



OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 4/2023, ročník III.

Měsíčník SMS - služby s. r. o.

www.dpopro.cz

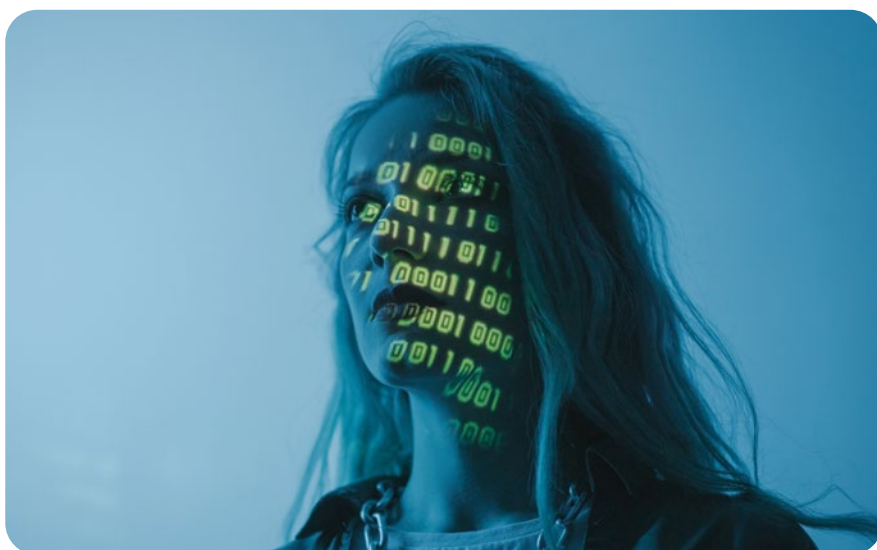
Ochranu osobních údajů vnímám jako jednu z částí, které tvoří celkovou bezpečnost v organizaci

Rozhovor

Jak zvládl Úřad pro ochranu osobních údajů přechod na novou právní úpravu v roce 2018? Jaké to je ocitnout se na „druhé straně barikády“ a přejít z práce na dozorovém úřadu k práci pověřence pro ochranu osobních údajů? Jak souvisí ochrana osobních údajů a bezpečnost obecně? Také nad těmito otázkami se v rozhovoru zamýšlí Vojtěch Dlouhý, který se ochranou osobních údajů v nejrůznějších aspektech zabývá již mnoho let.

Pracoval jste na Úřadu pro ochranu osobních údajů v době, kdy obecné nařízení (GDPR) nabylo účinnosti. Šlo nepochybně o velkou změnu na dozorovém úřadu, a to nejen pro správce a zpracovatele, ale i pro zaměstnance. Jak na to vzpomínáte?

Vybavuji si, že z mého pohledu, coby řadového zaměstnance, bylo nejdůležitější především správně uchopit veškeré procesní náležitosti, které byly spojeny s tím, že sice obecné nařízení nabylo účinnosti, ale chyběla doprovodná národní úprava. Po hmotně-právní stránce si nemyslím, že bychom v oblasti ochrany osobních údajů zažili s nabytím účinnosti obecného nařízení revoluci, nicméně řada lidí a společností vnímala jeho příchod jako velkou hrozbu. Tady vidím jisté za-



Vážení čtenáři,

nejen pověřencům pro ochranu osobních údajů je určeno dubnové číslo časopisu DPO PRO.

Letos si připomínáme pět let od zavedení GDPR a i v návaznosti na toto výročí vzpomínáme na začátky obecného nařízení hned v úvodním rozhovoru s Vojtěchem Dlouhým, jenž se ochraně osobních údajů věnuje již řadu let, a to v různých pozicích. Zeptala jsem se ho třeba na to, jak v roce 2018 zvládl Úřad pro ochranu osobních údajů, na němž tehdy pracoval, přechod na novou právní úpravu či jaké to je ocitnout se na „druhé straně barikády“ a přejít z práce na dozorovém úřadu k práci pověřence pro ochranu osobních údajů.

Ve zpravodaji ani tentokrát nechybí aktuální informace o činnosti Spolku pro ochranu osobních údajů, který v květnu udělí ocenění Pověřenec roku 2022.

Lhůta stanovená zákonem vyvolává očekávání, že údaje budou po jejím uplynutí vymazány, uvedl generální advokát Soudního dvora EU, který se zabýval zpracováním osobních údajů z veřejných rejstříků.

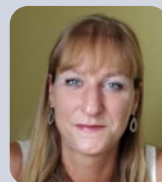
V jaké míře ztrácíme ve svém profesním životě kontrolu nad svojí podobou a souvisejícími osobnostními projevy (jejich zachycením a šířením)? Mohou lidé nahrávat zaměstnance úřadů a jsou úředníci povinni nahrávání strpět? Otázkami se s pomocí stanovisek soudů a veřejného ochránce práv zabývala Veronika Gabrišová.

Ačkoli mají bankovní tajemství a ochrana osobních údajů principiálně jeden hlavní společný cíl – tedy regulace nakládání a zajištění ochrany (zabezpečení) určité legislativou definované sady údajů, v mnoha aspektech se tyto instituty podstatně liší. Nad hlavními odlišnostmi se ve svém článku zamýšlela Sylvie Milerová.

Ptáte se, zda je to vše? Kdepak. Časopis obsahuje i další informace a inspirativní podněty pro vaši práci.

Ničím nerušené čtení a krásné jaro vám přeje

Eva Janečková, šéfredaktorka DPO PRO



váhání na straně dozorového orgánu, protože o příchodu této právní normy nekomunikoval dostatečně.

Co podle vás mělo být jinak?

Kdyby Úřad zařadil v komunikaci alespoň dvojku rychlost, mohl nejen lépe vysvětlit důsledky obecného nařízení, ale měl by také jedinečnou příležitost vysvětlit široké veřejnosti, proč je pro naši společnost přínosem a proč je důležité nastavit zpracování osobních údajů mantinely a hlídat, aby nedocházelo k jejich překračování. V neposlední řadě mohl Úřad zvýšenou komunikací minimalizovat spanilé jízdy různých „odborníků“, kteří za ceny příliš připomínající drahotu „školili“ o obecném nařízení ve firmách, přičemž přínos těchto školení byl v některých případech přinejmenším diskutabilní. Tento bobřík mlčení, který si Úřad naordinoval, vedl k enormnímu nárůstu počtu dotazů, které nebylo možné ignorovat. Úřad následně reagoval zavedením telefonní linky pro dotazy spjaté s obecným nařízením, a pokud si vzpomínám dobře, měla tato horká linka úspěch.

A význam této komunikace, předpokládám, zůstává i nadále...

Důležitost ochrany osobních údajů, o níž Úřad mohl a stále může komunikovat, lze spojit také se vzrůstajícím počtem kybernetických útoků a útoků prostřednictvím telefonních hovorů (fingované hovory z bank apod.), protože i zde dochází k využití osobních údajů – elektronické pošty, telefonního čísla. Novinových článků na toto téma vychází v poslední době celá řada, útoky jsou totiž stále sofistikovanější. Na druhou stranu je třeba férově přiznat, že část odpovědnosti leží na každém z nás. Ve velké míře je na nás samotných, kde všude zanecháváme své osobní údaje a digitální stopu. Výměna osobních údajů za slevové karty a informace sdílené na sociálních sítích a na internetu jako takovém jsou zlatým dolem.

Co by tedy bylo ideálním řešením?

Osobní údaje by dle mého názoru neměly být „posvátnou krávou“, ale musíme umět nastavit takové hranice, ať již legislativní, nebo naše vnitřní, aby nám osobní údaje a informace jednak sloužily, ale aby zároveň byly minimalizovány riziko jejich zneužití. Nemusíme chodit daleko do historie, abychom se podívali, jak zveřejňované osobní údaje dokáží vytvořit profil člověka, který může sloužit např. v politickém boji, jako se tomu stalo v případě Cambridge Analytiky.

Když si to shrneme, bylo nabytí účinnosti obecného nařízení zásadním zlomem?

Domnívám se, že nebylo. Bylo výsledkem vývoje odvětví ochrany osobních údajů a zároveň s sebou přineslo do té doby neopakovatelnou možnost komunikovat s širokou veřejností o přínosech této právní úpravy v každodenním životě každého člověka. Tento potenciál však nebyl zcela využit, Úřad se zakuklil a motýl se z něj bohužel nestal. Nicméně, jak jsem již uvedl, zásadní je rovněž chování každého z nás.

Vedl jste Inspektorát IV, který se zabýval nevyžádanými obchodními sděleními. V této oblasti došlo k legislativní změně, která byla tématem mnoha článků a školení. Odrazila se ale nějak i v praxi? Je skutečně zohledňována při marketingových kampaních firem?

V době, kdy jsem Inspektorát 4 vedl, jsme se zabývali čistě ochranou osobních údajů ve světle obecného nařízení a oblast nevyžádaných obchodních sdělení byla přidělena specializovanému oddělení.

Myslím, že doba „kobercového bombardování“ nejrůznějšími nabídkami už pomínula, a je to dle mého důsledek několika faktorů.

Můžete to blíže specifikovat?

V první řadě si troufnu tvrdit, že na poli nevyžádaných obchodních sdělení odvedl Úřad a oddělení nevyžádaných obchodních sdělení opravdu dobrou práci, k čemuž dle mého pomohl i koncept odpovědnosti šířitele obchodního sdělení, který Úřad začal razit a který v roce 2020 prošel rovněž testem u Městského soudu v Praze pod č. j. 14 A 242/2018. Zjednodušeně lze říci, že Úřad výkladem zákona dospěl k závěru, a Městský soud v Praze tento závěr potvrdil, že odpovědný je nejen ten, kdo „stiskne“ tlačítko odeslat, ale rovněž ten, kdo si takovou rozesílku objedná, a objednatel se tedy nemůže „schovávat“ za nějakou skořápkovou firmu, za firmu ze zahraničí nebo ze třetí země.

Druhým faktorem jsou nemalé pokuty, které se Úřad za nezákonné zasílání obchodních sdělení nebojí ukládat.

Třetím faktorem je proměna reklamy v online prostoru. Z dříve zasílaného velkého množství letáků na všechny adresy je dnes reklama více personalizovaná a zaměřující se na skutečného koncového adresáta a jeho



Vojtěch Dlouhý

vystudoval Právnickou fakultu Univerzity Karlovy, už během studií začal pracovat na ÚOOÚ a zabýval se nevyžádanými obchodními sděleními, po skončení studií řídil na ÚOOÚ Inspektorát IV a vedl kontroly v oblasti ochrany osobních údajů. Poté pracoval jako pověřenec pro ochranu osobních údajů na Ministerstvu financí a později poskytoval služby jako externí pověřenec pro ochranu osobních údajů v soukromém sektoru v poradenské firmě zabývající se zabezpečením. V současné době je manažerem bezpečnosti a zabývá se ochranou informací, osobních údajů a fyzickou bezpečností.

potřeby. Tato skutečnost je dána cílením reklamy na sociálních sítích, což se děje za pomoci algoritmů, které vědí, v jakém okamžiku nám ukázat tu správnou nabídku. Je třeba mít na paměti, že i toto je důsledkem sběru a analýzy osobních údajů.

Máte také zkušenosti jako pověřenec pro ochranu osobních údajů. Jaké to bylo ocitnout se „na druhé straně“?

S trochou nadsázky lze říci, že to byla skutečně druhá strana barikády. Ne, že bych začal dozorový orgán vnímat jako nepřitele, proti kterému je třeba bojovat, ale měl jsem možnost srovnat svou tehdejší situaci v roli pověřence s požadavky, které jsme na organizace kladli z pozice dozorového orgánu. Každému bych tuto zkušenost doporučil. V pozici dozorového orgánu bylo snadné dostat na stůl případ, vyžádat si materiály a z tepla a klidu kanceláře společně s kontrolním týmem rozhodnout, zda je zpracování v pořádku či nikoli. Pověřenec obvykle zůstává dost osamocen se svojí snahou o zajištění kvalitního zpracování

Další obsah

Duben byl ve znamení přednášek, v květnu již popáté oceníme nejlepšího pověřence roku!

str. 4

Lhůta stanovená zákonem vyvolává očekávání, že údaje po jejím uplynutí zmizí

str. 5

Nahrávání úředních osob? Co na sebe nechcete prozradit, nikomu nesdělujte

str. 8

Bankovní tajemství a ochrana osobních údajů – jsou si tyto instituty skutečně tak blízké, jak se může na první pohled zdát?

str. 12

Francouzský dozorový úřad udělil vysokou pokutu kvůli cookies

str. 13

osobních údajů, a pokud mu nejvyšší vedení neposkytne dostatečnou podporu, vykonává často vyložené sisyfovskou práci.

Vykonával jste pozici interního i externího pověřence. Je v tom nějaký rozdíl?

Dle mého názoru je rozdíl ve výkonu těchto funkcí diametrální. Významným aspektem výkonu funkce pověřence je pochopení kontextu a vnitřního nastavení organizace, kde pověřenec působí. Není třeba si nalhávat, že by všichni tíhli láskou k ochraně osobních údajů. Z mé zkušenosti se oblast ochrany osobních údajů často setkávala, a bohužel ještě stále setkává, s nepochopením a označením jako „taková zbytečnost“ (v lepším případě). Domnívám se, že prvotním úkolem pověřence v organizaci, ve které působí, je zvýšit povědomí o tom, proč je důležité zpracovávat osobní údaje zákonným způsobem a že vhodné nastavená pravidla jsou spíše ku pomoci než k „otravování“ ostatních zaměstnanců. Stále je to však dle mého názoru spíše běh na dlouhou trať, který s sebou nese nutnost obrnit se a trpělivě a pravidelně vysvětlovat důležitost tohoto odvětví, a tak si postupně vytvořit pozici, která se stane vítaným pomocníkem při plnění každodenních agend. Ne všude to jde rychle, ne všude se to zdáří. Proměnných, které v tom hrají roli, je celá řada, od složitých vnitřních procesů po podporu nejvyššího managementu, kterou vnímám jako stěžejní.

V současné době se věnujete bezpečnostnímu poradenství. Je to zásadní posun od ochrany osobních údajů nebo spolu tyto dvě oblasti souzní?

Ochranu osobních údajů vnímám jako jednu z částí, které tvoří celkovou bezpečnost v organizaci. Ochrana osobních údajů a bezpečnostní poradenství mají jedno společné, a tím je přístup založený na poznání rizika, vyhodnocení jeho závažnosti a přijetí dostatečně účinných opatření ke zmírnění rizika, případně jeho akceptování. Z tohoto pohledu to te-

dy zásadní posun není. V oblasti bezpečnostního poradenství však pro mě bylo nemilým zjištěním, že, zjednodušeně řečeno, „kamery vyřeší vše“ a posouzení k nim je „administrativní blbost“. Z mé zkušenosti bylo pro většinu klientů podstatnější zajistit ochranu majetku stůj co stůj a navržená opatření, které sledovala rovněž soulad s obecným nařízením, byla přecházena taktickým mlčením (čest výjimkám!). Bezpečnost nelze dle mého rozdělit na jednotlivé části (fyzická, kybernetická atd.) a každé z těchto částí se věnovat samostatně, ale je třeba k ní přistupovat jako k celku právě proto, že mnoho procesů je propojených. Pokud se zamýšlím nad zavedením přístupových karet do budovy a kanceláří jako nad prvkem fyzické bezpečnosti, musím si zároveň uvědomit, že každá taková karta je odrazem konkrétní fyzické osoby a sděluje mi o ní celou řadu informací, které mohou dále rozklíčovat. Např. zda daná osoba dochází do práce ve stále stejnou hodinu, zda pravidelně během pracovní doby odchází (pak to může být kuřák) atd. V takovém případě se mi však fyzická bezpečnost propojuje s ochranou osobních údajů a musím si začít klást i otázky týkající se právního titulu zpracování, případně též zapojení zpracovatele (jsou docházková data ukládána v mém systému, nebo ne?).

Lze dostatečně zajistit bezpečnost i v malých organizacích v širším významu toho slova? S čím takové organizace bojují? Čeho lze dosáhnout např. u obcí, kde funguje sám starosta a úřaduje téměř z domova?

Jsem toho názoru, že pro malou společnost, stejně jako pro malou obec, je největším nepřitelem průměra regulace. Jak má malá firma nebo obec stíhat reagovat na množství právních předpisů, které se na nás jako na společnost valí, když povinnosti z nich vyplývající často nezvládá implementovat ani stát.

Mám dojem, že důležitost ochrany osobních údajů u nás nezapustila dostatečně kořeny. Proto není společností jako celkem přijímána (jak často nás otravují vyskakující

cookies lišty a souhlasy se zpracováním osobních údajů). To se odráží rovněž v přístupu správců osobních údajů, a to v kombinaci s výše uvedenou průměrnou regulací, kdy bych správce nepodezíral ani tak ze zlého úmyslu, jako spíše z prostého opomenutí jedné z tisíců povinností. Jak pak můžeme po neuvolněném starostovi malé obce požadovat byt' jen znalost obecného nařízení, když potřebuje opravit obecní kanalizaci, a navíc, řečeno slovy klasika, „tady se stejně všechno rozkecá“.

Domnívám se, že pro celou řadu společností nebo obcí může být toto problém, protože nemají lidské kapacity.

Co by tento problém mohlo vyřešit?

Řešením může být spolupráce s externistou, kdy si dovedu představit, že např. u malé výrobní firmy půjde o prvotní nastavení, které by mohlo být náročnější, a následné ověřování stavu a poskytování konzultací, což s sebou ale nese určité finanční náklady. Otázka nákladů může být zejména pro malé obce s ohledem na jejich rozpočet klíčová. A pokud starosta řeší dilema, zda opravit kanalizaci, aby v obci, „netekla špína po ulici“, nebo investovat do ochrany osobních údajů, která vlastně ani není vidět a obecně nemusí lidi tolik zajímat, je asi zjevné, pro co se rozhodne. Příznávám, že bych se rozhodoval stejně.

Oblast ochrany osobních údajů se neustále posouvá a prolíná s dalšími obory, jako je například kybernetická bezpečnost. Jak vidíte budoucnost osobních údajů?

Ačkoli jsem zde již uvedl, že ochrana osobních údajů u nás dostatečně nezapustila kořeny, jsem přesvědčen, že v právním řádu je již zakotvena bezpečně a bude se nadále vyvíjet. Její důležitost roste a poroste s tím, jak se celá řada agend přesouvá do automatizovaného zpracování v systémech a jak se jako stát pokoušíme o digitalizaci agend. A ruku v ruce s ochranou osobních údajů půjde kybernetická bezpečnost a další prvky bezpečnosti, čímž se zvolna dostávám k tomu, na co jsem již odpovídal – bezpečnost je třeba vnímat jako celek, ne jako dílčí části, a jako celek je třeba ji nastavovat.

Osobně ale ve veřejném prostoru postrádám větší důraz na ochranu osobních údajů, což je vidět i na některých legislativních návrzích, které, ač by měly, tak neobsahují posouzení vlivu na ochranu osobních údajů. Tento nešvar ostatně nedávno připomněl i Úřad, když vyhlásil veřejnou konzultaci k metodice posouzení vlivu na ochranu osobních údajů v návrzích právních předpisů.

Zvýšit povědomí o důležitosti ochrany osobních údajů je dle mého úkolem především Úřadu, ale pozadu by neměl zůstat ani Senát, který projednává výroční zprávy Úřadu, a rovněž odborná veřejnost.

Děkuji za rozhovor!

Eva Janečková



Duben byl ve znamení přednášek, v květnu již popáté oceníme nejlepšího pověřence roku!

Přednášky a workshopy pro své členy pořádal Spolek pro ochranu osobních údajů také v dubnu. Jaké byly a co se připravuje na květen?

Přednášky a semináře

V úterý 11. dubna pokračovala dalším dílem série workshopů s experty z Národního úřadu pro informační a kybernetickou bezpečnost. Luboš Příkrýl z oddělení strategických informací a analýz připravil přednášku na téma „Bezpečnost mobilních 5G sítí a budoucnost 6G sítí“.

V pondělí 17. dubna se konala přednáška s názvem „Hromadné zveřejňování rozsudků a jejich pseudonymizace“. O tématu hovořil Lukáš Králík, který je předním odborníkem na tuto problematiku.

Členové Spolku budou přednášet na mezinárodních akcích

Spolek je zakládajícím členem Evropské federace pověřenců pro ochranu osobních údajů. Ta sdružuje profesní asociace expertů na ochranu soukromí z více než deseti evropských, ale i mimoevropských států. Jejím prostřednictvím se Spolek více zapojuje do mezinárodní diskuse aktuálních témat zpracování osobních údajů.

Evropská federace uspořádá ve dnech 9. a 10. května evropský kongres v Berlíně, na kterém se bude mj. diskutovat o legislativních novinkách s dopadem na regulaci zpracování osobních dat. Spolek zastoupí Michal Nulíček, který v Berlíně vystoupí s příspěvkem na téma Data Act.

Na již 16. ročníku konference Computers, Privacy and Data Protection, která se uskuteční ve dnech 24. až 26. května v Bruselu, bude Spolek reprezentovat člen Výboru Spolku František Nonnemann. Vystoupí v rámci panelu s názvem „Nová evropská digitální legis-



Pověřenec roku – ilustrační foto z roku 2019

lativa a její vliv na roli dozorových úřadů a pověřenců pro ochranu osobních údajů.“

Veřejná konzultace Úřadu pro ochranu osobních údajů

Český dozorový úřad, Úřad pro ochranu osobních údajů, připravil návrh metodiky, jak v legislativním procesu posuzovat vliv a dopad nové legislativy na ochranu osobních údajů. Spolek byl osloven se žádostí o vyjádření, které také, po interní diskusi, úřadu zaslal. Spolek zejména ocenil, že dokument byl předložen k veřejné konzultaci, vyjádřil souhlas s jeho hlavními přístupy a procesy a zdůraznil několik bodů, ve kterých by metodika mohla v praxi pomoci i správcům a zpracovatelům osobních údajů. Jedná se především o detailní zpracování a dokumentování posouzení vlivu na ochranu osobních údajů zejména u těch případů, kdy je zvláštním předpisem zakládána povinnost osobní údaje zpracovávat a správcí v souladu s českým zákonem o zpracování

osobních údajů vlastní posouzení vlivu na ochranu osobních údajů provádět nemusí.

Kdo získá ocenění Pověřence roku 2022, se dozvíme 25. května v Praze

V březnu jsme ukončili přijímání nominací na Pověřence pro ochranu osobních údajů roku 2022. V pátém ročníku jsme obdrželi na tři desítky nominací pověřenců, kteří nejenže kvalitně vykonávají svoji činnost a u správců či zpracovatelů ve veřejném i soukromém sektoru monitorují soulad s požadavky obecného nařízení, dále správcům, zpracovatelům i subjektům údajů pomáhají s realizací jejich zájmů a práv, ale také mají přesah do dalších oblastí, dělí se o své zkušenosti atd.

V dubnu se nad nominacemi sejde odborná porota. Ta vybere pověřence, kteří si za svoji činnost zaslouží veřejné ocenění. Ocenění budeme předávat ve čtvrtek 25. května v Praze. Více informací naleznete na www.dporoku.cz.

SMS ČR Vzdělávání > www.smscr.education/



Datum a čas		Téma / Přednášející
3. 5.	14:00 – 15:00	Vymáhání dlužného školného a stravného JUDr. Mgr. Eva Janečková
4. 5.	13:00 – 15:00	Aplikační výzvy zákona o svobodném přístupu k informacím po jeho aktuální novelizaci / Ing. Mgr. Oldřich Kužílek
11. 5.	13:00 – 15:00	Školní výlet versus právo JUDr. Mgr. Eva Janečková
23. 5.	13:00 – 14:00	Směrnice NIS 2 o kyberbezpečnosti: Co od roku 2024 přinese obcím a školám? / Václav Řehoř
25. 5.	13:00 – 15:00	Veřejné zakázky a jejich novelizace Eliška Huk Kloučková
29. 5.	14:00 – 15:00	Na slovíčko o paragrafech ve školství JUDr. Mgr. Eva Janečková



Lhůta stanovená zákonem vyvolává očekávání, že údaje po jejím uplynutí zmizí

Generální advokát přednesl letos 16. března stanovisko, které se týkalo zpracování osobních údajů z veřejných rejstříků soukromou společností. „Skutečnost, že zákon stanoví pevnou dobu pro uchovávání údajů ve veřejných rejstřících, pravděpodobně vyvolává důvodné očekávání, že dotyčné údaje budou po uplynutí této doby vymazány,“ uvedl v tomto stanovisku.

Skutkový základ sporů, původní řízení a předběžné otázky

V rámci insolvenčního řízení bylo společností UF a AB soudními rozhodnutími povoleno předčasné osvobození od splacení zbytku dluhu (oddlužení). V souladu s § 9 odst. 1 insolvenčního řádu a § 3 odst. 1 a 2 InsBekV byla tato okolnost oficiálně zveřejněna na internetu a po uplynutí šesti měsíců odstraněna. [14]

Společnost SCHUFA, která je soukromou informační agenturou, eviduje zveřejněné informace o předčasném oddlužení ve svých vlastních databázích, ale jejich výmaz provádí až po třech letech od provedení záznamu. [15]

Na žádost společností UF a AB o výmaz záznamů, které se jich týkaly, jim společnost SCHUFA sdělila, že její činnost je v souladu s GDPR a že se na ni nevztahuje šestiměsíční lhůta pro výmaz stanovená v čl. 3 odst. 1 InsBekV. Společnosti UF a AB poté podaly stížnost u HBDI jako příslušného dozоровého úřadu. [16]

HBDI o těchto nárocích rozhodl ve dvou stanoviscích vydaných dne 1. března 2021 a dne 9. července 2021. Podle něj je společnost SCHUFA oprávněna uchovávat negativní záznamy o oddlužení nad řádné období osvobození od pohledávky. [17]

Společnosti UF a AB podaly proti stanovisku HBDI žalobu k Verwaltungsgericht Wiesbaden (Správní soud ve Wiesbadenu), který je předkládajícím soudem. Tvrdí, že HBDI je povinen v rámci svých úkolů a pravomocí přijmout opatření vůči společnosti SCHUFA, aby jí uložil výmaz záznamů, které se jich týkají. [18]

Předkládající soud pokládá otázku týkající se zákonnosti uchovávání údajů z veřejných rejstříků u obchodních informačních agentur. V této souvislosti soud uvádí, že tyto agentury získávají veškeré záznamy z veřejných rejstříků, tj. z rejstříku dlužníků a insolvenčního rejstříku, od státu. Tyto údaje podle HBDI slouží k posouzení úvěruschopnosti a smí být uloženy tak dlouho, dokud je to nezbytné pro účely, pro které byly uloženy. Kromě toho byly z důvodu neexistence příslušné právní úpravy vnitrostátního zákonodárce přijaty dozоровými úřady po konzultaci se sdružením obchodních informačních agentur kodexy chování, které stanoví výmaz přesně tři roky po vložení informací. [21]

Podle předkládajícího soudu vyvstává s ohledem na články 7 a 8 Listiny v této souvislosti otázka, zda mohou být záznamy z veřejných rejstříků v plném rozsahu přebírány do seznamů vedených soukromými subjekty, aniž existuje konkrétní důvod pro uložení těchto údajů. V konečném důsledku by se jednalo o hromadění údajů, zejména pokud



již byly údaje z vnitrostátního rejstříku vymazány z důvodu uplynutí doby uchovávání. Kromě toho je společnost SCHUFA pouze jednou z obchodních informačních agentur, takže by údaje byly v Německu uchovávány vícenásobně. [22]

Za těchto podmínek se Verwaltungsgericht Wiesbaden (správní soud ve Wiesbadenu) rozhodl přerušit řízení a položit Soudnímu dvoru následující předběžné otázky:

„1) Musí být čl. 77 odst. 1 ve spojení s čl. 78 odst. 1 GDPR chápán v tom smyslu, že závěr dozоровého úřadu, který sdělí subjektu údajů,

a) má povahu rozhodnutí o petici? Omezuje se v důsledku toho soudní přezkum rozhodnutí dozоровého úřadu o stížnosti podle čl. 78 odst. 1 GDPR zásadně na otázku, zda se tento úřad stížností zabýval, předmět stížnosti dostatečně přezkoumal a zda stěžovatele vyrozuměl o výsledku přezkumu?

nebo

b) je nutno jej považovat za úřední rozhodnutí ve věci? Musí v důsledku toho soud přezkoumat rozhodnutí dozоровého úřadu o stížnosti podle čl. 78 odst. 1 GDPR z obsahového hlediska v plném rozsahu, přičemž v konkrétním případě, kdy např. úřad nemá žádný prostor pro uvážení, může soud uložit dozоровému úřadu rovněž povinnost přijmout konkrétní opatření ve smyslu článku 58 GDPR?

2) Je s články 7 a 8 [Listiny] slučitelné uchovávání údajů u soukromé obchodní informační agentury, která uchovává osobní údaje z veřejného rejstříku, jako jsou například „vnitrostátní databáze“ ve smyslu čl. 79 odst. 4 a 5 [nařízení 2015/848], bez konkrétního podnětu, aby mohla na vyžádání poskytnout informace?

3) a) Jsou v zásadě přípustné paralelní soukromé databáze (zejména databáze obchodní informační agentury), které jsou vytvářeny mimo státní databáze a v nichž jsou údaje ze státních databází (v projed-

návané věci oznámení o insolvencích) uloženy po delší dobu, než jak je upraveno v úzkém rámci nařízení (EU) 2015/848 ve spojení s vnitrostátním právem?

b) V případě kladné odpovědi na třetí otázku písm. a), vyplývá z práva být zapomenut podle čl. 17 odst. 1 písm. d) GDPR, že tyto údaje musí být vymazány po uplynutí doby zpracování stanovené pro veřejný rejstřík?

4) Přichází-li čl. 6 odst. 1 první pododstavec písm. f) GDPR do úvahy jako jediný právní základ pro uchovávání údajů u soukromých obchodních informačních agentur, a to i ohledně údajů uložených ve veřejných rejstřících, jedná se o oprávněný zájem takové agentury již tehdy, když tento subjekt přebírá údaje z veřejného rejstříku bez konkrétního podnětu, aby pak tyto údaje měl k dispozici pro případ vyžádání?

5) Mohou kodexy chování, které byly podle článku 40 GDPR schváleny dozоровými úřady a které stanoví lhůty pro kontrolu a výmaz, jež jsou delší než doby uložení ve veřejných rejstřících, nahradit vyvažování podle čl. 6 odst. 1 prvního pododstavce písm. f) GDPR?“ [26]

K souladu praxe obchodních informačních agentur se zásadami zpracování osobních údajů zakotvenými v GDPR

Ustanovení čl. 5 odst. 1 písm. a) GDPR vyžaduje, aby osobní údaje ve vztahu k subjektu údajů byly zpracovávány korektně a zákonným a transparentním způsobem. Podle čl. 6 odst. 1 GDPR je zpracování osobních údajů zákonné pouze tehdy, pokud je splněna podmínka jednoho z důvodů uvedených v tomto ustanovení. Jak rozhodl Soudní dvůr, jedná se o taxativní a omezující výčet případů, v nichž lze zpracování osobních údajů považovat za zákonné. [59]

Podle judikatury Soudního dvora stanoví čl. 6 odst. 1 první pododstavec písm. f) GDPR



tři kumulativní podmínky pro to, aby bylo zpracování osobních údajů zákonné, a to za prvé sledování oprávněného zájmu správce nebo třetí strany, jimž jsou údaje sdělovány, zadruhé nezbytnost zpracování osobních údajů pro uskutečnění sledovaného oprávněného zájmu a zatřetí podmínku, že před tímto zájmem nemají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů. [60]

1) Existence „oprávněného zájmu“

Domnívám se, že v zásadě neexistuje žádný objektivní důvod pochybovat o oprávněnosti zájmu společnosti SCHUFA poskytovat svým klientům výše popsanou komerční službu ani o zájmu zákazníků společnosti SCHUFA využívat její služby k posouzení úvěruschopnosti potenciálních obchodních partnerů v uvedeném smyslu. Ačkoli je pravda, že poskytování těchto služeb je zaměřeno na získání odměny, a představuje tedy obchodní model soukromé společnosti, nestačí tato okolnost sama o sobě k tomu, aby bylo možné zpochybnit, že je v projednávané věci splněna první podmínka stanovená v čl. 6 odst. 1 prvním pododstavci písm. f) GDPR. [63]

2) „Nezbytnost“ zpracování údajů pro dosažení oprávněného zájmu

Co se týče podmínky nezbytnosti zpracování osobních údajů pro uskutečnění sledovaného oprávněného zájmu, výjimky ze zásady ochrany osobních údajů a její omezení musí být činitelné v mezích toho, co je naprosto nezbytné. Proto je třeba, aby existovala úzká vazba mezi zpracováním a sledovaným zájmem, pokud neexistují alternativy, které by více respektovaly ochranu osobních údajů, protože nestačí, že zpracování závisí na prosté užitečnosti pro správce údajů. [65]

Společnost SCHUFA považuje zpracování

údajů za nezbytné. Podle jejího názoru, pokud by obchodní informační agentura čekala na konkrétní žádost a teprve poté začala shromažďovat údaje, nebylo by možné poskytnout informace včas. Společnost SCHUFA je toho názoru, že skutečnost, že údaje jsou (také) po určitou dobu veřejně přístupné, nemá vliv na oprávněné zájmy obchodních informačních agentur ani na nezbytnost zpracování. [66]

3) Poměrování různých zájmů

Pokud jde konečně o poměrování zájmů správce údajů na jedné straně a zájmů nebo základních svobod a základních práv subjektu údajů na straně druhé, podle judikatury Soudního dvora je věcí předkládajícího soudu, aby zvážil dotčené zájmy. [69]

i) Posouzení „oprávněného zájmu“ správce údajů

Pokud jde o první kritérium, je třeba poznamenat, že zájem společnosti SCHUFA i jeho zákazníků je čistě ekonomické povahy. Soukromé společnosti uchovávají osobní údaje získané z veřejných rejstříků, aby mohly svým zákazníkům nabídnout službu poskytování informací o úvěruschopnosti subjektu údajů, mimo jiné s využitím těchto údajů. Jak jsem již vysvětlil dříve, takový zájem se pro účely této analýzy jeví jako legitimní. [70]

ii) Dopad zpracování údajů na subjektu údajů

Pokud jde o druhé kritérium, tj. dopad zpracování údajů na subjekt údajů, zdá se, že relevantním faktorem je lhůta pro výmaz. Čím déle jsou údaje uchovávány v databázích soukromých obchodních informačních agentur, tím větší je dopad na subjekt údajů. [71]

Z judikatury Soudního dvora vyplývá, že existují i další faktory, které by měly být při

analýze rovněž zohledněny, a to *pravidla pro přístup do databází a nabízené možnosti šíření osobních údajů*. Zjednodušeně řečeno, čím snadněji jsou informace přístupné veřejnosti, tím závažnější je zásah do základních práv subjektu údajů. To platí zejména v případě, že počet uživatelů s přístupem k údajům subjektu údajů je velký. Jeví se mi tedy jako jasné, že i když jsou údaje během tohoto období šesti měsíců již dostupné ve veřejných rejstřících, skutečnost, že jsou souběžně uchovávány a dostupné v databázích soukromých obchodních informačních agentur, má vedle negativních důsledků dostupnosti těchto údajů ve veřejných rejstřících další dopad na soukromí jednotlivce. [72]

Dalším faktorem, který je třeba při analýze zohlednit, je *případně citlivá povaha* příslušných údajů. Obecně lze říci, že dopad na subjekt údajů se zvyšuje s citlivostí osobních údajů. V této souvislosti je třeba poznamenat, že z judikatury Soudního dvora vyplývá, že osobní údaje týkající se vymáhání dluhů jsou skutečně citlivými údaji pro soukromý život subjektu údajů. Poskytnutí těchto údajů v *zásadě neomezenému počtu uživatelů* je proto třeba považovat za významný zásah do základních práv této osoby. [73]

V neposlední řadě si myslím, že je nutné vzít v úvahu také *faktor času*. Dokonce i zákonné zpracování údajů nemusí být během plynutí času v souladu s GDPR, pokud údaje nejsou nebo již nejsou relevantní nebo jsou nepřiměřené s ohledem na účel, pro který byly původně shromážděny. V této souvislosti si kladu otázku, jak by mohlo být odůvodněno uchovávání osobních údajů po dobu tří let, když se vnitrostátní zákonodárce domnívá, že doba uchovávání v délce šesti měsíců, tj. mnohem kratší doba, je více než dostatečná pro zohlednění obchodních zájmů hospodářských subjektů. [74]

iii) Předběžné závěry

Posouzení všech prvků uvedených v předchozích bodech mě vede k závěru, že značné negativní důsledky, které bude mít uchovávání údajů pro subjekt údajů po uplynutí daného šestiměsíčního období, zřejmě převáží nad obchodním zájmem soukromé společnosti a jejích zákazníků uchovávat údaje po uplynutí tohoto období. V této souvislosti je důležité zdůraznit, že oddlužení má *příjemci umožnit opětovné zapojení do hospodářského života*. Tento cíl by byl zmařen, pokud by soukromé obchodní informační agentury mohly uchovávat osobní údaje ve svých databázích i poté, co byly tyto údaje vymazány z veřejného rejstříku. [75]

4) Dílčí závěr

S ohledem na výše uvedené skutečnosti se domnívám, že uchovávání údajů soukromou obchodní informační agenturou nemůže být na základě čl. 6 odst. 1 prvního pododstavce písm. f) GDPR po výmazu osobních údajů týkajících se úpadku z veřejných rejstříků zákonné. [77]

K souladu se zásadami omezení účelu a minimalizace údajů [čl. 5 odst. 1 písm. b) a c) GDPR]

V souladu se zásadou omezení účelu podle čl. 5 odst. 1 písm. b) GDPR je třeba zajistit, aby osobní údaje shromážděné pro určitý účel nebyly dále zpracovávány způsobem, který je s tímto účelem neslučitelný. V projednávané věci byly údaje týkající se úpadku a oddlužení zpracovávány veřejnými orgány v souvislosti s plněním zákonných povinností. [79]

Pokud však jde o pozdější použití údajů soukromou společností, mělo by být podle GDPR a za použití kritérií stanovených v čl. 6 odst. 4 tohoto nařízení přezkoumáno, zda je zamýšlený účel slučitelný s původním účelem. [80]

Zprv se zdá, že *vazba mezi účely je slabá* už proto, že původní účel je stanoven zákonem, konkrétně právem EU, které členským státům ukládá povinnost vytvářet a vést rejstříky, a správcem údajů je veřejný orgán jednající v rámci úkolů, které mu byly svěřeny zákonem, zatímco pozdější účel sleduje soukromý subjekt v rámci obchodní činnosti spočívající v poskytování ekonomických informací o osobách. [81]

Za druhé, pokud jde o okolnosti, za nichž byly údaje shromážděny, je třeba poznamenat, že *neexistuje žádná vazba mezi správcem a subjektem údajů*, neboť údaje jsou shromážděny nepřímo prostřednictvím rejstříků, a subjekt údajů si proto není vědom skutečnosti, že jeho údaje mohou být později použity, ani kdo a za jakým účelem je použije. To se mi jeví jako obzvláště závažné z hlediska ochrany osobních údajů, neboť zpravidla nikdo nemůže důvodně očekávat, že jeho osobní údaje budou dále zpracovávány. Skutečnost, že zákon stanoví pevnou dobu pro uchovávání údajů ve veřejných rejstřících, pravděpodobně vyvolává důvodné očekávání, že dotyčné údaje budou po uplynutí této doby vymazány. [82]

Za třetí, pokud jde o možné důsledky, které může mít další zpracování údajů pro subjekty údajů, je třeba zdůraznit, že informace o insolvenčním řízení budou vždy použity jako *negativní faktor při budoucím posuzování úvěruschopnosti a platební schopnosti* dotčené fyzické osoby, což má významný dopad na práva této osoby. Chybná představa o ekonomické situaci může mít na dotčnou osobu nepříznivé dopady, výrazně ztěžovat výkon jejích svobod, a dokonce ji ve společnosti stigmatizovat. V rozsahu, v jakém může být subjekt údajů odepřeno zboží a služby, se může stát obětí neoprávněné diskriminace. [83]

Dále je třeba poznamenat, že již stanovením maximální lhůty šesti měsíců, během níž jsou při splnění zákonných podmínek zveřejněny informace o platební neschopnosti a rozhodnutí soudu o oddlužení, vzal *vnitrostátní zákonodárce v úvahu realizaci veřejného zájmu* a zvažil zájmy věřitelů na jedné straně a zájmy a práva osob v platební neschopnosti na straně druhé. Zpracovávání osobních údajů soukromými společnostmi po dobu šestkrát delší, než je zákonem stanovená doba pro veřejné rejstříky, se zdá být nepřiměřené

a *de facto* postihuje subjekt údajů, ačkoli zákon nic takového zjevně nepředpokládá. Jak jsem již uvedl, oddlužení má příjemci umožnit opětovnou účast na hospodářském životě. Tento cíl by byl zmařen, pokud by soukromé obchodní informační agentury mohly uchovávat osobní údaje ve svých databázích i poté, co byly tyto údaje vymazány z veřejného rejstříku. [85]

Kromě toho se zdá být nepřiměřené „opětovně použít“ minulou a již právně vyjasněnou situaci, jako je oddlužení, v budoucích posouzeních, místo aby se použily faktory aktualizované v době analýzy rizik, aby se zajistilo přesnější a objektivnější posouzení ekonomické situace dotyčné osoby. Lze totiž pochybovat o *hodnotě informací o ekonomické situaci osoby, které jsou staré několik let*. Osobní údaje vztahující se k okolnostem, které se týkají určitého minulého období, stěží poskytnou spolehlivé informace o stávající ekonomické situaci subjektu údajů. [86]

K dovolání se práva na výmaz (čl. 17 odst. 1 GDPR)

Předkládající soud si rovněž přeje vědět, zda „právo být zapomenut“ zakotvené v článku 17 GDPR znamená, že osobní údaje mají být vymazány z databází soukromé obchodní informační agentury, které existují vedle veřejných rejstříků a obsahují stejné údaje. Předkládající soud rozlišuje mezi obdobími, kdy jsou osobní údaje dostupné i ve veřejném rejstříku, a obdobími, kdy tam již dostupné nejsou. [90]

Domnívám se, že v zájmu účinné ochrany osobních údajů by neměly existovat žádné významné překážky pro výkon práva na výmaz, zejména pokud na trhu existuje několik obchodních informačních agentur, které vedou údaje souběžně s veřejným rejstříkem. Pokud by byl výkon tohoto práva příliš ztížen striktním výkladem čl. 17 odst. 1 GDPR, hrozilo by, že ochrana, kterou má GDPR poskytovat, by mohla být obcházena konkurencí. Je však třeba připomenout, že cílem unijního zákonodárce je – jak je uvedeno v bodě 10 odůvodnění GDPR – „zajistit soudržné a jednotné uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů“. Proto musí mít subjekt údajů možnost uplatnit svá práva vůči všem společnostem, které tato pravidla porušují. [94]

V této fázi analýzy je proto třeba poznamenat, že žalobci se v zásadě mohou dovolávat práva na výmaz podle čl. 17 odst. 1 GDPR. Výsledek by byl jiný pouze v případě, že by se soukromé obchodní informační agentuře podařilo prokázat, že existují „závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů“ ve smyslu čl. 21 odst. 1 GDPR. Pokud dostupné informace neumožňují rozeznat převažující důvody, které by mohly vyvstat v původním řízení, přísluší předkládajícímu soudu zjistit skutkový stav a případně poměřit dotčené zájmy. [95]

S ohledem na výše uvedené úvahy je nutno čl. 17 odst. 1 písm. d) GDPR vykládat v tom

smyslu, že *subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají*, pokud byly tyto údaje zpracovány protiprávně, jak stanoví čl. 6 odst. 1 tohoto nařízení. Ustanovení čl. 17 odst. 1 písm. c) GDPR je třeba vykládat v tom smyslu, že subjekt údajů má v zásadě právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, pokud vznesl námitku proti zpracování v souladu s čl. 21 odst. 1 tohoto nařízení. [96]

VI. Závěry

S ohledem na výše uvedené úvahy navrhuji, aby Soudní dvůr na předběžné otázky Verwaltungsgericht Wiesbaden (Správní soud ve Wiesbadenu) odpověděl takto:

„1) Ustanovení čl. 78 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), je nutno vykládat v tom smyslu, že z tohoto ustanovení vyplývá, že právně závazné rozhodnutí dozorového úřadu podléhá plnému soudnímu přezkumu ve věci samé.

2) Ustanovení čl. 6 odst. 1 prvního pododstavce písm. f) nařízení 2016/679 je nutno vykládat v tom smyslu, že brání tomu, aby soukromá obchodní informační agentura uchovávala osobní údaje z veřejného rejstříku, jako jsou „vnitrostátní databáze“ ve smyslu čl. 79 odst. 4 a 5 nařízení Evropského parlamentu a Rady (EU) 2015/848 ze dne 20. května 2015 o insolvenčním řízení, po dobu delší, než je doba uchovávání údajů ve veřejném rejstříku. Předkládajícímu soudu přísluší ověřit, zda uchovávání údajů po dobu povolenou pro veřejný rejstřík splňuje podmínky čl. 6 odst. 1 prvního pododstavce písm. f) nařízení 2016/679.

3) Ustanovení čl. 17 odst. 1 písm. d) nařízení 2016/679 je nutno vykládat v tom smyslu, že subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, pokud byly tyto údaje zpracovány protiprávně, jak stanoví čl. 6 odst. 1 tohoto nařízení.

Ustanovení čl. 17 odst. 1 písm. c) nařízení 2016/679 je nutno vykládat v tom smyslu, že subjekt údajů má v zásadě právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, pokud vznesl námitku proti zpracování v souladu s čl. 21 odst. 1 tohoto nařízení. Předkládajícímu soudu přísluší přezkoumat, zda výjimečně neexistují převažující oprávněné důvody pro zpracování.

4) Ustanovení čl. 40 odst. 2 a 5 nařízení 2016/679 je nutno vykládat v tom smyslu, že kodexy chování vypracované v souladu s těmito ustanoveními a případně schválené dozorovým úřadem nemohou stanovit právně závazné podmínky zákonného zpracování osobních údajů, které se liší od podmínek vymezených v čl. 6 odst. 1 tohoto nařízení.“ [105]

Zpracovala Eva Janečková

Nahrávání úředních osob? Co na sebe nechcete prozradit, nikomu nesdělujte

Fenoménem dnešní doby je focení a natáčení kde čeho a kdekoho. Prakticky všichni máme mobilní telefony, které nám to usnadňují. Jednoduché je i následné šíření neomezenému počtu osob kdekoliv ve světě. Před tímto trendem nejsme uchráněni ani my, zaměstnanci úřadů a veřejných institucí.

Citlivost nahrávání (pořizování obrazového nebo zvukového záznamu) spočívá v tom, že nahrávky zachycují nejen to, jak vypadáme (naši podobu, vzhled) a co říkáme (naš hlasový projev), ale i řadu dalších významných či méně významných informací (osobních údajů), které o nás mnohé vypovídají, např. odhalí tetování, vadu řeči nebo jiný zdravotní handicap. Podoba člověka je významným projevem osobní povahy.¹⁾ Zachováváme si ji i při výkonu úřední činnosti. Nemáme dvě tváře – jednu pro soukromý život a druhou pro ten profesní. V úředním styku si nenasazujeme žádnou masku. I v práci jsme to stále „jenom my“.

V jaké míře ztrácíme ve svém profesním životě kontrolu nad svojí podobou a souvisejícími osobnostními projevy (jejich zachycením a šířením)? Mohou lidé nahrávat zaměstnance úřadů a jsou úředníci povinni nahrávání strpět? Jako vodítko nám k odpovědím na tyto otázky poslouží stanoviska soudů a veřejného ochránce práv.

Výchozí pravidlo: Nelze nahrávat soukromý život úředních osob

Každý člověk vede tři životy: veřejný, soukromý a tajný.²⁾ Soukromí každého z nás nekončí tím, že odejdeme ze svého domova (obydli), kde právo na soukromí vnímáme nejintenzivněji. Soukromí má nepochybně svůj prostorový rozměr. Hranice soukromého života a života veřejného můžeme hledat pomocí vymezení „soukromého prostoru“ a „veřejného prostoru“.³⁾ Sféra osobního soukromí se ale může podle okolností přenášet i na místa veřejně přístupná či do veřejných prostor. Uzavřít soukromí do přesně vymezeného prostoru, kde by bylo nerušeně chráněno, není možné. Významnou část svého soukromí si nosíme s sebou.

Jak dovodila judikatura – Nejvyšší správní soud s odkazem na judikaturu Evropského soudu pro lidská práva (ESLP)⁴⁾; „pojem „soukromý život“ je vykládán v širokém smyslu a nezahrnuje pouze nejbližší okolí jednotlivce, v němž žije, chápáno jako domov a rodina. Na-

opak ESLP do tohoto pojmu zahrnuje rovněž život, ve kterém se člověk rozvíjí a navazuje vztahy s jinými lidmi (...), zahrnuje rovněž stránku obchodní a profesní...“⁵⁾

Také Ústavní soud připouští, že „zejména v dnešní době, kdy autonomní naplňování soukromého života a pracovní či zájmové aktivity spolu úzce souvisejí, nelze činit ostré prostorové oddělení soukromí v místech užívaných k bydlení od soukromí vytvářeného v místech a prostředí, sloužících k pracovní či podnikatelské činnosti anebo k uspokojování vlastních potřeb či zájmových aktivit, byť činnosti odehrávající se v prostorech veřejnosti přístupných, resp. neuzavřených, např. podnikatelská činnost, budou moci podléhat jistým omezením, která mohou představovat určitý zásah do práva na soukromý život“⁶⁾

I na pracovišti můžeme vést soukromý život, navazovat vzájemné vztahy a vytvářet vlastní sociální identitu⁷⁾

I v kanceláři tedy můžeme požívat a očekávat určitou míru soukromí. Primárně se však jedná



o prostory určené k činnosti pracovní, a pokud jsou běžně přístupné cizím osobám, musíme svá očekávání soukromí přizpůsobit realitě.

Soukromí zaměstnance je chráněno před zaměstnavatelem:

Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorech zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.⁸⁾

Soukromí zaměstnance je chráněno i před obdobnými zásahy ze strany jiných osob:

Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.⁹⁾

1) Výstižně to formuloval ESLP v rozsudku z 15. 1. 2009, ve věci Reklos a Davourlis proti Řecku, stížnost č. 1234/05: „Podoba jednotlivce je jedním ze základních znaků jeho osobnosti, neboť je výrazem jeho svébytnosti a umožňuje mu odlišit se od ostatních lidí. Právo člověka na ochranu podoby je tak jednou ze základních složek osobního rozvoje a předpokladem pro takové právo je především kontrola jednotlivce nad jeho podobou. Jestliže kontrola nad podobou jednotlivce znamená především jeho možnost odmítnout šíření snímků, na nichž je zobrazen, zahrnuje i právo každého bránit se proti tomu, aby kdokoli jiný zachycoval, přechovával či reprodukoval jeho podobu. Jelikož je totiž podoba jednou z inherentních vlastností osobnosti každého jednotlivce, je (...) podmínkou její účinné ochrany souhlas jednotlivce již v okamžiku jejího zachycení, a nikoli teprve v okamžiku jejího případného veřejného šíření. V opačném případě by kdokoli mohl přechovávat základní znak osobnosti jiné osoby, aniž by tato měla kontrolu nad jeho případným pozdějším užitím.“

2) Gabriel García Márquez: Život.

3) Jak právo rozlišuje veřejný a soukromý prostor a kde hledat hranice soukromí shrnuje Kristýna Bónová ve své práci Ochrana soukromí ve veřejném prostoru, Revue pro právo a technologie 25/2022, dostupné zde: <https://journals.muni.cz/revue/article/view/20966/16931>

4) Srov. zejména Niemietz proti Německu (stížnost č. 13710/88), ze dne 16. 12. 1992; Halford proti Spojenému království (stížnost č. 20605/92) ze dne 25. 6. 1997.

5) Srov. rozsudek Nejvyššího správního soudu ČR ze dne 25. 2. 2010, sp. zn. 9 As 38/2009 – 123; rozsudek Nejvyššího správního soudu ČR ze dne 5. 11. 2009, sp. zn. 1 Afs 60/2009 – 119.

6) Srov. Pl. ÚS 3/09 ze dne 8. 6. 2010 a judikaturu ESLP, na níž Ústavní soud odkazuje: „Proto ESLP pod právo na respektování obydlí podle čl. 8 odst. 1 Úmluvy zahrnuje i požadavek respektu k soukromí sídla společnosti, poboček či provozoven právnických osob (srov. rozhodnutí ze dne 16. 4. 2002 ve věci Sociétés Colas Est. proti Francii), kancelářské prostory (srov. rozhodnutí ze dne 25. 2. 1993 ve věci Crémieux proti Francii či rozhodnutí ze dne 25. 2. 1993 ve věci Mialhe proti Francii) nebo prostory advokátních kanceláří (srov. rozhodnutí ze dne 12. 12. 1992 ve věci Niemietz proti Německu).“

7) Srov. rozhodnutí ESLP ze dne 28. 11. 2017, č. stížnosti 70838/13 ve věci Antovič a Mirkovič proti České republice.

8) Srov. § 316 odst. 2 zákoníku práce.

9) Srov. § 81 odst. 2 občanského zákoníku.

Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.¹⁰⁾ Rozšiřovat podobu člověka je možné jen s jeho svolením.¹¹⁾

Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.¹²⁾

Zákaz pořizovat zvukový nebo obrazový záznam jiné osoby bez jejího svolení neplatí, „pokud se zvukový či obrazový záznam pořídí nebo použije k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob“¹³⁾ nebo „na základě zákona k úřednímu účelu“.¹⁴⁾

Nahrávky vytvořené v pracovním procesu, které zachycují naše jednání, během něhož nevystupujeme „za úřad či instituci, ale za sebe“ – typicky „soukromý telefonát či rozhovor s kolegyní či kolegou“ **mohou zasáhnout do našeho práva na soukromí, a jsou proto bez našeho svolení nepřipustné.**

Účastníci řízení mohou k ochraně svých procesních práv nahrávat úřední osoby v průběhu úředního jednání

Správní řád¹⁵⁾ jako procesní předpis, který upravuje vedení správního řízení, **mlčí o možnosti pořizování zvukových či obrazových záznamů účastníky správního řízení** (na rozdíl například od nahrávání soudního jednání¹⁶⁾). Pořídít obrazový nebo zvukový záznam bez souhlasu dotčených osob umožňuje výslovně (vedle protokolu o jednání) správnímu orgánu, tj. úřední osobě, která řízení vede.¹⁷⁾ Jedná se o tzv. úřední licenci – zmíněnou výjimku ze zákazu pořizování záznamu bez souhlasu osoby na základě zákona k úřednímu účelu.¹⁸⁾

Nejvyšší správní soud¹⁹⁾ **dovodil, že správní řád nahrávání účastníkům nezakazuje, naopak: „účastník řízení má právo realizovat svá procesní práva a oprávněné zájmy a správní orgán je povinen umožnit účastníkům**

kům řízení uplatňovat v rámci výkonu veřejné správy jejich práva a oprávněné zájmy, které jim garantuje zákon.“

Není relevantní, zda má být nahráváno jednání veřejné či neveřejné. Rozdíl spatřuje Nejvyšší správní soud pouze v okruhu osob, které se jednání zúčastní: v případě neveřejného jednání správní orgán připustí jen účast osob zúčastněných na řízení, tedy zástupce správního orgánu, účastníky řízení a jejich zástupce, předvolané svědky, znalce a tlumočníky, je-li jich třeba. Další osoby (zástupce veřejnosti) připustí správní orgán pouze u jednání veřejného.

Nejvyšší správní soud odkazuje na obecný princip „co zákon nezakazuje, je povoleno“.²⁰⁾

Odůvodnění rozsudku tak můžeme interpretovat dvojím způsobem:

1. **Účastníci řízení nepotřebují svolení úřední osoby s jejím nahráváním,**²¹⁾ protože projevy úředních osob v průběhu úředního jednání nejsou projevem osobní povahy. Nejvyšší správní soud přijímá argumentaci Nejvyššího soudu, dle jehož názoru „osobní povahu zpravidla nemají projevy, ke kterým dochází při výkonu povolání, při obchodní a veřejné činnosti.“²²⁾ Právní úprava obsažená v občanském zákoníku na nahrávání úředních osob nedopadá.
2. **Účastníci řízení nepotřebují svolení úřední osoby s jejím nahráváním, protože nahrávání úředních osob účastníky řízení je odůvodněné potřebou chránit jejich procesní práva – jde o výjimku ve smyslu § 88 odst. 1 občanského zákoníku.**

Obě interpretace rozsudku Nejvyššího správního soudu našly svoje uplatnění v praxi:

Na stranu účastníků správních řízení se postavil veřejný ochránce práv. Dokladem toho je jeho upozornění, že nelze účastníky správních řízení omezovat v pořizování audio a video nahrávek úředních osob: „účastník správního řízení má právo pořizovat obrazové a zvukové záznamy úředního jednání, např. ústního jednání či jiného úkonu v řízení, a zachycovat tak jednání úředních osob.“ Ochránce argumentuje tím, že „úřední osoba je veřejným činitelem a vystupuje vůči účastníkům řízení



a dalším dotčeným osobám jako subjekt veřejnoprávního vztahu. Proto se na ni nevztahuje ochrana (tj. poskytnout svolení) podle ustanovení § 81 a násl. občanského zákoníku. Úřední osoba, která jedná za správní orgán, nemůže zabránit tomu, aby si osoba, která se účastní veřejného ústního jednání, ať již jde o účastníka řízení, či jinou osobu, pořizovala obrazový nebo zvukový záznam jednání, pokud tím nenarušuje průběh jednání.“²³⁾

Naopak na stranu úředníků se postavil Krajský soud v Hradci Králové,²⁴⁾ když připustil nahrávání úředních osob bez jejich svolení v situacích, které obecně vymezil jako „případy, kdy bude docházet ke střetu práva na ochranu osobnosti s právy jinými, v daném případě s právy účastníka správního řízení na dodržování základních zásad činnosti správních orgánů vymezených ve druhé hlavě první části správního řádu. Konkrétně například s právem na to, aby věc byla projednána v souladu se zákonem (zásada zákonnosti správního řízení – § 2 odst. 1), aby správní orgány některé z účastníků řízení nezvýhodňovaly (zásada nestranného postupu správních orgánů a rovného

10) Srov. § 84 občanského zákoníku.

11) Srov. § 85 odst. 1 občanského zákoníku.

12) Srov. § 86 občanského zákoníku a zde zakotvený „svolovací princip“.

13) Srov. § 88 odst. 1 občanského zákoníku.

14) Srov. § 88 odst. 2 občanského zákoníku.

15) Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

16) Srov. § 6 odst. 3 zákona o soudech a soudcích: „Uskutečňovat obrazové nebo zvukové přenosy a pořizovat obrazové záznamy v průběhu soudního jednání lze jen s předchozím souhlasem předsedy senátu nebo samosoudce. S vědomím předsedy senátu nebo samosoudce lze pořizovat zvukové záznamy; kdyby způsob jejich provádění mohl narušit průběh nebo důstojnost jednání, může předseda senátu nebo samosoudce jejich pořizování zakázat.“

17) Srov. § 18 odst. 1 správního řádu.

18) Srov. § 88 odst. 2 občanského zákoníku.

19) Srov. rozsudky Nejvyššího správního soudu ze dne 31. března 2010, č. j. 5 As 37/2009-94; ze dne 21. 9. 2022, č. j. 7 As 47/2022-44 a ze dne 8. 12. 2022, č. j. 15A 24/202-100.

20) Srov. čl. 2 odst. 4 Ústavy: „Každý občan může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.“

21) K této argumentaci se lze přiklonit na základě hodnocení Nejvyššího správního soudu, které v posuzovaném případě činí ve vztahu k možnosti nahrávání svědeckých výpovědí strážníků městské policie. NSS dospívá k závěru, že pokud strážníci vypovídali o tom, co zjistili při výkonu své úřední činnosti, o zjištění porušení právních předpisů žalobcem, „nešlo o projev osobní povahy, protože to je z povahy věci, o které svědci vypovídali, naprosto vyloučeno.“

22) Srov. rozsudek Nejvyššího soudu ze dne 11. 5. 2005, č. j. 30 Cdo 64/2004.

23) Srov. text upozornění VOP ze dne 13. ledna 2016, sp. zn. 4869/2015/VOP/PL, je dostupný zde: <https://eso.ochrance.cz/Nalezene/Edit/3544>.

24) Srov. rozsudek ze 9. května 2013 č. j. 30 A 54/2012, dostupný v ASPI.

přístupu k dotčeným osobám – § 2 odst. 4, § 7 odst. 1), nebo aby se úřední osoby chovaly vůči dotčeným osobám zdvořile a vycházely jim vstříc (zásada charakterizující veřejnou správu jako službu veřejnosti – § 4 odst. 1).“ V posuzovaném případě dovedl, že „**Účastník správního řízení vedeného dle správního řádu má právo na pořízení obrazových a zvukových záznamů z úkonů v řízení**, o nichž se sepisuje protokol, **bez souhlasu přítomných úředních osob** zcela výjimečně, a to například tehdy, **pokud prokáže, že zájem nad dodržováním základních zásad činnosti správního orgánu v daném případě převáží nad zájmem na ochranu osobnostních práv úředních osob.** K prokázání takového účelu nejsou způsobilé fotografie úředních osob pořízené účastníkem řízení v průběhu ústního jednání. Zákaz správního orgánu pořizovat takové fotografie tak není nezákonným zásahem ve smyslu § 82 s. ř. s.“

Krajský soud v posuzovaném případě **nepřipustil fotografování úředních osob, protože fotografie samy o sobě nemohou vypovědět nic** o tom, zda úřední osoba dodržovala zásady činnosti správních orgánů, chovala se zdvořile, nestranně apod. Pořízení nahrávky (obrazového a zvukového záznamu jednání), která by naopak tyto rozhodné skutečnosti prokázat mohla, by však připustil. Je nerozhodné, že by se z hlediska potencionálního zásahu do osobnostních práv úřední osoby jednalo o významnější zásah; rozhodné je, že pouze pořízení nahrávky (místo fotografie) bylo způsobilé naplnit legitimní účel – ochranu práv účastníka řízení.

Přísněji než krajský soud, ale stále ještě ve prospěch poměřování práv úředníků a účastníků řízení, argumentoval v jiném případě **Nejvyšší správní soud**, když uvedl, že „ani úřední osoba, ačkoli ve správním řízení vystupuje jménem orgánu veřejné správy, nemůže být omezena ve svém právu na ochranu osobnosti. Oprávnění účastníka řízení pořizovat obrazové a zvukové záznamy úředních osob se proto zakládá teprve svolením těchto osob.“²⁵⁾ Současně Nejvyšší správní soud přiznal, že „svolovací princip ochrany osobnosti neplatí absolutně“, pokud dojde ke kolizi dvou protichůdných práv; v takovém případě je na místě poměřování práv stojících vůči sobě.

V posuzovaném případě Nejvyšší správní soud poukázal na to, že **z protokolu nevyplynají důvody, které účastníka řízení ved-**



ly k pořizování audiovizuálního záznamu.

Stěžovatel nevytkl nevhodné chování úředních osob a ani nevzněl výtku proti průběhu jednání. **Neuplatnil žádný z relevantních důvodů, pro které by mohl převážit zájem účastníka řízení nad osobnostními právy úřední osoby.** Pokud stěžovatel svým jednáním zamýšlel ochránit svá veřejná subjektivní práva, bylo vhodné uplatnit výtky v rámci správního řízení. Všechny stěžovatelem tvrzené důvody pro pořízení záznamů jsou dostatečně chráněny procesními instituty správního řízení a tvoří nezbytnou součást práv účastníka. Takto bylo na stěžovateli, aby zejména namítl podjatost úředních osob kdykoli v průběhu jednání (§ 14 odst. 2 správního řádu) či navrhl přezkoumat zákonost procesního postupu správního orgánu v odvolání (srov. § 81 a násl. správního řádu), příp. v řízení o žalobě proti rozhodnutí správního orgánu podle § 65 a násl. s. ř. s.

Pro úplnost je možné doplnit i **další argument pro povolení nahrávání úředního jednání účastníky řízení:** „účastník správního řízení má mimo jiné také právo nahlížet do spisu a činit si z něj výpisy (...). Uvedené dle krajského soudu²⁶⁾ znamená, že účastník má také právo činit si výpisy ze zvukového záznamu pořízeného správním orgánem o průběhu ústního jednání. Má-li účastník řízení právo na pořízení výpisu ze zvukového záznamu poříže-

ného správním orgánem o průběhu ústního jednání či jeho kopie, pak dle názoru krajského soudu má také právo, aby si i za splnění určitých podmínek o průběhu ústního jednání takový záznam pořídil sám. Uvedené krajský soud nepovažuje ani v rozporu se zásadou nevěřejnosti ústního jednání, protože pouhým pořízením zvukového záznamu z ústního jednání se nestává jednání veřejným, neboť i nadále se jej mohou kromě úředních osob účastnit jen účastníci řízení či jiné dotčené osoby.“

Co nám z toho vyplývá?

Účastníci řízení mohou k ochraně svých procesních práv nahrávat úřední osoby i bez jejich souhlasu. Tutéž možnost by pak dle mého soudu měl mít každý, kdo může být dotčený jednáním úřední osoby.²⁷⁾

Nahrávání úředních osob připouští i komentářová literatura: „pořízení záznamu z ústního jednání, resp. obecně záznamu úřední osoby při výkonu její pravomoci, aniž by k tomu úřední osoba musela dát svůj souhlas, obecně možné je“.²⁸⁾

Nepanuje shoda v tom, zda je nahrávání úředních osob způsobilé zasáhnout osobnostní práva úředních osob. Zůstává tudíž sporné, zda mají úřední osoby strpět nahrávání bez dalšího nebo zda mohou k ochraně svých osobnostních práv zjišťovat důvody nahrávání a blíže je hodnotit, a to zejména z toho úhlu pohledu, zda je pořízení nahrávky nezbytné k ochraně práv a zájmů osoby, která nahrávku pořizuje; zda daná osoba mohla využít a také využila k ochraně svých práv jiných opravných prostředků (stížnost, námitku podjatosti, odvolání, podnět k přezkumu apod.), či dokonce **zda k deklarovanému účelu nahrávání nepostačí zvukový záznam namísto obrazového záznamu.** Posledně zmíněné posuzování se nabízí zejména v situaci, kdy osoba s námi jednající uvádí, že si chce „jen“ nahrát, co jí říkáme. Pořízení zvukové nahrávky se tudíž zdá dostačujícím z hlediska svého účelu, a naopak pořizování obrazového záznamu jako nepřiměřené, pro daný účel zbytečné.²⁹⁾

Uznávám, že každý zásah do jiného práva je třeba poměřovat, zkoumat jeho nezbytnost a šetřit podstatu jednotlivých práv.³⁰⁾ Z praktického pohledu si ale myslím, že bychom nahrávání „úředního jednání“ neměli tolik „sešněrovávat“.³¹⁾ Otevřené (opak skrytého) na-

25) Srov. rozsudek Nejvyššího správního soudu ze dne 9. 10. 2013, č. j. 3 Aps 3/2013 – 25.

26) Cituji názor krajského soudu v Ostravě, jehož rozsudek č. j. 58 Ca 5/2006-60 z 27. 2. 2009 napadl žalobce kasační stížností a Nejvyšší správní soud o ní rozhodl zmíněným rozsudkem č. j. 5 As 37/2009-94 ze dne 31. března 2010.

27) Bez ohledu na to, zda se úřední jednání odehrává „za přepážkou“, na chodbě úřadu nebo v kanceláři.

28) VEDRAL, J.: Správní řád. Komentář. II. aktualizované a rozšířené vydání. Praha: RNDr. Ivana Hexnerová – BOVA POLYGON, 2012, ISBN 978-80-7273-166-4, s. 230.

29) Opřít se lze o obecný princip šetřit podstatu a smysl práv. Srov. čl. 4 odst. 4 Listiny základních práv a svobod.

30) Srov. princip proporcionality v judikatuře Ústavního soudu: IV. ÚS 157/97 ze dne 9. 2. 1998, Pl. ÚS3/02 ze dne 13. 8. 2002, I. ÚS 517/10 ze dne 15. 11. 2010.

31) Srov. doporučení (neprávní úvahu) soudu vyjádřenou v bodě 28 odůvodnění rozsudku Městského soudu v Praze ze dne 12. 12. 2017, č. j. 6 A 92/2016: „současný technický pokrok umožňuje v široké míře záznam téměř jakéhokoliv děje, ať už o tom zaznamenávaná osoba ví nebo neví. Za tohoto stavu by se jevílo spíše výhodnější obecně policisty instruovat v tom smyslu, že lepší je takovému záznamu nebránit a jej nezakazovat, neboť k tomu není racionální důvod. V tomto konkrétním případě je ze záznamu patrné, že se policisté chovali slušně, trvali, byť důrazně, pouze na provedení svého příkazu a provedli kontrolu totožnosti. Žádný exces v chování policistů soud nezjistil. Proto se domnívá, že nechuť policie k pořizování těchto záznamů nemá žádný racionální důvod, když v současné době tyto záznamy stejně mohou být pořizovány např. i bez vědomí zasahujících policistů, a zákaz takového záznamu pak zbytečně zvýší určité napětí při prováděném zásahu.“

hrávání může splnit „preventivní“ (odrazující) účel – zajistit, že s námi úřední osoba jedná tak, jak jí právo ukládá. Může mít smysl ale i tehdy, chce-li si nahrávající osoba „pouze“ zpětně ověřit, zda úřední osoba postupovala správně, například zda zaprotokolovala průběh jednání, tak jak se odehrál, zda ji náležitě informovala či poučila. Nahrávkou lze doložit nezákonné či neprofesionální jednání konkrétní úřední osoby. Naopak bez jejího pořízení se zpravidla dotčená osoba nachází v situaci jejího tvrzení vs. tvrzení úřední osoby. Důsledné vyžadování neúspěšného vyčerpání všech opravných prostředků k nápravě tedy v konečném důsledku nemusí být (na rozdíl od jedné dobře pořízené nahrávky) vůbec efektivní.

Nahrávání úředních osob může být také projevem veřejné kontroly výkonu veřejné činnosti³²⁾

Věci veřejnou jsou veškeré agendy státních institucí, jakož i činnost osob působících ve veřejném životě, tj. např. činnost politiků místních i celostátních, úředníků, soudců, advokátů, popř. kandidátů či čekatelů na tyto funkce; (...) a dále vše, co na sebe upoutává veřejnou pozornost. Tyto veřejné záležitosti, resp. veřejná činnost jednotlivých osob, mohou být veřejně posuzovány. Při kritice veřejné záležitosti vykonávané veřejně působícími osobami platí z hlediska ústavního presumpce o tom, že jde o kritiku dovolenou. Jde o výraz demokratického principu, o výraz participace občanské společnosti na věcech veřejných.³³⁾

V této souvislosti lze tedy připustit nahrávání úředních osob i osobou, která není jedním z konkrétních úředních osob reálně dotčená.³⁴⁾ Tato možnost má však, jak vysvětlím vzápětí, své praktické limity, které jsou dány tím, že úřední osoba zpravidla nejedná sama se sebou, ale s jinými (soukromými) osobami a u nich je nezbytné (ne)svolení s nahráváním respektovat.

Nahrávání úředního jednání má své limity

Nahrávání by nemělo narušit průběh jednání (výkon úřední činnosti). Lze proto nepřipustit nahrávání nebo vyzvat nahrávající

osobu k jeho ukončení v případě, že se v průběhu jednání začne chovat agresivně, útočně, vulgárně, urážejícím či jinak nevhodným chováním.³⁵⁾ Ani v této souvislosti nezapomínejme na obecně platný zákaz zneužití práva: nikdo nemůže vykonávat svoje práva na újmu druhému.³⁶⁾

Nahrávání lze omezit, pokud nahrávka zachycuje osoby, které nejsou úředními osobami a s nahráváním nesouhlasí. Pro nahrávání ostatních (neúředních) osob platí bezvýhradně zákaz nahrávání bez jejich svolení dle občanského zákona.

V praxi to znamená, že účastník správního řízení si nemůže v průběhu ústního jednání pořizovat zvukový nebo obrazový záznam bez výslovného svolení dotčené osoby, která se projevuje (např. podává vysvětlení, svědeckou výpověď). Úřední osoba, která řízení vede, by se tedy měla vždy dotčených osob dotázat, zda s pořízením nahrávky souhlasí a v případě jejich nesouhlasu, nahrávání odmitnout, aby bylo možné jednání uskutečnit. Takto by měla úřední osoba postupovat, pokud si všimne, že někdo nahrává „cizí“ úřední jednání.

Co říci závěrem?

I když správní praxe připustila nahrávání úředních osob za účelem ochrany procesních práv, nemusíme se bát, že by každé naše úřední vystupování bylo nahráváno. Většina lidí, s nimiž úředně jednáme, nemá zájem či potřebu nás nahrávat. I přes stávající technologický rozvoj je nahrávání nás zaměstnanců profesionálů spíše výjimečné.

Navzdory této výjimečnosti v nás představuje nahrávání vyvolává nejistotu a obavu. Bojíme se, že budeme „usvědčeni“ z chyby; chybovat je ale lidské a i úředník je jen člověk. Bojíme se zneužití, poškození či zesměšnění, protože nemáme kontrolu nad tím, jak osoba, která nás nahrává, s nahrávkou naloží. Že se něco takového může stát i nám, nelze vyloučit. Není to ale relevantní argument, s jehož pomocí bychom mohli nahrávání našeho úředního jednání bránit. Ke své obraně můžeme využít jiné prostředky obrany.³⁸⁾

Co ovlivnit můžeme, je to, jak budeme v úředním styku vystupovat. Snažme se být proto profesionály, nezavdáváme příčinu tomu, aby kdokoliv měl zájem na naše jednání upozorňovat nebo je sdílet například prostřednictvím sociálních sítí.

Bojíme-li se o své soukromí, nezapomínejme, že **žádná nahrávka (přiznaná ani skrytá) nezachytí víc, než co se o nás mohou druhí dozvědět, když s nimi jednáme.** S výjimkou informací o tom, jak vypadáme a jak mluvíme, většinu toho, co o sobě dáváme druhým vědět, máme plně ve své moci. Ani ve veřejném prostoru nepřicházíme o právo rozhodovat o tom, jaké „další“ osobní údaje a komu je zpřístupníme. Existuje proto jednoduchá rada: co na sebe nechcete prozradit, nesdělujte. Nechcete-li, aby konkrétní osoba věděla, že máte dvě děti, neříkejte jí to. Nechcete-li, aby věděla, že pijete kávu, nepijte ji při úředním jednání. Pak vám nehrozí, že „TO“ bude nahráno, nebo dokonce zneužito.



Veronika Gabrišová

Autorka pracuje v Kanceláři veřejného ochránce práv, je vedoucí odboru veřejného pořádku a místní správy, pověřenkyní pro ochranu osobních údajů a členkou rozkladové komise Úřadu pro ochranu osobních údajů.

32) Za tímto účelem připouští pořizování záznamů policistů při výkonu služby také Stanovisko odboru bezpečnostní politiky MV k pořizování záznamů policistů při výkonu služby aktualizované k 16. 10. 2014. Obdobně také usnesení Nejvyššího soudu ze dne 24. 9. 2019, sp. zn. 4 Tdo 1064/2019 a na něj odkazující rozsudky Nejvyššího správního soudu ze dne 8. 12. 2022, č. j. 15A 24/2020-100 a ze dne 21. 9. 2022 č. j. 7 As 47/2022-44.

33) Srov. Ústavní soud, IV. ÚS 23/05-2, [111/2007 USn.]

34) Bez ohledu na to, zda je to „hlídací pes“, tedy osoba, která plní úkoly či posílání dozoru veřejnosti nebo „kverulant“, tedy osoba stěžující si velmi často, přičemž její podání nemívají věcný základ, jsou bezúčelné a pouze (nejen časově) zatěžují postup úřadu. K pojmu „hlídací pes“ viz platový náleží Ústavního soudu – náleží ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16. K šikanoznímu uplatňování práva blíže usnesení NSS ze dne 28. 2. 2013, č. j. 8 As 130/2012 – 10.

35) Jak uvedl Nejvyšší správní soud v rozsudku ze dne 1. 6. 2010, č. j. 2 As 35/2010 – 62, „[z]e zásady, že veřejná správa je službou veřejnosti a každý zaměstnanec správního úřadu je povinen se k dotčeným osobám chovat zdvořile a vstřícně (§ 4 odst. 1 správního řádu) však určitě neplatí, že si musí nechat ze strany účastníka řízení

vše nechat líbit.“ Obdobně také cit. rozsudek Nejvyššího správního soudu č. j. 5 As 37/2009-94 ze dne 31. března 2010, dostupný na www.nssoud.cz

36) Znaky zneužití práva vymezil NSS např. již v rozsudku ze dne 10. 11. 2005, č. j. 1 Afs 107/2004 – 48, č. 869/2006 Sb. NSS. Zneužitím práva se rozumí „situace, kdy někdo vykoná své subjektivní právo k neodůvodněné újmě někoho jiného nebo společnosti; takovéto chování, jímž se dosahuje výsledku nedovoleného, je jenom zdánlivě dovolené“.

37) To neplatí v případě, že dotčenou osobou je úřední osoba, resp. vypovídá-li o úřední věci obdobně, jako vypovídali strážníci městské policie o tom, co zjistili při výkonu své úřední činnosti. Srov. rozsudek č. j. 5 As 37/2009-100 ze dne 31. března 2010.

38) Srov. § 82 odst. 1 občanského zákoníku.

39) Právo jednotlivce na takzvané informační sebeurčení: Každý z nás je oprávněn rozhodnout o tom, jaké údaje o sobě poskytneme, pokud zákon neukládá povinnost určité údaje zpřístupnit. Takovou výjimku představují tzv. osobní údaje vypovídající o naší úřední činnosti, funkčním nebo pracovním zařazení, které lze poskytnout dle § 8a odst. 2 zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Bankovní tajemství a ochrana osobních údajů – jsou si tyto instituty skutečně tak blízké, jak se může na první pohled zdát?

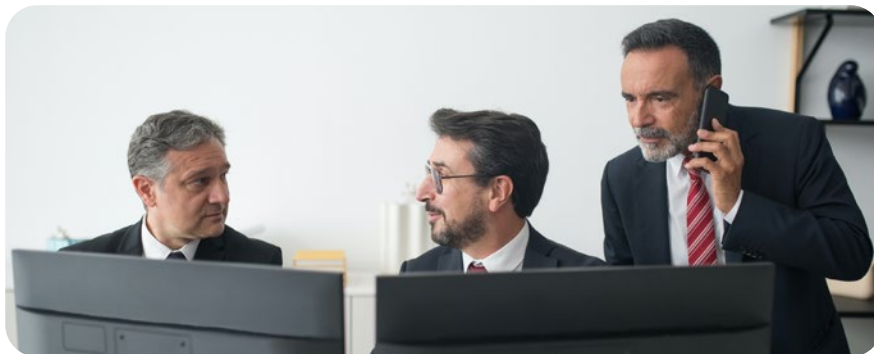
Ačkoli mají bankovní tajemství a ochrana osobních údajů principiálně jeden hlavní společný cíl – tedy regulace nakládání a zajištění ochrany (zabezpečení) určité legislativou definované sady údajů, v mnoha aspektech se tyto instituty podstatně liší. A které jsou ty hlavní odlišnosti?

Vývoj obou institutů

Institut bankovního tajemství je mnohem starší než problematika ochrany osobních údajů – podle některých autorů je možné zárodky bankovního tajemství vystopovat v pramenech o počátcích civilizace, konkrétně o starověkých chrámech, které díky darům a obětem věřících disponovaly volným finančním kapitálem. Mystický a okultní charakter jejich činnosti tak tedy zřejmě dal vzniknout nejen dalšímu dodnes dobře známému tajemství – tajemství zpovědnímu, ale právě rovněž tajemství bankovnímu. Každopádně obecně je za první nesporné zachycení institutu bankovního tajemství považován kodex Banco Ambrosiano Milano z roku 1593 a patrně nejznámějším je pak švýcarský zákon o bankách z roku 1934, kdy se tento institut dostal poprvé do zákona. Motivace švýcarských zákonodárců pro toto rozhodnutí není jasná, nicméně jako jedna z možných variant se udává snaha ochránit vklady židovských klientů před silicím nacistickým režimem v Německu.

Rovněž počátky snah regulovat nakládání s osobními údaji a jejich ochranu lze vystopovat v historických pramenech vztahujících se ke druhé světové válce – konkrétně ke zneužívání „citlivých“ osobních údajů (např. národnost, vyznání, sexuální orientace atd.) nacistickým režimem a jejich zpracování v dosud nevídaném rozsahu a šíři automatizovanými prostředky zpracování (prostřednictvím děrných štítků). Tyto snahy měly nejprve podobu mezinárodních dohod a zřejmě nejpropracovanějším systémem regulace zpracování a ochrany osobních údajů (ačkoli rozhodně není dokonalý) dnes disponuje EU zejména prostřednictvím GDPR.

A zatímco ochrana osobních údajů je v poslední době jednoznačně „in“ a její cíle jsou, nebojím se říci, univerzálně vnímány jako pozitivní (i když vnímání prostředků zvolených zákonodárci k jejich dosažení takto jednoznačně již vnímáno není), bankovní tajemství je naopak „out“ – v posledních letech nabylo totiž spíše negativní nádehe, neboť je spojováno zejména s problematikou praní špinavých peněz a financování terorismu a z těchto a dalších mnoha důvodů, které zákonodárci zrovna najde, postupně erodová-



no, takže si troufám říci, že dnes z něj již mnoho nezbývá.

Vzájemný vztah mezi bankovním tajemstvím a ochranou osobních údajů

Bankovní tajemství se dle § 38 odst. 1 zákona o bankách¹⁾ vztahuje na všechny bankovní obchody, peněžní služby bank, včetně stavů na účtech a depozit. Naproti tomu za osobní údaje je dle čl. 4 (1) GDPR třeba považovat veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Pokud se tedy zaměříme na informace zpracovávané bankou, množina údajů, které spadají pod bankovní tajemství, bude širší než množina údajů, které spadají pod ochranu osobních údajů. Je tomu tak jednak proto, že zatímco regulace ochrany osobních údajů se vztahuje pouze na údaje týkající se fyzických osob, bankovní tajemství chrání i údaje týkající se osob právnických. Další podstatný rozdíl je ten, že zatímco v České republice se regulace ochrany osobních údajů netýká údajů fyzických osob, které zemřely, bankovní tajemství toto rozlišení nezná.

V širším slova smyslu pak regulace obou institutů sice řeší, co je osobním údajem, resp. co spadá do bankovního tajemství, nicméně regulace zpracování osobních údajů je dále mnohem komplexnější a řeší poměrně detailně, za jakých podmínek je možné osobní údaje zpracovávat²⁾, zatímco regulace bankovního tajemství se omezuje na řešení toho, s kým a za jakých podmínek je možné údaje podléhající bankovnímu tajemství sdílet.

Možnosti sdílet osobní údaje, resp. údaje podléhající bankovnímu tajemství se třetí osobou

Příjemcem osobních údajů podle GDPR může být buď zpracovatel osobních údajů při splnění podmínek kladených na zajištění vztahu mezi správcem a zpracovatelem, nebo jiný správce osobních údajů za předpokladu, že pro takové předání osobních údajů existuje některý z právních základů stanovených v čl. 6 GDPR, přičemž tyto právní základy jsou stanoveny obecně tak, aby pod vhodně zvolený právní základ bylo možné přiřadit téměř jakékoli zpracování osobních údajů.

Naproti tomu sdílení údajů podléhajících bankovnímu tajemství se třetí osobou je dle zákona o bankách možné pouze ve dvou případech – buď k němu dá klient banky souhlas, anebo se jedná o jeden z případů vyjmenovaných v zákoně.³⁾

Skutečně ale v praxi dochází ke sdílení údajů podléhajících bankovnímu tajemství jen v těchto případech?

Nikoli. Nesmíme zapomenout na outsourcing, kdy banka některou činnost, kterou by mohla vykonávat sama, nakupuje u externího dodavatele (ve většině případů je takový dodavatel rovněž zpracovatelem osobních údajů), přičemž samotný outsourcing je samozřejmě legitimní a regulovaný celou řadou pravidel ze strany EBA a ČNB. Vyžadování souhlasu je však pro účel outsourcingu nereálné a zároveň v žádném zákoně průlom do bankovního tajemství z tohoto důvodu nenajdeme. Přes-

1) Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů.

2) Tím mám na mysli celý komplex opatření dle GDPR – zajištění informovanosti subjektů údajů, identifikace právních základů pro zpracování, nastavení a zasmulvnění vztahů při předávání osobních údajů, nastavení opatření pro ochranu osobních údajů atd.

3) Bohužel, seznam průlomů do bankovního tajemství obsažený v zákoně o bankách není kompletní, takže průlomy jsou obsaženy i v dalších zákonech – např. zákon č. 96/1993 Sb., o stavebním spoření a státní podpoře stavebního spoření, ve znění pozdějších předpisů, zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů a další právní předpisy.

to má však každá banka desítky až stovky dodavatelů, se kterými údaje svých klientů sdílí. Tato skutečnost se zřejmě dá legitimizovat tím, že zatímco u ostatních průlomů do bankovního tajemství, kdy příjemci těchto informací dále sami nakládají s přijatými údaji dle vlastního uvážení, v tomto případě je poskytovatel služby nadále vázán pokyny banky a banka za výsledek zpracování údajů dále odpovídá tak, jako kdyby údaje zpracovávala sama. K této otázce se vyjádřila také ČNB ve svém stanovisku⁴⁾, kde přijala poněkud kreativní výklad: „Banka může sdělit údaje chráněné bankovním tajemstvím třetí osobě pouze v případech, kdy tak zákon výslovně stanoví, nebo pokud klient se sdělením údajů souhlasí. (...) Právní předpisy nebrání bance vykonávat některé činnosti prostřednictvím jiné osoby (outsourcing). Podstatné je však řízení s tím souvisejících rizik a dodržení dalších souvisejících povinností.“ Může tedy podle ČNB banka sdělit údaje podléhající bankovnímu tajemství se třetí osobou kdykoli, kdy taková situace není upravena zákonem, ale zároveň ji v takové aktivitě právní předpisy nebrání (za předpokladu, že ze svého pohledu ošetří související rizika)? Alespoň okrajově si dovoluji zmínit ještě jeden zajímavý případ – převzetí

a fúze bank (nebo případně prodej části podniku banky). Opět, souhlas je nepoužitelný, zákon mlčí a mlčí také již shora zmiňované stanovisko ČNB. A přesto se tak v praxi velmi často děje a nikomu to nevadí.

Závěr

Bankovní tajemství již dávno není tím, čím bývalo – v případech stanovených zákonem, někdy zcela automaticky (např. Centrální evidence účtů), jindy odůvodněně (např. správci daně), mají k údajům, které mu podléhají, přístup desítky úřadů. Zákonodárce tento katalog průlomů neustále rozšiřuje, rovněž ve jménu mezinárodní spolupráce v boji proti praní špinavých peněz a financování terorismu. K údajům podléhajícím bankovnímu tajemství pak má přístup i celá řada soukromých subjektů, aniž by existoval souhlas klienta s takovým průlomem nebo průlom dle zákona. Naproti tomu regulace zpracování osobních údajů a jejich ochrany jde spíše opačným směrem a nebojím se říci, že je dnes v podstatě přísnější než u údajů podléhajících bankovnímu tajemství. Dle mého názoru je tedy na místě položit si dvě, pro mnohé možná kontroverzní, otázky, a sice zda bankovní tajemství není (ve vztahu k fyzickým

osobám) již přežitkem, a pokud není, zda by vzhledem k možnosti bank působit v rámci EU přeshraničně nebyla vhodná harmonizace tohoto institutu prostřednictvím předpisu EU.



Sylvie Milerová

Autorka je samostatnou advokátkou v Praze, zaměřuje se na problematiku finanční regulace a regulace zpracování osobních údajů.

4) Stanovisko ČNB k institutu bankovního tajemství, aktualizovaná verze k 1. 2. 2023, dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2021-06/>.

Francouzský dozorový úřad udělil vysokou pokutu kvůli cookies

Dne 19. prosince 2022 vydal francouzský dozorový úřad (CNIL, Commission nationale de l'informatique) rozhodnutí o udělení pokuty ve výši 60 milionů euro společnosti Microsoft Ireland Operations Limited. Hlavním porušením zákonných ustanovení na ochranu osobních údajů byla špatně nastavená možnost odmítnout cookies, neboť jejich odmítnutí nebylo stejně snadné jako přijetí.¹⁾

Francouzský dozorový úřad věc šetřil na základě stížnosti na podmínky uchovávání cookies na stránce bing.com, tedy prohlížeče vyvinutého společností Microsoft. Opakovaná šetření na této stránce proběhla v září 2020 a v květnu 2021. Francouzský dozorový úřad získal doklady o tom, že se na terminál stránky prohlížeče bez souhlasu uživatelů ukládaly cookies. Ty byly dále využity mimo jiné k marketingovým účelům. Stránka rovněž neumožňovala, aby uživatel ukládání cookies odmítl stejně jednoduše, jako by je přijal. Vedle možnosti souhlasu nebylo hned na první stránce tlačítko pro odmítnutí.

Francouzský dozorový úřad bral v potaz pouze uživatele, jejichž zařízení se v době při-

pojení ke stránce bing.com nacházela na francouzském území, a zaměřil se na společnost Microsoft France jakožto na podnik skupiny Microsoft.

Dvě cookies se nahrály bez vědomí uživatele

Stránka bing.com již při první návštěvě uživatele automaticky a bez zásahu uživatele uložila do jeho zařízení cookie MUID, která měla několik účelů. Společnost uvedla, že jedním z nich byl i boj proti marketingovým podvodům, konkrétně v souvislosti s necílenou reklamou.²⁾ Cookie MUID má ovšem i marketingové účely. Podle stanoviska společnosti Microsoft se však tato funkce aktivovala jen



poté, co uživatel dal souhlas se zpracováním osobních údajů k reklamním účelům.³⁾ Tato cookie nicméně sleduje, jaké webové stránky uživatel navštívil, a tato data na dobu jednoho roku ukládá.⁴⁾ Šíře funkcí cookies MUID podle zpravodaje CNIL vylučuje možnost použití výjimky dané ve francouzském zákoně o ochraně údajů. Tu lze podle paragrafu 82 zákona využít jen tehdy, kdy je výlučným účelem cookies umožnění nebo usnadnění elektronické komunikace, nebo je-li cookies skutečně nezbytná pro poskytnutí online komunikační služby na výslovnou žádost uživatele.⁵⁾

1) <https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-microsoft-ireland-operations-limited> (přístup 5. 2. 2023).

2) Tamtéž.

3) [https://gdprhub.eu/index.php?title=CNIL \(France\) - Deliberation SAN-2022-024 of December 20, 2022](https://gdprhub.eu/index.php?title=CNIL%20(France)%20-%20Deliberation%20SAN-2022-024%20of%20December%2020%2C%202022) (přístup 19. 3. 2023).

4) <https://cookiedatabase.org/cookie/microsoft/muid/> (přístup 19. 3. 2023).

5) [https://gdprhub.eu/index.php?title=CNIL \(France\) - Deliberation SAN-2022-024 of December 20, 2022](https://gdprhub.eu/index.php?title=CNIL%20(France)%20-%20Deliberation%20SAN-2022-024%20of%20December%2020%2C%202022) (přístup 19. 3. 2023).



Další cookie ABDEF se do terminálu uživatele nahrála při použití prohlížeče Bing. Jednalo se o cookie s reklamními účely. I tato cookie se uložila, aniž by s tím uživatel souhlasil. Francouzský zákon však cookies tohoto druhu umožňuje ukládat pouze s výslovným souhlasem uživatele. Na to společnost reagovala, že v tomto případě byla cookie z její strany špatně zařazena kvůli lidské chybě, do terminálů uživatelů se nahrávala po krátkou dobu, než se její použití navázalo na souhlas uživatele. Dovolávala se proto, že má „právo na chybu“ a že jednala v dobré víře.⁶⁾

Odmítnutí nebylo stejně snadné jako přijetí cookies

Stránka umožňovala v podstatě okamžité přijetí ukládání cookies, na které stačilo jedno kliknutí. Jejich odmítnutí však stejně snadné nebylo. Tato akce vyžadovala kliknutí dvě. Francouzský úřad konstatuje, že tím provozovatel stránky odrazuje uživatele od odmítnutí cookies a podbízí jim snadnější volbu jejich akceptováním již na prvním okně stránky. Shledal tak porušení jak článku 7 odstavce 3 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále „obecné nařízení“), tak § 82 francouzského zákona na ochranu osobních údajů. Tímto zákonem Francie do svého právního řádu trans-

ponovala Směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).⁷⁾ Stejný zákon tak na národní úrovni upřesňuje některé principy zakotvené v obecném nařízení. Tlačítko s možností odmítnout všechny cookies se na první stránce objevilo 29. března 2022.

Francouzský dozorový úřad zde dále použil i článek 4, odstavec 11 obecného nařízení, kde je souhlas definován jako „jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“. Tento koncept rozvádí preambule obecného nařízení, konkrétně odstavec č. 42: „Souhlas by neměl být považován za svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen.“ Francouzský dozorový úřad zde k výroku o tom, že nemožnost odmítnout cookies stejně snadno, jako je všechny přijmout, je v rozporu s právem na ochranu osobních údajů, použil kombinaci všech zmíněných ustanovení a definic. Poukázal rovněž na to, že se v této záležitosti vyjádřil již 17. září 2020 v pokynech k použití § 82 zákona o ochraně údajů.⁸⁾

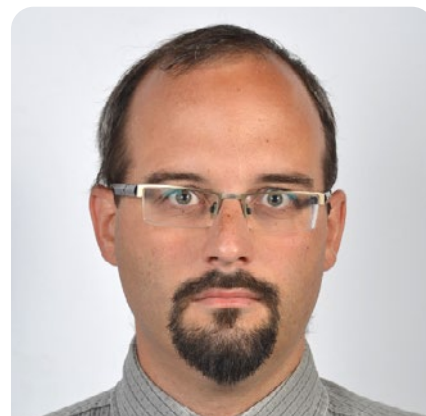
Vliv snadného odmítnutí cookies CNIL doložil i statistikou, podle které zavedení mož-

nosti odmítnout cookies stejně snadno, jako je přijmout, vedlo ke snížení míry souhlasu s cookies u uživatelů, kteří internetové stránky navštívili prostřednictvím počítače. Poměr těch, kteří přijali cookies, se snížil ze 70 % na 55 % v březnu a dubnu 2021 poté, co byla ve Francii k 31. 3. 2021 zavedena povinnost získat výslovný souhlas uživatele s použitím cookies.⁹⁾ Je tedy patrné, že uvedení možnosti odmítnout cookies hned na prvním okně webové stránky má svůj vliv.

Výše pokuty nemusí být konečná

Pokutu ve výši 60 milionů euro (přes 1,4 mld. Kč) CNIL zdůvodnil rozsahem zpracování, počtem dotčených subjektů osobních údajů a ziskem, který společnosti plynul z reklamních příjmů, nepřímo vytvořených i údaji získanými formou cookies.

Tato pokuta nemusí být konečná. Francouzský dozorový úřad společnosti vydal rovněž příkaz, aby ve lhůtě do tří měsíců získala souhlas jednotlivých uživatelů pobývajících ve Francii. Pouze s tímto souhlasem pak může ukládat cookies a sledovacích programů za účelem reklamy. Nesplnění této povinnosti by znamenalo další finanční sankci ve výši 60 000 euro za každý den prodlení. V době zpracování tohoto článku tato lhůta právě uplynula, ale o dalších krocích zatím nejsou dostupné žádné informace.



Pavel Janeček

Autor je odborník na mezinárodní vztahy

6) Tamtéž.

7) Podle § 82 francouzského zákona o ochraně osobních údajů „musí být každý účastník nebo uživatel služby elektronických komunikací jasně a úplně informován, pokud nebyl předem informován, správcem nebo jeho zástupcem:

1) o účelu každé činnosti, jejímž cílem je získat elektronickým přenosem přístup k informacím, které jsou již uloženy v jeho koncovém zařízení; elektronických komunikací, nebo zapsat informace do tohoto zařízení;

2) o prostředcích, které má k dispozici, aby se proti tomu bránil.“

8) <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179> (přístup 26. 3. 2023).

9) [https://gdprhub.eu/index.php?title=CNIL \(France\) - Deliberation SAN-2022-024 of December 20, 2022](https://gdprhub.eu/index.php?title=CNIL%20(France)%20-%20Deliberation%20SAN-2022-024%20of%20December%2020,%202022) (přístup 19. 3. 2023).

Příslušná studie je dostupná na <https://www.commandersact.com/en/barometer-privacy-2021-impact-market/> (přístup 27. 3. 2023).

U přístupů z mobilních telefonů nebyl vliv takový.