ČESKÁ REPUBLIKA

ROZSUDEK JMÉNEM REPUBLIKY

Nejvyšší správní soud rozhodl v senátu složeném z předsedkyně JUDr. Lenky Kaniové a soudců JUDr. Josefa Baxy a JUDr. Ivo Pospíšila v právní věci žalobce: **Internet Mall, a.s.,** se sídlem U Garáží 1611/1, Praha 7, zastoupen Mgr. Luďkem Šrubařem, advokátem se sídlem Hanusova 1537/1, Praha 4, proti žalovanému: **Úřad pro ochranu osobních údajů,** se sídlem pplk. Sochora 27, Praha 7, o žalobě proti rozhodnutí předsedkyně žalovaného ze dne 21. 9. 2018, č. j. UOOU-04073/18-11, v řízení o kasační stížnosti žalobce proti rozsudku Městského soudu v Praze ze dne 24. 6. 2021, č. j. 6 A 188/2018 - 57,

takto:

I. Rozsudek Městského soudu v Praze ze dne 24. 6. 2021, č. j. 6 A 188/2018 - 57, **se zrušuje.**

II. Rozhodnutí předsedkyně Úřadu pro ochranu osobních údajů ze dne 21. 9. 2018, č. j. UOOU-04073/18-11, **se zrušuje** a věc **se vrací** žalovanému k dalšímu řízení.

III. Žalovaný **nemá** právo na náhradu nákladů řízení o žalobě ani kasační stížnosti.

IV. Žalovaný je **povinen** uhradit žalobci k rukám jeho zástupce Mgr. Luďka Šrubaře, advokáta se sídlem Hanusova 1537/1, Praha 4, na náhradě nákladů řízení částku ve výši 25.456 Kč, a to do 30 dnů od právní moci tohoto rozsudku.

Odůvodnění:

I. Vymezení věci

[1] Předmětem sporu v projednávané věci je výklad § 13 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a zodpovězení otázky, zda se žalobce dopustil přestupku podle § 45 odst. 1 písm. h) téhož zákona.

[2] Žalovaný uznal žalobce rozhodnutím ze dne 23. 5. 2018, č. j. UOOU-04073/18-5 (dále jen „prvostupňové rozhodnutí“), vinným ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů, jehož se měl dopustit tím, že nepřijal opatření pro zajištění bezpečnosti zpracovávaných osobních údajů. Konkrétně bylo zjištěno, že žalobce nezabezpečil osobní údaje nejméně 735 956 zákazníků v rozsahu jméno, příjmení, e-mailová adresa, heslo uživatelského účtu, případně telefonní číslo před neoprávněným přístupem v období minimálně od 31. prosince 2014 do srpna 2017, v důsledku čehož došlo v době od 27. července 2017 do 25. srpna 2017 k jejich zpřístupnění na internetových stránkách www.ulozto.cz. Tímto jednáním žalobce porušil povinnost stanovenou v § 13 odst. 1 zákona o ochraně osobních údajů. Za spáchání uvedeného přestupku mu žalovaný uložil pokutu ve výši 1.500.000 Kč.

[3] Žalobce podal proti prvostupňovému rozhodnutí rozklad, který předsedkyně žalovaného rozhodnutím ze dne 21. 9. 2018, č. j. UOOU-04073/18-11, zamítla.

II. Rozsudek městského soudu

[4] Žalobce se dále bránil správní žalobou, kterou Městský soud v Praze (dále jen „městský soud“) v záhlaví specifikovaným rozsudkem zamítl.

[5] Předně neshledal, že by byla správní rozhodnutí nepřezkoumatelná či dokonce nicotná. Pokud se jedná o zákonnost napadeného rozhodnutí, zdůraznil, že žalobce odcizení osobních údajů po dobu několika let vůbec nezaznamenal, a to, že k němu došlo, zjistil náhodou. Nadto došlo ke zneužití dat, která se nezjištěnému subjektu podařilo dešifrovat a zveřejnit. Již z těchto skutečností je zjevné, že žalobcem přijatá opatření byla neúčinná. Soud přitom považoval za nerozhodné, že k prolomení zabezpečení šifrovaných údajů zřejmě došlo až po několika letech díky technologickému vývoji. Šifrování musí být vždy provedeno tak, aby zabránilo zneužití dat. To se v daném případě nestalo, pročež soud nepřisvědčil tvrzení žalobce, že provedení šifrování představovalo okolnost, která jej zbavovala odpovědnosti za daný delikt.

[6] Soud dále uvedl, že povinnost chránit osobní údaje nemůže být absolutní, neboť z podstaty věci nelze předvídat všechny potenciální scénáře, které mohou nastat. Vždy je proto třeba zohlednit adekvátnost učiněných opatření ze strany správce údajů. To však žalovaný učinil a shledal, že opatření jako celek nedosáhla potřebné úrovně. Jako měřítko přiměřenosti žalovaný uplatnil skutečnost, že pro vznik deliktní odpovědnosti není rozhodné, zda k neoprávněnému přístupu či ke zneužití osobních údajů skutečně došlo. Skutková podstata je naplněna již nepřijetím nezbytných opatření. Nebylo-li detekováno bezpečnostní riziko ani po odcizení dat, nemohla být přijatá opatření dostatečně kvalitní. Žalovaný nemusel komentovat jednotlivá žalobcem přijatá opatření a jejich dostatečnost, neboť vycházel ze skutečnosti, že zákonná dikce ponechává způsob a prostředky zabezpečení na vlastní úvaze správců a klade důraz pouze na výsledný účinek. Ten považoval žalovaný v posuzovaném případě za nedostatečný.

[7] Soud nepřisvědčil ani tvrzení žalobce, že žalovaný nezkoumal všechny znaky přestupku a nesprávně dovodil naplnění skutkové podstaty přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů. Za nedůvodnou označil i námitku existence liberačních důvodů. Uvedl, že liberační důvody jsou určené pouze pro aplikaci ve výjimečných případech. Žalobce v této souvislosti neunesl důkazní břemeno, neboť ani žalovanému ani městskému soudu nepodal důkaz o provedení takových opatření, která by představovala maximální možné úsilí směřující k zabránění vzniku bezpečnostní události.

[8] Soud se zabýval rovněž námitkou prekluze odpovědnosti za přestupek. Ztotožnil se s názorem žalovaného, že se jednalo o trvající delikt, neboť k ukončení protiprávního stavu

došlo až přijetím nových opatření pro zabezpečení osobních údajů, k čemuž žalobce přikročil až po zveřejnění odcizené databáze. Protiprávní stav tedy trval minimálně od 31. 12. 2014 do srpna 2017. Lhůta pro uložení pokuty či zahájení správního řízení tedy počala běžet až od okamžiku ukončení trvajícího protiprávního stavu a k prekluzi proto nedošlo.

[9] Konečně se soud zabýval i přiměřeností uložené pokuty. Uvedl, že odůvodnění výše pokuty v prvostupňovém rozhodnutí je stručné, ale obstojí. Žalovaný uložil žalobci pokutu na úrovni méně než třetiny zákonného rozmezí. Soud považoval porušení povinností za závažné, přičemž poukázal i na skutečnost, že žalobce je profesionálem v oboru a provádí rozsáhlé zpracování osobních údajů včetně uživatelských hesel. Na druhou stranu přihlédl soud k iniciativě žalobce při nápravě nezákonného stavu. S ohledem na všechny konkrétní okolnosti pak neshledal, že by byla pokuta uložena v nepřiměřené výši.

III. Obsah kasační stížnosti

[10] Žalobce (stěžovatel) podal proti rozsudku městského soudu kasační stížnost z důvodu podle § 103 odst. 1 písm. a) zákona č. 150/2002 Sb., soudní řád správní (dále jen „ s. ř. s."). Má za to, že soud nesprávně vyložil § 45 odst. 1 písm. h) zákona o ochraně osobních údajů ve spojení s § 13 odst. 1 téhož zákona.

[11] Soud vycházel ze skutečnosti, že přestupek podle citovaného ustanovení je konstruován jako odpovědnost za následek, jímž je ohrožení bezpečnosti zpracovávaných osobních údajů. S tímto závěrem se však stěžovatel neztotožňuje a domnívá se, že uvedený výklad je v rozporu s textem zákona a úmyslem zákonodárce. Dotčené ustanovení vychází z norem evropského práva, jejichž autoři si byli vědomi toho, že veškerá bezpečnostní opatření jsou vždy pozadu za jakýmikoliv hrozbami, pročež antivirové, ani jiné softwarové prostředky nikdy neposkytnou 100% ochranu. To lze ostatně ilustrovat i na sérii kybernetických útoků, jimiž byla zasažena např. některá zdravotnická zařízení v ČR. Výklad aplikovaný městským soudem by znamenal, že veškeré subjekty, které byly obětí takových útoků, by se dopustily přestupku, bez ohledu na to, jaká opatření reálně přijaly. Pokud se jedná o zmiňovaná zdravotnická zařízení, ta měla oproti stěžovateli „výhodu", neboť osoby, které data odcizily, jim znemožnily přístup k těmto datům a současně požadovaly výkupné. Proto se dotčené subjekty o útoku (na rozdíl od stěžovatele) dozvěděly. Pouze v případě, kdy by se stěžovatel o úniku dat dozvěděl ihned, by pak dle logiky městského soudu přicházelo v úvahu, aby se žalovaný zabýval jím přijatými opatřeními. Takový přístup je zcela chybný a stěžovatel trvá na tom, že pro naplnění skutkové podstaty uvedeného přestupku není podstatné, zda se osobní údaje podařilo ochránit či nikoliv, ale jaká opatření subjekt za účelem ochrany osobních údajů přijal.

[12] Podle § 13 zákona o ochraně osobních údajů pak není povinností správce údajů přijmout za účelem jejich ochrany všechna myslitelná opatření. Tento výklad koresponduje i s textem nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 (dále jen „obecné nařízení"), přičemž městský soud dospěl k závěru, že aplikace uvedeného předpisu není na místě, protože je pro stěžovatele přísnější. Pokud tedy ani přísnější předpis nepožaduje přijetí veškerých možných opatření, stěží lze uvedený výklad přijmout v nynější věci. Proto je nezbytné zabývat se povahou přijatých opatření. Pouze na základě jejich posouzení lze učinit závěr o odpovědnosti za přestupek podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů. Stěžovatel předložil žalovanému i městskému soudu bohaté penzum důkazů ohledně přijatých opatření, ani jeden z nich k nim však nepřihlédl. Jedinou výjimku představuje problematika šifrování, které však soud považoval za nedostatečné, byť k jeho prolomení došlo až po několika letech. Skutečnost, že k prolomení šifrování došlo až se značným časovým odstupem, přitom dle mínění stěžovatele

prokazuje, že v rozhodném období bylo zcela dostatečné. V době, kdy se ho neznámému hackerovi podařilo prolomit, již používal žalobce zcela jiný, pokročilejší typ zabezpečení.

[13] Stěžovatel je přesvědčený, že jím doložená opatření (která vyjmenoval i v kasační stížnosti, Nejvyšší správní soud je však nepovažuje za nezbytné na tomto místě rekapitulovat) mají dostatečnou kvalitu pro to, aby mohla být posouzena jako adekvátní opatření dle § 13 zákona o ochraně osobních údajů. Proto vůbec nedošlo k naplnění skutkové podstaty přestupku podle § 45 téhož zákona. Pro případ, že by kasační soud této argumentaci nepřisvědčil, uvádí stěžovatel, že přijatá opatření obstojí i jako liberační důvod dle § 21 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

[14] Pro úplnost stěžovatel poukazuje i na nedostatečné odůvodnění výše uložené pokuty, které z většiny sestává pouze z obecných formulací. Tvrzení soudu, že je profesionálem v oboru, považuje stěžovatel za zavádějící, neboť osobní údaje zpracovává výlučně proto, aby mohl provozovat svoji podnikatelskou činnost, která spočívá v prodeji zboží.

[15] Stěžovatel tedy navrhuje, aby Nejvyšší správní soud rozsudek městského soudu zrušil a věc mu vrátil k dalšímu řízení.

IV. Vyjádření žalovaného

[16] Žalovaný k obsahu kasační stížnosti uvádí, že prvotním smyslem § 13 odst. 1 zákona o ochraně osobních údajů sice bylo stanovení povinnosti přijmout určitá opatření. Tato opatření však musí mít takovou kvalitu, aby zabránila zneužití osobních údajů. Jak potvrdil i městský soud, v případě § 45 odst. 1 písm. h) citovaného zákona se jedná o tzv. ohrožovací delikt a pro vznik odpovědnosti tedy postačí potencialita ohrožení chráněného objektu. Výklad zastávaný stěžovatelem považuje žalovaný za lichý, neboť jeho přijetí by vedlo k nepřiměřenému zúžení okruhu postižitelných jednání.

[17] Žalovaný dále poukazuje na specifické skutkové okolnosti případu, které spočívají v tom, že došlo k odcizení databáze obsahující údaje o více než 700 000 zákazníků stěžovatele. Tento únik přitom nebyl v reálném čase zjištěn a stěžovatel jej neodhalil ještě několik následujících let. Takto se stalo až po zpřístupnění údajů na internetových stránkách www.ulozto.cz. Je tedy zjevné, že stěžovatelem přijatá opatření byla jako celek neúčinná a k naplnění skutkové podstaty přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů došlo. Za panujícího skutkového stavu nelze uvažovat ani o naplnění liberačních důvodů.

[18] Tvrzení stěžovatele, že k prolomení zabezpečení šifrované části databáze došlo až o několik let později, je pouhou spekulací (nebylo zjištěno, kdy k prolomení došlo) a nejedná se o relevantní okolnost. Pokud se jedná o stěžovatelem odkazované obecné nařízení, to je třeba vykládat stejně jako dřívější právní úpravu. Navíc však umožňuje uložit za obdobné jednání podstatně přísnější sankci.

[19] Žalovaný má rovněž za to, že dostatečným způsobem odůvodnil výši uložené pokuty. K tomu dodává, že stěžovatel patří mezi největší internetové nákupní galerie. Zpracování osobních údajů zákazníků proto tvoří imanentní součást jeho podnikatelské činnosti. Žalovanému je nadto z jeho úřední činnosti známo, že stěžovatel osobní údaje zpracovává i pro marketingové účely.

[20] Z uvedených důvodů žalovaný navrhuje, aby Nejvyšší správní soud kasační stížnost jako nedůvodnou zamítl.

V. Posouzení věci Nejvyšším správním soudem

[21] Nejvyšší správní soud posuzoval splnění podmínek řízení, přičemž shledal, že kasační stížnost byla podána včas, osobou oprávněnou a jedná se o kasační stížnost, která je ve smyslu § 102 s. ř. s. přípustná. Důvodnost kasační stížnosti posoudil v mezích jejího rozsahu a uplatněných důvodů, současně zkoumal, zda napadené rozhodnutí netrpí vadami, k nimž by byl nucen přihlédnout z úřední povinnosti (§ 109 odst. 3 a 4 s. ř. s.).

[22] Kasační stížnost je důvodná.

[23] V posuzované věci není sporné, že stěžovatel nezabránil neoprávněnému přístupu k osobním údajům (blíže specifikovaným v bodě [2] tohoto rozsudku) více než 700 tisíc jeho zákazníků. Odcizení údajů pak odhalil až se značným časovým odstupem, a to v návaznosti na jejich zveřejnění na internetových stránkách www.ulozto.cz. Stěžovatel nicméně v kasační stížnosti zpochybnil, že tyto skutečnosti samy o sobě postačují k tomu, aby jej žalovaný uznal vinným ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů. Domnívá se, že jak žalovaný, tak městský soud interpretovali citované ustanovení chybně, a trvá na tom, že bylo povinností žalovaného zkoumat, jaká opatření stěžovatel za účelem předejití neoprávněného přístupu k osobním údajům přijal.

[24] Nejvyšší správní soud předesílá, že v posuzované věci vycházeli žalovaný i městský soud z dřívější (dnes již neúčinné) právní úpravy. Městský soud se mimo jiné zabýval otázkou, zda není na místě použití pozdějších předpisů, dovodil však, že úprava obsažená v obecném nařízení by byla pro stěžovatele přísnější. Proto vycházel ze zákona o ochraně osobních údajů (jakož i z norem evropského práva), ve znění účinném v době spáchání přestupku. Relevantní ustanovení dotčených právních předpisů rekapituluje kasační soud níže.

[25] Podle § 13 odst. 1 zákona o ochraně osobních údajů *„[s]právce a zpracovatel jsou 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.“*

[26] Podle § 45 odst. 1 písm. h) téhož zákona *„[p]rávnická nebo podnikající fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů (§ 13)[.]*

[27] Uvedená úprava je odrazem (již zrušené) směrnice Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice 95/46/ES“), jejíž čl. 17 odst. 1 zněl: *„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. Tato opatření mají zajistit, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.*

[28] Pokud se jedná o pozdější právní úpravu, kasační soud připomíná především čl. 24 odst. 1 obecného nařízení, který stanoví, že „[s] *přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.*“

[29] Podle čl. 32 odst. 1 nařízení pak platí, že „[s] *přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.*“ Čl. 32 odst. 2 nařízení dále předepisuje, že „[p]*ři posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.*

[30] Nejvyšší správní soud se výkladem citované právní úpravy částečně zabýval v několika svých rozhodnutích. Již v rozsudku ze dne 10. 5. 2006, č. j. 3 As 21/2005 - 105, upozornil, že znění § 13 odst. 1 zákona o ochraně osobních údajů klade na správce a zpracovatele osobních údajů vysoké nároky, neboť na jednu stranu ponechává způsob a prostředky zabezpečení na jejich vlastní úvaze, na stranu druhou však v případě nedostatečnosti opatření stanoví poměrně vysoké sankce.

[31] V rozsudku ze dne 30. 1. 2013, č. j. 7 As 150/2012 - 35, dále zdůraznil, že směrnice 95/46/ES obsahuje pravidla vyznačující se jistou pružností, přičemž ponechává na členských státech, jakým způsobem podrobně upraví povinnosti dotčených subjektů. Z judikatury Soudního dvora EU však vyplývá, že je třeba posuzovat, zda byla vnitrostátní opatření přijata a aplikována v rámci směrnicí nastaveného prostoru pro uvážení. V tomto ohledu jsou členské státy limitovány zejména požadavkem proporcionality vyplývajícím právě z čl. 17 směrnice (srov. např. rozsudky ve věcech C-101/01 *Lindqvist*, body 83-85; a C-468/10 a C-469/10 *ASNEF*, body 35-36).

[32] Pokud se jedná o nyní projednávanou věc, je zjevné, že městský soud považoval za zásadní, zda došlo k ochraně osobních údajů, potažmo zda stěžovatel zneužití osobních údajů včas odhalil. Vzhledem k tomu, že se tak nestalo, nebylo dle něj zapotřebí zabývat se kvalitou stěžovatelem přijatých opatření. Jinak řečeno, pokud stěžovatel osobní údaje neochránil a ani včas nezjistil, že k odcizení došlo, je dle mínění městského soudu bez dalšího zjevné, že jím přijatá opatření byla nedostatečná. Na podporu svého tvrzení poukázal i na skutečnost, že přestupek dle § 45 odst. 1 písm. h) představuje tzv. ohrožovací delikt, pročež postačí, pokud pouze hrozí (v důsledku nedostatečných opatření) neoprávněné nakládání s osobními údaji. Jestliže však k uvedenému negativnímu následku v posuzované věci došlo, neměl městský soud o naplnění skutkové podstaty přestupku pochyb.

[33] Se zde nastíněným výkladem se však Nejvyšší správní soud neztotožňuje. S žalovaným a městským soudem lze souhlasit potud, že pro vznik odpovědnosti za přestupek podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů postačí ohrožení bezpečnosti osobních údajů. Znakem skutkové podstaty dotčeného přestupku tedy není existence následku v podobě neoprávněného nakládání s osobními údaji (viz rozsudek Nejvyššího správního soudu ze dne 28. 12. 2016, č. j. 3 As 121/2014 - 35). To však ještě neznamená, že by existence takového následku vedla bez dalšího k závěru, že správce či zpracovatel osobních údajů si počínal v rozporu s § 13 odst. 1 zákona o ochraně osobních údajů. Posledně citované ustanovení upravuje povinnost „*přijmout taková opatření, aby nemohlo dojít 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*“. Přestože jeho dikce vyznívá poněkud striktně, nelze z ní činit kategorický závěr, že za dostatečná lze považovat pouze taková opatření, která v každém myslitelném případě zabrání zneužití osobních údajů. Nejvyšší správní soud zdůrazňuje, že nelze vycházet toliko z jazykového výkladu, ale je třeba mít na zřeteli rovněž smysl a účel citovaného ustanovení. V této souvislosti poslouží jako výkladové vodítko evropská úprava, v níž nachází citované ustanovení svůj předobraz. Čl. 17 odst. 1 směrnice 95/46/ES

pak hovoří o nutnosti přijetí *„vhodných opatření“*, která mají zajistit *„s ohledem na stav techniky a na náklady na jejich provedení přiměřenou úroveň bezpečnosti“*. Uvedená úprava tedy nevyznívá ani zdaleka tak přísně jako § 13 odst. 1 zákona o ochraně osobních údajů.

[34] Jak kasační soud vyložil již v rozsudku č. j. 7 As 150/2012 - 35, směrnice 95/46/ES sice ponechávala členským státům jistou volnost v tom, jakým způsobem upraví povinnosti správců a zpracovatelů osobních údajů. Členské státy jsou však limitovány právě kritériem přiměřenosti vyplývajícím z čl. 17 směrnice (viz bod [31] tohoto rozsudku). Nejvyšší správní soud je tedy přesvědčený, že § 13 odst. 1 zákona o ochraně osobních údajů je třeba vykládat souladně s tímto článkem směrnice, který nepředpokládá, že by odpovědnost správců a zpracovatelů osobních údajů byla bezbřehá, ale klade důraz na to, aby dotčené subjekty vynaložily za účelem ochrany osobních údajů náležité úsilí.

[35] K velmi obdobným závěrům ostatně kasační soud dospěl již v rozsudku ze dne 27. 6. 2019, č. j. 4 As 140/2019 - 27, který se zabýval srovnáním úpravy obsažené v obecném nařízení a § 13 odst. 1 zákona o ochraně osobních údajů. Přitom vyslovil, že citované ustanovení nelze vykládat tak, že „*stanoví ‚absolutistický‘ požadavek na zabezpečení osobních údajů oproti čl. 24 a čl. 32* [obecného nařízení], *které hovoří o ‚vhodných opatřeních‘ a ‚vhodné úrovni bezpečnosti‘.*“ Obecné opatření, stejně jako před ním směrnice 95/46/ES povinnosti dotčených subjektů relativizuje (nečiní je zcela absolutními) a obdobným způsobem je třeba přistupovat rovněž k interpretaci § 13 odst. 1 zákona o ochraně osobních údajů. Takový postup je ostatně zcela logický, neboť jak správně poznamenal městský soud v bodě 60 rozsudku, správce či zpracovatel osobních údajů nemůže předvídat všechny potenciální scénáře, které mohou nastat. Městský soud nicméně ihned vzápětí svoji tezi popřel, neboť dovodil, že stěžovatel svým povinnostem nemohl dostát, jelikož jím přijatá opatření nezabránila bezpečnostnímu incidentu a ani jej neodhalila. Takový závěr považuje Nejvyšší správní soud za vskutku absurdní. Je třeba si uvědomit, že v nyní projednávané věci žalovaný nezjistil (a zřejmě ani nezjišťoval) jakým způsobem k úniku dat došlo. Současně se odmítl zabývat tím, jaká byla kvalita opatření, která stěžovatel přijal a dodržoval v době odcizení dat. Žalovaný tedy stěžovatele shledal vinným ze spáchání přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů, ačkoliv neznal žádnou ze stran rovnice, z nichž jednu tvoří právě opatření za účelem ochrany osobních údajů, druhou pak způsob odcizení dat ze strany neznámého subjektu.

[36] Nejvyšší správní soud nezpochybňuje, že primárním smyslem a účelem § 13 odst. 1 zákona o ochraně osobních údajů je zajištění bezpečnosti osobních údajů. Na zpracovatele a správce osobních údajů však nelze přenášet neomezenou odpovědnost za jakoukoliv (mnohdy i protiprávní či dokonce trestnou) činnost jiných subjektů. Tento požadavek se obzvlášť silně projevuje právě v oblasti kybernetických útoků, o nějž se zřejmě mohlo jednat i v projednávané věci (žalovaný se k této otázce žádným způsobem nevyjádřil, tvrzení stěžovatele nicméně nezpochybnil). Ačkoliv totiž musel být stěžovatel připraven i na možnost takového protiprávního jednání, stěží lze očekávat, že jím přijatá bezpečnostní opatření budou natolik silná, aby byla schopná odrazit případně i sofistikovaný a cílený kybernetický útok.

[37] Kasační soud připomíná, že odpovědnost za přestupek podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů není vázána na vznik poruchového negativního následku spočívajícího v neoprávněném nakládání s osobními údaji, ale na zjištěný deficit v přijetí náležitých opatření za účelem jejich ochrany. Jinak řečeno, pro vznik odpovědnosti za přestupek není rozhodující, zda se osobní údaje v konečném důsledku podaří ochránit či nikoliv (na což správně poukázal i stěžovatel). V praxi to pak znamená, že přestupku podle citovaného ustanovení se dopustí osoba, která nepřijme dostatečná opatření za účelem ochrany osobních údajů, a to i v situaci, kdy k neoprávněnému nakládání s těmito údaji nedojde. Častější variantu pak bude představovat

situace, kdy k negativnímu následku v podobě neoprávněného nakládání s údaji dojde. V takovém případě se však musí žalovaný zabývat tím, jaká opatření dotčený subjekt přijal a dodržoval. Byla-li opatření nedostatečná, nastupuje odpovědnost za uvedený přestupek. Pakliže však opatření odpovídají kritériím vyplývajícím z čl. 17 směrnice 95/46/ES, potažmo čl. 24 odst. 1 a čl. 32 odst. 1 obecného nařízení, a přesto k porušení bezpečnosti osobních údajů dojde, nejsou znaky přestupku podle § 45 odst. 1 písm. h) naplněny a odpovědnost za přestupek nevzniká. Za náležitá je přitom potřeba (s ohledem na odkazovanou evropskou úpravu) považovat především taková opatření, která zajišťují přiměřenou úroveň ochrany, a to s ohledem na stav techniky a náklady na jejich provedení. Přiměřenost a vhodnost opatření je pak nezbytné vnímat rovněž jako kategorii, jejíž obsah se bude také odvíjet od rozsahu a obsahu zpracovávaných údajů.

[38] V případě stěžovatele, který je významným subjektem na trhu zpracovávajícím osobní údaje řádově minimálně několika set tisíc osob (jak je patrné z nyní projednávané věci), pak budou požadavky na přijatá opatření nesrovnatelně vyšší, než kupříkladu u subjektů které zpracovávají osobní údaje pouze jednotek osob (např. vlastních zaměstnanců). Nejvyšší správní soud tedy nemá pochyb o tom, že stěžovatel měl předvídat i případné riziko kybernetického útoku. To však neznamená, že musel být schopen se jakémukoliv obdobnému jednání skutečně ubránit. Z tohoto důvodu bylo povinností žalovaného, aby se zabýval přijatými opatřeními a zjistil, nakolik odpovídala dostupné úrovni ochrany v rozhodném období. Pouze ze skutečnosti, že k odcizení údajů došlo (aniž by tuto skutečnost stěžovatel toho času zjistil), nelze dovozovat nedostatečnost přijatých opatření, a to zejména za situace, kdy žalovaný ani nemá povědomost o tom, jakým způsobem k odcizení údajů došlo a nakolik bylo jednání případného hackera (či jiné osoby, která údaje získala) sofistikované. Jakkoliv zřejmě nemusí být v možnostech žalovaného zjistit, jak přesně a za použití jakých prostředků k neoprávněnému přístupu do databáze osobních údajů došlo, nepochybně je schopen za použití výše uvedených hledisek vyhodnotit kvalitu stěžovatelem přijatých a dodržovaných opatření. Jak totiž sám uvádí ve vyjádření ke kasační stížnosti, touto problematikou se dlouhodobě zabývá a je v ní náležitě orientovaný.

[39] Žalovaný ani městský soud se však opatřeními, která stěžovatel dokládal, žádným způsobem nezabývali a nevyjádřili se k nim. Dílčí výjimku představuje problematika šifrování, jíž se městský soud věnoval především v bodech 58 a 59 rozsudku s tím, že šifrování bylo zjevně nedostatečné, neboť se jej podařilo prolomit. Přitom nepovažoval za rozhodné, zda se tak stalo až s odstupem několika let. S touto argumentací se nicméně Nejvyšší správní soud neztotožňuje, neboť má ve shodě se stěžovatelem za to, že s ohledem na technologický pokrok je požadavek na absolutní neprolomitelnost šifrování (kdykoliv do budoucna) zcela nesplnitelný. Ačkoliv žalovaný uvádí, že tvrzení o prolomení šifrování až několik let po odcizení databáze je čirou spekulací, nelze popřít, že městský soud s touto domněnkou v rámci své argumentace pracoval a použil ji na podporu své argumentace.

[40] Kasační soud dodává, že nedostatky výkladu zastávaného žalovaným (a aprobovaného městským soudem) lze ilustrovat i na skutečnosti, že stěžovatele shledal vinným ze spáchání trvajícího přestupku. Přitom za počátek protiprávního stavu považoval okamžik odcizení osobních údajů, za jeho konec pak přijetí nových opatření v srpnu roku 2017. Je tedy zjevné, že protiprávní stav žalovaný spojoval s existencí nedostatečných opatření za účelem ochrany osobních údajů, to však za situace, kdy se kvalitou těchto opatření vůbec nezabýval (jejich nedostatečnost dovodil toliko ze vzniku bezpečnostního incidentu, resp. ze samotného nepříznivého následku, jímž byl únik osobních údajů a jejich zveřejnění), ani neřešil otázku, zda v mezidobí (od odcizení osobních údajů do jejich zveřejnění) nepřijal stěžovatel opatření nová. Obdobně pak podrobněji nevysvětlil, v čem jsou opatření přijatá v srpnu roku 2017 vhodnější, a zda by zabránila opakování bezpečnostního incidentu.

[41] Nejvyšší správní soud tedy shrnuje, že městský soud a žalovaný pochybili, neboť vycházeli z chybného předpokladu, že k naplnění skutkové podstaty přestupku podle § 45 odst. 1 písm. h) zákona o ochraně osobních údajů postačí, došlo-li k neoprávněnému přístupu k osobním údajům a současně stěžovatel tuto skutečnost v rozhodné době neodhalil. Zákon o ochraně osobních údajů totiž nestanoví absolutní povinnost k ochraně osobních údajů a vznik odpovědnosti za uvedený přestupek neváže na vznik nepříznivého následku, ale na nepřijetí náležitých opatření za účelem zajištění bezpečnosti osobních údajů (§ 13 odst. 1 zákona o ochraně osobních údajů). Za daných okolností si tedy žalovaný i městský soud počínali v rozporu se zásadou *nullum crimen sine lege*, podle níž může být přestupkem pouze takové jednání, u něhož tak zákon výslovně stanoví.

[42] Pro úplnost soud doplňuje, že projednávaná věc se naprosto zásadně odlišuje od případu posuzovaného v rozsudku ze dne 28. 12. 2016, č. j. 3 As 121/2014 - 35 (na který odkazoval žalovaný), v němž tento soud dovodil, že pokud v několika případech prokazatelně došlo k neoprávněnému nakládání s osobními údaji (neprovedení likvidace dokladů, ale pouze jejich vyhození na skládku), svědčí již sama o sobě tato skutečnost o tom, že přijatá opatření byla nedostatečná. V odkazované věci se totiž jednalo o chybný postup na straně správce či zpracovatele osobních údajů, který odpovídá za likvidaci dokladů s osobními údaji, a tato činnost je přímo v jeho dispozici. Odpovědnosti za její řádné provedení se přitom nemohl zprostit přenesením uvedené činnosti na třetí osobu na základě soukromoprávního jednání (smlouvy). V nyní projednávané věci se jedná o situaci od základu odlišnou, neboť k neoprávněnému přístupu k osobním údajům došlo zjevně v důsledku cíleného protiprávního jednání jiného subjektu. Stěžovatel přitom sice musí obdobné jednání předvídat, nemůže však za něj nést automaticky odpovědnost bez ohledu na to, jaká opatření za účelem ochrany osobních údajů přijal, a nakolik promyšlený a propracovaný byl útok neznámého subjektu, který údaje z databáze odcizil.

[43] Nejvyšší správní soud tedy souhlasí se stěžovatelem, že rozsudek městského soudu trpí vadou ve smyslu § 103 odst. 1 písm. a) s. ř. s., neboť soud nesprávně posoudil rozhodnou právní otázku. Vzhledem k tomu, že v zásadě z totožného chybného právního náhledu vycházel již žalovaný, nepovažuje kasační soud za účelné vracet věc k dalšímu řízení městskému soudu, ale bez dalšího přikročil i ke zrušení napadeného správního rozhodnutí. Soud přitom nepředjímá výsledek správního řízení a nečiní jakékoliv závěry ohledně toho, zda se stěžovatel přestupku dopustil či nikoliv. Bude však na žalovaném, aby zohlednil všechna stěžovatelem přijatá opatření a zabýval se tím, jestli byla s ohledem na dostupnou úroveň ochrany v rozhodném období, charakter činnosti stěžovatele a rozsah jím zpracovávaných údajů dostatečná. V této souvislosti by měl přihlédnout také ke kritériím vyplývajícím z evropské úpravy.

[44] Pro úplnost soud dodává, že se nezabýval námitkou týkající se nepřiměřenosti uložené sankce, neboť dosud nebylo ani postaveno na jisto, zda se stěžovatel přestupku dopustil. V této fázi by tedy bylo posuzování přiměřenosti výše pokuty předčasné.

VI. Závěr a náklady řízení

[45] Nejvyšší správní soud považuje kasační stížnost za důvodnou, a proto rozsudek městského soudu zrušil (§ 110 odst. 1 s. ř. s.) a současně za použití § 110 odst. 2 písm. a) s. ř. s. zrušil i napadené rozhodnutí předsedkyně žalovaného a věc vrátil žalovanému k dalšímu řízení (§ 78 odst. 3 a 4 s. ř. s.). Žalovaný je vázán právním názorem vysloveným Nejvyšším správním soudem v tomto zrušujícím rozhodnutí (§ 110 odst. 2 s. ř. s. ve spojení s § 78 odst. 5 s. ř. s.).

[46] Nejvyšší správní soud je soudem, který o věci rozhodl jako poslední, proto musí určit náhradu nákladů soudního řízení. Ve vztahu k výsledku celého soudního řízení je pak nutno posuzovat procesní úspěšnost účastníků řízení. Podle § 60 odst. 1 s. ř. s. ve spojení s § 120 s. ř. s. má úspěšný účastník právo na náhradu důvodně vynaložených nákladů proti účastníku řízení, který úspěch ve věci neměl. Ve věci měl úspěch žalobce, pročež mu soud přiznal náhradu nákladů řízení.

[47] Náklady řízení spočívají v prvé řadě v náhradě za zaplacený soudní poplatek ve výši 4.000 Kč v řízení o žalobě (3.000 Kč podání žaloby, 1.000 Kč návrh na přiznání odkladného účinku) a 5.000 Kč v řízení o kasační stížnosti.

[48] Stěžovatel byl v řízení o žalobě i o kasační stížnosti na základě plné moci zastoupen advokátem Mgr. Luďkem Šrubařem, který učinil čtyři úkony právní služby - převzetí a příprava zastoupení, sepsání žaloby, účast na ústním jednání a sepsání kasační stížnosti [§ 11 odst. 1 písm. a), d) a g) vyhlášky č. 177/1996 Sb., o odměnách advokátů a náhradách advokátů za poskytování právních služeb (advokátní tarif)]. Za tyto úkony náleží odměna ve výši 4 x 3.100 Kč [§ 7, § 9 odst. 4 písm. d) advokátního tarifu], a paušální částka ve výši 4 x 300 Kč (§ 13 odst. 4 advokátního tarifu). Vzhledem tomu, že uvedený advokát jen plátcem DPH, zvýšil soud částku odměny o příslušnou daň. Náklady za právní zastoupení proto činí 16.456 Kč.

[49] Žalovaný je tedy povinen uhradit stěžovateli na náhradě nákladů řízení celkovou částku 25.456 Kč, a to ve lhůtě stanovené ve výroku IV tohoto rozsudku, k rukám jeho zástupce.

P o u č e n í : Proti tomuto rozhodnutí **n e j s o u** opravné prostředky přípustné.

V Brně dne 11. listopadu 2021

JUDr. Lenka Kaniová
předsedkyně senátu