16. 8. 2019

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Zmrazená data – zatím s otazníky

Z pohledu laické veřejnosti, nejspíš ale i z pohledu veřejnosti odborné se zcela nepozorovaně v trestním řádu ocitlo ustanovení, které významně rozšiřuje to, čemu se obecně říká povinné ukládání dat, jinak též data retention. Stalo se tak novelou trestního řádu, realizovanou zákonem č. 287/2018 Sb., která nabyla účinnosti 1.2.2019.

Odstavec 1 nově instalovaného § 7b tr. řádu, umožňuje v případě, kdy je zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací policii, státnímu zástupci či předsedovi senátu nařídit osobě, která uvedená data drží, nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu. A učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat. Jak patrno, oproti úpravě povinného ukládání provozních a lokalizačních údajů u poskytovatelů telekomunikačních služeb, lze příkazem dle § 7b odst. 1 tr. řádu „dosáhnout“ na jakákoliv data a u kohokoliv. S tím rozdílem, že poskytovatel telekomunikačních služeb je povinen data uchovávat po dobu šesti měsíců automaticky, ale příkaz se může týkat jen dat, které ke dni jeho doručení povinná osoba (dále držitel dat) skutečně drží, nebo je má pod svojí kontrolou. Data, na které se příkaz vztahuje, musí být v příkazu označena a musí být uveden důvod jejich uchování. Doba, po kterou musí držitel data uchovávat je maximálně 90 dnů. Otázkou je, zda tuto lhůtu lze dalším příkazem prodloužit. Ustanovení § 7b odst. 1 tr. řádu stanoví i další povinnost. Na jednu stranu, podle mne zcela logickou, na stranu druhou, vzhledem k tomu, že uchování dat může být uloženo komukoliv, tedy i naprostému laikovi, dost problematickou. Jde o povinnost učinit potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat.

Odstavec 2 § 7b tr. řádu umožňuje za obdobných formálních podmínek vydání příkazu, aby držitel dat znemožnil přístup jiných osob k takovým datům. Zákonným důvodem je potřeba zabránit pokračování v trestné činnosti nebo jejímu opakování.

I když rámcově je vcelku srozumitelné oč navrhovateli zákona a po něm i zákonodárcům šlo, a je tedy

třeba aby každý, kdo provozuje počítačový systém nebo nosič informací počítal s možností, že jedna nebo druhá povinnost mu bude uložena, několik nejasností, pokud jde o interpretaci obou norem, existuje. Začnu-li od toho, co mne jako advokáta může zajímat nejvíce, pak je to odpověď na otázku, zda se tato povinnost a to co po ní následuje, týká také těch, kteří mají ze zákona uloženou povinnou mlčenlivost, tedy například advokátů. K tomu se ještě vrátím.

Dost zásadní je, že ustanovení § 7b odst. 1 tr. řádu nedává odpověď na otázku, co s uchovanými daty poté, kdy uplyne stanovená doba, ale v podstatě i kdykoliv před ní. Přitom norma jasně deklaruje, dokonce jako zákonnou podmínku, že musí jít o data důležitá pro trestní řízení. Tedy jak se dostanou do rukou těch, kteří realizují trestní řízení? Praxe, pokud je mi známo, řeší další krok aplikací různých ustanovení tr. řádu. Policejní orgán nárokuje vydání uložených dat s poukazem na § 8 tr. řádu a povolení soudu k sledování osob a věcí dle § 158d odst. 3 tr. řádu. Konkrétně jsem viděl formulaci, podle níž policejní orgán žádá o provedení úkonu sledování osob a věcí dle § 158d odst. 1 3 tr. řádu, za podmínek § 88 odst. 1 tr.řádu, a to „…vydání obsahu e-mailové schránky, uchované na základě dřívějšího příkazu policejního orgánu.“ Tento postup není příliš přesvědčivý. Striktně vzato, policie přikázala zmrazit data a nyní soud povoluje držiteli uchovaných dat, aby je vydal policii. Naprosto samozřejmá je otázka, a co když držitel dat je nebude chtít vydat? Povolení přeci není příkaz! A povinnosti lze ukládat toliko zákonem.

Obě ustanovení, § 7b odst. 1 i § 7b odst. 2 tr. řádu používají pojmy „data“, „počítačový systém“ či „nosič informací“, případně hovoří o „opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat“ anebo o „znemožnění přístupu jiných osob k takovým datům“. Všechny tyto pojmy či popisy povinností ale nemají jednoznačný obsah a lze je vykládat různými způsoby.

Jediným zdrojem odpovědí na interpretační problémy, je v současné době důvodová zpráva k návrhu zákona, takto parlamentního tisku 79. Problém je v tom, že důvodová zpráva vychází z Úmluvy Rady Evropy o počítačové kriminalitě, což by jistě byl dostatečný důvod pro zákonnou úpravu, ovšem naprosto to nestačí k větší srozumitelnosti obou norem. A to, i kdybychom obsah důvodové zprávy akceptovali jako podklad k výkladu právní normy.

V důvodové zprávě je kupříkladu vysvětleno, jak rozumí předkladatel návrhu pojmu „uchovávání dat“, „počítačový systém“ a „nosič informací“. Nemohu se ale zbavit pocitu, že tyto pojmy by měly být definovány v zákoně a nikoliv v důvodové zprávě.

Jak se má zacházet z uchovanými daty podle odst. 1 § 7b tr. řádu se nepokouší důvodová zpráva ani naznačit. Tím spíše, jak, byla-li data uchována pro trestní řízení, mohou být legálně pro tento účel využita. Jak se s problémem pokouší vypořádat praxe, jsem popsal výše. Rozhodně ale nemohu tvrdit, že nedochází i k jiným právním kreacím. Zmíněný mix tří nebo čtyř právních norem, na nichž stojí konstrukce povinnosti vydat uložená data je, jak také výše zmíněno, dost nepřesvědčivý. Jde o kombinaci povinnosti ukládané § 8 tr. řádu, tedy povinnosti kohokoliv, vyhovět dožádání orgánů činných v trestním řízení při plnění jejich úkolů, což by v tomto případě zřejmě byla povinnost vydat držená data. Ovšem dle současné praxe, až to povolí soud postupem dle § 158d tr. řádu. Podmínka povolení soudu, jakkoliv problematická, neboť fakticky nejde o souhlas, ten držitel dat k dispozici se svými daty většinou nepotřebuje, by svědčila o určité nejistotě, pokud jde o právní legitimaci požadavku na vydání zmrazených dat. K čemuž ještě v případě, který jsem měl možnost zkoumat, přibývá odkaz na ustanovení § 88 odst. 1 tr. řádu. Tedy aplikace ustanovení, které upravuje podmínky odposlechu a záznamu telekomunikačního provozu. Nicméně jedním dechem je třeba současně říci, že podřízení požadavku na vydání dat souhlasu soudu je jistě k právům právnických a fyzických osob šetrnější forma, než prostá aplikace § 8 tr. řádu.

V případě osob, které mají zákonem uloženou, případně státem uznanou mlčenlivost, ovšem není jasné, do jaké míry lze tato ustanovení aplikovat. Z mého pohledu nejde o meritum tohoto článku,

takže pouze zmíním, že v případě advokáta může být problémem realizace příkazu, nařizujícího kromě retence dat i utajení tohoto opatření. Znamená to i utajení před klientem, pokud jde o fakticky o data, která klient předal anebo souvisí s právní službou, která mu je poskytována? A pokud jde o případné vydání těchto uchovaných dat, pak typicky v případě advokáta by zřejmě nepřicházel v úvahu jiný postup, než ten, jaký pro prohlídku prostor v nichž je vykonávána advokacie a pro seznamování se s obsahem zajištěných listin, jak ji upravuje § 85 b tr. řádu. Na takovou možnost přijatá úprava vůbec nepamatuje. Přitom zákonů, ukládajících mimo jiné svým adresátům povinnou mlčenlivost je celá řada.

Výkladový problém působí i požadavek na opatření, jež mají zabránit zpřístupnění informace o tom, že bylo nařízeno uchování dat. Podobně i požadavek na znemožnění přístupu jiných osob k určitým datům v počítači. Jaká opatření to mají být a jací lidé mají být vyloučeni z přístupu k datům? Všichni, včetně zaměstnanců držitele dat?

Aby toho nebylo málo, důvodová zpráva uvádí k návrhu § 7b tr. řádu, že nařízení uchování dat může být významné zejména při vyšetřování počítačové kriminality páchané prostřednictvím internetu. Počítačová data lze podle důvodové zprávy snadno změnit a významný důkazní prostředek pro trestní řízení může být zničen z důvodu nedbalého nakládání nebo uchování dat, záměrné manipulace s nimi, nebo jejich smazání ať už záměrného nebo rutinního. To je nesporné. Podle důvodové zprávy mají orgány činné v trestním řízení možnost zajistit data na místě, nicméně pokud je správce dat[1] důvěryhodný, integrita dat může být zajištěna rychleji prostřednictvím příkazu k uchování dat a příkaz k uchování dat může být pro takového správce méně invazivním zásahem do jeho legitimní činnosti a šetrnější pro jeho reputaci. Jinými slovy zde předkladatel návrhu říká, že v případě přátelsky naladěného, důvěryhodného správce dat není třeba přistupovat k takovým postupům jako je výzva k předložení věci nebo vydání věci, odnětí věci případně domovní prohlídka. Z čehož lze dovodit, že podle předkladatele, by při úvaze o zvoleném postupu měl hrát podstatnou roli i předpokládaný či předpokládatelný přístup držitele dat. Konkrétně důvodová zpráva uvádí, že: „…pokud je správce nedůvěryhodný, bude vhodnější data rovnou zajistit, než se spolehnout na jejich uchovávání na základě příkazu, který lze neuposlechnout (obejít)“. Při takovémto členění ovšem automaticky vyvstává otázka, proč by zmíněný držitel dat měl činit opatření, aby o uložení dat nebyl informován někdo další, když jde o jednorázové opatření, vycházeje z důvodové zprávy, jehož alternativou je prostě okamžité zajištění dat aplikací jiných ustanovení trestního řádu. Které asi přehlédnout nelze a nelze ani požadovat jeho utajení.

Prakticky automaticky hned vyvstává další otázka. K čemu jsou data, která jsou uchovávána na základě příkazu, o kterém již navrhovatel zákona hovoří jako o něčem, co lze obejít. Tedy nerespektovat. Z navrhovatelova komentáře by se dalo usuzovat, že při rozhodování o dalším postupu k uchování důležitých dat nehraje zásadní roli naprostá jistota autentičnosti posléze vydaných dat, ale důvěra v to, že držitel zmíněných dat s těmito daty nemanipuloval. Lze si snad představit, že budou existovat držitelé dat, které bude možné současně označit za etalon poctivosti a důvěryhodnosti a jimi vydaná data budou vnímána jako data absolutně nezkreslená. Naproti tomu lze z aplikace § 7b tr. řádu vyloučit a priori nedůvěryhodné správce dat. A mezi těmito krajními body spektra bude nepochybně existovat rozsáhlá skupina správců dat, u kterých bude možné hovořit o jakési obecné důvěryhodnosti, ovšem zpochybnitelné například vztahem k věci, k podezřelým osobám atd.

Co tedy s případnou procesní námitkou, že důvěryhodný držitel dat nebyl zase až tak důvěryhodný a s uchovanými daty manipuloval. Jak bude prokazován opak a kdy bude mít držitel dat takříkajíc certifikát důvěryhodnosti?

Tuto nejistotu ale vyvolává i předpokládatelné ne zcela jasné určení dat, která mají být uchována zejména, půjde-li o méně rutinní, nebo dokonce neprofesionální správce dat. A bude každá osoba, jíž

bude určen příkaz dle § 7b odst. 1 tr. řádu schopna jednak data v příkazu uvedená bezpečně uchovat a k tomu ještě učinit potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat? V případě provozovatele portálu či webové stránky to pravděpodobně bude znamenat vytvoření paralelního webu či portálu a archivaci původního. Zda lze takovou operaci požadovat na komkoliv je minimálně velmi nejasné.

Jak již bylo naznačeno, podobně problematická bude aplikace § 7b odst. 2 tr. řádu, dle něhož má správce dat znemožnit přístup jiných osob k takovým datům. Tyto osoby nejsou nijak definovány, a není ani v zákoně požadavek na jejich definici. Ať již individuální, tedy konkretizaci těchto osob anebo obecnější. Například určitý okruh osob atd. Formulace, kterou zákonodárce posléze akceptoval, v podstatě ukládá správci dat, je-li jím fyzická osoba, aby jen a výhradně tento správce nadále obsluhoval počítačový systém nebo nosič informací, v němž jsou uložena konkretizovaná data, a znemožnil přístup jakékoliv jiné osobě, včetně svých zaměstnanců. Jak si s takovýmto příkazem poradí právnická osoba, pak už logicky vůbec není jasné. Při tom hrou náhody může pochopitelně dojít i k situaci, že právnická osoba pověří konkrétní fyzickou osobu, aby obsluhovala systém, v němž jsou data uložena a vyloučí z možnosti přístupu jiné osoby. Ovšem bez jistoty, že právě tato pověřená osoba není přesně tím, komu by přístup k počítačovému systému nebo nosiči informací měl být znemožněn.

Při porovnání § 7b tr. řádu s úpravou ukládání provozních a lokalizačních údajů u poskytovatelů telekomunikačních služeb dle zákona č. 127/2005 Sb. ve znění pozdějších předpisů, se objevuje další problém. Je zjevné, že případný přístup k datům, dle tohoto zákona, se děje na náklady přistupujícího a podle § 97 odst. 7 tohoto zákona, za plnění povinností v této souvislosti uložených náleží právnické nebo fyzické osobě od oprávněného subjektu, který si úkon vyžádal nebo jej nařídil, úhrada efektivně vynaložených nákladů. Trestní řád, jak je dlouhodobě známo, s žádnou takovou formou refundace nepočítá. Doposud se to týkalo zejména nákladů vynaložených v souvislosti s vyhověním dožádání orgánů činných v tr. řízení právnickými či fyzickými osobami podle § 8 odst. 1 tr. řádu. Nyní přibyl i příkaz podle § 7b odst. 1 a 2 tr. řádu, který nepochybně je mutací zákona č. 127/2005 Sb. Předkladatel návrhu zákona ale viditelně, vycházeje z důvodové zprávy, vůbec neřešil, jak takové uchovávání dat po dobu max. 90 dnů za současného opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat, může být nákladné. A zřejmě totéž lze říct i na adresu příkazu podle odst. 2 § 7b tr. řádu, kdy plnění takového příkazu může být také spojeno s relativně značnými výdaji.

Je patrné, že článek je převážně inventurou nejasností, plynoucích z nové úpravy povinnosti uchovat, chránit a případně znepřístupnit příkazem určená data. To ostatně deklaruje už jeho nadpis. Hledání technicky i právně schůdných řešení by si vyžádalo mnohem hlubší analýzu a též i větší publikační prostor. Pro tuto chvíli mi ale šlo jen o upozornění na novou povinnost, která se fakticky týká kohokoliv, kdo má nejen počítač, ale i jakýkoliv nosič informací. Tedy například mobilní telefon nebo flash disk.

JUDr. Tomáš Sokol,
advokát

Advokátní kancelář Brož & Sokol & Novák s.r.o.

Sokolská třída 60
120 00 Praha 2

Tel.: +420 224 941 946
Fax: +420 224 941 940
e-mail: advokati@akbsn.eu

---

[1] Jde o ne zrovna šťastně zvolený termín vzhledem k jeho významu v oblasti úpravy ochrany osobních údajů, a proto užívám v článku označení „držitel dat“.

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Kauza Skender Bojku: Putativní nutná obrana optikou ÚS
- Novela zákona o trestní odpovědnosti právnických osob
- Nový zákon o zbraních a střelivu
- Dětský certifikát
- Přerušení výkonu trestu odnětí svobody ze zdravotních důvodů
- Trestněprávní odpovědnost členů zastupitelstva při nakládání s nepotřebným majetkem
- Kolize formalismu a ochrany obětí: nový přístup Ústavního soudu k domácímu násilí
- Podmínečné propuštění po novele trestního zákoníku
- Porušení zásady presumpce neviny orgány činnými v trestním řízení a náhrada škody za nezákonné trestní stíhání
- Trestné činy z nenávisti (hate crimes) ve světle novely trestních předpisů
- Primární viktimizace dětských obětí sexuální trestnou činností