



ČESKÁ REPUBLIKA
ROZSUDEK
JMÉNEM REPUBLIKY

Krajský soud v Ústí nad Labem rozhodl v senátu složeném z předsedy Ing. Mgr. Martina Jakuba Bruse a soudců JUDr. Jiřího Derfla a Mgr. Vojtěcha Salamánka ve věci

žalobce: J. H., narozený X
bytem X
zastoupený advokátkou Mgr. Rebekou Mořovskou Židuliakovou
sídlem Husovo náměstí 139, 584 01 Ledec nad Sázavou

proti
žalovanému: Krajský úřad Ústeckého kraje
sídlem Velka Hradební 3118/48, 400 02 Ústí nad Labem

o žalobě proti rozhodnutí žalovaného ze dne 3. 1. 2025, č. j. KUUK/000227/2025

takto:

- I. Žaloba se **zamítá**.
- II. Žádný z účastníků **nemá** právo na náhradu nákladů řízení.

Odůvodnění:

- Magistrát města Chomutova (dále též „povinný subjekt“) rozhodnutím ze dne 4. 12. 2024, č. j. MMCH/155541/2024/OIA/Kuhn (dále též „prvostupňové rozhodnutí“), podle § 15 odst. 1 ve spojení s § 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 197/2024 (dále jen „InfZ“) odmítl žalobcovu žádost o poskytnutí informace v části, již bylo žádáno o sdělení IP adresy prvního serveru, na který jsou přenášeny snímky ze silničního rychloměru, který je umístěn na pozemní komunikaci R02_Písečná v Chomutově na souřadnicích 50° 29' 24,179" severní šířky a 13° 26' 39,222" východní délky.

Shodu s prvopisem potvrzuje G. Z.

2. Prvostupňové rozhodnutí bylo potvrzeno a proti němu směřující odvolání zamítnuto rozhodnutím žalovaného ze dne 3. 1. 2025, č. j. KUUK/000227/2025 (dále jen „napadené rozhodnutí“), které žalobce napadl posuzovanou žalobou.

Žaloba

3. Žalobce předeslal, že dle odůvodnění prvostupňového rozhodnutí by bylo poskytnutí požadované informace „*schopno narušit či ohrozit kybernetickou bezpečnost*“, jelikož „*poskytnutí IP adresy je rovno potenciálnímu ohrožení kybernetické bezpečnosti celého systému*“, neboť IP adresa může být zneužita pro kybernetické útoky, např. DDoS útoky. V odůvodnění žalobou napadeného rozhodnutí k tomu bylo připodotknuto, že „*i když se v případě IP adresy serveru nejedná o utajovanou skutečnost, její zpřístupnění by mohlo vést k významnému ohrožení zařízení, jehož prostřednictvím je naplňováno zákonné zmocnění*“ a že znalost IP adresy daného serveru není věcí veřejného zájmu.
4. Žalobce považuje prvostupňové rozhodnutí i rozhodnutí žalovaného za nepřezkoumatelná. Zákonné důvody, které zakládají povinnému subjektu právo omezit poskytnutí informace, totiž nebyly v rozhodnutích vyjasněny a odůvodněny. Povinný subjekt nemůže dle žalobce odmítnout poskytnout informaci, která je schopna narušit kybernetickou bezpečnost, ale jen takovou informaci, která významně nebo přímo ohrožuje konkrétní bezpečnostní opatření, stanovené zvláštním právním předpisem. Povinný subjekt ani žalovaný však nspecifikovali konkrétní bezpečnostní opatření, jehož účinnost může být poskytnutím informace narušena, ani nevyjasnili, kterým zvláštním právním předpisem je toto bezpečnostní opatření stanoveno.
5. Podle žalobce je pravdou, že při znalosti IP adresy může být realizován DDoS útok. Stejně tak ale při znalosti fyzické adresy úřadu může být úřad vykraden a mohou z něj být odneseny spisy, které obsahují citlivé osobní údaje. To však dle žalobce neznámá, že by byl povinný subjekt oprávněn tajit fyzickou adresu úřadu. IP adresa přitom není dle žalobce názoru žádným chráněným údajem. Například IP adresa serveru povinného subjektu (Magistrátu města Chomutov) je 217.75.213.173. Každý, kdo má zájem tuto IP adresu zjistit, tak může vcelku jednoduše učinit zadáním příkazu *tracert* s označením domény do příkazového řádku. Nepodléhá-li tedy utajení internetová adresa webové prezentace úřadu, nepodléhá dle žalobce utajení ani IP adresa úřadu, která je z takové internetové adresy zjistitelná. Žalobci tudíž není zřejmé, proč by měla podléhat utajení IP adresa prvního serveru, na který jsou ukládány záznamy z radaru.
6. Žalobce poznamenal, že na serveru povinného subjektu se nacházejí tatáž data, která se nacházejí na serveru, jehož IP adresu požadoval žalobce (tedy na prvním serveru, na který jsou snímky z radaru přenášeny). Žalobce se tak domnívá z důvodu, že povinnému subjektu jsou tato data následně postupována za účelem projednávání přestupků. Je-li tedy veřejně známa IP adresa jednoho serveru, na kterém jsou data (v důsledku) uložena, pak není důvod tajit IP adresu jiného serveru, přes který jsou tato data transferována.
7. Žalobce se rovněž vymezil vůči závěru žalobou napadeného rozhodnutí, že není dán veřejný zájem na veřejnosti IP adresy prvního serveru. Žalobce se pouze snažil zjistit, zda data z rychloměru jsou ukládána přímo na server úřadu či obecní policie, anebo jsou nejprve ukládána na serverech třetích stran (např. obchodních společností participujících na měření). Dle žalobce názoru je ve veřejném zájmu vědět, jak je nakládáno s osobními údaji zaznamenanými rychloměrem a zda jsou tyto od samého počátku v ryzí dispozici orgánu

veřejné moci, anebo také v dispozici soukromoprávních společností. To platí dle žalobce tím spíše, je-li na základě těchto údajů přístupováno ke správnímu trestání.

8. Žalobce proto navrhl, aby soud napadené rozhodnutí zrušil.

Vyjádření žalovaného k žalobě

9. Žalovaný ve svém vyjádření ze dne 8. 4. 2025 uvedl, že povinnost chránit bezpečnost a integritu informačních systémů základní služby a elektronických komunikací vyplývá ze zákona č. 127/2005 Sb., o elektronických komunikacích a změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „zákon o elektronických komunikacích“) a zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“). Dle žalovaného je nepochybné, že jedním ze základních způsobů ochrany informačních systémů a elektronické komunikace [v tomto případě základní služby v odvětví dopravy dle § 2 písm. j) bodu dva zákona o kybernetické bezpečnosti] je prosté nesdělování informací, které by kybernetický útok umožnily. Zveřejňování IP adres systémů povinného subjektu není možné z důvodu ochrany důvěrnosti a integrity informační infrastruktury; tyto informace jsou považovány za citlivé a jejich zveřejnění by mohlo vést k ohrožení bezpečnosti provozovaných systémů, přičemž zveřejnění IP adres lze chápat jako porušení principu minimalizace zveřejňování technických detailů, které spadají pod chráněné části dokumentace.
10. Za absurdní označil žalovaný žalobcem užitý přírůbek s vykradením sídla povinného subjektu při znalosti jeho adresy. Budovy úřadu jsou chráněny bezpečnostními systémy (mechanickými, elektronickými či personální ostrahou); samozřejmě přístupové kódy k zabezpečení budov nejsou a nemohou být veřejně přístupné. Kybernetická bezpečnost je dle žalovaného z povahy věci podstatně odlišná od bezpečnosti fyzické. K realizaci kybernetického útoku skutečně postačí pouhá znalost IP adresy, přičemž útok může být veden na dálku a spočívat jen v prostém sledování, ale i zahlcení IP adresy či zablokování s následným vydíráním provozovatele či vyřazení zařízení. Znalost IP adresy je prvním a nezbytným krokem k takovým útokům.
11. Žalovaný dále upozornil, že žalobci bylo v odpovědi na bod 10 dané žádosti o poskytnutí informací povinným subjektem sděleno, že *„snímky jsou v pravidelných intervalech odesílány automaticky na server Městské policie, kde se zpracovávají v programu ARCHIV“*. Dle žalovaného je z takovéto odpovědi dostatečně zřejmé, že prvním serverem, na který jsou snímky přenášeny, je server Městské policie Chomutov, a jsou tedy od počátku až do konce v dispozici orgánů veřejné moci.
12. V návaznosti na žalobcův argument, že není-li z důvodů kybernetické bezpečnosti utajována IP adresa internetových stránek povinného subjektu, nemá být tajena ani IP adresa prvního serveru k přijímání radarem pořízených záznamů, žalovaný odkázal na odůvodnění žalobou napadeného rozhodnutí. V němž totiž popsal, že právě kvůli veřejné dostupnosti IP adresy internetových stránek se staly terčem kybernetického útoku například internetové stránky Městského úřadu v Ostrově, což je dle žalovaného naopak argumentem pro neposkytnutí IP adresy serveru sloužícího k přijímání radarových záznamů, a to v zájmu prevence podobného bezpečnostního incidentu.
13. Podle žalovaného rovněž není pravdou, že je-li známa IP adresa koncového serveru, na němž jsou data uložena, není třeba chránit důvěrnost IP adresy mezičlánků (serverů) transferu dat

mezi radarem a koncovým serverem. Případným kybernetickým útokem totiž může být napaden právě přenos dat mezi radarem a prvním serverem, případně mezi prvním serverem a koncovým serverem, a data tak mohou být zničena či zneužita. Na cílovém serveru naopak mohou být data chráněna například jejich stažením na síti nepřístupné médium.

14. Závěrem žalovaný zopakoval, že ke získání informací o způsobu nakládání s osobními údaji zaznamenanými rychloměrem, resp. ověření, zda jsou tyto údaje od počátku do konce pouze v dispozici orgánů veřejné moci (anebo se naopak alespoň v některé fázi ocitají i v dispozici soukromoprávních subjektů), není nezbytné znát IP adresu serveru, na který rychloměr zasílá pořízené záznamy. Dle žalovaného se žalobci dostalo v celkovém kontextu všech bodů jeho informační žádosti takových informací, jimiž měl být uspokojen i bez znalosti IP adresy prvního serveru.
15. Žalovaný vyjádřil pochybnost, zda se žalobce žádostí o sdělení IP adresy daného rychloměru skutečně pokouší naplnit právo na veřejnou kontrolu činnosti správních orgánů, či jde o zneužití práva. Ve vztahu k osobě žalobcovy zástupkyně, advokátky Mgr. Rebecky Mořovské Židuliakové, přitom poukázal na závěry o systémových obstrukcích podané zejména v bodech 19 a 22 rozsudku Městského soudu v Praze ze dne 18. 12. 2024, č. j. 5 A 107/2024-31.
16. Žalovaný navrhl, aby soud žalobu jako nedůvodnou zamítl.

Žalobcova replika k vyjádření žalovaného

17. Žalobce v reakci na vyjádření žalovaného podal soudu repliku ze dne 22. 4. 2025. V ní podotkl, že je sice povinností správních orgánů dbát bezpečnosti a integrity informačních systémů, avšak nevyjímá je to z povinnosti poskytovat informace v souladu s InfZ. Střet obou zájmů (kyberbezpečnosti a poskytování informací) je výslovně řešen v § 11 odst. 1 písm. d) daného zákona. Ten jasně stanoví, že právo na informace lze omezit pouze tehdy, pokud by poskytnutí informace významně nebo přímo ohrožovalo účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku. Všechny tyto podmínky musí být dle žalobcova názoru splněny kumulativně. Žalovaný přitom netvrdí, že by byla splněna byť jediná z těchto podmínek; netvrdí to ve vyjádření k žalobě ani v napadeném rozhodnutí. Podle žalobce není pravdou, že by kybernetické útoky směřovaly pouze na servery, jejichž IP adresy byly zveřejněny.
18. Pokud žalovaný zmiňoval interní směrnici povinného subjektu č. 2023-19 s tím, že na jejím základě lze zveřejnění IP adres chápat jako porušení principu minimalizace zveřejňovaných technických detailů, které spadají pod chráněné části dokumentace, má žalobce za to, že interní směrnice povinného subjektu nemůže popírat zákonné právo na informace. Žalobce se rovněž nedomnívá, že by IP adresa serveru k přijímání radarových záznamů mohla být „*detailem spadajícím pod chráněné části dokumentace a zároveň velmi citlivou informací z hlediska bezpečnosti*“. Dle žalobce si žalovaný přečetl směrnici a její část o ochraně velmi citlivých informací a z nevysvětleného (a nevysvětlitelného) důvodu mezi tyto velmi citlivé informace zařadil IP adresu.
19. Žalobce dále k vyjádření žalovaného uvedl, že nemá výraznější pochybnost o tom, že snímky jsou odesílány na server městské policie. Zásadně však pochybuje o tom, že tam jsou zasílány přímo. Žalobce má (blíže nespecifikované; pozn. soudu) poznatky o tom, že snímky „putují“ přes servery třetích stran, tzn. že fakticky měří obchodní společnost, která pak pouze

připravená oznámení přestupku postoupí městské policii k formálnímu postoupení úřadu. Dle žalobce žalovaný nechce sdělit IP adresu prvního serveru, na který jsou snímky odesílány, právě proto, že nejde o server obecní policie ani města. Žalobce nadto pochybuje, že by městská policie měla vlastní server. Jednak proto, že způsobilost nabývat majetek má toliko obec, zadruhé proto, že by dle žalobce bylo zvláštní budovat dvě paralelní IT infrastruktury v rámci jedné obce a jejích orgánů tím spíše, že žalovaný argumentuje nemožností informaci poskytnout s odkazem na Systémovou příručku pro oblast informační bezpečnosti IS Magistrátu města Chomutova. Na jedné straně tedy žalovaný argumentuje, jako kdyby server patřil magistrátu, jinde však tvrdí, že ochrana osobních údajů je zaručena, protože snímky jsou transferovány rovnou na server městské policie. To jen podtrhuje zájem žalobce o požadovanou informaci. Žalobce má za to, že pokud by fotografie byly vskutku přímo transferovány na server městské policie, nebylo by důvodu jeho IP adresu tajit. InfZ dle žalobce navíc nepodmiňuje poskytnutí informace prokázáním veřejného zájmu, a proto žalobce považuje za nadbytečnou argumentaci žalovaného absencí veřejného zájmu na zveřejnění IP adresy.

20. Žalobce nadále považuje znalost IP adresy za zcela klíčovou, neboť není ochoten se spokojit s nepodloženým ujištěním, že radarová data neopouštějí sféru orgánů veřejné moci. K tomu žalobce poznamenal, že například měření v obci Varnsdorf či Šternberk bylo také správními orgány zpočátku prezentováno jako legální, avšak posléze byly zjištěny detailnější informace o jeho fungování, pro které pak Nejvyšší správní soud označil takové měření za nezákonné. Žalobce tedy informaci potřebuje k tomu, aby se případně mohl v jiných soudních řízeních bránit proti měření provedenému takovýmto radarem, resp. proti použití radarových záznamů jakožto důkazu proti své osobě.

Posouzení věci soudem

21. O žalobě soud rozhodl v souladu s § 51 odst. 1 zákona č. 150/2002 Sb., soudní řád správní, ve znění pozdějších předpisů (dále jen „s. ř. s.“) bez jednání, neboť žalobce s tímto postupem výslovně souhlasil (což vyjádřil v bodu I své žalobní repliky) a žalovaný nesdělil soudu do dvou týdnů od doručení výzvy svůj nesouhlas s takovýmto projednáním, ačkoli byl ve výzvě výslovně poučen, že nevyjádří-li se v dané lhůtě, má se za to, že souhlas s rozhodnutím bez jednání byl udělen. Jednání nebylo třeba konat ani kvůli dokazování, neboť soud vyšel plně z obsahu žalovaným předloženého správního spisu, jímž se dokazování dle ustálené judikatury neprovádí, a účastníci ve svých podání žádné důkazní návrhy neuplatnili.
22. Napadené rozhodnutí soud přezkoumal v řízení podle části třetí hlavy druhé prvního dílu s. ř. s., který vychází z dispoziční zásady vyjádřené v § 71 odst. 1 písm. c), písm. d), odst. 2 věty druhé a třetí a v § 75 odst. 2 s. ř. s. Z této zásady vyplývá, že soud přezkoumává zákonnost napadeného rozhodnutí správního orgánu pouze v rozsahu, který žalobce uplatnil v žalobě nebo během dvouměsíční lhůty po oznámení rozhodnutí dle § 72 odst. 1 s. ř. s. Povinností žalobce je proto tvrdit, že správní rozhodnutí nebo jeho část odporuje konkrétnímu zákonnému ustanovení a toto tvrzení i zdůvodnit. Nad rámec žalobních námitek musí soud přihlídnout toliko k vadám napadeného rozhodnutí, k nimž je nutno přihlížet bez návrhu nebo které vyvolávají nicotnost napadeného rozhodnutí podle § 76 odst. 2 s. ř. s. Takové nedostatky však v projednávané věci nebyly shledány.
23. Na tomto místě soud předesílá, že po přezkoumání skutkového a právního stavu projednávané věci dospěl k závěru, že žaloba není důvodná.

24. Soud se nejprve zabýval uplatněnou námitkou nepřezkoumatelnosti. Podle žalobce nebyly v prvostupňovém ani v žalobou napadeném rozhodnutí vyjasněny zákonné důvody, které zakládají povinnému subjektu právo omezit poskytnutí informace. Žalobce má za to, že nepostačí obecné tvrzení o tom, že požadovaná informace může narušit kybernetickou bezpečnost. Musí být vysvětleno, proč poskytnutí takové informace významně nebo přímo ohrozí bezpečnostní opatření stanovené zvláštním předpisem, o jaké bezpečnostní opatření jde a jakým předpisem je stanoveno. Soud tuto námitku neshledal, z níže uvedených důvodů, opodstatněnou.
25. Rozhodnutí je nepřezkoumatelné pro nedostatek důvodů, jestliže z jeho odůvodnění není seznatelné, proč správní orgán považuje námitky účastníka za liché, mylné nebo vyvrácené, které skutečnosti vzal za podklad svého rozhodnutí, proč považuje skutečnosti tvrzené účastníkem za nerozhodné, nesprávné nebo jinými řádně provedenými důkazy vyvrácené, podle které právní normy rozhodl a jakými úvahami se řídil při hodnocení důkazů. Nepřezkoumatelnost rozhodnutí pro nedostatek důvodů musí být vykládána ve svém skutečném smyslu, tj. jako nemožnost přezkoumat určité rozhodnutí pro nemožnost zjistit v něm jeho obsah nebo důvody, pro které bylo vydáno (srov. usnesení rozšířeného senátu Nejvyššího správního soudu ze dne 19. 2. 2008, č. j. 7 Afs 212/2006-76).
26. S ohledem na zásadu jednotnosti správního řízení je nutné rozhodnutí správního orgánu prvního stupně (zde povinného subjektu) a rozhodnutí odvolacího orgánu (zde žalovaného) posuzovat jako celek (srov. usnesení rozšířeného senátu Nejvyššího správního soudu ze dne 12. 10. 2004, č. j. 5 Afs 16/2003-56, či přiměřeně rozsudek téhož soudu ze dne 27. 2. 2013, č. j. 6 Ads 134/2012-47).
27. Z prvostupňového rozhodnutí vyplývá, že povinný subjekt odmítl poskytnout žalobci příslušnou informaci z důvodu uvedeného v § 11 odst. 1 písm. d) InfZ. Podle tohoto ustanovení platí, že *povinný 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*. K tomu prvostupňové rozhodnutí obsahuje citaci z publikace autorů Tuháček, M., Jelínková, J. *Zákon o svobodném přístupu k informacím. Praktický komentář*. § 11 [Systém ASPI]. Wolters Kluwer. ASPI_ID KO106_1999CZ: „Ustanovení § 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.“ (zvýraznění převzato z prvostupňového rozhodnutí; pozn. soudu). Následuje pak povinným subjektem vyjádřený názor, že „poskytnutí požadované informace je schopno narušit či ohrozit kybernetickou bezpečnost. Poskytnutí IP adresy je rovno potenciálnímu ohrožení

kybernetické bezpečnosti celého systému. Neposkytnutím IP adresy předcházíme zneužití IP adresy pro kybernetické útoky, které mohou vést k neoprávněnému napadení. Dále může poskytnutí IP adresy znamenat potenciální ohrožení DDoS útoky, která mohou způsobit přetížení sítě a narušení její funkčnosti, potenciální umožnění neoprávněného přístupu, narušení bezpečnosti sítě, zařízení i dat“.

28. V odůvodnění žalobou napadeného rozhodnutí žalovaný konstatoval, že „odmítnutí poskytnout informaci o IP adrese prvního serveru, na který jsou přenášeny snímky z rychloměru, je odůvodněné a v souladu s omezením právo na informaci tak, jak je vymezeno v ustanovení § 11 odst. 1 písm. d) zákona č. 106/1999 Sb.“. Zcela se ztotožnil „s odůvodněním povinného subjektu, v němž odkazuje jak na komentářovou literaturu, tak dále odmítnutí odůvodňuje rizikem zneužití IP adresy pro např. útoky DDoS“. K tomu žalovaný v napadeném rozhodnutí dodal, že „v současné době je již obecně známou skutečností, že k útokům DDoS (...) postačuje znalost právě IP adresy (...), která slouží k identifikaci zařízení, resp. serveru, v internetovém prostředí, a že k takovým útokům na objekty veřejné správy dochází, viz např. kybernetický útok na Městský úřad v Ostrově na Karlovarsku z měsíce září minulého roku (žalovaný připojil hypertextový webový odkaz na konkrétní článek internetových stránek města Ostrov; pozn. soudu). V případě útoku DDoS je cílený server pod příslušnou IP adresou zahlcen množstvím požadavků, jež není schopen zpracovat, a dochází k jeho kolapsu a nedochází k přenosu dat. V tomto případě záznamů přestupků v dopravě. Tedy i když se v případě IP adresy serveru nejedná o utajovanou skutečnost, její zpřístupnění by mohlo vést k významnému ohrožení zařízení, jehož prostřednictvím je naplňováno zákonné zmocnění, viz ustanovení § 79a zákona č. 361/2000 Sb.“ (který žalovaný citoval; pozn. soudu). Dalším důvodem pro zamítnutí žádosti byla dle žalovaného „i skutečnost, že server s požadovanou IP adresou slouží k přijímání dat o přestupkovém, tedy trestním jednání, tedy dat značně citlivých, a znalost této IP adresy tak rozhodně nemůže být ve veřejném zájmu, jak tvrdí žadatel. Nadřízený orgán tak ve shodě s povinným subjektem dospěl k závěru, že požadovanou IP adresu serveru nelze z důvodu potenciálního ohrožení kybernetickým útokem poskytnout“.
29. Z výše citovaného odůvodnění prvostupňového rozhodnutí je soudu zřejmé, že povinný subjekt nekonkretizoval, co přesně považoval za „bezpečnostní opatření stanovené na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku“ zmiňované v § 11 odst. 1 písm. d) InfZ. Toto pochybení, jež by samo o sobě způsobovalo nepřezkoumatelnost prvostupňového rozhodnutí, nicméně v žalobou napadeném rozhodnutí zhojil žalovaný konstatováním, že ačkoli IP adresa není utajovanou skutečností, její zpřístupnění by mohlo vést k významnému ohrožení zařízení, jehož prostřednictvím je naplňováno zákonné zmocnění obsažené v § 79a zákona č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), ve znění pozdějších předpisů (dále jen „zákon o silničním provozu“). Podle poslední zmíněného ustanovení platí, že za účelem zvýšení bezpečnosti provozu na pozemních komunikacích je policie a obecní policie oprávněna měřit rychlost vozidel. Obecní policie tuto činnost vykonává výhradně na místech určených policií, přitom postupuje v součinnosti s policií.
30. Dle soudu tedy žalovaný v napadeném rozhodnutí dodatečně ozřejmil, že „první server“, na který daný rychloměr zasílá pořízené záznamy měření, je zařízením, jehož prostřednictvím je naplňováno zákonné zmocnění obecní policie měřit za účelem zvýšení bezpečnosti provozu na pozemních komunikacích rychlost vozidel, a že zpřístupnění informace o jeho IP adrese by mohlo vést k významnému ohrožení plnění účelu daného rychloměru [které žalovaný podle celkového vyznění napadeného rozhodnutí považoval za „bezpečnostní

opatření“ ve smyslu § 11 odst. 1 písm. d) InfZ stanovené na základě § 79a zákona o silničním provozu k zajištění **bezpečnosti** silničního provozu].

31. Současně má soud za to, že v žalobou napadeném rozhodnutí (ve spojení s rozhodnutím prvostupňovým) bylo srozumitelně, a tudíž přezkoumatelně, vysvětleno, proč případné kyberbezpečnostní hrozby (zejména DDoS útoky), umožněné znalostí IP adresy serveru, jsou správními orgány považovány za významné ohrožení funkčnosti bezpečnostního opatření (rychloměru a přenosu jím pořízených snímků až do přímé dispozice obecní policie).
32. Není tudíž důvodná žalobní námitka, že napadené rozhodnutí dostatečně nespecifikovalo konkrétní bezpečnostní opatření, jehož účinnost může být poskytnutím informace narušena, nevyjasnilo, kterým zvláštním právním předpisem je toto bezpečnostní opatření stanoveno ani nevysvětlilo podstatu významného ohrožení konkrétního bezpečnostního opatření. Napadené rozhodnutí (ve spojení s rozhodnutím prvostupňovým) je ohledně těchto otázek srozumitelně a přezkoumatelně odůvodněno.
33. Soud v kontextu výše vypořádané námitky nepřezkoumatelnosti považuje za nezbytné upozornit, že otázku správnosti výše citovaných závěrů obou správních rozhodnutí posuzuje soud vždy v mezích řádně uplatněných žalobních bodů. Konstatuje-li tedy soud přezkoumatelnost závěrů či názorů učiněných v žalobou napadeném rozhodnutí (či jemu předcházejícím prvostupňovém rozhodnutí), nevyjadřuje se tím k jejich správnosti.
34. Pokud žalobce dále namítal, že obdobně i znalost fyzické adresy obecního úřadu je nezbytná pro „jeho vykradení“, a přesto není úřad oprávněn tuto adresu tajit, činil tak nedůvodně. K budově (sídlu) obecního úřadu se totiž výslovně vztahuje celá řada zákonných ustanovení, jež v konečném důsledku znemožňují vůbec uvažovat o tom, že by sídlo úřadu mohlo plnit svou funkci, jestliže by jeho adresa zůstala utajena. Na rozdíl od toho v případě IP adresy serveru určeného k prvotní recepci dat rychloměru tomu tak není, přičemž správní orgány důvodně poukazovaly na zcela elementární kyberbezpečnostní požadavek spočívající v nesdělování údajů o technické infrastruktuře (vč. IP adresy serveru), jež mohou být zneužity ke kybernetickému útoku (tzv. *security through obscurity*, tedy „bezpečnost skrze utajení“ či „bezpečnost založená na neznalosti“; k tomu srov. rozsudek Městského soudu v Praze ze dne 17. 4. 2024, č. j. 8 A 82/2023-43). Dle soudu je žalobcem uplatněná analogie zcela nepřipadná už jen proto, že s adresou obecního úřadu jakožto „sídlem ohlašovny“ počítá např. § 3 odst. 3 písm. g) zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), ve znění pozdějších předpisů, a v důsledku toho může být i adresou, na kterou mohou být za zákonem stanovených podmínek doručovány účastníku soudního řízení soudní písemnosti (srov. § 50m zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů). Údaj o adrese sídla správního orgánu (tedy i obecního úřadu) je také nezbytný pro určování místní příslušnosti v mnoha různých typech správních či soudních řízení. Dle soudu je tedy zřejmé, že žalobce porovnává neporovnatelné.
35. Stejně tak soud neshledává relevantní žalobcem zmiňovanou veřejnost IP adresy internetových stránek povinného subjektu (jež je součástí internetových stránek města Chomutov). Jednak je zřejmé, že primárním účelem internetových stránek města Chomutov je zprostředkování informací směrem k veřejnosti a mimo to také plnění zákonné povinnosti zveřejňovat obsah úřední desky způsobem umožňujícím dálkový přístup (§ 26 odst. 1 *in fine* zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů). Veřejný přístup

k takovým internetovým stránkám se předpokládá (bez něj by postrádaly jakéhokoli smyslu), s čímž se samozřejmě pojí i možnost veřejnosti zjistit IP adresu těchto stránek, jak demonstroval žalobce v žalobě. Naproti tomu server určený k prvotnímu přijímání rychloměrem pořízených záznamů takovému ani žádnému obdobnému účelu neslouží. Za podstatné však soud považuje, že žalovaný v napadeném rozhodnutí netvrdil, že by IP adresa serveru přijímajícího data z rychloměru byla „chráněným údajem“, jak v žalobě navozuje žalobce. Důvodem pro odmítnutí poskytnutí informace nebyla její „ochrana“ ve smyslu zákonem (či jiným obecně závazným předpisem) výslovně zakotvené výluky zveřejňování. Byl jím závěr žalovaného, že poskytnutí této informace by ve faktické rovině snižovalo účinnost (ohrožovalo plnění funkce) bezpečnostního prostředku představovaného instalovaným rychloměrem. Žalobce ostatně tento závěr žalovaného nijak kvalifikovaně v žalobě nespороval, když i sám připustil, že při znalosti IP adresy může být realizován DDoS útok na daný server.

36. Žalobce v souvislosti se zjistitelností IP adresy internetových stránek povinného subjektu také namítal, že je-li veřejně známa IP adresa koncového serveru, na kterém jsou data uložena (server povinného subjektu), pak není důvod tajit IP adresu jiného serveru, přes který jsou tato data transferována. Daná námitka je však dle názoru soudu lichá. Jak soud uvedl již výše v tomto rozsudku, žalobou napadené rozhodnutí je založeno na závěru, že žalobcem požadovaná informace, stane-li se veřejně známou, může vést k významnému ohrožení funkčnosti daného serveru, a tím i celého procesu přenosu dat pořízených příslušným rychloměrem, který byl instalován jako bezpečnostní opatření dle § 11 odst. 1 písm. d) InfZ ve spojení s § 79a zákona o silničním provozu. Z hlediska posouzení, zda jsou splněny zákonné podmínky pro odmítnutí poskytnutí informace o IP adrese jednoho ze serverů, jímž rychloměrem pořízená data protékají (v této věci konkrétně prvotního serveru přijímajícího záznamy z rychloměru), je irelevantní, zda IP adresy předchozích, dalších, či dokonce posledního článku řetězce zařízení zajišťujících transfer dat jsou veřejně známé. Podstatné naopak je, zda poskytnutí konkrétní informace může významně ohrozit účinnost bezpečnostního opatření ve smyslu § 11 odst. 1 písm. d) InfZ. Koncový server, je-li jeho IP adresa veřejnosti přístupná, může být jeho provozovatelem buďto odpovídajícím způsobem zabezpečen proti hrozícímu typu útoku (například odpovídajícím typem firewallu či jiným softwarovým řešením); konkrétně pak data pořízená rychloměrem mohou být (jak poznamenal žalovaný ve svém vyjádření k žalobě) stažena na pevný nosič či na disk bez přístupu k veřejné síti.
37. Pokud se žalobce v žalobě rovněž vymezil vůči závěru žalobou napadeného rozhodnutí, že není dán veřejný zájem na veřejnosti IP adresy prvního serveru, soud žalobci přisvědčuje v tom, že i pokud by takový veřejný zájem dán nebyl, nešlo by o důvod k odmítnutí poskytnutí příslušné informace. Podmínka prokázání veřejného zájmu na poskytnutí informace (doplněná o podmínku převahy takového zájmu nad zájmem na ochraně informace), vyjádřená v § 8c odst. 1 písm. b) InfZ, se vztahuje pouze na informování o příjmech fyzických osob. Žádné obdobné ustanovení s univerzální aplikovatelností však daný zákon neobsahuje, a proto nejde o obecný předpoklad poskytnutí každé požadované informace. Pokud tedy žalovaný v žalobou napadeném rozhodnutí uvedl, že *„dalším důvodem pro zamítnutí žádosti je i skutečnost, že server s požadovanou IP adresou slouží k přijímání dat o přestupkovém, tedy trestním jednání, tedy dat značně citlivých, a znalost této IP adresy tak rozhodně nemůže být ve veřejném zájmu, jak tvrdí žadatel“*, reagoval tím sice na žalobcovo tvrzení o existenci veřejného zájmu na zveřejnění IP adresy daného serveru, avšak nesprávně přitom shledal, že jde o další důvod pro zamítnutí (správně odmítnutí; pozn.

soudu) žádosti. Tato zjevná vada žalobou napadeného rozhodnutí však nemůže být sama o sobě příčinou jeho zrušení, neboť výrok žalobou napadeného rozhodnutí bude nesprávný pouze tehdy, neobstojí-li žádný z důvodů odmítnutí žádosti. Jak již soud uvedl výše, žalobce v žalobě nezpochybnil právní názor, že příslušný rychloměr je bezpečnostním opatřením ve smyslu § 11 odst. 1 písm. d) InfZ ve spojení s § 79a zákona o silničním provozu, a žalobní námitky sporující významné ohrožení jeho účinnosti zveřejněním IP adresy serveru prvotně přijímajícího rychloměrem pořízené záznamy neshledal soud důvodnými. Daný důvod pro odmítnutí žalobcovy žádosti (v části požadující poskytnutí IP adresy „prvního serveru“), tedy v nynějším soudním přezkumu (limitovaném uplatněnými žalobními) body obstál, a proto obstálo i žalobou napadené rozhodnutí.

38. Soud neopomněl, že žalobce ve své replice uvedl, že interní směrnice povinného subjektu č. 2023-19 nemůže založit důvod pro odmítnutí žádosti o informace a že IP adresa serveru k přijímání radarových záznamů nemůže být *„detailem spadajícím pod chráněné části dokumentace a zároveň velmi citlivou informací z hlediska bezpečnosti“*. Žalobce tím reagoval na obsah vyjádření, jež předtím žalovaný podal k jeho žalobě. Soud si však nemohl nepovšimnout, že nejen žalobce, ale i žalovaný (byť je autorem žalobou napadeného rozhodnutí) pominul, že napadené rozhodnutí je založeno na posouzení příslušného rychloměru jako bezpečnostního opatření dle § 11 odst. 1 písm. d) InfZ ve spojení s § 79a zákona o silničním provozu, a hodnocení poskytnutí IP adresy prvního serveru jako významného ohrožení tohoto bezpečnostního opatření. Žalovaný tedy ve svém vyjádření k žalobě poněkud mimoběžně (a nadto obecně) argumentoval zákonem o kybernetické bezpečnosti či zákonem o elektronických komunikacích, jako by snad žalobou napadené rozhodnutí mělo být naopak postaveno na posouzení „nesdělování IP adresy prvotního serveru“ jako bezpečnostního opatření dle § 11 odst. 1 písm. d) ve spojení s dílčími ustanoveními zákona o kybernetické bezpečnosti či zákona o elektronických komunikacích. Polemika, kterou žalobce ve své replice směrem k vyjádření žalovaného uplatnil, nemá pro posouzení důvodnosti žaloby význam, jelikož nesměruje proti výše popsanému důvodu, na němž je žalobou napadené rozhodnutí založeno, a který i ve světle uplatněných žalobních námitek obstál.
39. Žalobce v replice rovněž obsáhle reagoval na žalovaným zopakovaný názor, dle kterého mělo žalobci pro účely zjištění, zda rychloměrem pořízené snímky unikají v některé fázi datového transferu z dispoziční sféry orgánů veřejné moci, postačovat zodpovězení jiného bodu jeho informační žádosti (a to konkrétně bodu 10, k němuž bylo žalobci sděleno, že *„snímky jsou v pravidelných intervalech odesílány automaticky na server Městské policie, kde se zpracovávají v programu ARCHIV“*). Soud opět odkazuje na již výše uvedené, a to konkrétně v ohledu, že pro posouzení důvodnosti žaloby bylo podstatné, zda v přezkumu provedeném v mezích žalobních bodů ob stojí nosný důvod odmítnutí žádosti o informaci. Mezi účastníky řízení přitom nebylo sporu o tom, že příslušná dílčí informace (IP adresa „prvního serveru“ přijímajícího snímky pořízené daným rychloměrem) nebyla žalobci poskytnuta a že žádost byla v této části prvostupňovým rozhodnutím odmítnuta. Důvodem pro odmítnutí přitom nebylo přesvědčení povinného subjektu (či žalovaného) o tom, že se žalobce pro účely uspokojení své informační potřeby měl spokojit toliko s poskytnutím informací požadovaných v ostatních bodech jeho žádosti. Tuto argumentaci (vůči níž se žalobce v replice vymezoval) uplatnil žalovaný až ve svém vyjádření k žalobě, a není tedy součástí důvodů žalobou napadeného rozhodnutí; současně tedy platí, že její validita nemůže být rozhodující pro posouzení důvodnosti žaloby. Žalovaný navíc touto argumentací

podepřel svou domněnku (rovněž formulovanou až ve vyjádření k žalobě) o možné zneužívající povaze daného bodu žalobcovy informační žádosti.

40. K tomu soud považuje za vhodné poukázat na názor vyjádřený Nejvyšším správním soudem v rozsudku ze dne 27. 6. 2007 č. j. 6 As 79/2006-58, č. 1342/2007 Sb. NSS, dle něhož „*povinný subjekt není oprávněn jakkoli zkoumat a zabývat se otázkou účelnosti a důvodnosti žadatelovy žádosti či jeho motivy*“. Zdejší soud si tento názor osvojil, byť upozorňuje, že jej nelze vnímat ryze dogmaticky (a to zejména se zřetelem na obecný právní princip zákazu zneužití práva). Přesto ale lze uvést, že veškerá žalobcem v replice předestřená argumentace ve vztahu k motivaci ke získání IP adresy příslušného serveru je nepodstatná, neboť povinný subjekt (ani žalovaný) nebyl oprávněn tuto jeho motivaci jakkoli zkoumat či se jí zabývat. To se týká žalobcem líčených pochybností o tom, zda rychloměrem pořízené snímky putují přes servery „třetích stran“, a také žalobcem proklamované potřeby ověřit právě pomocí znalosti IP adresy „prvního serveru“, zda tomu tak případně není. Je třeba navíc zdůraznit, že povinný subjekt v prvostupňovém rozhodnutí mezi důvody pro odmítnutí žádosti ani neuváděl jakoukoli domněnku o možné nekalé žalobcově motivaci. Stejně tak ji neuváděl ani žalovaný v napadeném rozhodnutí. Důvody pro odmítnutí příslušné části žádosti byly jiné, jsou popsány výše v tomto rozsudku a soud na ně pro stručnost odkazuje.
41. Soud samozřejmě nezamýšlí popřít, že v demokratickém právním státě obecně platí zákaz zneužití práva jako obecný právní princip. Žalovaný přitom poukazoval ve svém vyjádření k žalobě na možné zneužití práva na svobodný přístup k informacím, a to ve vztahu k osobě žalobcovy nynější zástupkyně, advokátky Mgr. Rebecky Mořovské Židuliakové, jež se měla dle bodů 19 a 22 rozsudku Městského soudu v Praze ze dne 18. 12. 2024, č. j. 5 A 107/2024-31, dopouštět systémových obstrukcí v řízení o žalobě týkající se právě poskytování informací dle InfZ. Soud k této domněnce žalovaného poznamenává, že její míra obecnosti prakticky brání tomu, aby se jí soud blíže zabýval. Z žalovaným poukazovaného rozsudku Městského soudu v Praze nevyplývá ohledně naznačované zneužívající povahy počínání samotného žalobce ničeho, což je patrné už jen z iniciál jména tehdejšího žalobce (Z. Š.) či iniciál jmen dalších žalobců uvedených tamním soudem v závěru bodu 20 odůvodnění („Z. S., J. O. či K. K. a další“). Je pravdou, že uvedené osoby pojí totožná osoba zástupkyně, a sice výše jmenovaná advokátka. To však dle zdejšího soudu bez dalšího nedokládá zneužívající povahu nynější žádosti o poskytnutí informace. Žalovaným odkazovaný rozsudek Městského soudu v Praze navíc popisuje obstrukční praktiky v přestupkových řízeních (což se netýká nyní posuzované věci), případně šikanózní množství opakujícími se subjekty podávaných repetitivních či nesmyslných žádostí o poskytnutí konkrétních písemností ze správního spisu za účelem generování průtahů s vyřizováním těchto žádostí povinnými subjekty a následného obohacování se o náhradu nákladů řízení o žalobách na ochranu proti nečinnosti. Ani to však dle názoru soudu *prima facie* nijak nesouvisí s nyní posuzovanou věcí. Soud tedy uzavírá, že prvostupňové ani napadené rozhodnutí neodůvodňují odmítnutí příslušné části žádosti zneužitím práva na svobodný přístup k informacím a nic nenasvědčuje ani tomu, že by zneužití práva mělo být spatřováno v podané žalobě proti napadenému rozhodnutí.
42. S ohledem na všechny shora uvedené skutečnosti po přezkoumání dané věci v rozsahu žalobních námitek dospěl soud k závěru, že žaloba není důvodná, a proto ji výrokem I rozsudku podle § 78 odst. 7 s. ř. s. zamítl.

43. Současně v souladu s § 60 odst. 1 věty první s. ř. s. výrokem II rozsudku nepřiznal žádnému z účastníků právo na náhradu nákladů řízení, neboť žalobce neměl ve věci úspěch a žalovanému náklady řízení nad rámec jeho běžné úřední činnosti nevznikly.

Poučení:

Proti tomuto rozhodnutí lze podat **kasační stížnost** ve lhůtě dvou týdnů ode dne jeho doručení. Kasační stížnost se podává ve dvou vyhotoveních u Nejvyššího správního soudu, sídlem Moravské náměstí 611/6, 657 40 Brno. O kasační stížnosti rozhoduje Nejvyšší správní soud.

Lhůta pro podání kasační stížnosti končí uplynutím dne, který se svým označením shoduje se dnem, který určil počátek lhůty (den doručení rozhodnutí). Připadne-li poslední den lhůty na sobotu, neděli nebo svátek, je posledním dnem lhůty nejblíže následující pracovní den. Zmeškání lhůty k podání kasační stížnosti nelze prominout.

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

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

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

Ústí nad Labem 10. prosince 2025

Ing. Mgr. Martin Jakub Brus v. r.
předseda senátu