



odbor bezpečnostní politiky  
Nad Štolou 3  
170 34 Praha 7

Č. j. MV-115844-2/OBP-2019

Praha 21. srpna 2019

## **Stanovisko OBP k aplikaci ustanovení § 7b trestního řádu**

### **Obecná východiska**

Článek 16 Úmluvy o počítačové kriminalitě ze dne 23. listopadu 2001 (vyhlášené pod č. 104/2013 Sb. m. s, dále jen „Budapeštská úmluva“) ukládá smluvním státům povinnost přijmout legislativní a jiná opatření, která budou nezbytná k tomu, aby umožnila svým příslušným orgánům příkázat anebo obdobně zajistit urychlené uchovávání specifických počítačových dat, včetně provozních dat, která byla uložena prostřednictvím počítačového systému, zejména pokud existují důvody pro přesvědčení, že tato počítačová data jsou zvláště ohrožená ztrátou nebo pozměněním. Stát má mít možnost rovněž správci nebo jiné osobě, která má uchovat počítačová data, stanovit povinnost udržovat tyto příkazy v tajnosti po dobu stanovenou svými vnitrostátními právními předpisy.

Je však zásadní rozdíl mezi uchováním ve smyslu zakonzervování dat (preservation) a uchováním ve smyslu zadržení dat (retention). Na to jasně poukazuje i vysvětlující zpráva k Budapeštské úmluvě. Přestože v běžném jazyku se rozdíl stírá, ve vztahu k počítačovým datům je nutno odlišovat, kdy dochází k uchování – zakonzervování dat, tedy k uložení těch dat, které již existují, s cílem uchránit je před zničením či pozměněním, a zadržení dat (retention), tedy proces uložení vznikajících dat. Povinnost uložení (preservation) nemá znamenat zadržení dat (retention).

### **Příkaz k zajištění dat dle § 7b trestního řádu**

Ustanovení Budapeštské úmluvy bylo do našeho právního řádu implementováno vložением § 7b do zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů (dále jen „tr. řád“).

Uchování dat na základě § 7b tr. řádu je předběžným opatřením, které orgánům činným v trestním řízení poskytuje čas potřebný k následnému zajištění dat. Toto předběžné opatření lze použít, je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém



systemu nebo na nosiči informací<sup>1</sup>. Příkaz k uchování dat by měl být užit zejména v případě, lze-li předpokládat, že taková data jsou zvláště zranitelná/náchylná ke ztrátě nebo změně.

Jak vyplývá z dikce uvedeného ustanovení, jedná se o uchování již existujících dat, § 7b tr. řádu se nevztahuje na sběr a uchování dat do budoucna a na přístup k aktuálně přenášeným datům. Při využití § 7b tr. řádu tak dojde k uchování a následně k zajištění dat k okamžiku, kdy osoba uvedená data drží nebo je má pod svojí kontrolou. Tím se zamezí manipulaci s daty (smazání, pozměnění atp.) v mezidobí.

V žádném případě nelze po adresátech příkazu požadovat, aby uchovávali data, která v budoucnu teprve vzniknou, tedy aby uchovávali všechna data, která budou uložena v počítačovém systému nebo na nosiči informací od okamžiku vydání příkazu dle § 7b tr. řádu do okamžiku vydání povolení k použití některého ze zajišťovacích institutů. Důvodem k tomuto postupu nemůže být ani to, že se k některým datům nebude později možné dostat v důsledku časové prodlevy. Zcela jednoznačně by se totiž jednalo o nezákonný postup.

Rovněž platí, že ustanovení nemá být užíváno preventivně tak, že OČTŘ příkaz vydá a teprve následně vyhodnocuje, zda byl tento příkaz vůbec potřeba. Pro vydání příkazu dle § 7b tr. řádu musí orgán činný v trestním řízení pečlivě zvažovat skutkové okolnosti, zejména pak posuzovat přiměřenost svého postupu při posuzování doby, po kterou mají být data uchovávána, a jejich rozsahu. Při určování rozsahu dat, která mají být osobou, jež uvedená data drží nebo je má pod svojí kontrolou, uchována, je zapotřebí dbát principu přiměřenosti tak, aby do práv osob, jichž se takové úkony dotýkají, bylo zasaženo jen v nezbytné míře pro zajištění účelu trestního řízení. V případě příkazu k uchování dat, jejichž vyžádáním je zasahováno do listovního tajemství nebo je zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků (typicky se bude jednat o obsah e-mailové komunikace) je zapotřebí, aby zde orgán činný v trestním řízení vedly konkrétní skutkové okolnosti k přesvědčení, že obsah komunikace je nenahraditelný pro vyšetřování trestného činu.

V praxi běžně dochází k situacím, kdy mezi podáním žádosti a povolením určitého procesního postupu, např. sledování podle § 158d odst. 3 tr. řádu, uběhne i podstatná doba. Objevuje se otázka, zda lze v takových situacích – když má být kupříkladu pomocí sledování zjišťován obsah e-mailové komunikace - využít také

---

<sup>1</sup> Co se rozumí počítačovým systémem či nosičem informací vysvětluje důvodová zpráva k zákonu č. 287/2018 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony.



postupu podle § 7b, vydat příkaz k uchování obsahu e-mailové schránky a následně vyžádat povolení podle § 158d odst. 3 tr. řádu.

I v takovýchto případech platí právní úvahy naznačené výše, tj. bude záležet na konkrétních skutkových okolnostech daného případu. Pokud zjištěné konkrétní skutkové okolnosti vedou k závěru, že se v e-mailové schránce s vysokou pravděpodobností nachází komunikace, která je důležitá pro trestní řízení, lze takového postupu využít (nebezpečí ztráty nebo pozměnění dat bude v takovém případě vzhledem k technickým okolnostem dáno zřejmě vždy). Konkrétní okolnosti vedoucí policejní orgán k závěru o nenahraditelnosti této již uskutečněné komunikace pro trestní řízení pak přirozeně musí být součástí zdůvodnění jeho žádosti.

O jinou situaci se však bude jednat v případě, kdy má být předmětem sledování teprve budoucí e-mailová komunikace (přestože bude využit stejný procesní institut § 158d odst. 3 tr. řádu) a příkaz podle § 7b tr. řádu by měl vést k jakémusi „překlenutí“ doby mezi žádostí a vydáním povolení soudce. Vzhledem k výše popsanému charakteru tohoto ustanovení (uchování dat se může vztahovat pouze na data, která již existují v okamžiku vydání příkazu, nikoli na data, která teprve vzniknou) vůbec nelze takového cíle dosáhnout – poměrně nelogicky by došlo k uchování právě v daný okamžik existujícího obsahu e-mailové schránky, komunikace proběhlá v mezičase mezi podáním žádosti a vydáním povolení by nebyla „pokryta“ a následně by došlo ke sledování komunikace od vydání povolení. Kromě toho by se jednalo o obcházení zákona – zákonodárce do samotného ustanovení § 158d tr. řádu zařadil mechanismus postupu pro případy, kdy věc nesnese odkladu. Z něj však explicitně vyloučil případy podle odst. 3. Nahrazování výslovně vyloučeného postupu využitím ustanovení § 7b tr. řádu je tak třeba hodnotit jako postup nezákonný.

K závěru o tom, zda v dané situaci bude využití § 7b tr. řádu postupem přípustným či nepřípustným bude vždy rozhodující hodnocení konkrétních skutkových okolností – jak je naznačeno výše – a zásadní bude i dostatečné uvedení takových okolností v odůvodnění jednotlivých úkonů policejního orgánu. Vzhledem k významu chráněných zájmů, které jsou těmito instituty narušovány, se nelze v žádném případě spokojit např. pouze s obecným poukazem na možnou důležitost dat, která mají být získána, pro probíhající trestní řízení.

Obdobně je třeba hodnotit využití § 7b tr. řádu v kombinaci se zjišťováním údajů o uskutečněném telekomunikačním provozu podle § 88a tr. řádu. Zde jde o údaje, jejichž využití pro účely trestního řízení je vyčerpávajícím způsobem řešeno zvláštní právní úpravou (§ 88a tr. řádu v kombinaci s § 97 zákona č. 127/2005 Sb., o elektronických komunikacích a prováděcími právními předpisy), včetně doby jejich uchování u podnikatelů poskytujících telekomunikační služby. Je nepřipustné



takovouto zvláštní úpravu obcházet využitím tohoto institutu. Rutinní užití kombinace institutů podle § 7b a § 88a trestního řádu je nutné jednoznačně odmítnout, v naprosto výjimečných a konkrétními poznatky odůvodněných případech ji však vyloučit zcela nelze.

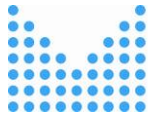
Při stanovování doby, po kterou mají být data uchovávána či po kterou k nim má být znemožněn přístup, musí být orgán činný v trestním řízení zdrženlivý. Rozhodně není možné přisvědčit tomu, aby bylo ve všech případech uloženo data uchovávat po maximální dobu, tedy po dobu 90 dní. Dobu, po kterou mají být data uchovávána nebo po kterou k nim má být znemožněn přístup, je nutné stanovit s přihlédnutím k době, v jaké je obvykle o obdobných příkazech soudcem či státním zástupcem rozhodováno. V případě, že by mělo dojít k uplynutí stanovené doby dříve, než bylo rozhodnuto o příkazu k vyžádání uchovávaných dat, a hrozilo tedy smazání dat důležitých pro trestní řízení, je samozřejmě možné tuto dobu prodloužit, vždy však pouze tak, aby ve svém souhrnu nepřesáhla maximální dobu stanovenou zákonodárcem, tedy 90 dní.

### **Vyžádání uložených dat**

Od samotného příkazu dle § 7b tr. řádu je však třeba odlišovat způsob, jakým si následně policie uchovaná data vyžádá, a to s ohledem na charakter těchto dat. Platí, že návrh na vydání příslušného zajišťovacího institutu je nezbytné podat neprodleně po vydání příkazu dle § 7b tr. řádu.

### **Organizace vydávání příkazů podle § 7b tr. řádu v policii**

Způsob, jakým policie interně organizuje vyžádání a vydávání příkazů podle § 7b tr. řádu, a jejich následné doručování adresátům, není, přísně vzato, primárně právní otázkou, ale otázkou organizační. Avšak při vědomí, že chráněné dotčené zájmy jsou nejčastěji tytéž, jako ty, které jsou dotčeny při využití § 88, § 88a či § 158d tr. řádu, stejně tak jde o obdobný okruh povinných soukromých subjektů a také je třeba řešit podobné ústavní, zákonné i praktické otázky, se nabízí využití analogického mechanismu jako v případě citovaných „tradičních“ institutů. Mechanismus, kdy jsou takovéto instituty využívány cestou jediného servisního útvaru (ÚZČ), se dosud v praxi osvědčil a má i významný interní kontrolní a preventivní aspekt a účinně brání excesům, což jsou vážné důvody pro jeho využití i v případě § 7b tr. řádu. Navíc takovéto řešení má potenciál šetřit náklady (např. zavedením technických standardů vzájemné komunikace) a snižovat logistické obtíže na straně povinných technologických subjektů, čímž je samozřejmým naplněním zákonného principu minimalizace státních zásahů, proto by mu měla být dána přednost.



## **Závěr**

- **příkaz k uchování dat podle § 7b tr. řádu lze využívat pouze vůči již existujícím datům, je nepřipustné žádat uchování dat, která teprve vzniknou**
- **příkaz musí být vždy dostatečně odůvodněn konkrétními skutkovými okolnostmi, je nepřipustné vydávat jej „preventivně“ s obecným odůvodněním**
- **příkazem nelze překonávat praktické problémy (doba do vydání soudního povolení), ani obcházet užití speciálních ustanovení trestního řádu, potřeba příkazu se vždy odvíjí od konkrétních skutkových okolností, z nichž musí vyplývat potřeba uchování konkrétních dat pro konkrétní trestní řízení**

Mgr. Radek Šubrt  
zástupce ředitele