PROTI POSKYTNUTÍ INFORMACÍ POVINNÝM SUBJEKTEM PŘIŠLY 4 STÍŽNOSTI:

První stížnost navazovala na žádost o poskytnutí informace, kterou povinný subjekt vyhodnotil jako šikanózní podle § 11a odst. 1 písm. a) a vydal rozhodnutí o odmítnutí. Rozhodnutí o odmítnutí adresoval zástupci společnosti, který prostřednictvím své osobní datové schránky podal žádost a současně byl na konci žádost výslovně uveden ve smyslu *Společnost se sídlem, zastoupena XXX, ředitelem*. Stížnost podala společnost s tvrzením, že jim nebyla poskytnuta informace na jejich žádost. Povinný subjekt na to sdělil, že Rozhodnutí bylo zasláno řediteli do jeho datové schránky, prostřednictvím které byla žádost podána a současně s tím vydal rozhodnutí o odmítnutí ve stejném znění i vůči společnosti.

Druhá stížnost byla podána proti poskytnutí informace na žádost, kterou se žadatel dotazoval na:

- způsoby vyřízení žádosti o uplatnění opatření proti nečinnosti
- jaká konkrétní opatření byla učiněna k řešení nesprávných úředních postupů
- jaké konkrétní úkony v řízení o námitce provedl povinný subjekt, včetně čísel jednacích a dat
- jaká je průměrná doba řízení

Žadateli byly poskytnuty informace s jejichž rozsahem nebyl spokojen a podal stížnost. Povinný subjekt doplnil informace a současně vydal rozhodnutí o částečném odmítnutí žádosti s tím, že neexistuje žádné usnesení, které by mohl poskytnout, a že nemůže poskytnout všechna čísla jednací v zákonné lhůtě, když je oprávněná úřední osoba v pracovní neschopnosti, ale že je doplní okamžitě, jak se vrátí na pracoviště.

Žadatel se proti tomuto rozhodnutí odvolal a nadřízený orgán přikázal informace poskytnout, když u neexistujícího usnesení z pohledu povinného subjektu přikázal poskytnout své usnesení, kterým postoupil „žádost o uplatnění opatření proti nečinnosti“ povinnému subjektu jako věcně a místně příslušnému. Povinný subjekt nerozporoval, že s největší pravděpodobností nejde o usnesení, kterého se žadatel domáhal vydat, když toto usnesení nadřízeného orgánu obdržel, a usnesení poskytl. Stejně tak doplnil na základě příkazu čísla jednací, která by tak jako tak doplnil po návratu oprávněné osoby na pracoviště.

Třetí stížnost vycházela spíše z nedorozumění, když žadatel žádal zaslat oznámení o přestupku a fotografie z konkrétního spisu. Povinný subjekt poskytl Oznámení o zahájení řízení včetně fotodokumentace, na což žadatel zareagoval stížností, že mu byla poskytnuta fotodokumentace, ale nikoliv Oznámení o přestupku, které by měla vyhotovit Městská policie. Povinný subjekt obratem zaslal Oznámení o přestupku vyhotovené Městskou policií.

Čtvrtá stížnost byla podána proti poskytnuté informaci ve formě dokumentu s částečně anonymizovanými osobními údaji, což v souladu s § 15 odst. 3 zákona č. 106/1999 Sb. nemusí být řešeno vydáním Rozhodnutí o odmítnutí. Žadatelka si však podala stížnost, ve které trvala na vydání rozhodnutí o odmítnutí podle § 15 odst. 3. Povinný subjekt následně vydal Rozhodnutí o částečném odmítnutí.

OPIS PODSTATNÝCH ČÁSTÍ SOUDNÍHO ROZSUDKU

Rozsudek Krajského soudu v Ústí nad Labem č.j 141 A 13/2025-29 ze dne 10. prosince 2025 ve věci žalobce J.H proti žalovanému Krajský úřad Ústeckého kraje.

Žaloba směřovala proti rozhodnutí Krajského úřadu Ústeckého kraje, jakožto nadřízenému orgánu statutárního města Chomutova, který potvrdil rozhodnutí o částečném odmítnutí poskytnutí informace v první stupni. Statutární město Chomutov nemělo žádné náklady s řízením.

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, jíž 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.

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.

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.

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 nespecifikovali konkrétní bezpečnostní opatření, jehož účinnost může být poskytnutím informace narušena, ani nevyjasnili,
kterým zvláštním právním předpisem je toto bezpečnostní opatření stanoveno.

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 neznamená, že by byl povinný subjekt oprávněn tajit fyzickou adresu úřadu. IP adresa přitom není dle žalobcova 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.

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 žalobcova 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 přistupováno ke správnímu trestání.

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 potencionální ohrožení DDoS útoky, která mohou způsobit přetížení sítě a narušení její funkčnosti, potenciální umožnění neoprávněného přístupu, narušení bezpečnosti sítě, zařízení i dat*“.

V odůvodnění žalobou napadeného rozhodnutí žalovaný konstatoval, že „*odmítnutí poskytnout informaci o IP adrese prvého 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 identifikací 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*“

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 posledně 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.*

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].

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).

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 adresazůstala 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 nepřípadná 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.

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 nesporoval, když i sám připustil, že při znalosti IP adresy může být realizován DDoS útok na daný server.

Žalobce v souvislostí 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 útoků (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.