ČESKÁ REPUBLIKA

ROZSUDEK JMÉNEM REPUBLIKY

Nejvyšší správní soud rozhodl v senátu složeném z předsedy Ivo Pospíšila, soudkyně Sylvy Šiškeové a soudce Petra Pospíšila v právní věci žalobce: **J. H.**, zastoupen Mgr. Rebekou Moťovskou Židuliakovou, advokátkou se sídlem Husovo náměstí 139, Ledeč nad Sázavou, proti žalovanému: **Krajský úřad Ústeckého kraje**, sídlem Velká Hradební 3118/48, Ústí nad Labem, o žalobě proti rozhodnutí žalovaného ze dne 3. 1. 2025, č. j. KUUK/000227/2025, v řízení o kasační stížnosti žalobce proti rozsudku Krajského soudu v Ústí nad Labem ze dne 10. 12. 2025, č. j. 141 A 13/2025 - 29,

takto:

I. Kasační stížnost **se zamítá**.

II. Žalobce **nemá právo** na náhradu nákladů řízení o kasační stížnosti.

III. Žalovanému se náhrada nákladů řízení o kasační stížnosti **nepřiznává**.

Odůvodnění:

I. Vymezení věci

[1] V projednávané věci se Nejvyšší správní soud zabýval neposkytnutím IP adresy prvního serveru, na který rychloměr zasílá fotografie zaznamenaných vozidel, a to z důvodu, že by to mohlo ohrozit bezpečnostní opatření [§ 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím].

[2] Žalobce podal u statutárního města Chomutov (povinná osoba) žádost podle zákona o svobodném přístupu k informacím. Požadoval informace vztahující se k rychloměru umístěnému na ulici Písečná v Chomutově (provozovatel, způsob fungování, technická specifikace, přenos dat a počet změřených vozidel). Povinná osoba na všechny otázky odpověděla, odmítla však sdělit IP adresu prvního serveru, na který rychloměr přenáší

pořízené snímky. V následně vydaném rozhodnutí povinná osoba odmítnutí založila na možném narušení nebo ohrožení kyberbezpečnosti, ke kterému by poskytnutím IP adresy serveru mohlo dojít.

[3] Žalovaný odvolání žalobce napadeným rozhodnutím zamítl a prvostupňové rozhodnutí potvrdil, neboť se s ním zcela ztotožnil. IP adresa by mohla být zneužita k tzv. DDoS útoku (*Distributed Denial of Service*, tj. přehlcení serveru a znemožnění přenosu záznamů o přestupcích v dopravě), přičemž nejde pouze o hypotetickou možnost, jelikož k takovým útokům na zařízení provozovaná orgány veřejné moci již dochází. Rychloměr přitom považoval za bezpečnostní opatření ve smyslu § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím, a to s ohledem na pravomoc policie a obecní policie měřit rychlost vozidel za účelem zvýšení bezpečnosti provozu na pozemních komunikacích podle § 79a zákona č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu).

[4] Následně podanou žalobu krajský soud zamítl. Konstatoval, že napadené rozhodnutí je přezkoumatelné (body 29 až 32 napadeného rozsudku). Dále odmítl, že lze srovnávat IP adresu serveru a veřejnost fyzické adresy obecního úřadu. Totéž platí pro porovnání s veřejně dohledatelnou IP adresou internetových stránek města Chomutov (body 34 a 35 tamtéž). Za relevantní nepovažoval ani to, že IP adresa posledního serveru, na němž jsou snímky nakonec uloženy, je opět známá, jelikož přenos dat ohrožuje právě znalost IP adresy prvního serveru (bod 36 tamtéž). Žalobce nezpochybnil závěr, že rychloměr je bezpečnostním opatřením a jeho námitky proti případnému ohrožení jeho účinnosti byly nedůvodné (bod 37 tamtéž).

II. Obsah kasační stížnosti a vyjádření žalovaného

[5] Žalobce (dále jen „stěžovatel“) napadl rozsudek krajského soudu kasační stížností, v níž navrhl, aby Nejvyšší správní soud rozsudek zrušil a věc vrátil krajskému soudu k dalšímu řízení.

[6] Předně stěžovatel namítl, že krajský soud potvrdil nepřezkoumatelné úvahy žalovaného. Z napadeného rozhodnutí totiž srozumitelně neplyne, účinnost kterého bezpečnostního opatření by měla být přímo ohrožena a v čem toto ohrožení spočívá. Stejně tak není zřejmé, který právní předpis označuje rychloměr za bezpečnostní opatření. Krajský soud poté napadené rozhodnutí vyložil bez opory v textu a nedostatky jeho odůvodnění nahradil vlastními úvahami.

[7] Dále stěžovatel nesouhlasil, že by rychloměr mohl být bezpečnostním opatřením. Tím se totiž rozumí souhrn úkonů zajišťujících bezpečnost informací v informačních systémech. Výklad krajského soudu fakticky vede k vyloučení možnosti získat jakékoliv technické informace.

[8] Konečně se stěžovatel vymezil proti srovnání IP adresy a fyzické adresy úřadu. Obecně platí, že existují určitá běžná rizika související s dispozicí s informacemi – kdo zná adresu úřadu, může jej vykrást. To ovšem neznamená, že by úřad byl pravidelně vykrádán, stejně jako znalost IP adresy neznamená, že bude pravidelně napadána DDoS útoky. Míra ohrožení je tak srovnatelná s těmi, kterým povinný subjekt běžně čelí. Žalovanému a krajskému soudu stěžovatel nakonec vytknul, že neprovedli test proporcionality.

[9] Žalovaný se ve svém vyjádření ke kasační stížnosti zcela ztotožnil s napadeným rozsudkem s tím, že stěžovatel pouze opakuje svoji předchozí argumentaci. Kasační stížnost proto navrhnul zamítnout.

III. Právní hodnocení Nejvyššího správního soudu

[10] Nejvyšší správní soud dospěl k závěru, že kasační stížnost je projednatelná. Následně přezkoumal rozsudek krajského soudu v rozsahu důvodů uplatněných v kasační stížnosti, včetně důvodů, ke kterým je povinen přihlížet z úřední povinnosti [§ 109 odst. 3 a 4 zákona č. 150/2002 Sb., soudní řád správní (dále jen „s. ř. s.")]. Kasační stížnost **není důvodná**.

[11] Již na tomto místě je nutné uvést, že námitka směřující proti neprovedení testu proporcionality, je nepřípustná, jelikož ji stěžovatel poprvé uplatnil až v kasační stížnosti (§ 104 odst. 4 s. ř. s.). Jak kasační soud ověřil ze žaloby, stěžovatel v řízení před krajským soudem v tomto ohledu pouze namítal, že poskytnutí požadované IP adresy je ve veřejném zájmu (část IV. žaloby). Takové vyjádření se ovšem nevztahuje k proporcionalitě, jelikož nemíří na vyvažování protichůdných zájmů, ale pouze uvádí další důvod pro poskytnutí informace. Nejvyšší správní soud nemá jako první řešit otázku, kterou stěžovatel nepředložil již u krajského soudu (ve vztahu k námitce proporcionality u poskytování informací viz rozsudek NSS ze dne 12. 11. 2025, č. j. 10 As 242/2024 - 41, bod 14; či usnesení ÚS ze dne 15. 2. 2022, sp. zn. III. ÚS 2175/21, body 13 až 15).

III.a K přezkoumatelnosti

[12] Stěžovatel namítal, že krajský soud aproboval nepřezkoumatelné rozhodnutí. Podle stěžovatele z něj totiž neplyne, které zařízení je oním bezpečnostním opatřením, ani jaký předpis je za ně označuje. Námitka je nedůvodná.

[13] Napadený rozsudek i napadené rozhodnutí splňují požadavky kladené judikaturou Nejvyššího správního soudu na přezkoumatelnost rozhodnutí (viz např. rozsudky NSS ze dne 14. 7. 2005, č. j. 2 Afs 24/2005 - 44, č. 689/2005 Sb. NSS; ze dne 27. 2. 2019, č. j. 8 Afs 267/2017 - 38; či nověji ze dne 18. 9. 2025, č. j. 1 As 235/2024 - 44, bod 18). Z jejich odůvodnění je seznatelné, jaké důvody krajský soud vedly k zamítnutí žaloby, stejně jako důvody žalovaného pro zamítnutí odvolání, přičemž všechny nosné námitky stěžovatele oba orgány vypořádaly, vždy alespoň implicitně (srov. např. rozsudek NSS ze dne 27. 5. 2015, č. j. 6 As 152/2014 - 78, bod 23).

[14] Lze sice připustit, že odůvodnění napadeného rozhodnutí je poměrně lakonické, pokud jde o vyjádření relevantních závěrů. Nejde však o tak vážné nedostatky, zejména ne takové, z nichž by plynula nepřezkoumatelnost rozhodnutí. Nejvyšší správní soud se ztotožňuje s krajským soudem, že z kontextu napadeného rozhodnutí vyplývá, že bezpečnostním opatřením byl myšlen právě rychloměr a § 79a zákona o silničním provozu je onou normou, která jej takto má označovat (bod 30 napadeného rozsudku). Srozumitelné jsou i úvahy o ohrožení, v nichž žalovaný i krajský soud odkazují na možnost DDoS útoků, z nich vyplývající omezení funkčnosti rychloměru, znemožnění zaznamenávat rychlost vozidel, a tedy omezený dohled nad bezpečností provozu

na pozemních komunikacích (bod 31 tamtéž). Napadené rozhodnutí i rozsudek jsou tak v těchto ohledech přezkoumatelné.

III.b K pojmu bezpečnostní opatření

[15] Dále stěžovatel namítal, že rychloměr nemůže být bezpečnostním opatřením, a proto na něj aplikovaná zákonná výluka nedopadá. Námitka není důvodná.

[16] Nejvyšší správní soud zde předesílá, že tuto námitku stěžovatel uplatnil poprvé až v kasační stížnosti, ač ji mohl uplatnit již dříve, což může být důvod její nepřípustnosti (§ 104 odst. 4 s. ř. s.). V žalobě totiž namítal pouze nepřezkoumatelnost napadeného rozhodnutí v této části, nikoliv nesprávnost výkladu. Současně ovšem platí, že správní soudy jsou povinny z úřední povinnosti zkoumat, zda právní předpis nebo jeho ustanovení, která byla použita, na danou věc skutečně dopadají (usnesení rozšířeného senátu ze dne 28. 7. 2009, č. j. 8 Afs 51/2007 - 87, č. 1926/2009 Sb. NSS). Pokud by rychloměr nebyl bezpečnostním opatřením, nebylo by poté vůbec namístě aplikovat tuto zákonnou výluku z práva na informace a kasační soud by v rámci hodnocení hrozícího rizika podával výklad k ustanovení, které na věc nedopadá (obdobně viz rozsudek NSS ze dne 24. 2. 2025, č. j. 8 As 41/2024 - 38, bod 17). Kasační soud proto k námitce přihlédl a nastolenou otázku věcně vypořádal.

[17] V projednávaném případě založily správní orgány neposkytnutí IP adresy prvního serveru, na který se odesílají snímky z rychloměru, na § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím. Dle tohoto ustanovení [p]*ovinný subjekt může omezit poskytnutí informace, pokud její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku.* Je tak zřejmé, že pro aplikaci výjimky musí jít o 1) bezpečnostní opatření, 2) které má právní základ ve zvláštním předpise, a 3) které chrání některý z uvedených cílů. Zároveň také musí dojít k dostatečně závažnému ohrožení účinnosti takového opatření.

Bezpečnostní opatření (podmínka 1)

[18] Nejvyšší správní soud předně uvádí, že pojem bezpečnostního opatření není možné omezit pouze na jeho „kyberbezpečnostní“ význam, jak činí stěžovatel. Jak je uvedeno v důvodové zprávě k tomuto ustanovení, „[j]*edná se o neurčitý právní termín, jehož obsah bude moci být flexibilně vykládán a definován a má zahrnovat veškerá opatření, jejichž účelem je zajišťování bezpečnosti* [....] *Například půjde o detaily ostrahy objektů, strategické a taktické postupy bezpečnostních sborů, informace, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost atd.*“ (pozměňovací návrh Ondřeje Profanta, dokument č. 1075, sněmovní tisk č. 139 z osmého volební období Poslanecké sněmovny). Platí tedy, že jde o vlastní pojem zákona o svobodném přístupu k informacím, a nelze tak vycházet z definice v jiném předpise.

[19] Tento výklad podporuje i vztah mezi § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím a § 10a zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Druhé citované ustanovení zakazuje poskytnout informace podle zákona o svobodném přístupu k informacím, pokud by jejich zpřístupnění *mohlo ohrozit zajišťování kybernetické*

bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila. Jedná se totiž o dva samostatné důvody pro odmítnutí poskytnutí informací (viz rozsudek Krajského soudu v Ostravě ze dne 20. 8. 2025, č. j. 25 A 18/2025 - 26, body 7 až 9), přičemž citované ustanovení se – na rozdíl od vykládaného ustanovení – vztahuje výslovně pouze ke kybernetické bezpečnosti.

[20] Bezpečnostní opatření podle § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím tak nutně nemusí být pouze opatření vztahující se k ochraně kyberbezpečnosti (např. přístupové údaje) či spadající pod pojem „bezpečnostní opatření“, která definoval § 5 zákona o kybernetické bezpečnosti (resp. nyní upravené v § 14 zákona č. 264/2025 Sb., o kybernetické bezpečnosti). Jak plyne z citované důvodové zprávy, nyní vykládané ustanovení umožňuje chránit i „analogové“ formy ochrany „analogových“ prostředků (např. rozpis stráží skladu, harmonogram jejich pochůzek či trasy, informace vztahující se k zajišťování požární ochrany či přestěhování chráněné osoby). Za takové situace pak bezpečnostním opatřením může být provoz jakéhokoliv prostředku, který zajišťuje ochranu zákonem předpokládaného zájmu, a to při naplnění souvisejících podmínek.

[21] Pro projednávanou věc z toho vyplývá, že provoz rychloměru je bezpečnostním opatřením ve smyslu § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím. Představuje totiž nástroj, který směřuje k ochraně bezpečnosti (podmínka 1). Z napadeného rozhodnutí plyne (str. 3), že první server je důležitou „součástí“ (tzv. *back-end*) celého systému, neboť jeho vyřazení z provozu „*by mohlo vést k významnému ohrožení zařízení*“, jehož prostřednictvím se měří rychlost a zajišťuje záznam přestupků v dopravě.

Stanovení zvláštním předpisem (podmínka 2)

[22] Dále je nutné, aby bezpečnostní opatření *stanovoval zvláštní předpis*. Tím je omezen dosah širokého pojmu *bezpečnostní opatření*, a to pouze na taková opatření, která upravuje určitý zvláštní právní předpis. Pokud tedy opatření není právním řádem předpokládané, nemůže se na něj tato výjimka aplikovat. Už jen z tohoto důvodu je lichý stěžovatelův argument, že je zcela znemožněno získat technické informace. Citovaná důvodová zpráva výslovně odkazuje na tyto předpisy:

- § 22 odst. 2 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě, který stanovuje, že [o]*rganizace je povinna učinit včas potřebná preventivní opatření a bezodkladně odstraňovat stavy, které by mohly ohrozit její bezpečný provoz nebo zájmy chráněné podle zvláštních právních předpisů, zejména bezpečnost a ochranu zdraví osob při nakládání s výbušninami*;
- § 3 odst. 1 zákona č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, například stanovuje, že [z]*vláštní ochrana a pomoc je soubor opatření, která zahrnují přestěhování chráněné osoby včetně příslušníků její domácnosti*;
- § 5 odst. 1 písm. a) zákona č. 133/1985 Sb., o požární ochraně, například uvádí, že [p]*rávnické osoby a podnikající fyzické osoby jsou povinny obstarávat a zabezpečovat v potřebném množství a druzích požární techniku, věcné prostředky požární ochrany a požárně bezpečnostní zařízení se zřetelem na požární nebezpečí provozované činnosti a udržovat je v provozuschopném stavu.*

[23] Pokud jde o právní základ rychloměru jako bezpečnostního opatření, odkázal žalovaný na § 79a zákona o silničním provozu, dle kterého – mimo jiné – platí, že [z]*a účelem zvýšení bezpečnosti provozu na pozemních komunikacích je policie a obecní policie oprávněna měřit rychlost vozidel.* Nejvyšší správní soud souhlasí se stěžovatelem, že jde o kompetenční normu; ostatně soud opakovaně vyžadoval naplnění všech podmínek tohoto ustanovení pro uznání oprávnění městské policie měřit rychlost (např. rozsudek NSS ze dne 1. 6. 2017, č. j. 9 As 274/2016 - 37, bod 48 a judikatura tam citovaná).

[24] Nicméně tím zároveň poskytuje rychloměru právní základ. Toto ustanovení se neodlišuje od ostatních, která důvodová zpráva demonstrativně uvádí. Není vyloučeno, aby na základě jedné normy byla určitému orgánu svěřena kompetence, definován pojem či někomu stanovena povinnost, a zároveň tatáž norma byla právním podkladem pro stanovení prostředku jako bezpečnostního opatření. Ostatně citované ustanovení se výslovně zmiňuje o měření rychlosti vozidel jako prostředku zvyšování bezpečnosti provozu. Rychloměr je tak bezpečnostním opatřením předpokládaným zvláštním předpisem, a proto splňuje druhou podmínku.

Ochrana předpokládaných cílů (podmínka 3)

[25] Zákonem předpokládanými cíli ochrany přitom podle vykládaného ustanovení může být pouze ochrana bezpečnosti osob, majetku či veřejného pořádku. Jiné cíle bezpečnostních opatření zákon nepředpokládá. Sledování těchto cílů bezpečnostním opatřením přitom musí být zřejmé z jeho účelu či fungování.

[26] V projednávané věci je zřejmé, že zvýšení bezpečnosti provozu – ke kterému měření rychlosti směřuje – cílí k zákonem předpokládaným důvodům ochrany, a to dokonce všem třem. Dodržování rychlosti směřuje k nižší nehodovosti, která se vztahuje jak k ochraně bezpečnosti osob (zejména života a zdraví chodců a dalších účastníků silničního provozu), tak i majetku (vozidel účastnících se provozu a dalších prvků infrastruktury). Překročení rychlosti také zakládá přestupkovou odpovědnost pachatele, a tedy kontrola jejího dodržování je taktéž součástí širší ochrany veřejného pořádku.

[27] Lze tak uzavřít, že rychloměr je bezpečnostním opatřením stanoveným na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku dle § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím.

III.c K hrozícímu riziku

[28] Dále stěžovatel rozporoval, že poskytnutím požadované IP adresy dojde k významnému nebo přímému ohrožení účinnosti bezpečnostního opatření. Dle něj je míra ohrožení zcela běžná. Námitka není důvodná.

[29] Výluka v § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím může být aplikována pouze v případě, že by sdělení informace vedlo k významnému nebo přímému ohrožení účinnosti bezpečnostního opatření. To znamená, že určitým kvalifikovaným způsobem musí být ohroženo jeho řádné fungování, například hrozícím úplným vyřazením z provozu, usnadněním přístupu k obsahu anebo dostatečně intenzivním omezením funkčnosti. Stěžovatel své úvahy o nízkém riziku založil na dvou srovnáních. Ani jedno z nich ovšem není namístě.

[30] Předně Nejvyšší správní soud souhlasí se závěrem krajského soudu o nepřípadnosti srovnání veřejné dostupnosti IP adresy a fyzické adresy úřadu. Nejenže adresa povinné osoby je zveřejňována jako součást povinně zveřejňovaných informací (body 4.1 a 4.2 přílohy č. 1 vyhlášky č. 515/2020 Sb., o struktuře informací zveřejňovaných o povinném subjektu a o osnově popisu úkonů vykonávaných v rámci agendy; viz bod 34 napadeného rozsudku). Klíčová je zejména odlišnost *offline* a *online* prostředí, kterou stěžovatel dostatečně nedoceňuje.

[31] Stěžovateli tak lze na jednu stranu přisvědčit, že veřejná znalost IP adresy neznamená, že se najednou stane cílem DDoS útoku, stejně jako budova úřadu nebude vykradena po zveřejnění její adresy. Nicméně oba druhy útoků mají znatelně odlišný *modus operandi*. Vloupání do budovy úřadu vyžaduje osobní přítomnost, což snižuje anonymitu, zvyšuje možnost přistižení při činu a vyžaduje déletrvající (fyzickou) aktivitu. Kromě toho musí také osoba fyzicky překonat různé překážky (zámky nebo hlídač). Je zde také nízká možnost automatizace a opakování útoku.

[32] Oproti tomu kybernetické útoky (např. zmíněný DDoS útok) lze provést jen s přístupem k internetu bez rizika fyzického zpozorování útočníka v místě útoku, při ztíženém odhalení identity a v krátkém časovém úseku. To významně snižuje náklady a náročnost útoku. Zatímco tedy úřad lze vykrást pouze při osobní přítomnosti, server může se znalostí IP adresy napadnout osoba sedící za počítačem na Novém Zélandu. Stěžovatel přitom nikterak nerozporuje, že takto lze dostupnost serveru omezit či zcela ochromit,

a pouze takové riziko označuje za „běžné“. Nicméně, jak je z uvedeného zřejmé, stěžovatel skutečně srovnává nesrovnatelné.

[33] Stěžovatel také IP adresu prvního serveru připodobnil k IP adrese webové stránky úřadu. Ani toto srovnání není případné, a to jak z důvodu odlišného účelu, tak výsledku případného útoku.

[34] Zaprvé, jak uvedl krajský soud, podstatou webových stránek statutárního města Chomutov je jejich veřejná dostupnost, která s sebou nese i možnost dohledání IP adresy serveru provozovatele. Oproti tomu server se záznamy z měření je ze své podstaty neveřejný (bod 35 napadeného rozsudku).

[35] Přitom to, že nějaká informace (IP adresa) je dostupná ve vztahu k jedné věci (server hostující webové stránky) nutně neznamená, že tatáž informace musí být také dostupná u jiné věci (server přijímající záznamy z kamer). Obdobně tato úvaha platí například u poskytování informací o příjmech fyzických osob dle § 8c zákona o svobodném přístupu k informacím. Podle této úpravy se totiž v případě některých osob (např. členové vlády či jejich náměstci) údaje o příjmech poskytují [§ 8c odst. 1 písm. a) citovaného zákona], zatímco u jiných osob zákon předpokládá před poskytnutím provedení dalších úvah [písm. b) citovaného ustanovení]. Jinými slovy to, že plat člena vlády se k žádosti poskytuje, neznamená, že se k žádosti poskytne i informace o příjmech zaměstnanců jeho ministerstva.

[36] Zadruhé, při napadení webové stránky úřadu hrozí „pouze“ její nedostupnost pro veřejnost (nemožnost otevřít úřední desku, zjistit aktuality nebo kontakty). Při výpadku serveru u rychloměru ovšem není přestupkové jednání zaznamenáno. Taková informace se vytrácí a není možné její „ztrátu“ jakkoliv následně nahradit. Důsledky nedostupnosti způsobené útokem na tento server jsou tak odlišné, v důsledku čehož je rozdílná i rizikovost zveřejnění jeho IP adresy. Nadto webová stránka úřadu je ze své povahy veřejná a její provoz a zajišťování dostupnosti není bezpečnostním opatřením.

[37] Z uvedeného pak vyplývá, že míra hrozícího rizika pro řádné fungování rychloměru při poskytnutí požadované IP adresy není srovnatelná s běžnými riziky, která povinná osoba denně podstupuje proto, že jsou veřejné známé adresa jejího sídla nebo IP adresy jejích webových stránek. Naopak se Nejvyšší správní soud ztotožňuje s krajským soudem (bod 36 napadeného rozsudku), že sdělení IP adresy prvního serveru, na který jsou přenášeny záznamy z měření rychlosti, by mohlo vést k přímému ohrožení účinnosti bezpečnostního opatření – rychloměru. V případě omezení tohoto spojení (např. z důvodu DDoS útoku) by rychloměr přestal plnit svou funkci, jelikož by nemohl přenášet záznamy o překročení rychlosti a předávat je k dalšímu postupu.

IV. Závěr a náklady řízení

[38] Nejvyšší správní soud tak uzavírá, že zajišťování provozu rychloměru je bezpečnostním opatřením ve smyslu § 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím. Zveřejnění informace obsahující IP adresu prvního serveru, na který rychloměr zasílá záznamy o překročení rychlosti, může významně ohrozit funkčnost tohoto zařízení, tj. účinnost bezpečnostního opatření, neboť zvyšuje riziko útoku na toto zařízení. V důsledku toho by hrozilo úplné ochromení přenosu záznamů o dopravních přestupcích.

Závěr krajského soudu, který akceptoval neposkytnutí této IP adresy ze strany žalovaného, je proto v souladu se zákonem.

[39] Nejvyšší správní soud kasačním námitkám nepřisvědčil a neshledal ani vadu, ke které by musel přihlédnout z úřední povinnosti. Kasační stížnost proto zamítl podle § 110 odst. 1 poslední věty s. ř. s.

[40] O náhradě nákladů řízení rozhodl kasační soud v souladu s § 60 odst. 1 ve spojení s § 120 s. ř. s. Stěžovatel ve věci neměl úspěch, a proto nemá právo na náhradu nákladů řízení o kasační stížnosti. Žalovanému v souvislosti s tímto řízením nevznikly žádné náklady nad rámec běžné úřední činnosti. Soud mu tedy náhradu nákladů řízení nepřiznal.

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

V Brně dne 26. března 2026

Ivo Pospíšil
předseda senátu