013	7518	1	0	0	0	0	122764
Dánsko	2433	628	143	33	20	1	7	3	3268
Německo	Nedodáno								
Estonsko	248	58	35	28	0	0	0	0	369
Irsko	4326	820	230	240	57	63	52	37	5825
Řecko	Nedodáno								
Španělsko	17403	12114	7444	3052	0	0	0	0	40013
Francie	Nedodáno								
Itálie	Nedodáno								
Kypr	23	3	0	0	0	0	0	0	26
Lotyšsko	8928	2298	1085	746	394	257	0	0	13708
Litva	55484	23375	14	20	0	0	0	0	78893
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	575	53	0	0	0	0	0	0	628
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nedodáno								
Slovensko	Nedodáno								
Finsko	Nedodáno								
Švédsko	Nedodáno								
Spojené království	22937 5	52241	2622 8	1604 0	333 3	52 1	33 9	134 4	329421
<b>Celkem</b>	<b>41702 7</b>	<b>10860 3</b>	<b>4269 7</b>	<b>2016 0</b>	<b>380 4</b>	<b>84 2</b>	<b>39 8</b>	<b>138 4</b>	<b>594915</b>

Tabulka č. 11: Žádosti o uchovávané provozní <i>internetové údaje</i> , kde údaje byly předány, podle stáří, v roce 2008									
Stáří požadovaných údajů (v měsících) / členský stát	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Celkem
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	737	412	137	168	0	0	0	0	1454
Dánsko	102	14	11	2	3	1	0	1	134
Německo	Nedodáno								
Estonsko	Nedodáno								
Irsko	492	460	498	1422	0	0	0	0	2872
Řecko	Nedodáno								
Španělsko	3278	2323	2113	1403	0	0	0	0	9117
Francie	Nedodáno								
Itálie	Nedodáno								
Kypr	0	0	0	0	0	0	0	0	0
Lotyšsko	424	150	75	219	74	34	0	0	976
Litva	Nedodáno								
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	76	3	0	0	0	0	0	0	79
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nedodáno								
Slovensko	Nedodáno								
Finsko	Nedodáno								
Švédsko	Nedodáno								
Spojené království	31170	9046	3097	2605	1917	2015	147	57	50054
<b>Celkem</b>	<b>36279</b>	<b>12408</b>	<b>5931</b>	<b>5819</b>	<b>1994</b>	<b>2050</b>	<b>147</b>	<b>58</b>	<b>64686</b>

## Statistické údaje dodané členskými státy za rok 2009

Tabulka č. 12: Žádosti o uchovávané údaje podle stáří v roce 2009									
Stáří požadovaných údajů (v měsících) / členský stát	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Celkem
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	210975	56623	11620	1053	0	0	0	0	280271
Dánsko	2980	685	179	104	54	38	12	14	4066
Německo	Nedodáno								
Estonsko	4299	1836	1210	1065	0	0	0	0	8410
Irsko	8117	1652	805	297	168	134	69	41	11283
Řecko	Nedodáno								
Španělsko	29775	19346	13999	6970	0	0	0	0	70090
Francie	Nerozčleněno podle stáří								514813
Itálie	Nedodáno								
Kypr	31	8	1	0	0	0	0	0	40
Lotyšsko	20758	2414	1088	796	565	475	0	0	26096
Litva	30247	35456	5886	884	0	0	0	0	72473
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	3336	362	151	174	0	0	0	0	4023
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Polsko	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovinsko	Nerozčleněno podle stáří								1918
Slovensko	Nerozčleněno podle stáří								5214
Finsko	2000	1310	532	152	76	0	0	0	4070
Švédsko	Nedodáno								
Spojené království	Nedodáno								
<b>Celkem</b>	<b>954845</b>	<b>297998</b>	<b>110996</b>	<b>64021</b>	<b>27961</b>	<b>24571</b>	<b>14065</b>	<b>34683</b>	<b>2051085</b>

<b>Tabulka č. 13: Žádosti o uchovávané provozní údaje podle druhu údaje v roce 2009</b> (v závorkách případný počet případů, u kterých nebylo možné žádosti vyhovět)				
<b>Druh údajů / členský stát</b>	<b>Telefonie v pevné síti</b>	<b>Telefonie v mobilní síti</b>	<b>Internetové údaje</b>	<b>Celkem</b>
Belgie	Nedodáno			
Bulharsko	Nedodáno			
Česká republika	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Dánsko	133 (0)	3771 (10)	162 (1)	4066 (11)
Německo	Nedodáno			
Estonsko	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Irsko	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Řecko	Nedodáno			
Španělsko	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Francie	Nerozčleněno podle druhu			514813
Itálie	Nedodáno			
Kypr	0 (0)	23 (3)	14 (0)	40 (3)
Lotyšsko	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Litva	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Lucembursko	Nedodáno			
Maďarsko	Nedodáno			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Nizozemsko	Nedodáno			
Rakousko	Nedodáno			
Polsko	Nerozčleněno podle druhu			1048318
Portugalsko	Nedodáno			
Rumunsko	Nedodáno			
Slovinsko	Nerozčleněno podle druhu			1918 (48)
Slovensko	Nerozčleněno podle druhu			5214 (157)
Finsko	Nerozčleněno podle druhu			4070
Švédsko	Nedodáno			
Spojené království	Nedodáno			
<b>Celkem</b>				<b>2051082 (1069885)</b>

<b>Tabulka č. 14: Žádosti o uchovávané údaje o telefonii v pevné síti, kde byly údaje předány, podle stáří, v roce 2009</b>									
<b>Stáří požadovaných údajů (v měsících) / členský stát</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Celkem</b>
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	9919	2907	47	36	0	0	0	0	12909
Dánsko	105	19	7	2	0	0	0	0	133
Německo	Nedodáno								
Estonsko	2254	866	599	424	0	0	0	0	4143
Irsko	3934	337	69	70	50	39	16	11	4526
Řecko	Nedodáno								
Španělsko	2371	1492	844	348	0	0	0	0	5055
Francie	Nedodáno								
Itálie	Nedodáno								
Kypr	0	0	0	0	0	0	0	0	0
Lotyšsko	744	253	157	143	68	89	0	0	1454
Litva	469	773	73	6	0	0	0	0	1321
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	83	25	18	20	0	0	0	0	146
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nedodáno								
Slovensko	Nedodáno								
Finsko	Nedodáno								
Švédsko	Nedodáno								
Spojené království	Nedodáno								
<b>Celkem</b>	<b>19879</b>	<b>6672</b>	<b>1814</b>	<b>1049</b>	<b>118</b>	<b>128</b>	<b>16</b>	<b>11</b>	<b>29687</b>

<b>Tabulka č. 15: Žádosti o uchovávané údaje o telefonii v mobilní síti, kde byly údaje předány, podle stáří, v roce 2009</b>									
<b>Stáří požadovaných údajů (v měsících) / členský stát</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Celkem</b>
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	197620	48841	472	0	0	0	0	0	246933
Dánsko	2777	639	162	98	47	19	12	7	3761
Německo	Nedodáno								
Estonsko	318	397	96	70	0	0	0	0	881
Irsko	3669	835	220	210	115	92	50	28	5219
Řecko	Nedodáno								
Španělsko	24065	15648	11147	5273	0	0	0	0	56133
Francie	Nedodáno								
Itálie	Nedodáno								
Kypr	17	16	0	0	0	0	0	0	23
Lotyšsko	18832	1912	778	515	394	263	0	0	22694
Litva	25713	19595	28	0	0	0	0	0	45336
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	2332	246	111	122	0	0	0	0	2811
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nedodáno								
Slovensko	Nedodáno								
Finsko	Nedodáno								
Švédsko	Nedodáno								
Spojené království	Nedodáno								
<b>Celkem</b>	<b>275343</b>	<b>88119</b>	<b>13014</b>	<b>6288</b>	<b>556</b>	<b>374</b>	<b>62</b>	<b>35</b>	<b>383791</b>

<b>Tabulka č. 16: Žádosti o uchovávané <i>internetové údaje</i>, kde byly údaje předány, podle stáří, v roce 2009</b>									
<b>Stáří požadovaných údajů (v měsících) / členský stát</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Celkem</b>
Belgie	Nedodáno								
Bulharsko	Nedodáno								
Česká republika	3369	4811	861	942	0	0	0	0	9983
Dánsko	98	27	10	4	4	7	0	1	151
Německo	Nedodáno								
Estonsko	315	145	56	102	0	0	0	0	618
Irsko	489	455	502	0	0	0	0	0	1446
Řecko	Nedodáno								
Španělsko	3339	2206	2008	1349	0	0	0	0	8902
Francie	Nedodáno								
Itálie	Nedodáno								
Kypr	12	2	0	0	0	0	0	0	14
Lotyšsko	852	198	74	90	88	86	0	0	1388
Litva	4060	15087	1	88	0	0	0	0	19236
Lucembursko	Nedodáno								
Maďarsko	Nedodáno								
Malta	150	14	0	0	0	0	0	0	164
Nizozemsko	Nedodáno								
Rakousko	Nedodáno								
Polsko	Nedodáno								
Portugalsko	Nedodáno								
Rumunsko	Nedodáno								
Slovinsko	Nedodáno								
Slovensko	Nedodáno								
Finsko	Nedodáno								
Švédsko	Nedodáno								
Spojené království	Nedodáno								
<b>Celkem</b>	<b>12684</b>	<b>22945</b>	<b>3512</b>	<b>2575</b>	<b>92</b>	<b>93</b>	<b>0</b>	<b>1</b>	<b>41902</b>