



ČESKÁ REPUBLIKA

ROZSUDEK

JMÉNEM REPUBLIKY

Městský soud v Praze rozhodl v senátě složeném z předsedkyně JUDr. Ing. Viery Horčicové a soudců Mgr. Jiřího Lifky a Mgr. Kamila Tojnera v právní věci žalobkyně: **Česká republika – Vězeňská služba České republiky**, proti žalovanému: **Úřad pro ochranu osobních údajů**, se sídlem pplk. Sochora 27, 170 00 Praha 7, o žalobě proti rozhodnutí předsedy Úřadu pro ochranu osobních údajů ze dne 20. 5. 2013, č. j. UOOU-00182/13-27,

t a k t o :

- I. Žaloba se z a m í t á .
- II. Žádný z účastníků n e m á p r á v o na náhradu nákladů řízení.

O d ů v o d n ě n í :

Žalobkyně se domáhala přezkoumání a zrušení rozhodnutí předsedy Úřadu pro ochranu osobních údajů ze dne 20. 5. 2013, č. j. UOOU-00182/13-27, kterým byl zamítnut rozklad žalobkyně proti rozhodnutí Úřadu pro ochranu osobních údajů ze dne 25. 3. 2013, č. j. UOOU-00182/13-2120.5.2013 (dále i „rozhodnutí správního orgánu prvního stupně“). Rozhodnutím správního orgánu prvního stupně byla žalobkyně uznána vinnou ze spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále „zákon o ochraně osobních údajů“) a byla jí podle § 45 odst. 3 tohoto zákona uložena pokuta ve výši 50 000 Kč a povinnost nahradit náklady řízení ve výši 1000 Kč. Vytýkané jednání žalobkyně podle rozhodnutí správního orgánu prvního stupně spočívalo v tom, že „jako správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., v souvislosti se zpracováním osobních údajů vězněných osob, tím, že v jím provozovaném vězeňském informačním systému měli přístup ke všem údajům vedeným v tomto systému všichni zaměstnanci oprávnění v něm pracovat (cca 5000 osob), v důsledku čehož došlo v době mezi 14. květnem a 5. červnem 2012

k neoprávněnému přístupu k osobním údajům 8 osob umístěných ve vazebních věznicích v souvislosti s kauzou a zatčením MUDr. D. R. a následnému zveřejnění fotografií těchto osob v deníku B. dne 2. a 5. června 2012, porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů“.

Žalobkyně v žalobě namítla, že vymezení skutku v rozhodnutí správního orgánu prvního stupně, jehož spáchání mělo naplnit skutkovou podstatu vytykaného správního deliktu, je ze své podstaty vnitřně rozporné, neboť není možné, aby osoba oprávněná k přístupu a vkládání údajů v informačním systému z něj získala údaje neoprávněně. Podle žalobkyně tak nemohlo dojít k porušení § 13 odst. 1 zákona o ochraně osobních údajů, podle něhož jsou správce a zpracovatel povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, a tedy ani naplnění skutkové podstaty správního deliktu podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů. Žalobkyně uvedla, že osoby, které poskytly fotografie osob figurujících v kauze MUDr. D. R. ke zveřejnění, tyto fotografie získaly řádně a oprávněně. Nezákonnost spočívala až v dalším nakládání s těmito fotografiemi, tedy jejich poskytnutí ke zveřejnění, přičemž tento postup nemohla žalobkyně nijak ovlivnit. Žalobkyně neshledává jakoukoli příčinnou souvislost mezi počtem osob s oprávněním k přístupu a vkládání informací v informačním systému žalobkyně a zveřejněním fotografií osob figurujících v kauze MUDr. D. R. Správní orgány obou stupňů se podle žalobkyně nijak nezabývaly otázkou, zda by ke zveřejnění fotografií osob figurujících v kauze MUDr. D. R. došlo i v případě omezení počtu osob s tímto oprávněním, a to jak ve vztahu ke všem informacím v informačním systému žalobkyně, tak ve vztahu k informacím pouze některým. Jediné, oč žalovaný závěr o porušení povinnosti podle § 13 odst. 1 zákon o ochraně osobních údajů opírá, je skutečnost, že ve vězeňském informačním systému provozovaném žalobkyní měli přístup ke všem údajům vedeným v tomto systému všichni zaměstnanci oprávnění v něm pracovat (cca 5000 osob). Subjektivní názor žalovaného, že přístup do informačního systému pro 5000 osob je příliš, považuje žalobkyně za irelevantní. Tento názor by podle žalobkyně vedl k neudržitelnému závěru, že zaměstnavatelé s vyšším počtem přístupů do informačního systému, než je 5000, jsou automaticky pachatelé deliktu dle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů. Pokud u žalobkyně pracuje cca 10 000 zaměstnanců, lze považovat počet 5000 oprávnění v informačním systému za zcela odpovídající. Žalobkyně nicméně takové názory správního orgánu ohledně přiměřenosti počtu osob oprávněných ke vstupu do systému považuje za fakty nepodložená přesvědčení, která z hlediska zásady zákonnosti nemohou být důvodem pro uložení sankce.

Žalovaný veden svým subjektivním názorem, že 5000 osob s přístupem ke všem údajům vedeným v informačním systému je příliš, podle žalobkyně neuvažoval o důvodech tohoto stavu, činnostech, které žalobkyně zajišťuje, jakými procesy tyto činnosti zajišťuje apod. Oprávnění v informačním systému byla u žalobkyně nastavena dle potřeb zaměstnanců tak, aby mohli řádně a na základě maximálně možného rozsahu informací plnit své pracovní úkoly. Jako příklad žalobkyně uvedla přemísťování odsouzených, kdy je třeba, aby se jednotlivé osoby v přijímající věznici/vazební věznici, kteří budou vůči odsouzenému plnit své povinnosti (vychovatelé, psychologové, zvláštní pedagogové, apod.) seznámily s profilem konkrétního odsouzeného/obviněného, aby se příslušníci provádějící eskorty či transport, kteří nejsou z téže věznice/vazební věznice, mohli seznámit s konkrétní osobou eskortovaného, aby pracovníci metodických a evidenčních útvarů (ať již generálního ředitelství či jednotlivých

věznic/vazebních věznic) mohli nahlížet a čerpat z údajů o všech odsouzených/obviněných apod.

Jako obdobný protimluv jako v případě vymezení skutku zakládajícího naplnění skutkové podstaty správního deliktu žalobkyně hodnotí úvahu žalovaného, že „*interní předpis upravující užívání informačního systému žalobkyně umožňoval, aby k veškerým osobním údajům měl přístup každý zaměstnanec, který byl jakýmkoli způsobem povinen pracovat s daty vězněných osob*“, přičemž tento stav měl „*evidentně svědčit*“ o nedostatečném plnění povinností. Žalobkyně namítla, že jestliže je zaměstnanec povinen v rámci své náplně práce pracovat s určitými daty, pak k těmto datům musí mít přístup, přičemž plnění těchto zákonných povinností nemůže naplnit skutkovou podstatu správního deliktu.

Za irelevantní v dané souvislosti žalobkyně považuje argumentaci žalovaného týkající se úprav přidělení oprávnění v informačním systému žalobkyně po provedené kontrole, a to obzvláště v situaci, kdy žalovaný sám zohlednit budoucí stav zcela odmítá.

Konečně pak žalobkyně vyslovila též pochybnost nad její delikt ní způsobilostí ke spáchání správního deliktu podle § 45 odst. 1 zákona o ochraně osobních údajů, neboť návětí tohoto ustanovení jako delikt ně způsobilé subjekty vymezuje právnické osoby nebo fyzické osoby podnikající podle zvláštních předpisů. Toto ustanovení tak podle žalobkyně, pokud se užije výkladu příznivějšího pro „pachatele deliktu“, který by měl být dle základních zásad správního trestání a trestání vůbec přijímán, může být pachatelem pouze podnikající právnická nebo fyzická osoba, což žalobkyně není. Absence čárky před slovem „nebo“ tento výklad podporuje. V této souvislosti rovněž žalobkyně uvedla pochybnost, zda ji vůbec lze podřadit pod pojem „právnická osoba“, pokud základní dělení subjektů práva rozeznává fyzické osoby, právnické osoby a stát.

S ohledem na uplatněné žalobní body žalobkyně navrhla, aby Městský soud v Praze napadené rozhodnutí i rozhodnutí správního orgánu prvního stupně zrušil a věc vrátil žalovanému k dalšímu řízení.

Žalovaný ve vyjádření k žalobě uvedl, že výrok rozhodnutí správního orgánu prvního stupně není vnitřně rozporný a námitky žalobkyně vyplývají spíše z nepochopení principů zabezpečení osobních údajů a systematiky zákona o ochraně osobních údajů. Situaci řešenou v nyní projednávané věci připodobnil k situaci, kdy zaměstnanec orgánu veřejné moci má přístup do evidence obyvatel, tj. k údajům o všech občanech České republiky. I v takovém případě však může oprávněně přistupovat k osobním údajům pouze tehdy, pokud je to nutné při výkonu jeho konkrétní pracovní činnosti. To znamená, že pokud by takový zaměstnanec v lepším případě náhodně v evidenci obyvatel vyhledával známé, přátele apod., v horším případě vyhledával osobní údaje na zakázku a za úplatu, jedná se v obou případech o neoprávněný přístup ke konkrétním osobním údajům, ačkoliv je daný zaměstnanec osobou oprávněnou k přístupu a vkládání osobních údajů do informačního systému. Podle žalovaného tedy nemůže jít o dvě vzájemně rozporné skutečnosti. Proto také žalovaný považuje tvrzení žalobkyně o tom, že její zaměstnanci získali fotografie řádně a oprávněně, a nezákonnost spočívala až v jejich dalším nakládání, za dosti alarmující a závažné. Znamená to totiž, že jednotliví zaměstnanci žalobkyně si zřejmě mohou bez relevantního důvodu spočívajícího v předmětu jejich práce prohlížet veškeré záznamy ve vězeňském informačním systému.

Žalovaný k otázce zabezpečení osobních údajů uvedl, že § 13 zákona o ochraně osobních údajů zahrnuje celý komplex činností a opatření, které je každý správce povinen

učinit. Z ustanovení § 13 odst. 1 zákona o ochraně osobních údajů vyplývá cíl a smysl těchto opatření, tedy zabránit tomu, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, přičemž k tomu v daném případě nepochybně došlo. Ustanovení § 13 odst. 3 zákona o ochraně osobních údajů stanovuje, jakým způsobem správce posuzuje některá rizika, přičemž přijatá opatření by měla zajistit, aby zaměstnanci plnili pokyny pro zpracování osobních údajů, aby opatření zabránila neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje. V případě automatizovaného zpracování, kterým nepochybně vězeňský informační systém je, je poté dle odst. 4 uvedeného ustanovení povinností správce zajistit, aby systém používaly pouze oprávněné osoby a aby tyto osoby měly přístup pouze k údajům odpovídajícím oprávnění těchto osob.

Podle žalovaného informační systém obsahující osobní údaje vězňů nemůže být nastaven tak, aby mělo cca 5 000 osob (tj. 1/2 všech zaměstnanců žalobkyně) přístup ke všem osobním údajům vězňů, které jsou v něm evidovány. Takto široce nastavená přístupová práva sama o sobě vytvářejí riziko zneužití osobních údajů ze strany zaměstnanců a správci (žalobkyni) neumožňují efektivní kontrolu toho, zda zaměstnanci svá přístupová práva nezneužívají a nevynášejí osobní údaje. Podle žalovaného tedy žalobkyně nedostatečně vyhodnotila rizika zpracování osobních údajů, neboť přijatá opatření neumožňují zajistit, aby zaměstnanci plnili pokyny pro zpracování osobních údajů, a aby přijatá opatření (nastavení přístupu) bránilo neoprávněnému čtení, vytváření, kopírování atd. osobních údajů.

Podle žalovaného dále porušení povinnosti dle § 13 zákona o ochraně osobních údajů nezávisí na konkrétním počtu osob s přístupem, jak naznačuje žalobkyně, ale na jejich pracovním zařazení a úkolech ve spojení s nastaveným oprávněním přístupu. Podle žalovaného není nejmenší důvod pro to, aby např. vychovatelé, psychologové a zvláštní pedagogové měli přístup k osobním údajům vězňů mimo věznici, kde jsou zaměstnáni. Je poté nepochybně možné systém nastavit tak, aby v případě přesunu vězně získali přístup k údajům tohoto konkrétního vězně (a to např. na základě systémového nastavení, tj. vložení pokynu k přesunu do systému, které by automaticky zpřístupnilo údaje oprávněným osobám v cílové věznici, nebo na základě dodatečného schválení nadřízeným). Proto ani důvody uváděné žalobkyní neshledává žalovaný relevantními pro nastavení informačního systému zjištěným způsobem.

Podle žalovaného tedy z ustanovení § 13 zákona o ochraně osobních údajů vyplývá povinnost každého správce nastavit přístupová práva k osobním údajům takovým způsobem, aby byl schopen relevantně vysvětlit důvodnost a nezbytnost přístupu konkrétního zaměstnance, přičemž toto nastavení musí z důvodu zajištění ochrany osobních údajů vycházet z minimálního rozsahu přístupových práv (s případnými výjimkami stanovovanými a případně i schvalovanými individuálně) a nikoliv z maximálního možného nastavení jako v případě žalobkyně. V opačném případě ztrácejí bezpečnostní opatření a nastavení přístupových práv svůj hlavní smysl, a to omezit počet osob s přístupem k osobním údajům a předejít tak jejich neoprávněnému zneužití. Teprve na tato opatření navazují další, jako je např. logování přístupu, která ovšem sama o sobě zneužití osobních údajů nezabrání a působí až následně při vyšetřování.

Pokud jde o deliktní způsobilost žalobkyně, ustanovení § 45 odst. 1 zákona o ochraně osobních údajů podle žalovaného rozlišuje dvě skupiny subjektů správního deliktu, na straně jedné právnickou osobou, a na straně druhé fyzickou osobou podnikající podle zvláštních předpisů, přičemž spojka „nebo“ bez čárky zde vyjadřuje slučovací význam ve smyslu volby alternativy. K odpovědnosti státu za správní delikt žalovaný uvedl, že stát je i v oblasti

veřejného práva nepochybně právníckou osobou (veřejnoprávní korporací). Stát má tedy správnědeliktní odpovědnost za svoje jednání.

Z obsahu správního spisu vyplynuly následující pro věc podstatné skutečnosti:

Z kontrolního protokolu ze dne 5. 12. 2012, č. j. INSP1-5838/11-26/BYT, vyplývá, že správní orgán prvního stupně zjistil, že se v deníku B. z 2. června 2012 a z 5. června 2012 objevily fotografie vazebně stíhaného dr. D. R. a dalších sedmi spoluobviněných osob, které unikly z vazební věznice. Protože tím vzniklo podezření, že došlo k porušení zákona o ochraně osobních údajů, podal předseda Úřadu podnět k zahájení kontroly. Na základě kontroly logů orgány činné v trestním řízení společně se žalobkyní zjistily, že tyto fotografie pocházejí z Vězeňského informačního systému provozovaného žalobkyní (dále i „VIS“) a že je zpřístupnil příslušník Vězeňské služby, který ovšem pracoval ve funkci dozorce v jiné věznici, než kde byli obvinění umístěni. Na data všech osmi obviněných nahlížel dle zjištění Generální inspekce bezpečnostních sborů ještě občanský pracovník ve funkci psycholog a opět z jiné věznice. Aspoň na jednoho z obviněných nahlíželo přitom dalších 80 osob. Dle zjištění žalobkyně byly fotografie pořízeny z VIS pomocí mobilu, nešlo tudíž o přímý výstup z VIS.

Kontrolní protokol dále obsahuje popis VIS, podle něhož tento tento systém zpracovává osobní údaje vězňů, tj. osob vazebně stíhaných a odsouzených, nikoliv zaměstnanců Vězeňské služby. Část VIS „Správa vězňů“ je série 5 modulů (evidence vězňů, výkon vazby a trestu, Vězeňská a justiční stráž, zaměstnání vězňů a ekonomika vězně). Data vznikají převážně na jednotlivých věznicích a jsou přenášena na Generální ředitelství. VIS obsahuje zejména tyto osobní údaje vězňů: údaje identifikační (poslední adresa, rodné číslo, fotografie), důvody současného uvěznění (trest, paragraf, vazba), charakteristika (nebezpečnost, útek, násilí), pracovní zařazení, dieta.

V době před uvedeným incidentem dle vyjádření Vězeňské služby v přístupech k osobním údajům vězňů nebylo rozlišováno mezi vězni z věznice vlastní a jiné. Následně po incidentu byl systém přestaven tak, že žádné funkční místo ve správě vězňů jako takové neumožňuje nahlížet na vězně jiných věznic. Současně bylo všem funkčním místům ve správě vězněných osob zamezeno nahlížet na všechny vězněné osoby, resp. vyhledávat je v seznamu vězňů, bez znalosti jména, příjmení a data narození nebo kódu vězně. Pro tyto činnosti byly vytvořeny speciální role, které jsou přidělovány jednotlivě, pouze vybraným uživatelům, na základě odůvodněné a ředitelem organizační jednotky schválené písemné žádosti, přičemž žádosti ředitelům organizačních jednotek schvaluje generální ředitel. Nové upravený stav přístupových práv ve VIS byl ověřen v navštívených věznicích (Litoměřice, Vlnáři), kde bylo zjištěno, že do VIS mají přístup zaměstnanci Vězeňské služby podle úkolu, který provádějí, a to tak, aby všechny osobní údaje, které jsou jim zobrazeny, byly nezbytně nutné k právě prováděnému úkolu. K vyhledání informací ve VIS je vždy třeba znát jméno, příjmení a datum narození (resp. kód vězně), tudíž nelze prohledávat vězně jiných věznic bez těchto konkrétních znalostí. Není možné vyhledávání v jiné věznici způsobem, že by se objevil seznam všech vězněných osob. Jedná se o úkoly, které provádějí buď bezprostřední dozorcí: povolování návštěv, korespondence, výchovné problémy, žádosti a stížnosti, diety apod. nebo zaměstnanci správního oddělení, vězeňští pedagogové a lékaři, vrchní dozorcí, vedoucí oddělení výkonu vazby, ředitel a zástupce ředitele věznice. Pokud jde o rozsah osob s oprávněním nahlížet do osobních údajů vězňů v jiných věznicích, bylo potvrzeno, že přístup má ředitel, který na základě písemné žádosti v odůvodněných případech povoluje přístup i pro další zaměstnance. Těmi jsou zejména zástupce ředitele věznice, pracovníci správního

oddělení a vedoucí oddělení výkonu trestu a vazby. Důvodem, proč je nahlíženo do databáze vězněných osob i v jiné věznici, je získání informací o případném příchodném vězni, o jeho možnosti být zaměstnán, o jeho nebezpečnosti apod. Důvodem pro nahlížení do cizích věznic správního odboru je příprava spisů a kontrola údajů pro rozhodování o případném příjmu vězně z jiné věznice, popř. naopak dodání pošty vězni eskortovanému do jiné věznice.

Z těchto informací poskytnutých žalobkyní správní orgán prvního stupně učinil kontrolní závěr v tom smyslu, že oprávnění přístupu do osobních údajů vězňů z jiné věznice byl před incidentem nastaven tak, že jej měli všichni zaměstnanci, kteří měli funkční místo ve správě vězňů. Naopak nyní mají pouze vybraní uživatelé VIS přístup k osobním údajům osob vězněných v jiných věznicích.

Z hlediska právního posouzení dospěl kontrolní orgán v rámci kontroly k závěru, že došlo k porušení ustanovení § 13 odst. 1 zákona o ochraně osobních, neboť žalobkyně nepřijala dostatečná opatření, aby k úniku osobních údajů nemohlo dojít – systém VIS sice byl zajištěn logováním, takže bylo možno pachatele objevit, ale možnost nahlížet do osobních údajů vězňů a osob vazebně stíhaných měli i zaměstnanci, kteří s nimi neměli žádnou povinnost pracovat.

Na základě těchto kontrolních zjištění správní orgán prvního stupně zahájil správní řízení pro podezření ze spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů.

Žalobkyně ve vyjádření k zahájenému správnímu řízení uvedla, že k vězeňskému informačnímu systému, konkrétně k fotografiím jednotlivých vězňů, měl přístup každý zaměstnanec účastníka řízení, který je jakýmkoliv způsobem povinen pracovat s daty vězněných osob. Jednalo se o pracovní pozice ředitele, zástupce ředitele, správních referentů úseku správního, dozorců výkonu vazby a výkonu trestu, vychovatelů výkonu trestu a vazby, sociálních pracovníků, pedagogů, psychologů, strážných vězeňské stráže, příslušníků prevence a stížnosti, zaměstnanců zdravotních středisek, materiálních intendantů, zaměstnanců úseku zaměstnávání vězněných osob, účetních, duchovních zaměstnanců a příslušných vedoucích funkcionářů. Žalobkyně dále uvedla, že v době, kdy došlo k nahlížení do informačního systému ze strany dvou zaměstnanců, kteří následně fotografie obviněných poskytli tisku, platil interní předpis Nařízení generálního ředitele č. 20/2005, o provozu výpočetní techniky. Ten v § 4 definoval činnost uživatele v počítačové síti, a to včetně zákazů. Podle odstavce 7 tohoto ustanovení uživatel odpovídá při práci s údaji za dodržování předpisů o ochraně osobních údajů v informačních systémech. V § 10 nařízení pak byla uvedena další opatření pro ochranu osobních údajů v síti účastníka řízení.

Na doplňující výzvu správního orgánu prvního stupně žalobkyně dne 12. 2. 2013 sdělila, že k vězeňskému informačnímu systému, konkrétně k fotografiím jednotlivých vězňů, mělo přístup cca 5000 zaměstnanců žalobkyně.

Správní orgán prvního stupně v rozhodnutí o uožení pokuty konstatoval, že údaje o fyzické osobě vedené ve vězeňském informačním systému, a to včetně fotografie, jako jejich nosiče, jsou osobní údaje ve smyslu § 4 písm. a) zákona o ochraně osobních údajů a že žalobkyně tím, že stanovila účel, prostředky a způsob zpracování osobních údajů osob ve výkonu vazby (resp. obecné vězněných osob), tj. jejich zpracování ve vězeňském informačním systému, se stala správcem osobních údajů ve smyslu § 4 písm. j) zákona o

ochraně osobních údajů, a tedy odpovídá za dodržování povinností stanovených pro jejich zpracování, včetně povinnosti vyjádřené v § 13 odst. 1 zákona o ochraně osobních údajů.

Dále správní orgán konstatoval, že ustanovení § 13 odst. 1 zákona o ochraně osobních údajů ukládá správci osobních údajů povinnost přijmout mj. taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, resp. obecně k jejich neoprávněnému zpracování. S tím souvisí povinnost správce podle §13 odst. 4 písm. b) zákona o ochraně osobních údajů v oblasti automatizovaného zpracování osobních údajů v rámci opatření podle § 13 odst. 1 zákona o ochraně osobních údajů zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby. Skutková podstata správního deliktu v § 45 odst. 1 písm. h) zákona o ochraně osobních údajů je podle žalovaného formulována jako odpovědnost za následek. Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona (neoprávněnému nebo nahodilému přístupu k osobním údajům), což bylo v dané věci podle správního orgánu nepochybně naplněno, znamená to, že se správce osobních údajů dopustil správního deliktu, přičemž odpovědnost za správní delikt je postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění).

Pokud jde o možný liberační důvod podle § 46 odst. 1 zákona o ochraně osobních údajů, správní orgán prvního stupně konstatoval, že vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí, které bylo možno požadovat, a nikoliv např. spravedlivé požadovat, požadovat s ohledem na poměry atp.). V případě žalobkyně bylo zřejmé, že nepřijala dostatečná opatření pro zabezpečení osobních údajů, v důsledku čehož měl každý zaměstnanec, který byl povinen pracovat s informačním systémem, přístup k osobním údajům všech vězněných osob, a to i v případě, kdy tento přístup nebyl nezbytný k výkonu jeho práce. Pouhé vymezení povinnosti, zákazů a oprávnění při práci s informačním systémem ve vnitřním předpise nelze považovat za veškeré možné úsilí, které mohl účastník řízení vynaložit k tomu, aby zabránil neoprávněnému přístupu k osobním údajům.

Žalobkyně v rozkladu proti rozhodnutí o uložení pokuty namítla, že se správního deliktu nedopustila, přičemž není vyloučeno zahájení řízení o přestupku vůči konkrétním osobám, jejichž jednáním došlo ke zveřejnění fotografií 8 osob umístěných ve vazebních věznicích v souvislosti se zatčením MUDr. D. R. K údajům ve vězeňském informačním systému musí mít podle žalobkyně, přístup všichni zaměstnanci, kteří je do tohoto systému vkládají nebo používají ke své práci. Těmito zaměstnanci nesmí a nemohou být pouze zaměstnanci konkrétní věznice, ve které je vězněná osoba umístěna. Přehodnocení přístupu konkrétních zaměstnanců, ke kterému přikročila, tento princip nikterak nezměnilo. Počet zaměstnanců oprávněných k přístupu nemá dle jeho vyjádření se zveřejněním předmětných fotografií žádnou souvislost. Dále žalobkyně uvedla, že promítla povinnosti při ochraně osobních údajů do svých vnitřních předpisů. Porušení povinností stanovených zákonem o ochraně osobních údajů i vnitřními předpisy o ochraně osobních údajů v informačních systémech konkrétními zaměstnanci nelze žalobkyni podle jejího názoru přičítat k tíži.

Žalovaný v rámci rozhodnutí o rozkladu uplatnil obdobnou argumentaci jako ve vyjádření k žalobě.

Městský soud v Praze žalobou napadené rozhodnutí, jakož i řízení, které jeho vydání předcházelo, přezkoumal v rozsahu uplatněných žalobních bodů, kterými je vázán, a vycházel přitom ze skutkového a právního stavu, který tu byl v době rozhodování správního orgánu. Městský soud v Praze přitom dospěl k závěru, že námitky žalobkyně nejsou důvodné.

Soud se v první řadě zabýval námitkou delikt ní nezpůsobilosti žalobkyně, kterou opírá o návěti ustanovení § 45 odst. 1 zákona o ochraně osobních údajů („*Právnícká osoba nebo fyzická osoba podnikající podle zvláštních předpisů se jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů...*“). V argumentaci žalobkyně lze přitom odlišit dvě roviny.

V první rovině argumentace žalobkyně namítla, že jako organizační složka státu (resp. stát) není právníckou ani fyzickou osobou, nespadá tedy ani pod vymezení delikt ně způsobilých subjektů podle § 45 odst. 1 zákona o ochraně osobních údajů. Tento závěr nelze ovšem akceptovat.

K postavení státu jako adresáta vrchnostenského působení sebe samého se obšírně vyslovil (byť v poněku jiných souvislostech, neboť šlo primárně o žalobní legitimaci státu podle § 65 a násl. s. ř. s.) Nejvyšší správní soud v rozsudku ze dne 11. 11. 2004, č. j. 2 As 36/2004 – 46, v němž zejména konstatoval, že je třeba předně vycházet z dvojího postavení státu podle typu právních vztahů, v nichž vystupuje. V této souvislosti odkázal na právní názor Ústavního soudu, obsažený ve sjednocujícím stanovisku jeho pléna č. 9/99 ze dne 9.11.1999 (Sbírka nálezů a usnesení, sv. 16, str. 372 a násl.), podle něhož platí, že „*pokud stát vystupuje v právních vztazích v pozici subjektu veřejného práva, čili jako nositel veřejné moci, z povahy věci není a nemůže být nositelem (subjektem) základních práv a svobod. Přístup opačný by znamenal popření smyslu základních práv a svobod tak, jak byly zformovány staletým vývojem evropské a anglosaské kultury. Z pohledu teoretického takovýto postup znamená popření fundamentálního rozdílu mezi pojmy oprávnění (subjektivního práva) a pravomoci (kompetence), jenž je akceptován v postavení paradigmatu právního myšlení v dosahu evropské kontinentální a anglosaské právní kultury*“. Z toho Nejvyšší správní soud vyvodil, že stát (prostřednictvím svých orgánů) vystupuje buď ve vrchnostenském postavení, anebo v postavení zcela srovnatelném s ostatními účastníky právních vztahů. Praktickým kritériem pro rozlišování tohoto postavení je povaha konkrétního právního vztahu.

Nejvyšší správní soud dále výslovně odmítl názor, že pojem „právnícká osoba“ je pojmem výhradně soukromého práva, a protože stát ve veřejném právu není pozitivním právem definován, nemůže ve veřejnoprávním vztahu (kterým, jak Nejvyšší správní soud zdůraznil, je nesporně i vztah sankční odpovědnosti) vystupovat jako právnícká osoba. Klíčovou výpovědí je přitom následující argumentace Nejvyššího správního soudu: „*Z pouhé absence pozitivně upravené definice státu jako právnícké osoby ve veřejném právu (veřejnoprávní korporace) totiž nelze soudit, že stát takovouto způsobilostí nedisponuje. V tomto směru je možno především namítat, že stát představuje originální subjekt právních vztahů, a to ve smyslu vnitrostátním i mezinárodním. Toliko za splnění této podmínky může plnit svoje vnitřní a vnější funkce. Pokud by mělo platit, že subjektivitu státu lze dovodit až z existence pozitivního právního předpisu, znamenalo by to - dovedeno ad absurdum - ve svých důsledcích, že subjektivita by byla konstituována normativním aktem, jehož autorem by musel být samotný stát. To znamená, že by tento akt přijal stát ještě v postavení ne-subjektu právních vztahů a teprve od jeho přijetí by se tímto subjektem stal. Tento názor však zjevně pomíjí fakticitu existence a autonomní povahu státu, založenou na přítomnosti konstitutivních prvků (v obecně přijímaném Jellinekově pojetí: státní moc, území, obyvatelstvo), a nikoliv na*

výslovně pozitivněprávní reglementaci. Rovněž z organického hlediska je zřejmé, že jakkoliv organizační složky státu, tzn. jeho orgány, nedisponují vlastní právní subjektivitou: představují - ve starší terminologii - "údy státu", tedy za stát jednájí a zavazují jej. Nikoliv náhodně proto např. Ústava ČR výslovně stanoví, že soudní moc vykonávají "jménem republiky" nezávislé soudy. Vydávají proto rozhodnutí jménem subjektu, kterým je stát, a to i ve veřejném právu. Druhým dílčím závěrem je proto konstatování teoretické neudržitelnosti právního názoru, že stát ve veřejném právu není právnickou osobou (podobně viz též např. D. Hendrych: Správní právo. Obecná část. 4. vyd., str. 259 a násl.; V. Pavlíček a kol.: Ústavní právo a státověda. I. díl, str. 45 a násl.).“

Žalobkyni je tak třeba i v oblasti veřejného práva považovat za právnickou osobu, a to o to spíše, že v nyní projednávané věci vystupovala jako adresát právní povinnosti směřující vůči jakémukoliv subjektu práva, měla tedy stejné postavení jako jakákoliv jiná právnická či fyzická osoba. Pokud by totiž byla přijata argumentační linie žalobkyně, mj. by to znamenalo zcela neudržitelný závěr již jen z hlediska ústavní zásady rovnosti, a sice, že by jako správce osobních údajů byla obdobně jako jiné právnické a fyzické osoby adresátem povinností stanovených zákonem o ochraně osobních údajů, nicméně vynucení plnění těchto povinností by bylo prostředky sankční odpovědnosti zcela vyloučeno.

Pokud jde o druhou argumentační linii, žalobkyně se dovolává domnělého gramatického smyslu ustanovení § 45 odst. 1 zákona o ochraně osobních údajů a dovozuje, že toto ustanovení vymezuje jako deliktně odpovědné subjekty právnickou osobu podnikající podle zvláštních předpisů a fyzickou osobu podnikající podle zvláštních předpisů. Rovněž tato argumentace je ovšem neudržitelná.

V rámci veřejnoprávní odpovědnosti za protispolečenská jednání teorie rozeznává zejména trestné činy, přestupky, jiné správní delikty; v další specifikaci pak ještě správní disciplinární delikty a správní delikty pořádkové. Deliktním je jen takové porušení povinností (konání či opomenutí), které konkrétní zákon takto označuje. Rozlišovacím kritériem mezi jednotlivými druhy deliktů podle závažnosti je míra jejich typové společenské nebezpečnosti vyjádřená ve znacích skutkové podstaty, u jiných správních deliktů a disciplinárních deliktů pak ještě právě okruh subjektů, které se deliktu mohou dopustit. Obdobné vymezení deliktně způsobilých subjektů jako v ustanovení § 45 odst. 1 zákona o ochraně osobních údajů obsahuje celá řada předpisů správního práva hmotného. Přitom nikdy ani v aplikační praxi, ani v literatuře nevznikly pochybnosti o tom, že jde na jedné straně o právnické osoby bez dalšího rozlišení, na druhé straně o zvláštní skupinu fyzických osob, u nichž právě rozlišující znak podnikání podle zvláštního zákona opravňuje užití jiné než přestupkové odpovědnosti, a že právě takové vymezení je kritériem pro označení příslušného deliktu jako tzv. „jiného správního deliktu“. Jak totiž uvádí literatura (srov. zejména např. Hendrych a kol.: Správní právo, C.H.Beck Praha 2009, str. 451 a násl. a str. 477 a násl.), důvody pro tuto koncepci vymezení deliktně odpovědných subjektů jako právnických osob na jedné straně a fyzických osob podnikajících, byly jednak historické, jednak teleologické.

Již zmíněný Hendrych a kol. poukazují na to, že současná právní úprava správní odpovědnosti není založena na jednotných základech. Ze soudní trestní pravomoci se v poslední třetině 18. století vydělil postih disciplinárních deliktů. Z potřeby reagovat na porušování nebo neplnění právních povinností právnickými osobami a v reakci na malou efektivnost sankcí ukládaných pouze fyzickým osobám, které za právnickou osobu jednaly, vznikly ve 20. správní delikty právnických osob (dříve „organizací“). Subjektem deliktu se stala právnická osoba, protiprávní jednání statutárních orgánů, zaměstnanců a jiných osob,

kteř ke své činnosti použila, se přičítá právnické osobě. Dále se vedle přestupků jako správních deliktů fyzických osob od padesátých let minulého století začaly objevovat delikty fyzických osob, které nebyly označeny za přestupky (nevztahoval se tedy na ně režim přestupkového zákona), jejich postih byl upraven zvláštními zákony (často v návaznosti na výkon správního dozoru). Od roku 1990 pak přibýly (s obnovenou možností podnikání fyzických osob) správní delikty fyzických osob v postavení podnikatele, tzv. podnikajících fyzických osob. Protiprávní jednání podnikajících fyzických osob nebyla označena za přestupky, ale podmínkami odpovědnosti i vymezením skutkových podstat se odpovědnost za ně přiklonila k odpovědnosti za správní delikty právnických osob. V důsledku tohoto historického vývoje správní delikty právnických osob v jejich „čisté podobě“ se téměř nevyskytují a většina zákonů upravuje správní delikty právnických osob v kombinaci se správními delikty fyzických podnikajících osob. Teleologickým důvodem pro tuto koncepci vymezení subjektů jiných správních deliktů byla skutečnost, že po roce 1989 se fyzickým osobám otevřela cesta k provozování činností, které byly do té doby monopolem státu, resp. všemožných „organizací“. Přitom jde o činnosti kvalifikované, jejichž provádění je vázáno řadou veřejnoprávních povinností, jež fyzické podnikající osoby musí dodržovat stejně jako právnické osoby, které je vykonávají. Podnikající fyzické osoby mohou tyto kvalifikované činnosti vykonávat přitom osobně, ale též prostřednictvím svých zaměstnanců. Podnikající fyzické osobě se tedy (podobně jako u právnických osob) přičítá protiprávní jednání jejich zaměstnanců, příp. dalších osob, které za ni jednají. Tyto skutečnosti byly důvodem pro sjednocení podmínek odpovědnosti právnických osob a fyzických podnikajících osob. Většina právních předpisů vydávaných zejména od druhé poloviny 90. let tak upravuje delikty právnických osob a fyzických podnikajících osob společně (podmínky odpovědnosti, skutkové podstaty i sankce jsou stanoveny shodně, rozhodují o nich stejné správní orgány ve stejném procesním režimu). Důraz je při formulaci skutkových podstat kladen v první řadě na to, že odpovědná osoba vykonává určitou činnost, resp. má určité speciální postavení. Jednotlivým znakem těchto deliktů je tedy charakter činnosti a nikoli povaha osoby (zda jde o osobu právnickou či fyzickou), která ji vykonává.

Znak podnikání jako znak rozlišující se tedy v takto vymezených skutkových podstatách správních deliktů váže právě a pouze k fyzické osobě, neboť ji odlišuje od postavení jiných fyzických osob a připodobňuje jejich postavení k osobám právnickým.

Druhý okruh námitek žalobkyně se týkal otázky naplnění samotné skutkové podstaty správního deliktu podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů ve spojení s § 13 odst. 1 téhož zákona. Ani tyto námitky neshledal soud důvodnými.

Předně je třeba konstatovat, že žalobkyní nijak nebylo vyvráceno (ostatně ani nijak napadáno) skutkové zjištění žalovaného v rámci kontroly, a to, že v době incidentu spojeného se zneužitím fotografií obviněných osob měl každý příslušník, resp. občanský zaměstnanec, který měl přístup do VIS, přístup ke všem údajům všech evidovaných osob, a to především i osob umístěných v jiných věznicích, než byla věznice, v níž ten který pracovník působil. Dále nijak žalobkyně nebrojí proti skutkovému závěru, že v reakci (přínejmenším časově) na provedenou kontrolu žalobkyně zásadně změnila nastavení přístupových oprávnění do VIS, a to tak, že napříště žádné funkční místo ve správě vězňů jako takové neumožňuje nahlížet na vězně jiných věznic. Současně bylo všem funkčním místům ve správě vězněných osob zamezeno nahlížet na všechny vězněné osoby, resp. vyhledávat je v seznamu vězňů, bez znalosti jména, příjmení a data narození nebo kódu vězně. Pro tyto činnosti byly vytvořeny speciální role, které jsou přidělovány jednotlivě, pouze vybraným uživatelům, na základě

odůvodněné a ředitelem organizační jednotky schválené písemné žádosti, přičemž žádosti ředitelům organizačních jednotek schvaluje generální ředitel.

Podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů se právnická osoba nebo fyzická osoba podnikající podle zvláštních předpisů jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů. Ustanovení § 45 odst. 1 písm. h) zákona o ochraně osobních údajů přitom odkazuje normativním odkazem na ustanovení § 13 zákona o ochraně osobních údajů.

Ustanovení § 13 zákona o ochraně osobních údajů jako celek vymezuje komplex opatření k zajištění bezpečnosti zpracování osobních údajů. Má přitom vnitřní logickou strukturu, kterou je při jeho výkladu třeba respektovat.

Ustanovení § 13 odst. 1 zákona o ochraně osobních údajů lze označit za generální klauzuli ochrany bezpečnosti osobních údajů, která vymezuje v nejobecnější rovině cíl ochrany osobních údajů a vymezuje princip, podle něhož je správce (zpracovatel) povinen přijmout veškerá možná opatření (jež v této generální klauzuli nejsou blíže specifikována) k naplnění vymezeného cíle. Podle zmíněného ustanovení jsou totiž *„[s]právce a zpracovatel ... povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.“* V této podobě jde o obecnou implementaci obdobného ustanovení čl. 17 odst. 1 směrnice Evropského parlamentu a Rady ze dne 24. října 1995 č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, podle kterého členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování. Podle téhož ustanovení a recitálu 46 směrnice 95/46/ES platí, že tato opatření mají zajistit, s ohledem na stav techniky a náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.

Pokud jde o pojmy „neoprávněný“ nebo „nahodilý“ přístup k osobním údajům, případně „zneužití“ osobních údajů užitě v ustanovení § 13 odst. 1 zákona o ochraně osobních údajů, je třeba jimi rozumět s ohledem na systematiku zákona jakékoliv zpracování osobních údajů (k zpracování srov. definici uvedenou v § 4 písm. e) zákona o ochraně osobních údajů) s osobními údaji, které se přičítají účelu zpracování vymezenému správcem podle § 5 odst. 1 písm. a) zákona o ochraně osobních údajů. Základní podmínkou přípustného zpracování osobních údajů je právě totiž soulad tohoto zpracování s vymezeným účelem. Ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů tuto zásadu výslovně zakotvuje, pokud stanoví, že správce je povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Jedinou výjimkou z tohoto pravidla je zpracování v mezích ustanovení § 3 odst. 6 zákona o ochraně osobních údajů, nebo pokud k tomu dal subjekt údajů předem souhlas.

Shrnutě řečeno, ustanovení § 13 odst. 1 zákona o ochraně osobních údajů vymezuje cíl úpravy ve formě zamezení jakémukoliv zpracování osobních údajů mimo stanovený účel, resp. mimo limity ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, přičemž

nerozlišuje mezi zdroji rizika neoprávněného zpracování (mohou mít původ v selhání technických zařízení, působení živelních pohrom či lidském faktoru) a nedefinuje ani jednotlivé prostředky zajišťující bezpečnost osobních údajů.

Již z tohoto vymezení je zřejmé, že zásadní bod argumentace žalobkyně v podobě domnělé vnitřní rozpornosti popisu skutku, jímž měla naplnit vytýkaný správní delikt, je zcela nepřipadný. Z výše uvedeného vymezení pojmů neoprávněnosti, resp. zneužití přístupu k osobním údajům užitých v ustanovení § 13 odst. 1 zákona o ochraně osobních údajů je třeba vyvodit pro posuzovanou věc zcela zásadní závěr, který žalobkyně přehlíží, a na který žalovaný správně poukázal ve svém vyjádření k žalobě, a sice že nikoliv každý přístup k osobním údajům obecně k takovému přístupu oprávněné osoby správce či zpracovatele bude též oprávněný ve smyslu § 13 odst. 1 zákona o ochraně osobních údajů, ale oprávněným v tomto smyslu bude pouze tehdy, pokud bude též respektovat účel zpracování vymezený správcem. Pokud tedy v posuzované věci došlo k situaci, že účel zpracování osobních údajů ve VIS zjevně v inkriminovaném případě úniku fotografií vězněných osob nebyl zachován, je třeba souhlasit se závěrem žalovaného v tom, že došlo k neoprávněnému přístupu k osobním údajům, resp. obecně vzato k jejich zneužití ve smyslu § 13 odst. 1 zákona o ochraně osobních údajů. Normativní obsah ustanovení § 13 odst. 1 zákona o ochraně osobních údajů přitom ukládá správci a zpracovateli povinnost takovému zneužití zabránit.

Pokud jde o konkrétní prostředky k zabránění následku definovaného v ustanovení § 13 odst. 1 zákona o ochraně osobních údajů, na toto ustanovení přímo navazují ustanovení § 13 odst. 3 a 4 zákona o ochraně osobních údajů, jež nad rámec dalších možných opatření správci či zpracovateli osobních údajů výslovně ukládají jednak posuzovat rizika týkající se plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům, zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování, zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a opatření, která umožní určit a ověřit, komu byly osobní údaje předány (§ 13 odst. 3 zákona o ochraně osobních údajů), ale zejména pro oblast automatizovaného zpracování osobních údajů (což je i případ žalobkyní provozovaného systému VIS) ustanovení § 13 odst. 4 písm. a) zákona o ochraně osobních údajů stanoví povinnost zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby, v písm. b) pak stanoví povinnost správce nebo zpracovatele v rámci opatření podle § 13 odst. 1 zákona o ochraně osobních údajů zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby. Z výše uvedeného popisu cíle ochrany osobních údajů tedy vyplývá, že k naplnění účelu ochrany podle § 13 odst. 1 zákona o ochraně osobních údajů (ochrana před užitím osobních údajů k jinému účelu než k účelu vymezenému) zákon v ustanovení § 13 odst. 4 stanoví jasně povinnost nastavení přístupových oprávnění k systému automatizovaného zpracování osobních údajů tak, aby tato oprávnění odpovídala rozsahu, v němž ta která fyzická osoba oprávněná k přístupu k těmto systémům potřebuje příslušné osobní údaje k jejich užití v souladu s účelem vymezeným podle § 5 odst. 1 písm. a) zákona o ochraně osobních údajů.

Pokud soud vyjde z takto vymezeného normativního obsahu ustanovení § 13 odst. 1 ve spojení s ustanovením § 13 odst. 4 zákona o ochraně osobních údajů, je třeba jako zcela správný závěr hodnotit úvahu žalovaného, že pokud žalobkyně provozovala systém VIS s takovým nastavením přístupových oprávnění, že umožňoval přístup všech osob oprávněných nějakým způsobem v prostředí VIS pracovat ke všem údajům bez vztahu

k jejich konkrétní relevanci pro konkrétní pracovní úkoly těchto osob, šlo o porušení povinnosti podle ustanovení § 13 odst. 1 ve spojení s § 13 odst. 4 písm. a) a b) zákona o ochraně osobních údajů, neboť nebyla respektována zásada, aby přístupová oprávnění v systému automatizovaného zpracování osobních údajů v maximální míře odstraňovala riziko neoprávněného (tedy v rozporu s účelem zpracování informací) užití osobních údajů. Že takto široce nastavená přístupová oprávnění nebyla pro výkon činnosti žalované nezbytná, jak žalovaná v žalobě poukazuje, prokazuje zcela jasně sama skutečnost, že žalovaná tato oprávnění výrazně restriktivním způsobem v návaznosti na kontrolu žalovaného upravila. V tomto ohledu jde o skutečnost zcela klíčovou, nikoliv irelevantní, jak tvrdí žalobkyně.

Závěr žalovaného formulovaný ve skutkové větě rozhodnutí o pokutě, tedy že porušení povinnosti stanovené v § 13 odst. 1 zákona o ochraně osobních údajů lze spatřovat v tom, že ve vězeňském informačním systému měli přístup ke všem údajům vedeným v tomto systému všichni zaměstnanci oprávnění v něm pracovat, je tedy správný. Přitom není vůbec rozhodný počet k přístupu oprávněných osob – správní orgán prvního stupně ostatně onu cifru 5000 osob uvedl v závorce jako ilustrativní údaj. Z hlediska naplnění skutkové podstaty správního deliktu kladeného žalobkyni k tíži je zcela nerozhodné, zda přístup do příslušného systému má 5, 10, 100 nebo 1000 osob. Nejde tu o hledisko kvantitativní, ale o hledisko kvalitativní – žalobkyni není vytýkána skutečnost, že měl do systému přístup nadměrný počet osob, ale skutečnost, že přístupová oprávnění těchto osob byla nastavena způsobem, který nerespektoval jejich skutečnou potřebu osobních údajů k plnění pracovních (služebních) úkolů.

Za této situace shledává soud rovněž zcela správným závěr žalovaného o tom, že v případě žalobkyně nebylo možné aplikovat liberační důvod podle § 46 odst. 1 zákona o ochraně osobních údajů. Podle tohoto ustanovení platí, že právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Jestliže ze skutkových zjištění vyplývá, že jednotlivá přístupová oprávnění osob oprávněných vstupovat do systému VIS bylo lze nastavit mnohem cíleněji a restriktivněji, než byla původní praxe žalobkyně, již tato okolnost evidentně závěr o tom, že žalobkyně vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila, vylučuje. Liberačním důvodem nemůže být ani poukaz žalobkyně na to, že přijala vnitřní předpisy upravující pravidla nakládání s údaji evidovanými ve VIS a že inkriminované zneužití těchto údajů bylo porušením těchto vnitřních předpisů. Vydání takového vnitřního předpisu bylo pouze naplněním povinnosti žalobkyně podle § 13 odst. 2 zákona o ochraně osobních údajů, podle něhož je správce nebo zpracovatel povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy. Pokrušení této povinnosti však žalobkyni nebylo kladeno k tíži. Správní delikt žalobkyně totiž nespočívá v tom, že by její příslušníci popř. zaměstnanci porušili přijatá opatření k zajištění bezpečnosti zpracovávaných osobních údajů, ale že tato opatření byla z hlediska zákonného požadavku vyjádřeného v ustanovení § 13 odst. 4 písm. b) zákona o ochraně osobních údajů nedostatečná. Zcela prostě řečeno – zprostit odpovědnosti za nedůsledné nastavení přístupových oprávnění do systému automatizovaného zpracování osobních údajů se nelze poukazem na to, že bylo osobám majícím takové objektivně nepřiměřené přístupové oprávnění vnitřním předpisem zakázáno osobní údaje zneužít.

Za těchto okolností tedy soud dospěl k závěru, že žaloba nebyla podána důvodně, a proto ji podle ustanovení § 78 odst. 7 s. ř. s. zamítl.

O nákladech řízení soud rozhodl podle ustanovení § 60 odst. 1 s. ř. s. – žalobkyně ve věci nebyla úspěšná, nadto jí ani žádné náklady řízení nevznikly, úspěšnému žalovanému pak rovněž žádné náklady řízení nad rámec běžné úřední činnosti nevznikly, proto soud vyslovil, že žádný z účastníků nemá právo na náhradu nákladů řízení.

P o u ě n í : Proti tomuto rozhodnutí lze podat kasační stížnost ve lhůtě dvou týdnů ode dne jeho doručení.

Kasační stížnost se podává ve dvou (více) vyhotoveních u Nejvyššího správního soudu, se sídlem Moravské náměstí 6, Brno. O kasační stížnosti rozhoduje Nejvyšší správní soud. Lhůta pro podání kasační stížnosti končí uplynutím dne, který se svým označením shoduje se dnem, který určil počátek lhůty (den doručení rozhodnutí). Připadne-li poslední den lhůty na sobotu, neděli nebo svátek, je posledním dnem lhůty nejblíže následující pracovní den. Zmeškání lhůty k podání kasační stížnosti nelze prominout.

Kasační stížnost lze podat pouze z důvodů uvedených v § 103 odst. 1 s. ř. s. a kromě obecných náležitostí podání musí obsahovat označení rozhodnutí, proti němuž směřuje, v jakém rozsahu a z jakých důvodů jej stěžovatel napadá, a údaj o tom, kdy mu bylo rozhodnutí doručeno.

V řízení o kasační stížnosti musí být stěžovatel zastoupen advokátem; to neplatí, má-li stěžovatel, jeho zaměstnanec nebo člen, který za něj jedná nebo jej zastupuje, vysokoškolské právnické vzdělání, které je podle zvláštních zákonů vyžadováno pro výkon advokacie.

Soudní poplatek za kasační stížnost vybírá Nejvyšší správní soud. Variabilní symbol pro zaplacení soudního poplatku na účet Nejvyššího správního soudu lze získat na jeho internetových stránkách: www.nssoud.cz.

V Praze dne 5. srpna 2016

JUDr. Ing. Viera Horčicová,
předsedkyně senátu