2006 ACTA UNIVERSITATIS CAROLINAE – IURIDICA 1 PAG. 99–123

OCHRANA OSOBNÍCH ÚDAJŮ V SCHENGENSKÉM INFORMAČNÍM SYSTÉMU

JIŘÍ VLASTNÍK

ÚVODEM

Schengenský systém byl nucen od svého vzniku, u něhož stálo v letech 1985 a 1990 pouze pět států[1], průběžně reagovat na přístup dalších členů a vývoj evropské integrace. Schengenská spolupráce, založená zpočátku na institutech mezinárodního práva, probíhá od vstupu Amsterdamské smlouvy v platnost v rámci užší spolupráce, využívaje institucionální struktury EU. Část schengenského acquis, týkající se společné vízové, azylové a přistěhovalecké politiky byla navíc komunitarizována, tedy začleněna do právního rámce smlouvy o evropském společenství.[2] Velkou výzvou a zároveň testem schengenského systému je rozšíření Evropské unie o 10 nových členských států k 1. 5. 2004. Byť se tyto státy neúčastní užší schengenské spolupráce okamžikem svého vstupu do EU, u všech je předpoklad, že se tak v blízké budoucnosti stane. Předběžnou podmínkou, která však musí být splněna, je změna stávajícího Schengenského informačního systému (SIS), který je základem pro efektivní policejní a trestní spolupráci v schengenském prostoru a který ve své současné podobě může z kapacitních důvodů fungovat nejvýše pro 18 států[3]. V plném běhu jsou v současnosti práce na zavedení Schengenského informačního systému druhé generace (SIS II), který by umožnil přístup dalším státům a zároveň přizpůsobil SIS požadavkům dnešní doby a nárokům, které jsou na něj kladeny v souvislosti s novými bezpečnostními hrozbami, ale též s ohledem na rozšiřování jeho administrativních funkcí. Je zřejmá tendence k tomu, aby byl SIS II v budoucnu propojen s dalšími informačními systémy (VIS, Eurodac) a stal se centrální evidenční databází osob a věcí v rámci Evropské unie.

---

[1] Dohoda mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích, podepsaná v Schengenu dne 14. června 1985; Úmluva k provedení schengenské dohody ze dne 14. června 1985.

[2] Článek 1 Protokolu o začlenění schengenského *acquis* do rámce Evropské unie, připojeného k Amsterdamské smlouvě.

[3] Dnes se SIS účastní původních 15 členských států, s určitými omezeními pro Spojené království a Irsko, a dále též Norsko a Island; srov. bod 2 preambule nařízení rady (ES) č. 2424/2001, resp. rozhodnutí Rady ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace (SIS II).

Nutnost rozšíření SIS implikuje zvýšené nároky na ochranu osobních údajů, které jsou v něm zpracovávány. Její zajištění musí být předpokladem a základním stavebním kamenem každého informačního systému, v němž informace překračují hranice národních jurisdikcí. Z těchto postulátů vychází i Haagský program o posílení svobody, bezpečnosti a práva v EU. Na jedné straně je základní zásadou dostupnost informací (principle of availability), dle které by od 1. 1. 2008 měl mít každý policista (případně jiný právo prosazující úředník), který potřebuje danou informaci k plnění svých úkolů, přístup do databáze jiného členského státu a pověřený bezpečnostní orgán v tomto státu by mu pro stanovený účel tuto informaci měl poskytnout. Na straně druhé je nezbytné zajistit efektivní ochranu těchto informací překračujících státní hranice v rámci celého společenství při všech fázích zpracování těchto informací, a to jak na úrovni jednotlivých členských států, tak na komunitární úrovni.[4]

Nezbytné je stanovení společných technických standardů ochrany informací, pravidel upravujících přístup k informacím, odpovídajících kontrolních mechanismů a způsobů nápravy. Ochrana osobních údajů prochází v oblasti veřejnoprávních i soukromoprávních databází vývojem, směřujícím k vytvoření uceleného evropského systému ochrany osobních údajů[5], založeného na principech, obsažených zejména ve směrnici o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.[6]

Tento příspěvek se zabývá funkcí a právní úpravou SIS a změnami, obsaženými v návrzích dokumentů, týkajících se zavedení SIS II (1). V navazující části je analyzována ochrana osobních údajů v policejních evidencích v komunitárním, unijním a národním právu se zaměřením na právní úpravu v ČR a ve Francii (2). Závěrem jsou shrnuty základní principy evropského systému ochrany osobních údajů v policejní oblasti a je poukázáno na některé nedostatky stávající právní úpravy (3).

1. SCHENGENSKÉ INFORMAČNÍ SYSTÉMY

1.1 SIS I

Odstranění kontrol na vnitřních hranicích jako hlavní cíl schengenských dohod bylo nutné kompenzovat efektivními opatřeními za účelem omezení bezpečnostních rizik, která z volného pohybu osob a věcí přes hranice plynou. Již schengenská dohoda z roku 1985 obsahuje závazek smluvních stran posílit výměnu informací, které by mohly být důležité pro ostatní smluvní strany v boji proti trestné činnosti (čl. 9). Takto obecně formulovaný závazek byl následně realizován prováděcí schengenskou prováděcí úmluvou z roku 1990 (dále SPÚ)[7], konkrétně jejími články 64 a 92–118. Byl zřízen SIS, tvořený vnitrostátní součástí každé ze smluvních stran (národní SIS), jejíž

[4] Viz Haagský program schválený Radou 27. 10. 2004, odd. 2.
[5] Srov. závěry Jarní konference Evropských úřadů na ochranu osobních údajů, Krakov, 25.–26. April 2005.
[6] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, viz závěry Jarní konference Evropských úřadů na ochranu osobních údajů, Krakov, 25.–26. April 2005.
[7] Úmluva k provedení schengenské dohody ze dne 19. června 1990.

provoz zajišťuje každý smluvní stát samostatně, a technickou podpůrnou jednotkou (centrální SIS) se sídlem ve Štrasburku, za jejíž provoz odpovídá Francie a která spadá do kompetence francouzského ministra vnitra. SIS byl uveden do provozu ke dni 26. 3. 1995 a od tohoto dne je přístupný pro orgány oprávněné přímo vyhledávat údaje v něm obsažené.[8] Jeho cílem je chránit veřejný pořádek a bezpečnost tím, že zajistí určeným orgánům přístup k záznamům o osobách a věcech při provádění hraničních a jiných kontrol v souladu s vnitrostátními právními předpisy, jakož i pro účely řízení o udělování víz, vydávání povolení k pobytu a řízení s cizinci při uplatňování úmluvy v oblasti pohybu osob (čl. 92, 93 SPÚ).

Databáze SIS je charakteristická svým hvězdicovitým uspořádáním. Údaje, zařazené do národního SIS, jsou přes centrální SIS kopírovány do národních SIS všech ostatních členských států. Tyto údaje mají nicméně velmi stručnou povahu. Z toho důvodu byly ve všech členských státech vytvořeny s poukazem na čl. 92 a 108 schengenské prováděcí úmluvy centrální jednotky SIRENE[9], zajišťující zprostředkování doplňujících informací pro efektivní využívání údajů SIS v terénu, případně v navazujících soudních či správních řízení. Jednotky SIRENE odpovídají též za zákonnost, správnost a pravidelnou aktualizaci všech záznamů v národním SIS, přičemž navzájem spolu komunikují nikoli přes centrální jednotku, ale přímo prostřednictvím zabezpečeného telekomunikačního systému SISNET. Nejčastěji komunikace probíhá přes telefonní linky, písemně jsou zasílány buď volné, anebo standardizované formuláře[10]. SIRENE jsou v současnosti základním pilířem SIS. Jejich fungování je upraveno Příručkou SIRENE,[11] jejíž podstatná část byla odtajněna v roce 2003.[12]

V současnosti SIS obsahuje šest druhů záznamů (čl. 95–100): (1) údaje o osobách, o jejichž zatčení za účelem vydání se žádá, (2) údaje o cizincích, jejichž vstup na území členského státu má být odepřen[13], (3) údaje o pohřešovaných osobách či osobách, které musí být v zájmu vlastní ochrany či předcházení nebezpečí umístěny dočasně na bezpečném místě, (4) údaje o osobách, které jsou potřebné pro účely trestního řízení, (5) údaje o osobách a vozidlech pro účely sledování či zvláštních kontrol, (6) údaje o věcech hledaných za účelem zabavení či hledaných nositelů důkazu. Záznamy jsou pořizovány v souladu s vnitrostátními předpisy. Je na členských státech ověřovat, zda závažnost daného případu odůvodňuje zařazení záznamu do SIS (čl. 94).

Podmínky pro zařazování cizinců do SIS byly stanoveny v Prohlášení výkonného výboru z 18. 4. 1996.[14] Z důvodu provázanosti SIS s ostatními instituty mezinárodní trestní spolupráce je stanoveno, že záznam v Schengenském informačním systému podle článku 95 má stejný účinek jako žádost o předběžnou vazbu osoby ve smyslu článku 16 Evropské úmluvy o vydávání ze dne 13. září 1957 nebo článku 15 Smlouvy zemí Beneluxu o vydávání a právní pomoci v trestních věcech ze dne 27. června

---

8 Rozhodnutí výkonného výboru ze dne 22. prosince 1994 (SCH/Com-ex (94) 29 rev. 2).
9 Supplementary Information Request at National Entry.
10 http://www.europarl.eu.int/comparl/libe/elsj/zoom_in/25_fr.htm
11 SCH/Comex (99) 5 z 28. dubna 1999.
12 Rozhodnutí Rady 2003/19/ES.
13 V současnosti se jedná o 90 % z více jak jednoho milionu záznamů vedených v SIS o osobách.
14 ÚV 2000, L 239, s. 458.

1962 ve znění protokolu ze dne 11. května 1974 (čl. 64). Obdobné ustanovení obsahuje i čl. 9 odst. 3 rámcového rozhodnutí o evropském zatýkacím rozkazu.[15]

Ustanovení SPÚ, týkající se SIS, byla pozměněna a funkce SIS rozšířeny v rámci akčního plánu z 21. 9. 2001 jako reakce na teroristické útoky z 11. září přijetím nařízení v oblasti spadající do prvního pilíře a rozhodnutí v oblasti policejní spolupráce[16]. Výslovně v textu byla zakotvena SIRENE pro výměnu doplňujících informací, rozšířeny byly kategorie zaznamenávaných údajů[17]. V části SIS, spadající do třetího pilíře, bylo rozšířeno právo přístupu i pro Europol a Eurojust (čl. 101A, 101B).

Informační databáze SIS slouží jednak jako zdroj poznatků pro přijímání operativních opatření a postupů při plnění zákonných úkolů státních orgánů v oblasti veřejného pořádku, bezpečnosti a předcházení trestné činnosti. Existence záznamu v SIS však může též v některých případech sloužit jako podklad pro navazující autoritativní rozhodování o právech a povinnostech subjektu údajů. Výslovně je tak stanoveno v čl. 5 odst. 2 u odepření práva vstupu a čl. 15, 16 SPÚ u udělování krátkodobých víz. Záznam má dopad též na možnost udělit jednou smluvní stranou vízum dlouhodobé a na režim pohybu držitele takového víza (čl. 18, 25 SPÚ). Není přitom vyloučeno, aby členské státy ve svých vnitrostátních předpisech stanovily existenci záznamů v SIS jako podklad pro vydávání též jiných správních rozhodutí. Je tedy zřejmé, že do popředí vystupuje potřeba odpovídajících garancí jednotlivci, zajišťujících, že informace o něm vedené jsou relevantní a odpovídají skutečnosti, což vyžaduje zavedení efektivních mechanismů kontroly z podnětu samotného subjektu údajů. Nutnost existence účinných kontrolních mechanismů a prostředků nápravy dokládají i kontroly společného kontrolního orgánu v jednotlivých členských státech, z jejichž výsledků pravidelně vyplývá, že řada údajů je nesprávných nebo zastaralých.

Ochranou osobních údajů v SIS se zabývá Hlava IV. schengenské úmluvy. Jako minimální standard, který je každá strana povinna zajistit, je stanovena Úmluva Rady Evropy o ochraně osob s ohledem na automatizované zpracování osobních údajů ze dne 28. ledna 1981 s přihlédnutím k doporučení Výboru ministrů Rady Evropy R (87) 15 ze dne 17. září 1987 o používání osobních údajů v policejní oblasti. Jsou zakotveny alespoň základní zásady pro shromažďování údajů v automatizovaném i neautomatizovaném systému: princip vázanosti užití informací na stanovený účel; omezený počet k vstupu oprávněných orgánů; kontrola správnosti údajů; odpovědnost za škodu osobě vzniklou nesprávnou evidencí údajů; evidence nakládání s údaji; společný orgán kontrolující technickou podpůrnou jednotku; vnitrostátní kontrolní orgány.

V případě, že by bylo dle názoru kontrolního orgánu jednoho členského státu vymazat z evidence záznamy, pořízené orgánem jiného členského státu, je nutno věc řešit

---

[15] Rámcové rozhodnutí Rady ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy č. 2002/584/SVV.

[16] Nařízení Rady (ES) č. 871/2004 ze dne 29. dubna 2004 o zavedení některých nových funkcí Schengenského informačního systému, také se zřetelem k boji proti terorismu, Rozhodnutí Rady 2005/211/SVV ze dne 24. února 2005 o zavedení některých nových funkcí v Schengenském informačním systému, včetně boje proti terorismu.

[17] Čl. 94, 99.

součinností příslušných národních kontrolních orgánů. V případě, že není možné dojít ke shodě, je věc předložena společnému dozorovému orgánu, jehož činnosti se ČR účastní v současnosti prostřednictvím pozorovatelů. Otázkou je, nakolik je tento postup efektivní z hlediska ochrany lidských práv zejména pro svou časovou náročnost, kdy po celou dobu šetření, trvajícího měsíce, setrvávají záznamy v evidencích se všemi důsledky pro jejich subjekt.

1.2 SIS II

Konstrukce SIS předpokládá účast nejvýše 18 států. S výhledem rozšíření EU, představila v roce 2001 Komise návrh přeměny SIS na SIS II.[18] Přípravné práce na změnu systému nicméně probíhají již od roku 1998. Jako referenční datum vytvoření SIS druhé generace byl stanoven rok 2006. Jasně je uvedeno, že SIS II je koncipován především jako nástroj předcházení bezpečnostním hrozbám, což jej odlišuje například od databází Europolu. Základní konstrukce systému zůstává stejná jako u SIS, nicméně návrhy obsahují některé významné změny.

1.2.1 Právní rámec SIS II

Jedním z důvodů nutnosti reformy SIS je potřeba reagovat na změnu právního rámce v důsledku Amsterdamské smlouvy, začleniví schengenské acquis do právního rámce EU.[19] Na jedné straně SIS přispívá k policejní a soudní spolupráci ve věcech trestních[20], na stranu druhou k politikám týkajícím se volného pohybu osob[21].

Právní základ jednotlivých ustanovení schengenského acquis byl určen rozhodnutím Rady s cílem jasně strukturovat povahu jednotlivých ustanovení jejich rozdělením mezi první a třetí pilíř EU.[22] Pokud jde však o SIS, nestalo se tak.[23] Z toho důvodu se ustanovení o SIS považují za právní akty na základě hlavy VI. SEU.[24] Důsledkem je skutečnost, že zásady přednosti a přímého účinku komunitárního práva se za stávajícího stavu u SIS neuplatní, neboť tyto jsou aplikovatelné pouze v oblasti prvního pilíře. Ustanovení o SIS se tak řídí pravidly mezinárodního práva v závislosti na jednotlivých vnitrostátních úpravách členských států. Za podmínek čl. 35 SEU se nicméně na výklad těchto ustanovení vztahuje rozhodovací pravomoc ESD.

Z důvodu uvedené dvoukolejnosti přijímaly evropské instituce při změnách SIS právní akty paralelní povahy jak v rovině komunitárního prvního pilíře, tak v rovině třetího pilíře. Nahrazení SIS za SIS II je předpokládáno v nařízení Rady č. 2424/2001, a rozhodnutí Rady č. 2001/886/SVV ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace. Následně se rozběhly práce v pracovních skupinách Komise, završené 31. 5. 2005 návrhem nařízení Evropského parlamentu a Rady

---

18 COM(2001) 720 final.
19 Protokol o začlenění schengenského acquis do rámce Evropské unie, připojený k Amsterdamské smlouvě.
20 Hlava VI. SEU.
21 Hlava IV. SES.
22 Rozhodnutí Rady 1999/436/ES ze dne 20. května 1999.
23 Viz Příloha A rozhodnutí.
24 Čl. 2 odst. 1, pododst. 4 Protokolu.

o SIS II (dále jen nařízení)[25] a návrhem rozhodnutí Rady o SIS II (dále jen rozhodnutí)[26]. Tyto dva návrhy jsou doplněny návrhem nařízení v rámci společné dopravní politiky dle čl. 71 SES o přístupu subjektů, odpovědných za vydávání osvědčení o registraci vozidel v členských státech, k SIS II.[27]

Uvedené návrhy představují základní rámec pro jediný informační systém. Nařízení spolu s rozhodnutím nahradí v případě přijetí čl. 92–119 SPÚ prováděcí úmluvy, jakož i rozhodnutí a prohlášení schengenského výkonného výboru, týkající se SIS. Původně mezinárodně právní postupy jsou tedy nahrazeny nástroji evropského práva, což mimo jiné umožní orgánům EU plné zapojení do legislativního procesu.

V části SIS II upravené nařízením budou vedeny záznamy, týkající se státních příslušníků třetí země za účelem odepření vstupu (dnešní čl. 96 SPÚ). Plně se zde uplatní zásady přednosti a přímého účinku komunitárního práva v souladu s judikaturou ESD, který bude mít v této oblasti obligatorní pravomoc pro všechny členské státy bez výjimky.

Část SIS II upravená rozhodnutím se bude spravovat stejně jako v současnosti režimem VI. hlavy SEU. V této části systému budou vedeny ostatní kategorie údajů, tedy (1) záznamy o osobách hledaných za účelem zatčení a předání nebo vydání, (2) záznamy o osobách k zajištění ochrany nebo předcházení nebezpečí, (3) záznamy o osobách hledaných za účelem soudního řízení, (4) záznamy o osobách a věcech pořízené pro účely utajeného sledování nebo zvláštních kontrol, (5) záznamy o věcech hledaných za účelem zabavení nebo za účelem zajištění důkazů v trestním řízení (nyní čl. 95, 97–100 SPÚ).

1.2.2 Úprava některých záznamů

Pozornost byla věnována zejména záznamům vedeným o osobách z důvodu odepření jejich vstupu, které mají význam jako podklad pro navazující správní akty. Rozdílná legislativa v jednotlivých členských státech vede dnes k tomu, že se významně liší postupy pro zařazování údajů do SIS dle čl. 96 SPÚ. To vedlo k upřesnění oproti stávající úpravě. Článek 15 nařízení obsahuje výčet případů, kdy záznam o osobě nemůže být učiněn, neboť osoba požívá práv přiznaných jí zvláštními komunitárními předpisy. I když toto vyplývalo již z výkladu SPÚ, vyjasnění je s ohledem na vnitrostátní správní praxi zcela žádoucí[28]. Zároveň se však návrh opírá o dosud nepřijatou „směrnici o navracení"[29]. Takovýto legislativní postup v každém případě vzbuzuje pochybnosti o naplnění požadavků judikatury Evropského soudu pro lidská práva (ESLP) na jasnost a předvídatelnost právní úpravy.

---

[25] Návrh nařízení Evropského parlamentu a Rady o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) – COM(2005)236 final.

[26] Návrh rozhodnutí Rady o zřízení, provozu a využívání Schengenského informačního systému druhé generace – COM(2005)230 final.

[27] COM(2005)237 final.

[28] K tomu srov. níže citované rozhodnutí ESD ve věci C-503/2003 Komise proti Španělsku.

[29] COM (2005)391, návrh směrnice Evropského parlamentu a Rady o společných normách a postupech v členských státech při vrácení nelegálně pobývajících státních příslušníků třetích zemí (návrh podán Komisí 1. 9. 2005).

Zároveň došlo k rozšíření druhů dat vedených v evidencích o osobách o biometrické údaje (otisky prstů a fotografie) a k prodloužení doby uchovávání údajů. Rozšířena byla též kategorie záznamů o hledaných věcech[30].

Důležitým prvkem je zakotvení možnosti vytvářet odkazy mezi záznamy (čl. 46 rozhodnutí), když vytváření odkazů je charakteristické zejména pro policejní databáze. V každém případě představuje nebezpečí nesprávného vzájemného propojení osob, či osob a věcí, a tím zvýšené riziko pro ochranu osobních údajů. Osoba totiž není posuzována pouze s ohledem na data, která se vztahují k ní, ale i na informace, které se vztahují k u ní uvedených odkazům. Odůvodněně je poukazováno na to, že vytvoření odkazu mazi záznamy by v žádném případě nemělo umožnit přístup k záznamu pro orgány, které by k němu jinak přístup neměly. Takové orgány by se o existenci odkazu neměly ani dovědět.[31]

1.2.3 Rozšíření práva přístupu

Účel SIS II je formulován značně obecněji než současný účel SIS (srov. Čl. 92, 93 SPÚ), když podle čl. 1 nařízení i rozhodnutí je jeho cílem umožnit příslušným orgánům členských států spolupracovat prostřednictvím výměny informací za účelem kontroly osob a věcí.

Orgány oprávněné k přístupu jsou v návrhu nařízení, resp. rozhodnutí, definovány zvlášť v závislosti na druhu záznamu. Oprávněné orgány musí jednat jednak v rámci obecného účelu SIS II, kterým je kontrola osob a věcí z důvodů bezpečnosti (čl. 1), jednak v rámci specifického účelu, pro který byl záznam pořízen, tedy s cílem identifikovat osobu či věc za účelem učinění konkrétního opatření.[32] V některých stanovených případech je však tato účelová vázanost práva přístupu narušena. Jedná se zejména o případ Europolu a Eurojustu a některých dalších orgánů k určitým kategoriím dat (čl. 18). Tyto orgány neužívají informační databáze jako podklad pro konkrétní opatření, ale jako informační zdroj pro své vlastní účely. Výslovně je navíc připuštěna možnost, že tyto orgány mohou údaje získané v databázích SIS II dále zpracovávat. Na zákonnost přístupu k údajům v SIS II a případné zpracování údajů Europolem a Eurojustem mají dozírat společné kontrolní orgány zřízené zakládajícími dokumenty těchto institucí[33]. Evropských inspektor ochrany údajů (EIOÚ) přitom vyjádřil názor, že by tyto orgány měly mít přístup pouze k údajům o osobách či věcech, které již figurují v jejich databázích tak, aby bylo zabráněno namátkovým lustracím v informačních databází SIS II. To by však nepochybně značně omezilo praktický význam SIS II pro tyto složky.

Ve třetím citovaném návrhu, týkajícím se SIS, Komise navrhuje rozšíření přístupu do SIS II pro orgány odpovědné za vydávání osvědčení o registraci vozidel, což je dle Komise odůvodněno nutností posílení spolupráce mezi členskými státy, založené na účinné výměně informací v rámci boje s podvody a nezákonným obchodováním s odcizenými vozidly v kontextu společné dopravní politiky. Otázkou je, zda jsou ustano-

[30] Srov. čl. 100 SPÚ a čl. 35 rozhodnutí nově zařazující zejm. odcizená či pohřešovaná osvědčení o registraci vozidel a SPZ a cenné papíry.

[31] Viz stanovisko EIOÚ k SIS II, www.edps.eu.int/legislation/Opinions_A/05-10-19_Opinion_SISII_EN.pdf

[32] Viz definice záznamu – čl. 3 písm. a) obou aktů.

[33] Čl. 53 odst. 2 návrhu nařízení.

vení SES upravující společnou dopravní politiku, konkrétně čl. 71 odst. 1 písm. d), odpovídajícím právním základem pro vydání uvedeného nařízení, když prioritně nesledují cíle společné dopravní politiky, ale související otázky předcházení a boje s trestnou činností v dopravní oblasti, a tedy spadají spíše do rámce třetího pilíře EU. Nicméně již směrnice 1999/37/ES o registračních dokladech vozidel sledovala jako jeden, byť nikoli prioritní cíl, usnadnění výměn informací mezi členskými státy za účelem boje proti nedovolenému obchodu s odcizenými vozidly.[34] Dle návrhu nařízení by měly subjekty, odpovědné v členských státech za vydávání osvědčení o registraci vozidel, přístup k údajům zařazeným do SIS II v souladu s čl. 35 písm. a), b) a f) rozhodnutí (údaje týkající se odcizených vozidel a přípojných zařízení, odcizených osvědčení o registraci a SPZ), za výhradním účelem ověření, zda vozidla předkládaná jim k registraci nebyla odcizena, neoprávněně použita nebo zda nejsou pohřešována. Výslovně je přitom stanoveno, že je-li pravomoc vydávat osvědčení o registraci vozidel svěřena soukromým osobám, mají tyto osoby do SIS II přístup pouze prostřednictvím státních orgánů.

1.2.4 Změny v ochraně osobních údajů

Systém ochrany údajů v SIS II je charakteristický svou komplexností z důvodu rozdělení materie mezi první a třetí pilíř.

Dle odst. 14 preambule návrhu nařízení se pro ochranu osobních údajů použijí jako lex generalis ustanovení směrnice 95/46/ES. Oproti tomu v oblasti upravené rozhodnutím je legi generali Úmluva 108. Tato úprava může vést k rozdílů v úrovni právní ochrany mezi oběma instrumenty. Preambule obou dokumentů v každém případě stanoví, že opatření, omezující přístup k údajům, musí být v souladu s požadavky čl. 8 ESLP a nesmějí vést ke snížení současné úrovně ochrany osobních údajů.

Významnou změnou je přenesení odpovědnosti za vedení centrálního systému na Komisi, s čímž souvisí podřízení veškerého zpracování údajů Komisí nařízení 45/2001[35] a nahrazení společného kontrolního orgánu (čl. 115 SPÚ) Evropským inspektorem ochrany údajů. Zároveň je stanovena povinnost koordinovat postup EIOÚ a národních kontroních orgánů.

Rozhodujícím zůstává, že jak návrh nařízení, tak návrh rozhodnutí stanoví, že právo na přístup se vykonává v souladu s právem členského státu, v němž se osoba uvedeného práva domáhá, přičemž nově je pevně stanovena lhůta 60 dnů pro vyřízení žádosti.[36] Z toho důvodu je stěžejní předložení návrhu rámcového rozhodnutí, sladujícím národní legislativu v této oblasti (viz níže).

Omezení pro přístup subjektů údajů k záznamům, stanovené v čl. 109 SPÚ, návrh nařízení neobsahuje a ponechává ji tak na národním právu. Může to být též důsledkem podpůrného uplatnění směrnice 95/46, která takovou možnost připouští ve svém čl. 13 v poměrně širokém rozsahu. Návrh rozhodnutí oproti tomu s možností zamítnout přístup výslovně počítá (čl. 51 odst. 4).

---

[34] Viz bod 9 preambule směrnice 1999/37 o registračních dokladech vozidel.

[35] Nařízení č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

[36] Čl. 29 návrhu nařízení, čl. 51 návrhu rozhodnutí.

V obou dokumentech je zakotveno[37] právo subjektu údajů na soudní přezkum v případě odepření práva na přístup k údajům, které se ho týkají, nebo k jejich opravě či výmazu, jakož i právo na poskytnutí informace nebo odškodnění v souvislosti se zpracováním jeho osobních údajů v rozporu s nařízením, resp. rozhodnutím. Právo na soudní přezkum je však oproti SPÚ upraveno v užší podobě. Čl. 111 SPÚ totiž neomezuje možnost soudního přezkumu na případy, kdy bylo právo přístupu k informacím odepřeno, ale jednotlivci dává právo na soudní přezkum zákonnosti zpracovávání osobních údajů. To lze charakterizovat jako závažné omezení práva jednotlivce na soudní ochranu. Na uvedeném nic nemění skutečnost, že připravované rámcové rozhodnutí (viz níže) obsahuje právo na soudní přezkum v širším rozsahu. Tento dokument však nebude mít přímý účinek a jeho působení bude záviset na provedení vnitrostátním zákonodárcem. V oblasti prvního pilíře se navíc neuplatní, nebude-li vnitrostáním zákonodárcem přistoupeno k jeho přesahující implementaci.

Systémovým požadavkem je existence nezávislého kontrolního orgánu, přičemž návrh nařízení činí výslovný odkaz na orgány, zřízené v souladu se směrnicí 95/46/ES. Z důvodu možnosti efektivnější zpětné kontroly zákonnosti zpracování a využívání záznamů je stanovena povinnost vést protokoly o veškerých výměnách údajů mezi národním systémem a SIS II (čl. 11).

2. OCHRANA OSOBNÍCH ÚDAJŮ V KOMUNITÁRNÍM A UNIJNÍM PRÁVU

2.1 EVROPSKÁ ÚMLUVA O OCHRANĚ LIDSKÝCH PRÁV A ZÁKLADNÍCH SVOBOD

Právo jednotlivce na ochranu jeho soukromí je tradičně součástí mezinárodních katalogů lidských práv. Ústředním kamenem evropského systému ochrany lidských práv je Evropská úmluva o ochraně lidských práv a základních svobod (dále Úmluva či EÚLP),[38] která se v důsledku judikatury ESD stala též základním privilegovaným pramenem poznání lidských práv a svobod v rámci evropských společenství.[39] Právo na ochranu osobních údajů je konkrétním projevem práva na respektování soukromého života (čl. 8), který je štrasburským soudem (ESLP) chápán jako „tělesná a duševní integrita jednotlivce".[40] Uchovávání i využívání informací, týkajících se osobního života jednotlivce, bez jeho souhlasu znamená zásah do práva zajištěného článkem 8 odst. 1[41], který musí respektovat omezení v odst. 2 čl. 8. Právo seznamovat se s údaji, uchovávanými o své osobě, pak za určitých okolností též spadá pod ochranu

---

[37] Čl. 30 nařízení, čl. 52 rozhodnutí.

[38] Evropská úmluva o ochraně lidských práv a základních svobod, sjednána v Římě 4. 11. 1950, podepsána jménem České a Slovenské Federativní Republiky v Madridu dne 21. února 1991 (vyhlášena sdělením FMZV č. 209/1992 Sb., v účinnosti od 18. 3. 1992).

[39] Např. ESD Rutili, 28. 10. 1975, Pecastaing 3. 5. 1981, TV 10 SA c. Commissariat voor de Media, 5. 10. 1994.

[40] X. a Y. proti Nizozemí, 26. 3. 1985 p. 22.

[41] Leander, cit., Kopp 25. 3. 1998, Rotaru 5. 5. 2000.

článku 8[42], nicméně z článku 8 neplyne toto právo v absolutní podobě a v určitých případech lze tedy přístup odepřít.[43]

Základním předpokladem pro oprávněnost zásahu do práva na ochranu soukromého života je soulad se zákonem. Zákon je přitom štrasburským soudem vykládán ve smyslu materiálním, tedy jako vnitrostátní právní úprava (zákonná i podzákonná) tak, jak ji aplikují vnitrostátní orgány, včetně aktuální soudní judikatury[44]. Podkladem pro omezení základní svobody může být i vydání správního aktu[45]. Je však důsledně vyžadována minimální kvalita právního předpisu, sloužícího jako podklad pro omezující zásah. Předpis musí být zejména dané osobě přístupný (v zásadě postačí, že byl akt publikován)[46], a musí být též dostatečně přesný, aby tato osoba mohla předvídat, jaké pro ni jeho aplikace bude mít důsledky. Po právní úpravě nicméně nelze požadovat, aby umožňovala předvídat důsledky své aplikace s absolutní přesností, když tento cíl je v praxi nedosažitelný[47]. Musí však v každém případě svému adresátovi poskytovat dostatečnou ochranu před svévolí správních orgánů. Tato nutná kvalita právního předpisu je nazývána požadavkem slučitelnosti s výsadním postavením práva (préeminence de droit).[48] V oblasti informačních databází zajišťujících bezpečnostní cíle nemá sice požadavek na předvídatelnost stejný význam jako v jiných oblastech a nelze například požadovat, aby jednotlivci bylo umožněno přesně předvídat, jaké prověrky budou vůči němu konány[49], právní předpis musí však být dostatečně přesný, pokud jde o podmínky za jakých jsou orgány státu oprávněny využít pravomocí pořizovat, uchovávat a využívat záznamy osobní povahy.

Byť ESLP v zásadě odmítá vykonávat abstraktní kontrolu souladu vnitrostátních předpisů s Úmluvou, oblast skrytého získávání informací o soukromí jednotlivce je natolik specifická, že dle názoru soudu může být jednotlivec za určitých podmínek oprávněn k podání stížnosti soudu nejen, pokud skutečně došlo k jeho efektivnímu monitorování státními orgány, ale též v případě pouhé existence nedostatečné právní úpravy, která umožňuje zásahy do jeho práva na ochranu soukromí. Nutno říci, že požadavek na kvalitu zákona se úzce prolíná s požadavkem na subsidiaritu a proporcionalitu zásahu, když soud v zásadě hodnotí konkrétní zákonnou úpravu ze všech těchto hledisek en bloc.

Omezující zásah musí být odůvodněn požadavkem nezbytnosti v demokratické společnosti z hlediska dosahování cílů uznaných odst. 2 (národní bezpečnost, veřejná bezpečnost, hospodářský blahobyt země, předcházení nepokojům a zločinnosti, ochrana zdraví nebo morálky, ochrana práv a svobod jiných). Prvky demokratické společnosti tvoří přitom zejména pluralismus, tolerance a otevřenost, jimiž musí být poměřováno i každé omezení svobody, garantované Úmluvou.[50] Nezbytnost potom vyžaduje exi-

[42] Gaskin 7. 7. 1989.
[43] Leander proti Švédsku, 26. 3. 1987.
[44] De Wilde, Ooms, Versyp, 18. 6. 1971, Sunday Times, 26. 4. 1979, Dudgeon, 22. 10. 1981, Chappel, 30. 3. 1989.
[45] Andersson, 25. 2. 1992.
[46] Sunday Times, 26. 4. 1979.
[47] Rekvényi proti Maďarsku, 1999, § 34.
[48] Kruslin proti Francii, 1990, Ekin proti Francii, 17. 7. 2001.
[49] Leander, cit. bod 51.
[50] Handyside, cit., Kjeldsen, Busk Madersen a Pedersen, 7. 12. 1993.

stenci naléhavé společenské potřeby[51]. Při posuzování podmínky nezbytnosti národní orgány užívají určité míry správního uvážení, přičemž soud zdůrazňuje, že mu nepřísluší hodnotit příslušnou legislativní techniku užitou zákonodárcem a užití správního uvážení správních orgánů. Správní uvážení však musí mít jasně stanovené limity. Ani v případě opatření v rámci boje proti terorismu či špionáži nemohou státy užívat jakákoli opatření, která pokládají za vhodná. V opačném případě by se totiž zásahy do práva na ochranu soukromí za účelem ochrany demokracie mohly stát prostředkem jejího zničení[52]. Zaznamenávaná informace musí být vždy objektivně nezbytná pro dosažení sledovaného účelu. Míra správního uvážení musí být potom vyvážena odpovídajícími zárukami jednotlivci, prostředky nápravy a přezkumu[53] tak, aby mezi obecným zájmem a zájmem jednotlivce byla nalezena spravedlivá rovnováha.

Lze shrnout, že zákon by měl definovat druh informací, které mohou být uchovávány, kategorie osob, o nichž mohou být informace vedeny, případy, kdy tak může být činěno, osoby oprávněné ke vstupu do databází, omezení doby, po kterou mohou být údaje uchovávány. Musí být zároveň zajištěny i efektivní prostředky zabránění zneužití systému a stanoveny odpovídající kontrolní mechanismy. Pokud tyto požadavky domácí právní předpis nesplňuje, dochází dle ESLP k porušení čl. 8.[54]

2.2 ÚMLUVA RADY EVROPY O OCHRANĚ OSOB S OHLEDEM NA AUTOMATIZOVANÉ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZE DNE 28. LEDNA 1981

Tato tzv. Úmluva 108 stanoví minimální standard ochrany osobních údajů v automatizovaných systémech, když na ní výslovně odkazují dokumenty, upravující vytváření informačních automatizovaných systémů[55]. Spolu s doporučením Výboru ministrů (87) 15 blíže vymezuje požadavky, kladené na zákonodárce a správní orgány při zpracovávání osobních údajů. Dopadá na automatizované systémy ve veřejném i soukromém sektoru (čl. 3), přičemž jejím cílem je zavést evropský standard ochrany osobních údajů v této oblasti a omezit bariéry mezi státy, bránící volnému toku informací, který je jedním ze základů moderní informační společnosti. Výslovně je upraveno možné přistoupení nečlenských států RE (k dnešnímu dni však žádný nečlenský stát tuto úmluvu nepodepsal). Každý stát může prohlásit, že na určité systémy se úmluva vztahovat nebude. Podmínkou nicméně je, aby tyto systémy nepodléhaly ochraně osobních údajů (čl. 3 odst. 2 písm. a), v případě policejních evidencí nepřichází tedy takový postup v úvahu.

Úmluva stanoví požadavky, týkající se kvality údajů (zákonnost, účelová vázanost shromažďování, přiměřenost, přesnost, časová omezenost záznamů, zabezpečení, zvláštní záruky pro shromažďování citlivých údajů). Právo na zjištění existence automatizovaného systému a přístup k datům, evidovaných o jednotlivci, na případnou

---

[51] Gillow, 24. 11. 1986.
[52] Klass 6. 9. 1978, p. 49.
[53] Leander, cit.
[54] Rotaru, cit.
[55] Kromě schengenské prováděcí úmluvy mimo jiné např. Úmluva o používání informační technologie pro celní účely ÚV 1995 C 316 s. 33.

opravu či vymazání je upraveno v čl. 8. Lze je odepřít pouze, je-li to nezbytné v zájmu ochrany bezpečnosti státu, veřejné bezpečnosti, měnových zájmů státu, nebo potírání trestné činnosti nebo z důvodu ochrany subjektu údajů nebo práv a svobod jiných osob (čl. 9). Upravena je dále spolupráce mezi národními úřady tak, aby mohl být zajištěn volný pohyb informací při současném udržení standardu ochrany.

2.3 DOPORUČENÍ VÝBORU MINISTRŮ RADY EVROPY R (87) 15 ZE DNE 17. ZÁŘÍ 1987 O POUŽÍVÁNÍ OSOBNÍCH ÚDAJŮ V POLICEJNÍ OBLASTI

Toto doporučení dotváří rámec pro ochranu osobních údajů v oblasti komunitárního práva, neboť přes jeho právní nezávaznost na něj odkazuje SPÚ. Obsahuje základní principy, jimiž by se používání osobních údajů v policejních evidencích mělo řídit. Konkrétně se jedná o povinnost zřízení nezávislého kontrolního orgánu mimo policejní struktury, kterému by byly notifikovány veškeré policejní evidence (automatizované i ad hoc vedené) a který by dohlížel nad stanovenými pravidly. Významným je princip oddělování různých evidencí dle toho, zda se jedná o potvrzené či nepotvrzené údaje, jakož i oddělování dat vedených ve správních evidencích. Rozveden je princip subsidiarity a proporcionality, který musí být respektován při vedení, používání a odmítnutí zpřístupňování záznamů jejich subjektům. Subjekt údajů je zásadně oprávněn k přístupu k informacím a případně k jejich opravě. V případě odmítnutí, které by mělo být vždy písemné a obsahovat odůvodnění, musí mít možnost obrátit se na kontrolní orgán či jinou nezávislou instituci.

2.4 CHARTA ZÁKLADNÍCH PRÁV EU

Charta základních práv Evropské Unie, podepsaná 7. 12. 2000 předsedy Evropského parlamentu, Rady a Komise, postrádá dosud právní závaznosti. Je vyjádřením vůle Unie garantovat základní lidská práva a svobody a její snahy zaplnit právní mezeru neexistence komunitárního katalogu těchto práv. Bez ohledu na její deklaratorní charakter se nicméně stala důležitým zdrojem poznání ochrany lidských práv, když ve svých rozhodnutích na ni odkazují jak Evropský soudní dvůr a Soud prvního stupně[56], tak i ústavní soudy členských států. Charta přitom nezasahuje do veškerých právních vztahů, ale pouze do oblasti dotčené výkonem působnosti společenství, když je určena orgánům, institucím a jiným subjektům Unie, a dále členským státům, pokud uplatňují právo Unie (čl. 53).

Oproti jiným dokumentům Charta rozlišuje mezi právem na ochranu soukromého života (čl. 7) a právem na ochranu údajů osobního charakteru (čl. 8), které je nicméně nutné interpretovat v souladu s výkladem čl. 8 Úmluvy Evropským soudem pro lidská práva (čl. 52 odst. 3 Charty). Dle čl. 8 Charty má každý člověk právo na ochranu údajů osobního charakteru, které se ho týkají (odst. 1), když s těmito údaji musí být nakládáno čestně, pouze k přesně danému účelu a na základě souhlasu dotyčné osoby[57] či

[56] Např. T-52/01 Schaefer.
[57] Viz zejména směrnice č. 95/46/ES.

na základě jiného legitimního opodstatnění uvedeného v zákoně. Výslovně je zakotveno právo jednotlivce na přístup k osobním údajům, i toto právo však podléhá obecné možnosti omezení z čl. 52, tedy na základě zákona, za účelem obecného zájmu, uznaného Unií, a při respektování subsidiarity a proporcionality. Pro zákonodárce je stanovena povinnost zřídit nezávislý orgán dohledu nad respektováním pravidel nakládání s osobními údaji (odst. 3).

2.5 JUDIKATURA EVROPSKÉHO SOUDNÍHO DVORA

Pokud jde o oblast SIS, spadající do 1. pilíře, je rozhodovací pravomoc ESD zřejmá. Právo na ochranu osobních údajů ESD, resp. SPS, několikrát posuzoval ve vztahu k ochraně informací týkajících se zdravotního stavu[58]. K přístupu k osobním údajům se ESD vyjádřil též v oblasti zemědělských evidencí vzhledem ke sdělování informací, získaných o dřívějším uživateli zemědělské půdy, jeho následovníkovi, který je potřebuje při svém rozhodování a dalším využití půdy. Aplikace principu subsidiarity a proporcionality, tedy dosahování rovnovážného stavu mezi zájmem jednotlivce a legitimního společenského cíle je patrná.[59]

Důležitým rozhodnutím, vykládajícím základní principy směrnice č. 95/46/ES, možnost omezení práva na ochranu osobních údajů a vzájemnou interakci ESD a národních soudů při posuzování souladnosti národní právní úpravy s komunitárním právem, je rozsudek *Österreichischer Rundfunk*[60], týkající se možnosti zveřejňování příjmů zaměstnanců ve veřejném sektoru spolu s plným uvedením jejich jména a příjmení. ESD se plně odvolává na výklad čl. 8 Úmluvy ESLP, který uvádí, že právo na ochranu osobních údajů nesmí být vykládáno restriktivně, a pod čl. 8 Úmluvy spadá. ESD souladně dovodil, že omezení práv na ochranu osobních údajů přichází v úvahu pouze při respektování zásad subsidiarity a proporcionality. Zásadní přitom je, že ESD ponechává posouzení tohoto souladu národním soudům. Pokud tyto soudy dovodí, že vnitrostátní opatření tyto zásady nerespektuje, je nutno dovodit i rozpor s komunitárním právem. Je zde zřejmá ustálenou judikaturou již několikrát potvrzená úzká součinnost mezi národními soudy a ESD při řízení o předběžné otázce, kdy ESD po vzoru ESLP vychází z toho, že národní soudy jsou nejblíže konkrétnímu časoprostoru, v němž je omezující opatření aplikováno. Není proto vyloučeno, že v různých státech mohou existovat obdobná omezující opatření, přičemž některá z nich budou posouzena jako jsoucí v rozporu s komunitárním právem, jiná nikoli. ESD, též inspirován ESLP, vyžaduje, aby zákonný podklad pro omezující opatření byl formulován dostatečně přesně za účelem zachování principu předvídatelnosti práva tak, aby adresáti v závislosti na tomto očekávání mohli přizpůsobit své chování. Posouzení předvídatelnosti zákona ponechává ESD též národním soudům.

V oblasti 3. pilíře je pravomoc ESD založena čl. 46 písm. d) SEU ve spojení s čl. 6 odst. 2 SEU a článkem 35 SEU, stanovícího specifika oprávnění ESD v oblasti 3. pilíře. Podmínkou je prohlášení státu tuto pravomoc uznávající. Toto prohlášení, obsa-

[58] Např. C-404/92 X. proti Komisi, T-121/89 X. proti Komisi.
[59] C-369/98 Fisher.
[60] C-465/2000 Österreichischer Rundfunk.

hující též upřesňující podmínky spolupráce mezi národními soudy a ESD ve smyslu čl. 35 odst. 3 SEU je přitom pokládáno za neodvolatelné. Výslovně je vyloučen přezkum oprávněnosti či proporcionality operací policejních a jiných bezpečnostních orgánů členských států (čl. 35, odst. 5), týkajících se veřejného pořádku a vnitřní bezpečnosti, když pro tento přezkum jsou kompetentní vnitrostátní soudy členských států. V případě komunitárního prvku přichází nicméně v úvahu předložení předběžné otázky ESD dle čl. 234 SES. Nezbytné je totiž připomenout, že i v oblastech, v nichž na společenství nebyly přeneseny žádné pravomoci, mají členské státy povinnost respektovat ustanovení komunitárního práva[61]. Jakékoli shromažďování osobních údajů o občanech členských států, byť při sledování zájmů na ochraně veřejného pořádku či bezpečnosti, které by se mohlo stát překážkou vnitřního komunitárního trhu, by na základě této judikatury nepochybně podléhalo komunitárnímu přezkumu.

Zásadním je zcela nový rozsudek z 31. 1. 2006 ve věci Komise proti Španělsku v řízení o porušení smlouvy[62], v němž se ESD vyjadřuje k otázce vztahu existence záznamu v SIS a možnosti omezení práva rodinných příslušníků občanů EU na vstup do členských států, jejíž limity jsou stanoveny směrnicí č. 64/221/EHS[63]. V daném případě španělské orgány omezily na podkladě záznamu v SIS, učiněného německými orgány, vstup dvěma alžírským občanům, manželům španělských státních občanek. ESD úvodem poukazuje na právní rámec a na prohlášení výkonného výboru, ustaveného schengenskou prováděcí úmluvou, ze dne 18. 4. 1996, v němž je stanoveno, že v rámci aplikace čl. 96 by v zásadě osoby, požívající výsad komunitárního práva neměly být uváděny na seznam osob, jimž má být odepřen přístup. Takové záznamy mohou být učiněny a zachovány v evidencích pouze, jsou-li v souladu s komunitárním právem. V opačném případě musí členský stát, který záznam provedl, učinit vše, co je nutné pro vymazání záznamu. V obou uvedených případech nebyl v SIS uveden důvod záznamu. ESD poukazuje, že důvody pro zařazení záznamu do SIS nejsou natolik striktně formulovány jako důvody pro odepření vstupu rodinného příslušníka občana členského státu. Směrnice č. 64/221, vyložená judikaturou ESD, vyžaduje existenci skutečné a dostatečně vážné hrozby, vztahující se k základnímu zájmu společnosti, a to nad rámec narušení společenského zájmu, které představuje každé porušení zákona.[64] Oproti tomu pro záznam dle čl. 96 schengenské úmluvy postačí, že přítomnost cizince na území představuje ohrožení veřejného pořádku, veřejné bezpečnosti nebo bezpečnosti státu, přičemž demonstrativně jsou uvedeny možné případy odůvodňující záznam. Není vyžadováno posouzení závažnosti konkrétní hrozby, kterou by přítomnost cizince na území členského státu přinesla. Z uvedeného ESD zcela logicky vyvodil, že smluvní stát může přistoupit k záznamu občana třetího státu, který je manželem občana členského státu, jen v případě, kdy bylo konstatováno, že přítomnost této osoby znamená skutečnou a dostatečně závažnou hrozby, vztahující se k základnímu

---

61 C-279/93 Finanzamt Koeln-Altstadt v Schumacker, C-80/94 Wielockx.

62 C-503/2003 Komise proti Španělsku.

63 Podle jejího článku 3 se opatření, přijatá z důvodů veřejného pořádku nebo veřejné bezpečnosti musí zakládat výlučně na osobním chování dotyčné osoby (odst. 1), přičemž odsouzení pro trestný čin samo o sobě přijetí takových opatření neodůvodňuje (odst. 2).

64 C-36/75 Rutili, C-30/77, b. 28, Boucherau, C-482/01, b. 35 a C-493/01 Orfanopoulos et Oliveri, b. 66.

zájmu společnosti ve smyslu směrnice 64/221. Záznam v SIS nepochybně představuje indicii toho, že vstup by osobě mohl být odepřen, nicméně tato indicie musí být, i přes nutnost respektovat zásadu vzájemné spolupráce a důvěry v provedené záznamy, potvrzena doplňujícími údaji, umožňujícími takové posouzení. V daném případě se však španělské orgány, ač jim byl prokázán status manžela občana členského státu EU, omezily na konstatování existence záznamu bez dalšího zdůvodnění. Za této situace, bez předchozího ověření souladu záznamů se směrnicí, nebyly oprávněny vstup odmítnout. Odepřením vstupu došlo k porušení směrnice 64/221/EHS. Je tedy zdůrazněn význam orgánů SIRENE a rychlost výměny informací[65]. Doba odpovědi by v žádném případě neměla převýšit rozumnou dobu vzhledem k okolnostem případu. Může se však lišit dle toho, zda jde pouze o překročení státní hranice nebo o udělení víza.

Z této judikatury je zřejmé, že tam, kdy záznamy v SIS mají vliv na právní vztahy upravené komunitárním právem, musí být zkoumán soulad opatření, která byla v návaznosti na existenci záznamů učiněna, s komunitárním právem a obecnými principy komunitárního práva včetně souladu se základními právy a svobodami ve výkladu ESLP.

2.6 SEKUNDÁRNÍ KOMUNITÁRNÍ A UNIJNÍ PRÁVNÍ PŘEDPISY

2.6.1 Směrnice 95/46/ES

Základním nástrojem Společenství v oblasti ochrany osobních údajů se stala směrnice č. 95/46/ES[66], jejíž principy se následně promítly do pozdějších komunitárních nástrojů. Směrnice byla nicméně přijata za účelem odstraňování překážek na vnitřním trhu zboží a služeb, spočívajících v omezení přeshraničního pohybu osobních údajů z důvodu rozdílné úrovně právní ochrany osobních údajů v jednotlivých členských státech. Z působnosti této směrnice je výslovně vyloučena oblast veřejné bezpečnosti a trestní spolupráce (čl. 3/2).

2.6.2 Nařízení 45/2001

Čl. 286 odst. 2 SES předvídá ustavení nezávislého orgánu dozoru nad zpracováním osobních údajů komunitárními orgány. K dotvoření komunitárního stupně ochrany osobních údajů bylo přijato nařízení č.45/2001[67]. Nařízení má obecnou povahu, tedy vztahuje se na zpracování veškerých osobních údajů ve všech orgánech a institucích Společenství jak v automatizovaných, tak neautomatizovaných systémech, pokud se toto zpracování provádí při výkonu činností, které zcela nebo zčásti spadají do oblasti působnosti práva Společenství (čl. 3), přičemž z této obecné působnosti nejsou stanoveny žádné výjimky. Spočívá na obdobných principech jako Úmluva č. 108, resp. směrnice 95/46/ES (zákonnost, účelovost vedení, proporcionalita a subsidiarita vzhledem ke sledovanému účelu, časová omezenost, pravidelná kontrola

---

[65] Viz bod 2.2.1 Příručky SIRENE.

[66] Směrnice č. 95/46/SES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[67] Nařízení č. 45/2001 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

a aktualizace, existence nezávislého kontrolního orgánu, možnost soudního přezkumu). Nařízením byl zřízen úřad Evropského inspektora ochrany údajů[68], jehož hlavním úkolem je dohlížet nad respektováním pravidel nakládání s osobními údaji orgány společenství. Nezanedbatelnou část agendy tvoří také zaujímání stanovisek k návrhům evropských aktů, předkládaných Komisí v oblasti osobních údajů (čl. 28 odst. 2). Rozhodnutí inspektora podléhají soudní pravomoci ESD. Stejně tak je ESD kompetentní i pro rozhodování o náhradě škody dle čl. 288 SES, vzniklé v důsledku nedovoleného zpracování osobních údajů nebo jiné činnosti neslučitelné s nařízením (čl. 32 odst. 4).

2.6.3 Návrh rámcového rozhodnutí

Úmluva 108 se vztahuje pouze na automatizované systémy s možností vyjmout některé systémy z její působnosti. Směrnice 95/46/ES výslovně nedopadá na oblast veřejné bezpečnosti a trestní spolupráce. S výjimkou vodítek daných judikaturou evropských soudních orgánů tak dosud neexistuje právní instrument, stanovící komplexně standard ochrany osobních údajů v oblasti policejní spolupráce. S cílem zaplnit tuto mezeru a v rámci plnění cílů haagského plánu předložila Komise návrh rámcového rozhodnutí o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech (dále rámcové rozhodnutí)[69], sjednocující národní standardy.[70] Jakkoli jde o akt třetího pilíře, lze očekávat, že v případě schválení tohoto rozhodnutí mohou vnitrostátní předpisy, které budou muset být přijaty na jeho základě, pokrývat též komunitární oblast SIS, vedenou na základě pilíře prvního. K podobné „přesahující implementaci" došlo v řadě států již při provedení směrnice 95/46/SES (příkladem je i český zákon č. 101/2000 Sb.).

Rámcové rozhodnutí se vztahuje na veškeré zpracování osobních údajů v jakýchkoli policejních či soudních evidencích, automatizovaných i neautomatizovaných, shromažďovaných za účelem předcházení trestným činům, jejich vyšetřování, odhalování a stíhání. Z jeho působnosti jsou výslovně vyloučeny pouze databáze Europolu, Eurojustu a celních orgánů. Nevztahuje se ani na databáze vedené zpravodajskými službami, což vyplývá z výkladu čl. 33 SEU.[71] Pro účely záležitostí, spadajících do oblasti působnosti SEU, nahrazuje články 126–130 SPÚ (čl. 33), přičemž jakýkoli odkaz na Úmluvu č. 108 se považuje za odkaz na rámcové rozhodnutí (čl. 34 odst. 2). Lhůta pro provedení rozhodnutí by v případě jeho schválení měla uplynout 31. 12. 2006.

Rámcové rozhodnutí vychází principielně z Úmluvy 108 a doporučení Výboru ministrů (87) 15, legislativně technicky pak ze směrnice č. 95/46/ES, když pojmy jsou definovány obdobně (správce, zpracovatel, osobní údaj aj.). Výslovně je upravena možnost zpracovávat údaje s rozdílným stupněm přesnosti a spolehlivosti, povinností

---

[68] Prvním Evropským inspektorem ochrany údajů byl jmenován Peter Hustinx, jeho zástupcem pak Joaquín Bayo Delgado (funkční období je pětileté).

[69] COM (2005) 475 final.

[70] Učinila tak v době, kdy se potřeba sjednotit národní standardy promítla mimo jiné do dohody uzavřené 27. května 2005 v Prümu mezi Německem, Rakouskem, Belgií, Nizozemskem, Lucemburskem, Francií a Španělskem s cílem umožnit policejním orgánům přímý přístup do automatizovaných databází poté, kdy budou provedeny vymezené změny ve vnitrostátním právním řádu.

[71] Viz stanovisko EIOÚ k návrhu Komise, s. 31.

je však vést takové záznamy odděleně od ostatních. Zvláštní důraz je kladen na přísnou kategorizaci údajů dle subjektu, jehož se týkají, s cílem zamezit omylu a chránit zájmy osob. Je stanovena povinnost pravidelného ověřování záznamů a dokumentace nakládání s nimi a zejména jejich předávání do jiných členských států. Za zákonem stanovených podmínek a při dodržení zásady subsidiarity a proporcionality je přitom možné i předání těchto záznamů soukromým osobám. (čl. 14). Předání do třetích zemí či jiným mezinárodním institucím (např. Interpol) je možné mimo jiné pouze, bude-li zajištěna odpovídající úroveň ochrany, a to pro každý konkrétní přenos či kategorii přenosů. Odepřít přístup k informacím, vedených o subjektu, lze pouze v taxativně stanovených případech, přičemž pro toto rozhodnutí je stanovena obligatorní písemná forma, jedná-li se o informace vedené o subjektu údajů bez jeho vědomí. Toto rozhodnutí je přezkoumatelné orgánem dozoru, případně soudem. O důvodech odepření přístupu musí být žadatel vyrozuměn, z čehož však existují výjimky (čl. 19 odst. 4).

Kromě zakotvení povinného zřízení nezávislých kontrolních orgánů je upraveno též právo soudního přezkumu (čl. 27). Toto právo není přitom omezeno na možnost soudního přezkoumání rozhodnutí o odepření přístupu jako v nařízení, resp. rozhodnutí o zavedení SIS II, ale na přezkum zákonnosti vedení osobních údajů jako takové. Náhrada škody spočívá na principu objektivní odpovědnosti správce údajů s možností liberace, která je ovšem stanovena poměrně nesrozumitelně[72] a bude tak na národním zákonodárci toto upřesnit. Orgány členských států odpovídají také za škodu vzniklou v důsledku jim předaných nepřesných či zastaralých údajů, po její úhradě disponují však právem následného regresu vůči orgánu státu, který jim tyto nesprávné údaje předal (čl. 28 odst. 2). Státy jsou povinny vytvořit též odpovídající rámec sankcí za porušování povinností nakládání s osobními údaji.

Návrh rámcového rozhodnutí je předkládán v úzké souvislosti s návrhem rámcového rozhodnutí Rady o výměně informací podle zásady dostupnosti[73], které by mělo vést k odstranění překážek pro výměnu těchto informací tím, že stanoví jednotné podmínky jejich výměny platné v celé EU. Jak zdůrazňuje ve svém stanovisku EIOÚ, k přijetí rámcového rozhodnutí o výměně informací by v žádném případě nemělo dojít bez přijetí rámcového rozhodnutí o ochraně údajů[74]. Rámcové rozhodnutí o výměně informací totiž předpokládá vytvoření evropského standardu ochrany osobních údajů tak, aby mohl být zaveden z hlediska trestní spolupráce žádoucí princip dostupnosti informací.

K ochraně informačních systémů v národním zákonodárství přispívá nutností harmonizace skutkových podstat trestných činů směřujících proti informačním systémům rámcové rozhodnutí Rady o útocích proti informačním systémům[75].

---

[72] Čl. 28 odst. 1 „Správce se může této odpovědnosti částečně nebo zcela zprostit, pokud prokáže, že za okolnost, jež vedla ke vzniku škody, neodpovídá."

[73] COM 2005/490/final.

[74] Bod II.1 stanoviska.

[75] Rámcové rozhodnutí Rady č. 2005/222/SVV ze dne 24. února 2005.

Hlavní tíha odpovědnosti za vytvoření právní úpravy, zajišťující účinnou ochranu osobních údajů v SIS, leží na vnitrostáním zákonodárci. To vyplývá ze skutečnosti, že normy mezinárodního, ale i komunitárního práva, upravují postupy pro provádění záznamů, pravidla shromažďování a zpracovávání osobních údajů a podmínky přístupu k osobním údajům pouze rámcovým způsobem, přičemž zejména obsahují důležité principy, které jsou zákonodárce a právo aplikující státní orgány povinny respektovat.

2.7.1 Právní úprava v ČR[76]

Pro ČR jsou v současnosti veškerá ustanovení schengenského acquis závazná, nicméně použitelnost některých z nich, (včetně ustanovení o SIS) je vázána až na dodatečné rozhodnutí Rady, vydané po konzultaci s Evropským parlamentem.[77] Tato konstrukce umožní začlenění nových členských států do struktury schengenského systému až po splnění všech nutných podmínek a zároveň po provedení popsané reformy SIS. V současné době probíhají přípravy na zapojení ČR do SIS. Nutné je zejména stanovit přesné postupy pro vytvoření počáteční sumy údajů, která bude tvořit základ českého národního SIS. Jasná pravidla této prvotní fáze jsou stěžejní. V některých členských státech nebylo totiž výjimkou, že záznamy byly odůvodněny velmi starými správními rozhodnutími, čímž se prodlužoval faktický právní účinek těchto rozhodnutí, kdy se navíc rozšířil na území všech států schengenského prostoru. Dle vyjádření Policejního prezídia ČR by do SIS měly být přeneseny údaje ze současných evidencí PATROS, PATRMV, KSV, OSH, CIS. Pravidla výběru dat pro zařazení do SIS II se v současnosti vytvářejí.

Právní úpravou, kterou se bude řídit zřízení a vedení SIS je zejména zákon o Policii ČR[78] (ZPČR) a zákon o pobytu cizinců na území ČR[79] (ZPC), v závislosti na kategorii vedených záznamů. Ochrana osobních údajů pak podléhá obecnému právnímu předpisu, zákonu č. 101/2000 Sb. o ochraně osobních údajů (dále ZOÚ), který do českého právního řádu promítl ustanovení směrnice 95/46/SES. ZOÚ jde přitom nad rámec směrnice v tom, že se vztahuje na veškeré osobní údaje, tedy i na osobní údaje vedené v oblasti veřejné bezpečnosti a trestní spolupráce.

Oblast policejních evidencí není jako taková vyjmuta z působnosti ZOÚ a Česká republika při nakládání s osobními údaji spadá pod pojem správce a dopadají na ni veškeré povinnosti s tímto postavením spojené. Určité odlišnosti jsou nicméně z důvodu bezpečnostních specifik stanoveny právě v ZPC a ZPČR, které mají vůči ZOÚ postavení legi speciali.[80] Určitá ustanovení ZOÚ se v oblasti policejních evidencí neuplatní

---

[76] Za konzultaci týkající se české právní úpravy velmi děkuji Mgr. Ludmile Novákové z Úřadu pro ochranu osobních údajů.

[77] Čl. 3 Aktu o podmínkách přistoupení 10 nových členských států a související Příloha I.

[78] § 42d an. zák. č. 283/1991 Sb. o Policii ČR v platném znění.

[79] § 158 odst. 1 písm. j) zák. č. 326/1999 Sb. o pobytu cizinců na území ČR a o změně některých zákonů v platném znění, § 158 odst. 1 písm. j).

[80] To platí i přes poměrně matoucí § 42d ZPČR, který jako zvláštní předpis označuje ZOÚ, nicméně blíže neupravuje vztah obou zákonů.

výslovně (§5 odst. 1, § 11, § 12 ZOÚ), v jiných případech je nutno užít výkladového pravidla lex specialis derogat legi generali.[81] V souladu s doporučením Výboru Rady Evropy (87) 15 je stanovena povinnost Policie ČR notifikovat Úřadu pro kontrolu osobních údajů (dále Úřad) neprodleně zřízení každé evidence obsahující osobní údaje.[82]

Jako nezávislý kontrolní orgán byl zřízen Úřad, jehož dozorová pravomoc je vyloučena pouze ve vztahu ke zpravodajským službám (§ 29 odst. 3) a vůči Policii ČR se tedy uplatňuje v plné šíři. V zákonech není blíže upraven vztah Úřadu k Policii ČR, nutno tedy aplikovat obecnou úpravu (zejm. § 21, § 37 an. ZOÚ).

Dle § 21 ZOÚ se může každý subjekt údajů obrátit na Úřad, domnívá-li se, že jeho osobní údaje jsou zpracovávány v rozporu se zákonem. Je však třeba poukázat na to, že účastníkem správního řízení, které Úřad zahajuje se správcem údajů v rámci postupu dle § 21 ZOÚ, není již stěžovatel, ale pouze správce, v konkrétním případě tedy ČR, jednající Ministerstvem vnitra ČR[83]. Subjekt údajů tak nemá možnost vystupovat v tomto řízení, ani možnost správního či soudního přezkumu rozhodnutí Úřadu ve věci. Úřad jej pouze vyrozumí o přijatých opatřeních. Úřad nebude oprávněn kontrolovat odůvodněnost záznamů v SIS, nicméně bude moci posoudit, zda jejich podklad spadá pod důvody, pro které mohou být údaje vedeny. Při tomto postupu bude moci vstoupit nejen do národního SIS, ale i do databází doplňujících informací, vedených SIRENE. Policie ČR by mu měla oprávněnost záznamu vždy zdůvodnit, nicméně tento postup není blíže upraven a zasluhoval by tak legislativní pozornosti. V případě, že by Úřad došel k závěru, že osobní údaj je veden nezákonně, byl by povinen uložit ČR (Polici ČR) odpovídající opatření k nápravě. Subjekt údajů však nemá možnost soudního přezkumu těchto závěrů Úřadu.

Třeba doplnit, že Policie ČR není oprávněna omezovat Úřadu přístup k informacím v SIS. Národní evidence, které jsou pro SIS zdrojem dat, nejsou utajovány. Pokud by v budoucnu k zařazení některých z nich mezi utajované skutečnosti došlo, byla by možnost přístupu k těmto evidencím vázána na splnění bezpečnostní prověrky inspektorem Úřadu[84]. Přestože nejde o utajované skutečnosti, řada dokumentů, které se k SIS vztahují, je označována na úrovni EU jako „LIMITÉ" a není zveřejňována. ČR postupuje obdobně.

Zpracování osobních údajů v policejních evidencích je charakteristické tím, že probíhá bez souhlasu subjektu údajů, čímž se zásadním způsobem liší od zpracování údajů soukromými subjekty. Z toho důvodu je nutné upravit též zvláštní postupy přístupu subjektu údajů k informacím o něm vedeným a zakotvit navazující kontrolní mechanismy tak, aby byla zajištěna kontrola zákonnosti a správnosti vedení údajů. Jak ZPČR (§ 42j), tak ZPC (§ 159) obsahují zvláštní ustanovení o přístupu subjektu k informacím.

ZPČR výslovně vyjímá řízení o poskytnutí informací ze správního řádu a neobsahuje žádné opravné prostředky. Rozhodnutí o neumožnění přístupu k informacím

---

81 Srov § 42g odst. 3 ZPČR, § 9 ZOÚ.
82 § 42g odst. 1 písm. e) ZPČR.
83 Policie Ř není jako taková účastníkem správního řízení z důvodu nedostatku její právní subjektivity – viz rozhodnutí NS č. Plsn 2/96, Sb. s. r. a s. 4/1997.
84 § 37 písm. c) ZOÚ.

spadá však pod definici rozhodnutí dle § 65 zák. č. 150/2002 Sb. soudního řádu správního (s. ř. s.), když se jím závazně určuje právo subjektu údajů na přístup k údajům o něm vedeným, které tvoří součást základního lidského práva na ochranu soukromí. Subjekt má tedy možnost soudního přezkumu tohoto rozhodnutí ve správním soudnictví. Takto však lze přezkoumat pouze zákonnost rozhodnutí o odmítnutí přístupu, případně sdělení, že o subjektu nejsou žádné informace zpracovávány[85], nikoli zákonnost vlastní existence záznamu. Tu by bylo možné zkoumat pouze v případě, kdy by se promítla do navazujícího správního aktu.

V úvahu přichází též možnost soudního přezkumu zákonnosti vedení osobních údajů dle § 82 s. ř. s., když nutno dovodit, že nezákonné vedení osobních údajů je nezákonným zásahem správního orgánu. Je však třeba vyčkat, jak se k této otázce postaví soudní praxe. Nebude-li nicméně provedena změna stávajícího právního rámce, bylo by nutné uvedeným výkladem překlenout nedostatek jiných opravných prostředků k soudu, jejichž existence je vyžadována komunitární právní úpravou (čl. 111 SPÚ, v budoucnu čl. 27 dosud neschváleného rámcového rozhodnutí). Možnost tohoto prostředku přezkumu je třeba připustit jak v případě, kdy jedinec má potvrzeno, že o něm jsou některé osobní údaje evidovány, tak v případě, kdy neví, zda tomu tak je (např. v případě oznámení, že o něm žádné údaje vedeny nejsou dle § 42j odst. 5 ZPČR).

Nedostatečnost právní úpravy se plnou měrou objevuje v souvislosti s odepřením vstupu, resp. zamítnutím žádosti o udělení víza dle ZPC. Jak již uvedeno shora, tato rozhodnutí se mohou opírat o existenci záznamu v SIS. Nepodléhají však správnímu řádu (§ 168 ZPC), ani soudnímu přezkumu (§ 171 ZPC)[86]. Rozhodnutí o odmítnutí přístupu k informacím dle § 159 ZPC je sice činěno ve správním řízení a soudní přezkum je možný, nicméně údaje, které je správní orgán povinen poskytnout jsou omezeny, když mezi nimi není zejména důvod vedení záznamu o subjektu (§ 159 odst. 1, 2 ZPC). Ve spojení s nemožností domáhat se soudního přezkumu postupu Úřadu při kontrole zákonnosti vedení osobních údajů v SIS dle § 21 ZOOÚ se naskýtá otázka, zda tato právní úprava respektuje základní právo jednotlivce na ochranu osobních údajů a na spravedlivý proces a požadavky, kladené na efektivní kontrolní mechanismy judikaturou ESLP.

Pokud by Úřad v rámci výkonu kontrolních oprávnění dle ZOÚ shledal porušení tohoto zákona, je oprávněn uložit opatření k nápravě, které může spočívat například v navržení systémových změn, či uložení likvidace údajů. Neprovedení takto uložených opatření nicméně není samostatným správním deliktem a uložení sankce tak nepřichází v úvahu. Ostatně možnost uložení sankce ČR (při spravování údajů Policií ČR) je v důsledku konstrukce zákona nejasná. Úřad totiž dohlíží pouze na dodržování těch povinností, které jsou stanoveny ZOÚ (v případě Policie ČR s výjimkou povinností, vyplývajících z § 5 odst. 1, §§ 11, 12). V důsledku této konstrukce jsou některé sankce, které může Úřad využít proti jiným správcům osobních údajů, v případě Policie ČR omezeny. V úvahu v zásadě přichází pouze postih pro správní delikt nepři-

[85] § 42j odst. 5 zák. 283/1991.
[86] Výjimkou je rozhodnutí o odepření vstupu rodinného příslušníka občana EU za podmínek § 5 odst. 1.

jmutí nebo neprovedení opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 45 odst. 1 písm. h), a ohrožení většího počtu osob neoprávněným zasahováním do soukromého a osobního života (§ 45 odst. 2 písm. a). Tuto problematiku by bylo nepochybně vhodné legislativně vyjasnit.

V případě vzniku nemajetkové újmy je obecným předpisem pro její náhradu občanský zákoník, při vzniku škody v důsledku nesprávného nakládání s osobními údaji v policejních evidencí by pak bylo nutné postupovat dle ustanovení zákona č. 82/1998 Sb. o náhradě škody způsobené nesprávným úředním postupem.[87]

2.7.2 Srovnání s vývojem právní úpravy a judikatury ve Francii

Z hlediska ČR je inspirativní sledovat problémy, s nimiž se v oblasti ochrany osobních údajů setkávají státy schengenského prostoru. Zajímavým vývojem prošla zákonná úprava a judikatura správních soudů ve Francii.

Podle čl. 109 odst. 1 SPÚ se právo na přístup vykonává za podmínek, stanovených národním právem. V čl. 109 odst. 2 nicméně SPÚ stanoví právo na přístup jako princip a případy odmítnutí jako výjimku. Vnitrostátní zákonodárství však tuto konstrukci často nepřebírá a zůstává na národních soudech dosáhnout cestou výkladu rozšíření ochrany jednotlivce před nedovolenými zásahy do jeho soukromí. I ve Francii je právními předpisy upraveno pouze právo na nepřímý přístup do SIS. Nejprve je třeba podat žádost k ústřednímu kontrolnímu orgánu (C. N. I. L.), která pověří jednoho ze svých členů provedením dalších kroků. Po jejich učinění informuje cizince o tom, že oprava údajů byla případně provedena.

Nejvyšší francouzský správní soud, Conseil d'Etat (dále CdE), však stanovil, že k některým záznamům v SIS musí mít subjekty zajištěn přímý přístup (přičemž se jedná zejména o rozhodnutí, která byla či měla být svým adresátům oznámena), nepřímý přístup pak má být pouze k těm údajům, u nichž by jejich sdělení mohlo ohrozit účel, pro který jsou vedeny[88]. Conseil d'Etat tak cestou soudního výkladu sbližuje národní právní úpravu s právní úpravou SPÚ.[89]

V Francii dále nemusela být, obdobně jako v současnosti v ČR, rozhodnutí o neudělení víza odůvodňována, a to až do přijetí zákona z 11. 5. 1998, který stanovil povinnost odůvodňovat některá z těchto rozhodnutí, mimo jiné právě rozhodnutí, zakládající se na existenci záznamu v SIS. Jako odůvodnění postačil původně odkaz na existenci záznamu v SIS. CdE nicméně dovodila, že takovéto odůvodnění nedostačuje. Odůvodnění by totiž dle ní mělo umožnit využití opravných prostředků proti existenci záznamu. Mělo by tak být zejména sděleno, který národní orgán k záznamu přistoupil.[90] Kontrola ze strany příslušného národního orgánu je totiž efektivnější než kontrola ze strany C. N. I. L.

CdE dále dovodila nejen oprávnění francouzských správních soudů být informován o záznamech, provedených orgánem jiného členského státu, ale též oprávnění pře-

---

87 Srov. § 25 ZOÚ.
88 CdE, 6. 11. 2002, M. Moon.
89 Srov Claire Saas: Les refus de délivrance de visas fondés sur une inscription au Système Information Schengen.
90 CdE, 9. 6. 1999, Hamssaoui.

zkoumávat zákonnost těchto záznamů! V konkrétním případě provedly německé orgány záznam z důvodu zamítnutí žádosti o azyl, CdE však shledala, že tento důvod nefiguruje v čl. 96 a proto byl záznam proveden nezákonně.[91] Toto rozhodnutí nutno blíže osvětlit.

Každému žadateli o azyl je v Německu v případě zamítnutí jeho žádosti stanovena lhůta k opuštění země. Za účelem ověření splnění této povinnosti je mu vystaveno potvrzení o překročení státní hranice, které by měl předložit na hranicích ve stanovené lhůtě. V případě, že tak neučiní, je o něm pořízen záznam za účelem eskorty na hranice, neboť se předpokládá, že pobývá v zemi neoprávněně. Tato úprava nicméně opomíjí například to, že žadatel o azyl zemi mohl opustit ještě předtím, než bylo o jeho žádosti rozhodnuto, popřípadě mohlo dojít k závadě v předání potvrzení mezi správními orgány. V obou těchto případech se vychází z hypotézy, že žadatel pobývá v Německu neoprávněně. Touto právní konstrukcí tak dochází ke smíšení záznamů o cizincích, vůči nimž bylo vydáno správní rozhodnutí o jejich vyhoštění, resp. o jejich eskortě na hranice, a cizincích, o kterých se má pouze za to, že se zdržují v Německu neoprávněně.

Rozšířenou kontrolou ve správním soudnictví nahrazuje CdE nedostatek harmonizace pravidel pro záznam v SIS, jakkoli je tento postup v rozporu se zásadou vzájemné důvěry v oprávněnost záznamů a zásadou loajality mezi členskými státy. V zásadě to znamená, že není-li důvod záznamu v jiném členském státě důvodem záznamu též ve Francii, je takový záznam prohlášen za nezákonný. Ve své navazující judikatuře CdE proto systematicky vyžaduje, aby důvody záznamů byly správnímu soudu ministerstvem zahraničí vždy sdělovány. Nestane-li se tak, je správní rozhodnutí prohlášeno za nezákonné.[92] Možnost přezkoumávat zákonnost záznamů, provedených orgány jiných členských států, nepřipouštějí proti francouzským soudům například soudy rakouské, které striktně vycházejí ze zásady vzájemného uznávání a důvěry.[93]

Třeba doplnit, že ve Francii existuje možnost podat proti rozhodnutí o zamítnutí žádosti o vízum opravný prostředek k Odvolací komisi, sloužící jako filtr před posouzením věci CdE. Správní soudce může též odložit vykonatelnost správního rozhodnutí do doby konečného rozhodnutí ve věci v případě (1) podání opravného prostředku, (2) nezbytnosti odkladu a (3) závažných pochybností o zákonnosti rozhodnutí.

ZÁVĚREČNÉ SHRNUTÍ

Právní úprava ochrany osobních údajů v rámci Schengenského informačního systému je charakteristická svou komplexností, víceúrovňovostí, dosavadním nedostatkem harmonizace a aktuálně probíhajícími legislativními pracemi na reformě. Hlavní tíha odpovědnosti v každém případě leží na vnitrostátním zákonodárci, který je povinen stanovit dostatečně transparentní právní rámec ochrany osobních údajů a zajistit, aby právní úprava nejen v teorii, ale i v praxi při své aplikaci státními orgány

[91] CdE, 9. 6. 1999, Forabosco.
[92] CE, 6. 10. 1999, Bafandi.
[93] Srov. Saase Claire, cit. S. 14.

respektovala základní principy, krystalizující v průběhu zákonodárného vývoje a související judikatury národních a mezinárodních soudních institucí. Tyto principy, jež možno pokládat za základ evropského systému ochrany osobních údajů v policejní oblasti, lze shrnout takto:

A. principy zpracování osobních údajů

1. jasnost a předvídatelnost právní úpravy;
2. zpracovávání osobních údajů pouze pro zákonem stanovený účel;
3. subsidiarita a proporcionalita způsobu zpracovávání osobních údajů vzhledem k jiným způsobům zajištění veřejného pořádku, bezpečnosti a předcházení trestné činnosti;
4. subsidiarita, proporcionalita a účelová vázánost možnosti státních orgánů vstupovat do databází osobních údajů;
5. přesnost osobních údajů a jejich pravidelná aktualizace, neověřené osobní údaje mohou být uchovávány jen při zamezení nebezpečí záměny s údaji ověřenými;
6. časová omezenost uchovávání údajů;
7. dostatečné zabezpečení databází údajů;
8. přeshraniční dostupnost evidovaných osobních údajů bezpečnostním složkám v rámci evropských společenství;
9. možnost poskytnutí údajů třetím zemím a institucím, je-li zajištěna stejná úroveň ochrany[94];

B. principy záruk jednotlivci

10. subsidiarita a proporcionalita omezení práva subjektu na přístup k údajům, které jsou o něm vedeny, na jejich opravu, výmaz či blokování;
11. právo jednotlivce na přímý přístup přinejmenším k osobním údajům, evidovaným o něm, měl-li již dříve právo seznámit se s nimi (záznamy prováděné jako důsledek vydání individuálního právního aktu);
12. právo jednotlivce na nepřímý přístup a kontrolu zákonnosti všech ostatních osobních údajů;
13. existence efektivních opravných prostředků proti rozhodnutí o zamítnutí přístupu k informacím;
14. odpovědnost za škodu a nemajetkovou újmu vzniklou v důsledku nezákonného zpracovávání osobních údajů;
15. kontrola ze strany nezávislého správního orgánu;
16. kontrola ze strany nezávislých soudů.

Při hodnocení komunitární právní úpravy de lege lata a současných reformních návrhů, předložených Komisí, lze konstatovat, že tato úprava v zásadě respektuje shora uvedené principy. Výjimkou je omezení práva na soudní přezkum na případy odepření práva přístupu k informacím, obsažené v návrzích rozhodnutí a nařízení o zavedení

[94] Úroveň ochrany nelze chápat jako úroveň zabezpečení evidencí proti zásahům zvnějšku, ale jako právní úpravu respektující.

SIS II. Problematické též zůstává, že zatímco v rámci třetího pilíře by mělo dojít k harmonizaci národních právních úprav prostřednictvím rámcového rozhodnutí o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech, v rámci prvního pilíře k harmonizaci v oblasti evidencí bezpečnostních složek dosud nedošlo, když směrnice 95/46/ES se na tuto oblast výslovně nevztahuje a rozšíření působnosti této směrnice není součástí reformy. V případě schválení reformních návrhů Komise ve stávající podobě by nicméně tento nedostatek mohl napravit národní zákonodárce přesahující implementací rámcového rozhodnutí o ochraně osobních údajů též na část SIS II, vedenou v rámci pilíře prvního. Nutno zdůraznit, že reformní návrhy Komise jsou navzájem provázány a zejména by nemělo dojít k reformě SIS II, aniž by bylo schváleno uvedené rámcové rozhodnutí.

V případě ČR nutno poukázat na nedostatečné vyjasnění vztahu Úřadu pro ochranu osobních údajů a Policie ČR. Pokud jde o rozsah přezkumného oprávnění Úřadu, bylo by vhodné upravit blíže postupy, na základě kterých by Úřad mohl hodnotit odůvodněnost záznamů v policejních evidencích. Vyjasnění by zasloužila též možnost ukládání sankcí Policii ČR ze strany Úřadu. Nedostatkem je i nemožnost jednotlivce účastnit se a jakkoli zasahovat do správního řízení, vedeného Úřadem s ČR pro porušení povinností týkajících se zpracování jeho osobních údajů. Tento nedostatek by bylo možné odstranit zakotvením účastenství jednotlivce v daném řízení s možnými výjimkami, pokud jde o seznamování se s obsahem spisů.

Dále je třeba vyčkat, jak se správní judikatura postaví k možnosti přezkoumávat zákonnost zpracovávání osobních údajů v policejních evidencích postupem dle § 82 s. ř. s. Vznikaly-li by při aplikaci tohoto ustanovení výkladové problémy, bylo by nutné pro soudní kontrolu této oblasti stanovit zvláštní právní úpravu.

Zásadním problémem zůstává stávající úprava řízení o udělení víza, která neobsahuje žádné záruky ochrany jednotlivce proti rozhodnutí o zamítnutí žádosti o vízum z důvodu evidence osoby v SIS. Pochybnosti navíc vzbuzuje způsob a metodika, na základě které bude v ČR vytvořena úvodní suma údajů k zařazení do SIS. Z hlediska komunitárního je třeba neustále rozvíjet komunikační kanály mezi jednotlivými národními kontrolními orgány s cílem zajistit bezproblémovou komunikaci zejména při výmazu údajů ze SIS, pořízených v různých členských státech. S ohledem na rozpracovanost legislativních prací zejména na komunitární úrovni je nicméně předčasné hodnotit veškeré dopady zapojení ČR do schengenské spolupráce pro oblast osobních údajů. Až budoucí praxe odhalí všechny nedostatky a slabá místa právní úpravy.

PROTECTION OF PERSONAL DATA
IN THE SCHENGEN INFORMATION SYSTEM

Summary

Enlarging of the European Union poses a great challenge to the Schengen cooperation which all new Member states are supposed to participace on without any exceptions. A free movement of persons being its foremost objective, the elimination of borders checks must be accompanied by compensatory measures, one of which is the creation of Schengen information system (SIS). Before the full integration of new EU Members to Schengen cooperation, the SIS must be substantially reformed to meet new technical and qualitative requirements. The Commission has already submitted all the relevant proposals to establish SIS II.

This work aims to give an overview of the SIS construction, functioning and reform, focusing on the protection of personal datas within the system. It approaches legal documents and recent Commission proposals one after another to give a complex survey of the personal data protection in SIS and SIS II, taking fully into account recent decisions of European Court of Justice and European Court of Human Rights.

Having analysed the European framework of the personal data protection the work examines the current Czech system of protection of datas in police evidences pointing at potential similarities in future development compared to France.

In conclusion the work summarizes the basic principles governing the current system of personal data protection and highlights the imperfections of the current legal framework especially in the Czech Republic.

Key words: Schengen Information System, Personal Data Protection, SIS, Right to Privacy, Schengen cooperation