ČESKÁ REPUBLIKA

ROZSUDEK
JMÉNEM REPUBLIKY

Krajský soud v Praze rozhodl senátu složeném z předsedy senátu Josefa Straky, soudkyně Johany Jandusové a soudce Karla Ulíka ve věci

žalobce: **J. H.**
bytem X
zastoupený advokátkou Mgr. Rebekou Moťovskou Židuliakovou
sídlem Husovo náměstí 139, 584 01 Ledeč nad Sázavou

proti
žalovanému: **Krajský úřad Středočeského kraje**
sídlem Zborovská 81/11, 150 21 Praha

o **žalobě proti rozhodnutí** žalovaného ze dne 20. 2. 2025, č. j. 031946/2025/KUSK,

takto:

I. **Žaloba se zamítá.**

II. **Žádný z účastníků nemá právo na náhradu nákladů řízení.**

Odůvodnění:

I. Vymezení věci

1. Žalobce podal dne 3. 12. 2024 k Městskému úřadu Votice (dále „povinný subjekt“) žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále „InfZ“). Předmětem žádosti bylo celkem 16 dotazů, které se týkaly rychloměru umístěného na silnici

č. I/3 v obci Miličín ve směru od Prahy na Tábor. Povinný subjekt na většinu dotazů odpověděl a požadovanou informaci poskytl. Odmítl však poskytnout informaci v rozsahu dvou otázek, které zněly:

- Z jakého serveru a jakým způsobem stahují strážníci snímky z rychloměru?
- Jaká je IP adresa prvého serveru, na který jsou snímky přenášeny z rychloměru?

2. Odmítnutí poskytnout informace v rozsahu shora zmiňovaných dvou otázek vyřídil povinný subjekt rozhodnutím ze dne 29. 1. 2025, 4432/2025/SD-Ho (dále „prvostupňové rozhodnutí"). Poukázal primárně na § 11 odst. 1 písm. d) InfZ, podle něhož lze 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. Současně s poukazem na zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále „zákon o kybernetické bezpečnosti"), shledal, že za bezpečnostní opatření je třeba považovat souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru. Dospěl přitom k závěru, že jeho vlastní bezpečnostní opatření, jichž je zapotřebí k ochraně informačních systému nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem či jeho řešením, by v případě poskytnutí žalobcem požadovaných informací mohlo být ohroženo. Proto shledal, že zájem na ochraně bezpečnosti osob, majetku a veřejného pořádku je třeba v tomto případě upřednostnit.

3. Proti prvostupňovému rozhodnutí podal žalobce odvolání, ve kterém namítal, že odůvodnění prvostupňového rozhodnutí je nedostatečné a založené na absurdních závěrech, a proto žádá, aby mu požadované informace byly plně poskytnuty. Žalovaný však rozhodnutím ze dne 20. 2. 2025, č. j. 031946/2025/KUSK (dále „napadené rozhodnutí"), odvolání žalobce zamítl a prvostupňové rozhodnutí potvrdil. Předně se ztotožnil se skutkovými i právními závěry povinného subjektu. Připomněl, že sdělení IP adresy je s ohledem na ochranu dat, datového toku a s tím souvisejících osobních údajů citlivou bezpečnostní záležitostí. Pokud jakákoli nepovolaná osoba disponuje IP adresou, skrze kterou probíhá tok dat souvisejících s výkonem veřejné moci, jejíž součástí je i správa osobních údajů, lze zcela legitimně uvažovat o riziku kybernetického útoku. Doplnil, že orgány veřejné moci v případě spolupráce s externími dodavateli podepisují dohody o mlčenlivosti, jejímž předmětem je mimo jiné i závazek nesdělovat citlivá data, přičemž IP adresa je jednou z nich.

4. Proti napadenému rozhodnutí nyní žalobce brojí žalobou podle § 65 a násl. zákona č. 150/2002 Sb., soudního řádu správního (dále jen „s. ř. s.").

II. Obsah podání účastníků

5. Žalobce považuje napadené i prvostupňové rozhodnutí za nepřezkoumatelné. Nenalézá v nich důvod, proč jím požadovaná informace byla odmítnuta. Správní orgány sice odkazovaly na § 11 odst. 1 písm. d) InfZ, nicméně podmínky plynoucí z tohoto ustanovení nebyly dle jeho názoru dostatečně prokázány. Žalobce se sice obecně ztotožňuje se správními orgány odkazovanou definicí bezpečnostního opatření ve smyslu zákona o kybernetické bezpečnosti, zároveň má však za to, že povinností správních orgánů bylo také vymezit

konkrétní bezpečnostní opatření, jehož účinnost by byla poskytnutím informace snížena. Takové vymezení však postrádá. Povinný subjekt v prvostupňovém rozhodnutí pouze uvedl, že poskytnutím požadované informace by mohlo dojít k ohrožení jeho bezpečnostního opatření. Dle názoru žalobce však pouze hypotetická možnost ohrožení nepostačuje. Právní předpis vyžaduje, aby účinnost bezpečnostního opatření byla snížena buď významně, nebo přímo. Povinný subjekt však nevymezil bezpečnostní opatření ani typově, ani neprokázal, že by jeho účinnost byla významně a přímo ohrožována v důsledku poskytnutí informace. Tento nedostatek neodstranil ani žalovaný v napadeném rozhodnutí, které je proto nepřezkoumatelné.

6. Žalobce rovněž nesouhlasí s argumentací žalovaného, že by sdělení IP adresy představovalo citlivou bezpečnostní záležitost. Naopak má za to, že IP adresa je veřejný údaj, který je srovnatelný s webovou adresou a který lze zjistit například z doručeného e-mailu. Takto si žalobce například zobrazil IP adresu žalovaného z e-mailu jeho podatelny (epodatelna@kr-s.cz), a podobně si zobrazil i IP adresu povinného subjektu z webových stránek města Votice (www.mesto-votice.cz). V této souvislosti připojuje hypertextové odkazy na konkrétní webové stránky včetně návodu k zobrazení IP adresy. Z toho dovozuje, že IP adresa není v žádném případě tajným údajem, její znalost nijak neohrožuje bezpečnost dat. Zároveň má za to, že tímto odůvodnil, proč IP adresu lze považovat za běžně dostupný údaj, zatímco žalovaný ani povinný subjekt nijak neodůvodnili, proč by IP adresa měla být tajným a nezveřejnitelným údajem. Tvrdí-li povinný subjekt, že poskytnutím IP adresy lze uvažovat o zvýšení rizika kybernetického útoku, pak dle žalobce se tímto riziko nezvyšuje, k čemuž opět argumentuje snadným získáním IP adresy z hlavičky e-mailu žalovaného. Žalovaný tedy odmítá poskytnout informaci, kterou neexistuje důvod tajit, aniž by doložil podmínky odůvodňující její neposkytnutí.

7. Žalobce připouští, že informaci o IP adrese považuje za kriticky důležitou, neboť vypovídá o tom, na jaký server jsou přenášeny fotografie pořizované z veřejného prostranství, jejichž součástí jsou osobní údaje. Buď jsou přenášeny na server obce, jejího obecního úřadu nebo obecní policie, nebo na server společnosti GEMOS CZ, spol. s r. o. (dále „GEMOS“), což je soukromá společnost, která je dle vyjádření povinného subjektu provozovatelem rychloměru. Pokud je však osobou, která měří rychlost, soukromá společnost, může se jednat o zásadní nezákonnost při měření a nakládání s osobními údaji zachycenými na snímcích. K tomu žalobce poukazuje na nezákonnou participaci obchodních společností zjištěnou v judikatuře ve věcech pojednávajících o měření rychlosti v obcích Varnsdorf, Chotěboř či Šternberk. Žalobce se domnívá, že právě to je skutečným důvodem, proč povinný subjekt nechce informaci poskytnout.

8. Žalovaný ve vyjádření k žalobě uvedl, že odůvodnění napadeného rozhodnutí považuje za dostačující. V momentě, kdy by nepovolaná osoba disponovala IP adresou, skrze kterou probíhá tok dat souvisejících s výkonem veřejné moci a osobní data zúčastněných osob, mohl by případný kybernetický útok tato data ohrozit. Zveřejnění údajů o serveru samo o sobě není nebezpečné, ale v kombinaci s informací o IP adrese se může výrazně zvýšit riziko útoku. IP adresa interního systému veřejné správy je neveřejná, na rozdíl od IP adresy webového serveru, který je veřejně přístupný. Omezení přístupu k IP adrese představuje legitimní bezpečnostní opatření k zajištění úrovně bezpečnosti, která odpovídá míře hrozícího rizika. Záměrné znepřístupnění IP adresy veřejnosti tím, že na IP adresu není navázána žádná veřejná doména, je v praxi nazíráno jako forma síťové segmentace, což je

doporučovaný bezpečnostní přístup. Z řečeného je zřejmé, co vedlo žalovaného k odmítnutí žádosti o informace v rozsahu výše uvedeném. Byť to prvostupňový orgán výslovně neuvedl, je z jeho odůvodnění zřejmé, že stejné odůvodnění se vztahuje i k informacím o serveru, ze kterého se stahují snímky.

III. Posouzení věci soudem

9. Soud ověřil, že žaloba byla podána včas, osobou k tomu oprávněnou, po vyčerpání řádných opravných prostředků a splňuje všechny formální náležitosti na ni kladené. Soud vycházel při přezkumu napadeného rozhodnutí ze skutkového a právního stavu, který tu byl v době rozhodování žalovaného (§ 75 odst. 1 s. ř. s.), přičemž napadené rozhodnutí přezkoumal v mezích uplatněných žalobních bodů, jimiž je vázán (§ 75 odst. 2 věta první s. ř. s.).

10. Soud o žalobě rozhodl bez jednání, jelikož účastníci ani na výzvu soudu ve stanovené lhůtě nesdělili, že by s tímto postupem nesouhlasili (§ 51 odst. 1 s. ř. s.). Soud nepovažoval za nezbytné jednání nařizovat, neboť veškeré rozhodné skutečnosti bylo možno zjistit z napadeného rozhodnutí, podání účastníků a obsahu správního spisu.

11. Žaloba není důvodná.

12. Předně nelze souhlasit, že by napadené rozhodnutí bylo nepřezkoumatelné pro nedostatek důvodů.

13. Zrušení rozhodnutí pro nepřezkoumatelnost je vyhrazeno těm nejzávažnějším vadám rozhodnutí, kdy pro absenci důvodů skutečně nelze rozhodnutí meritorně přezkoumat, např. tehdy, opomene-li správní orgán či soud na námitku účastníka zcela reagovat a neučiní tak ani implicitně [srov. rozsudky Nejvyššího správního soudu (dále „NSS“) ze dne 17. 1. 2013, č. j. 1 Afs 92/2012-45, či ze dne 29. 6. 2017, č. j. 2 As 337/2016-64]. To ovšem neznamená, že by odvolací správní orgán byl povinen ke každé námitce podrobně odůvodnit své stanovisko a vypořádat každý dílčí argument účastníka řízení. Postačí, pokud odvolací správní orgán prezentuje v odůvodnění právní názor odlišný od účastníka řízení, pakliže zdůvodnění tohoto názoru poskytuje dostatečnou oporu výroku rozhodnutí (srov. rozsudek NSS ze dne 27. 5. 2015, č. j. 6 As 152/2014-78).

14. V případě napadeného rozhodnutí jsou požadavky na přezkoumatelnost naplněny.

15. Žalovaným podané odůvodnění stran vypořádání sporné otázky je sice stručné, zároveň je však adekvátní rozsahu a kvalitě uplatněné odvolací námitky. Ta totiž byla vymezena velmi stručně až všeobecně. Žalobcovo odvolání proti prvostupňovému rozhodnutí znělo doslova takto: „*Jako důvod uvádím, že mi povinný subjekt opět odmítl poskytnout informace, o které jsem žádal. Konkrétně se jednalo o odpovědi na otázky: 'Z jakého serveru a jakým způsobem stahují strážníci snímky z rychloměru?' a 'Jaká je IP adresa prvého serveru, na který jsou snímky přenášeny z rychloměru?' Povinný subjekt argumentoval tím, že by poskytnutím informací mohla být narušena kybernetická bezpečnost a že by mohlo být ohroženo bezpečnostní opatření povinného subjektu. K tomuto bych chtěl sdělit, že povinný subjekt nijak neodůvodnil, jak by mohla být sdělením daných informací narušena kybernetická bezpečnost, nebo dokonce bezpečnostní opatření povinného subjektu. Toto tvrzení mi přijde stejně absurdní, jako kdyby mi povinný subjekt odmítl sdělit adresu úřadu, s tím, že ho poté někdo přijde vykrást. Rozhodnutí je nepřezkoumatelné a já tedy navrhuji, aby bylo zrušeno a aby mi byly požadované informace poskytnuty*.“

Shodu s prvopisem potvrzuje: A. Ř.

16. Z uvedeného je zřejmé, že žalobce v odvolání proti prvostupňovému především zrekapituloval průběh řízení před povinným subjektem, načež namítl, že dle jeho názoru není nijak odůvodněné, jak by mohla být sdělením daných informací narušena kybernetická bezpečnost, nebo dokonce bezpečnostní opatření povinného subjektu, a nakonec vyjádřil názor, že závěr povinného subjektu je absurdní. Nic víc žalobcovo odvolání neobsahovalo. Soud má za to, že jakkoli šlo o odvolání projednatelné, argumentačně bylo velice stručné a rozsah sporných otázek vymezovalo dosti úzce. Žalobce ve svém odvolání nepředestřel analýzu pojmu bezpečnostní opatření či rozbor zjistitelnosti IP adresy, jak později činil v žalobě proti napadenému rozhodnutí. Ta je argumentačně nepoměrně rozvinutější a rozsah sporných otázek vymezuje podstatně šířeji než odvolání proti prvostupňovému rozhodnutí.

17. Přestože uplatnění žalobní námitky v řízení před správním soudem není podmíněno předchozím uplatněním téže námitky v řízení před správními orgány, tak zároveň nelze považovat za vadu, pokud se správní orgány výslovně nezabývají otázkami, které účastník ve svých námitkách vůbec nijak neotevře. Nejinak je tomu i v případě řízení před odvolacím správním orgánem, neboť jak uvedl NSS v rozsudku ze dne 5. 12. 2019, č. j. 10 As 283/2019-36, odst. 9: „*Odvolání jako řádný opravný prostředek je plně v dispozici toho, kdo jej podal. Je to odvolatel, který má vymezit, s jakým okruhem otázek se má odvolací orgán vypořádat; nikdo jiný proto jeho úlohu a pozici nemůže nahradit. Řada skutkových otázek a v návaznosti i právních otázek, které je třeba řešit, totiž může být známa po přečtení odůvodnění prvostupňového rozhodnutí pouze odvolatel*“. To ostatně plyne i z dikce § 89 odst. 2 zákona č. 500/2004 Sb., správního řádu (dále „správní řád“), podle něhož je povinností odvolacího orgánu přezkoumat věcnou správnost prvostupňového rozhodnutí jen v rozsahu námitek uvedených v odvolání, jinak jen tehdy, vyžaduje-li to veřejný zájem, nebo jedná-li se o otázku souladu s právními předpisy. Z toho však nelze dovozovat, že by byl odvolací orgán povinen vyhledávat za odvolatele všechny myslitelné obranné argumenty a se těmi se detailně vypořádávat jako s odvolacími námitkami (srov. rozsudek NSS ze dne 15. 8. 2019, č. j. 10 As 36/2019-33, odst. 13). Po správních orgánech tedy nelze požadovat, aby za účastníka „domýšlely“ všechna myslitelná tvrzení a s těmi se vypořádávaly ve svých rozhodnutích, přičemž následný soudní přezkum správních rozhodnutí nemá povahu „odvolacího řízení s úplnou apelací“ a nemůže nahrazovat prostředky nacházející se uvnitř veřejné správy (srov. usnesení rozšířeného senátu NSS ze dne 2. 5. 2017, č. j. 10 As 24/2015-71, odst. 47).

18. To ve vztahu k nyní posuzované věci znamená, že ani po žalovaném nešlo požadovat, aby se v napadeném rozhodnutí zabýval všemi myslitelnými otázkami souvisejícími s problematikou kybernetické bezpečnosti jen na základě toho, že se této problematiky dotkla odvolací námitka, jež byla jinak velmi obecná. Podstata uplatněné odvolací námitky (její doslovná citace viz odst. 15 výše) spočívala pouze ve vyjádření nesouhlasu s tím, jak by sdělení dotazované informace (tj. dotaz na server, ze kterého jsou stahovány údaje o měření rychlosti a jeho IP adresa) mohlo narušit kybernetickou bezpečnost nebo bezpečnostní opatření. Pokud žalovaný uvedl, že přes servery používané při výkonu veřejné moci dochází k toku dat s osobními údaji a že přístup k IP adrese takového serveru by umožňoval riziko kybernetického útoku (viz str. 3 napadeného rozhodnutí), pak tím podal přezkoumatelnou odpověď na otázku vznesenou v odvolání, a zároveň doplnil mezery v odůvodnění prvostupňového rozhodnutí (s nímž tvoří jeden celek; srov. rozsudek NSS ze dne 31. 10. 2014, č. j. 6 As 161/2013-25). Míru stručnosti této odpovědi soud považuje za zcela adekvátní

míře stručnosti otázky položené v odvolání. Nebylo povinností žalovaného zabývat se otázkami typu schopnost běžného uživatele odhalit cizí IP adresu či mírou snížení účinnosti bezpečnostního opatření, které byly poprvé předestřeny až v žalobě a které si žalovaný v době vydání napadeného rozhodnutí mohl sotva domýšlet. Soud proto uzavírá, že napadené rozhodnutí považuje za přezkoumatelné.

19. Závěry žalovaného o důvodu odmítnutí žalobcem požadovaných informací považuje soud navíc i za věcně správné.

20. Žalovaný i povinný subjekt opřely důvod odmítnutí o úpravu § 11 odst. 1 písm. d) InfZ, podle kterého „[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*.“

21. Citované ustanovení bylo do InfZ vloženo s účinností od 24. 4. 2019 v rámci novelizace provedené zákonem č. 111/2019 Sb. Důvodová zpráva k tomuto uvádí, že „[n]*ávrh samotný je reakcí na požadavky na poskytnutí informací, které je obtížné podřadit pod některou z výjimek pro poskytování informací, avšak jejichž poskytnutí by mělo značně negativní dopady právě na efektivitu prosazování zájmů České republiky v zahraničí v rámci diplomatického vyjednávání, sjednávání smluv, dohod, hlasování, včetně hlasování tajného, přípravy na taková hlasování a jednání samotného, nebo pokud se např. jedná o osudu občanů, kteří se ocitli v zahraničí v nepříznivé situaci. Těmito informacemi mohou být např. instrukce pro tajné hlasování v mezinárodních organizacích, dokumenty od jiných států či mezinárodních organizací nebo podklady k jednání o občanech zadržovaných v zahraničí, které stricto sensu nelze považovat za utajované informace, avšak jejichž citlivost je značná a je jen obtížně představitelné, že by důvěrné informace či např. instrukce pro tajná hlasování byly poskytovány a návazně zveřejňovány*“.

22. Komentářová literatura dále upřesnila, že „[u]*stanovení § 11 odst. 1 písm. d) zák. o svobodném přístupu k informacím směřuje k ochraně účinnosti bezpečnostních opatření stanovených na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku. Pojem ‚bezpečnostní opatření' je neurčitým právním pojmem. Poskytnutím informace může být ohroženo i bezpečnostní opatření soukromé.* ***V praxi se bude jednat o informace, které sice nejsou utajované, ale i přesto jsou citlivé povahy a není žádoucí, aby vešly v obecnou známost. Například půjde o*** *detaily ostrahy objektů, strategické a taktické postupy bezpečnostních sborů,* ***informace, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost atd.*** *Aby toto ustanovení nemohlo být nadužíváno či zneužíváno, musí jít o opatření, které má svůj podklad v zákoně.* ***Například půjde o § 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti****; § 5 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, § 22 až 26 zákona č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě; § 3 zákona č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením; § 5 odst. 1 písm. a) zákona č. 133/1985 Sb., o požární ochraně; čl. 32 odst. 1 GDPR apod.*“ (in. JELÍNKOVÁ, J., TUHÁČEK, M. *Zákon o svobodném přístupu k informacím. Praktický komentář*. Wolters Kluwer. ISSN 2336-517X, zde rovněž citováni KORBEL, F., PRUDÍKOVÁ, D., HRADÍLEK, Š., ŠÍDLO, J. Velká novela zákona o svobodném přístupu k informacím. Právní rozhledy. 2023, č. 4, s. 120).

23. S výkladem shora citované komentářové literatury se soud ztotožňuje. Proto konstatuje, že pojem „bezpečnostní opatření“ užitý v § 11 odst. 2 písm. d) InfZ je neurčitým právním pojmem, který nelze přesně obsahově vymezit a jehož výklad a aplikace závisí na odborném

posouzení v každém jednotlivém případě, tudíž je povinností veřejné správy, aby ve vztahu ke konkrétnímu případu zhodnotila, zda konkrétní skutková situace do rozsahu daného pojmu spadá či nikoliv (k výkladu neurčitého právního pojmu srov. např. rozsudek NSS ze dne 30. 3. 2017, č. j. 10 As 252/2015-77, odst. 17, ze dne 12. 8. 2011, č. j. 5 As 47/2011-77, či ze dne 20. 10. 2004, č. j. 1 As 10/2003-58). Do kategorie informací, jejichž poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření, by tudíž měly spadat zpravidla takové informace, které sice nejsou přímo utajované, ale zároveň je jejich povaha natolik citlivá, že by jejich veřejné poskytnutí bylo nežádoucí s ohledem na jiný zájem chráněný zvláštním zákonem.

24. Zákon o kybernetické bezpečnosti – na který žalovaný i povinný subjekt v nyní posuzované věci shodně společně odkazovali – navíc obsahuje i vlastní definici pojmu „bezpečnostní opatření“. Konkrétně v § 13 odst. 1 tento zákon stanoví, že „[b]*ezpečnostními opatřeními jsou organizační a technická opatření, jejichž účelem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv*“. Vzhledem k této upřesňující definici má soud za to, že v oblasti kybernetické bezpečnosti bude pro podřazení určité informace do kategorie ohrožení bezpečnostního opatření ve smyslu § 11 odst. 1 písm. d) InfZ zpravidla postačovat, bude-li požadovaná informace součástí organizačních a technických opatření povinného subjektu směřují k zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. Poskytováním regulované služby kybernetické bezpečnosti aktiv se přitom rozumí činnosti vymezené v § 4 odst. 1 zákona o kybernetické bezpečnosti, kam podle § 4 odst. 1 písm. a) téhož ustanovení spadá i poskytování služeb v oblasti veřejné správy.

25. Soud má za to, že v nyní posuzované věci byl tento požadavek splněn.

26. Povinný subjekt definoval zájem na ochraně svých vlastních informačních systémů, sítí a elektronických komunikací před bezpečnostními hrozbami právě s poukazem na zákon o kybernetické bezpečnosti (viz str. 2 prvostupňového rozhodnutí). Ač to povinný subjekt neuvedl explicitně, je z kontextu zřejmé, že zmiňovanými vlastními informačními systémy, sítěmi a elektronickými komunikacemi měl na mysli právě takové, které souvisejí s výkonem veřejné správy na úseku silničního provozu (vzhledem k předmětu žádosti o informace – dotaz směřující na servery k měření rychlosti a jejich správu – sotva mohl myslet jiný druh své činnosti). Žalovaný následně doplnil, že skrz servery orgánů veřejné moci „tečou“ data s osobními údaji a že přístup k IP adrese takového serveru by umožňoval riziko kybernetického útoku (viz str. 3 napadeného rozhodnutí). Tím přinejmenším implicitně sdělil, že poskytnutím údajů o dotazovaném serveru či jeho IP adrese by se zvýšilo ohrožení funkčnosti zařízení pro měření rychlosti, a potenciálně i ohrožení osobních údajů zpracovávaných veřejnou správou.

27. To, že žalobcem dotazovaný server pro zaznamenávání naměřené rychlosti skutečně slouží k plnění povinností veřejné správy, je dle soudu zřejmé již jen ze samé podstaty této činnosti. Shromažďování údajů o rychlosti vozidel za účelem regulace silničního provozu je totiž výlučnou doménou orgánů veřejné moci realizovanou v rámci výkonu přenesené působnosti (srov. § 79a ve spojení § 124 a násl. zákona č. 361/2000 Sb., o silničním provozu). Je proto logické, že data procházející serverem (například záznamy o naměřené rychlosti vozidel, jejich registrační značky apod.) budou použita právě za účelem výkonu veřejné moci na úseku silniční dopravy (například v řízení o přestupku), s čímž se nedílně pojí i správa

osobních údajů (typicky ve vztahu k účastníkům řízení), jak správně upozornil žalovaný. Soud přitom považuje za legitimní, že přístup k takovému serveru – ať už přímo prostřednictvím sdělením IP adresy počítače zajišťujícího chod daného serveru či nepřímo prostřednictvím popisu způsobu stahování či nahrávání dat na daný server – se orgány veřejné moci snaží omezovat kvůli riziku hrozeb kybernetické povahy.

28. Skutečnost, že se v napadeném ani prvostupňovém rozhodnutí hovoří pouze obecně o kybernetických hrozbách a bezpečnostních incidentech a není zde explicitně pojmenován konkrétní druh útoku (jako například DDoS útok, který žalovaný zmiňuje poprvé až ve vyjádření k žalobě), soud nepovažuje za vadu. Dle soudu není nezbytné, aby v souvislosti s vymezováním bezpečnostního opatření v režimu § 13 odst. 1 o kybernetické bezpečnosti musela být specificky dokládána konkrétní hrozba či újma. To je dáno již samotnou povahou hrozeb v oblasti kybernetiky, která se odehrávají primárně v *online* prostoru a logicky se tak liší od „fyzických" hrozeb v *offline* prostoru. Kybernetické útoky lze totiž *„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"* (srov. rozsudek NSS ze dne 26. 3. 2026, č. j. 1 As 208/2025-34, odst. 32). S ohledem na uvedené lze pro účely této věci – mj. i s přihlédnutím k obsahu odvolacích námitek (srov. odst. 15-17 výše) – považovat za dostačující žalovaným podané vymezení, že charakter bezpečnostního opatření je zřejmý ze samotné povahy serveru, přes který „tečou" data s osobními údaji používanými pro účely výkonu veřejné moci. Opět nelze než zopakovat, že jakkoli jde o vymezení stručné, tak je z něj dostatečně zřejmé, před jakým druhem rizik mají být elektronické systémy veřejné správy chráněny.

29. Nad rámec nutného odůvodnění soud dodává, že v realitě 21. století lze považovat za obecně známou skutečnost (notorietu), že typickou hrozbou pro fungování serverů jsou právě tzv. DDoS (Distributed Denial of Service) útoky spočívající v zahlcení serveru enormním množstvím požadavků z mnoha zdrojů, čímž mohou omezit nebo i zcela vyřadit jeho funkci. Právě v případě serverů pro zaznamenávání rychlosti byl tento druh hrozby jako relevantní hrozba dovozeno v rozsudku Krajského soudu v Ústí nad Labem ze dne 10. 12. 2025, č. j. 141 A 13/2025-29 (potvrzeného výše zmiňovaným rozsudkem NSS ze dne 26. 3. 2026, č. j. 1 As 208/2025-34), jenž se týkal obdobné věci a s jehož nosnými závěry se zdejší soud ztotožňuje.

30. Soud dále nesouhlasí s argumentací žalobce, že IP adresa nemůže představovat citlivou bezpečnostní záležitost, neboť jde o veřejně zjistitelný údaj. Žalobce má samozřejmě pravdu, že v mnoha případech jsou IP adresy skutečně snadno zjistitelné i v rámci běžného užívání internetu, zároveň však přehlíží, že napadené ani prvostupňové rozhodnutí nesměrovalo k paušálnímu odmítnutí jakékoliv IP adresy. Žalovaný ani povinný subjekt nikdy nevyslovili, že IP adresa je obecně tajným a nezveřejnitelným údajem, jak je jim v žalobní argumentaci zčásti podsouváno. Z obsahu napadeného a prvostupňového rozhodnutí je naopak zřejmé, že odmítnutí se týká výlučně jedné konkrétní IP adresy, která je spojená právě se serverem, jímž procházejí data o měření rychlosti vozidel v silničním provozu, a k němuž směřovala žádost o poskytnutí informací.

31. Dle soudu je přitom IP adresu takového serveru nutno odlišovat od IP adres, na nichž žalobce demonstruje snadnost jejich dohledávání. Lichá je proto žalobcova analogie se zjištěním IP adresy žalovaného skrz hlavičku e-mailu jeho podatelny (epodatelna@kr-s.cz). Účelem e-mailové adresy podatelny úřadu je zajistit jeho komunikaci s veřejností, tudíž se logicky předpokládá její široké zpřístupnění, s čímž se pojí i možnost veřejnosti zjistit v rámci komunikace IP adresu adresáta e-mailu. Účel zařízení k přenosu snímků z rychloměru je však odlišný, k němu se přístup široké veřejnosti z povahy věci nepředpokládá, neboť – jak již bylo několikrát zmíněno – jde o shromažďování údajů pro účely správních (zpravidla přestupkových) řízení. Z téhož důvodu je lichá i žalobcem uváděna analogie se zjištěním IP adresy povinného subjektu přes jeho internetové stránky města Votice (www.mesto-votice.cz). Smyslem internetových stránek města (popř. městského úřadu) je jednak zprostředkování informací směrem k veřejnosti, a jednak plnění zákonné povinnosti zveřejňovat obsah úřední desky způsobem umožňujícím dálkový přístup (srov. § 26 odst. 1 in fine správního řádu). Logicky se tudíž předpokládá široký přístup k takovým internetovým stránkám, s čímž se pojí i možnost veřejnosti zjistit jejich IP adresu. Naproti tomu server určený k prvotnímu přijímání rychloměrem pořízených záznamů takovému ani žádnému obdobnému účelu neslouží (srov. též rozsudek Krajského soudu v Hradci Králové ze dne 11. 2. 2026, č. j. 30 A 76/2025-93, odst. 22). To, že nějaká informace (konkrétní IP adresa) je dostupná ve vztahu k jedné věci (server hostující internetové stránky pro běžné uživatele) nutně neznamená, že tatáž informace musí být také dostupná u jiné věci (server přijímající záznamy z kamer), nehledě na to, že v případě napadení internetové stránky úřadu hrozí „pouze“ její nedostupnost pro veřejnost (např. nemožnost otevřít úřední desku, zjistit aktuality nebo kontakty), zatímco při výpadku serveru u rychloměru hrozí ztráta důkazu zaznamenávajícího případné protiprávní jednání (srov. rozsudek NSS ze dne 26. 3. 2026, č. j. 1 As 208/2025-34, odst. 35-37). Nelze tedy než uzavřít, že žalobce sice činí zajímavou komparaci, avšak nepracuje s porovnatelnými proměnnými.

32. V závěru žaloby je namítáno, že není zřejmé, zda server, přes který mají procházet data o měření rychlosti, je skutečně serverem obce či serverem soukromé společnosti GEMOS. Soud má z příslušné části žaloby za to, že se žalobce patrně snaží naznačit, proč považuje znalost údajů o provozovateli serveru za legitimní z hlediska zájmů chráněných InfZ, neboť má zřejmě za to, že v případě „odhalení“ soukromého provozovatele serveru by bylo možno zpochybnit zákonnost podkladů pořízených rychloměrem a tím jejich důkazní použitelnost v přestupkových řízeních.

33. Soud připouští, že je jistě legitimní znát informaci o identitě subjektu, který obstarává faktický chod měřícího zařízení užívaného orgánem veřejné moci. K tomu však postačí sdělit právě identitu daného subjektu, a nikoliv sdělovat bližší údaje identifikující konkrétní server, ať už jde o IP adresu či jiné údaje umožňující technickou identifikaci konkrétního zařízení. V tomto případě však správní orgány nijak netajily, kdo je provozovatelem měřícího zařízení, a naopak toto žalobci k jeho dotazu sdělily. Jak plyne ze správního spisu, součástí žalobcovy žádosti o informace byl (vedle řady dalších) mj. i dotaz, kdo je provozovatelem rychloměru v obci Miličín. Na to mu povinný subjekt odpověděl, že právě společnost GEMOS. Žalobci se tedy dostala informace, kdo je subjektem, který zajišťuje faktický provoz zařízení pro měření rychlosti.

34. V této souvislosti je třeba připomenout, že není vyloučeno, aby servis a technické zabezpečení zařízení používaných k činnosti orgánů veřejné moci obstarávaly soukromé subjekty, pokud neprofitují z výsledků tohoto měření, jak opakovaně dovodila judikatura (srov. rozsudky NSS dne 2. 4. 2008, č. j. 1 As 12/2008-67, č. 1607/2008 Sb. NSS, ze dne 17. 12. 2014, č. j. 9 As 185/2014-27, ze dne 30. 5. 2018, č. j. 10 As 107/2018-36, č. 3765/2018 Sb. NSS, či ze dne 23. 5. 2019, č. j. 5 As 175/2018-29, nebo např. usnesení NSS ze dne 15. 1. 2026, č. j. 5 As 193/2025-33, jež se týkalo právě situace, kdy rychlostní zařízení obsluhovala společnost GEMOS zmiňovaná i v nyní posuzované věci). Ve vztahu k nyní posuzované věci tudíž nelze vyloučit – a dokonce je to i velmi pravděpodobně –, že společnost GEMOS bude zároveň také tím, kdo fakticky zajišťuje i chod serveru, jímž procházejí data o měření rychlosti, a proto IP adresa tohoto serveru klidně může směřovat ke koncovému zařízení vlastněnému právě společností GEMOS. Nicméně i kdyby tomu tak bylo, tak to dle soudu samo o sobě nevypovídá nic o případné využitelnosti zde ukládaných dat pro činnost orgánů veřejné moci. Měření rychlosti silničního provozu a s tím související shromažďování údajů je totiž stále agendou v rámci výkonu veřejné moci, za kterou nese odpovědnost příslušný správní orgán, a to bez ohledu na to, zda mu technický servis zajišťuje nějaký soukromý subjekt. Případné odhalení serveru s IP adresou soukromé společnosti proto soud nepovažuje za nic *a priori* „skandalizujícího“, co by mělo potenciál zpochybnit zákonnost výsledků rychlostního měření pro účel dokazování v případných přestupkových řízení (jak se patrně domnívá žalobce). Proto zde není žádný zájem veřejnosti, před nímž by musela ustoupit rizika vyplývající ze zpřístupnění IP adresy či jiného údaje umožňující technickou identifikaci konkrétního zařízení, na kterém běží server pro stahování či ukládání dat ze zařízení pro měření rychlosti silničního provozu. Jak již bylo vysvětleno, důvodem pro nesdělování údajů tohoto typu není chránit identitu subjektu zajišťujícího chod serveru, nýbrž chránit samotný server – a skrz něj protékající data – před rizikem kyberútoků, jejichž proveditelnost je v případě znalosti IP adresy či jiného serverového identifikátoru snazší (srov. odst. 28 výše).

35. Zmiňoval-li se žalobce v souvislosti s angažovaností soukromých subjektů o „*nezákonnosti měření z důvodu nezákonné participace obchodních společností v judikatuře soudů srov. rozsudky projednávající měření v obci Varnsdorf, Chotěboř či Šternberk*“ (viz str. 5 žaloby), měl tím patrně na mysli věci projednávané v rozsudku NSS ze dne 23. 1. 2023, č. j. 3 As 275/2020-37 (kauza měření rychlosti ve Varnsdorfu), a rozsudku Krajského soudu v Ostravě – pobočka v Olomouci ze dne 11. 7. 2018, č. j. 72 A 176/2017-47 (kauza měření rychlosti ve Šternberku), v nichž správní soudy odmítly uznat výsledky měření jako podklady pro přestupkové řízení z důvodu pochybností, že soukromý subjekt zajišťující servis měřícího zařízení mohl – s ohledem na obsah smluvních podmínek konkrétní smlouvy o nájmu měřícího zařízení - profitovat z výsledků měření zaznamenávajících překročení rychlosti. Závěry posledně zmiňovaných rozsudků však nejsou nijak v rozporu s tím, že sběr dat v souvislosti s měřením rychlosti silničního provozu je agendou spadající výlučně pod výkon veřejné moci – naopak tuto tezi zcela podporují. Nelze proto než zopakovat, že i kdyby IP adresa žalobcem dotazovaného serveru skutečně směřovala na počítač či jiné koncové zařízení spravované či vlastněné společností GEMOS, neměnilo by to nic na tom, že odpovědnost související se sběrem dat procházejících přes daný server – jakož i odpovědnost za jejich případnou (ne)použitelnost pro účely správních řízení – nese správní orgán s kompetencí na úseku zákona o silničním provozu. Logicky mu tudíž přísluší i odpovědnost za zabezpečení

daného serveru, například právě omezením přístupu k IP adrese zařízení zajišťujícího jeho chod, případně nesdělováním podrobností o procesech stahování či nahrávání dat.

IV. Závěr a náklady řízení

36. S ohledem na výše uvedené soud neshledal žalobu důvodnou, a proto ji podle § 78 odst. 7 s. ř. s. zamítl.

37. O nákladech řízení účastníků soud rozhodl podle § 60 odst. 1 s. ř. s. Žalobce nemá právo na náhradu nákladů řízení, neboť nebyl procesně úspěšný. Procesně úspěšnému žalovanému žádné náklady nad rámec jeho běžné úřední činnosti nevznikly.

Poučení:

Proti tomuto rozsudku lze podat kasační stížnost ve lhůtě dvou týdnů ode dne jeho doručení. Kasační stížnost se podává ve dvou vyhotoveních u Nejvyššího správního soudu, se sídlem Moravské náměstí 6, Brno. O kasační stížnosti rozhoduje Nejvyšší správní soud.

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

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

Praha 31. března 2026

Josef Straka v.r.
předseda senátu

Shodu s prvopisem potvrzuje: A. Ř.