

Překonání bezpečnostního opatření (hesla) k účtu FACEBOOK coby trestný čin

V usnesení sp. zn. 7 Tdo 1134/2020, ze dne 4. 11. 2020 se Nejvyšší soud zabýval v současné době nikoliv ojedinělým trestním případem z oblasti kyberkriminality, jehož podstata spočívala ve zneužití přístupového hesla k účtu FACEBOOK a v němž si Nejvyšší soud propůjčil na podporu své argumentace přirovnání s porušením domovní svobody užitě státním zástupcem Nejvyššího státního zastupitelství ve vyjádření k dovolání obviněného.

Obviněný byl soudem prvního a druhého stupně uznán vinným mj. právě ze spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1 tr. zákoníku, kterého se dopustil tím, že dne 29. 3. 2019 na přesně nezjištěném místě překonal za pomoci telefonního čísla bezpečnostní opatření – přístupové heslo k účtu poškozené na sociální síti facebook.com, které následně změnil, čímž uživatelce znemožnil užívat její účet na sociální síti, kdy toto nezpůsobil žádnou škodu na majetku.

Proti užití právní kvalifikaci obviněný v rámci dovolání namítl, že pachatel musí neoprávněně získat přístup k počítačovému systému překonáním bezpečnostních opatření (např. hesla), ale on v žádném případě bezpečnostní opatření nepřekonal, protože to byl on, kdo zřizoval daný počítačový účet a měl k němu také přístup. I okresní soud, v bodě 46. odůvodnění dle obviněného uvedl, že neoprávněně využil heslo, které znal z dřívější doby, a to proto, aby zablokoval přístup k facebookovému účtu poškozené. Nepřekonal tak žádnou překážku, neboť heslo k danému účtu znal.

Nejvyšší soud dovolání obviněného odmítl s tím, že považuje za příléhavé přirovnání uvedené státní zástupkyní ve vyjádření k dovolání, a to sice že profil na Facebooku je v podstatě virtuální prostor a má podobnou povahu jako „obydlí“, jehož „dveře“ tvoří počítačový systém, či jiný nosič informací, přičemž „klíčem“ k těmto „dveřím“ je bezpečnostní opatření, jimiž je lze odemknout. Trestní zákon při ochraně ústavou zaručeného práva na soukromí sankcionuje jakýkoli neoprávněný vstup do obydlí, a to i za pomoci shodného klíče, aniž by pachatel musel dveře do domu prolamovat násilím. Obdobně je tedy nutno postihovat případy, kdy pachatel prolomí „dveře“ do virtuálního prostoru například za pomoci hesla, které znal z dřívější doby, či za pomoci telefonního čísla, na který jsou tyto soukromé účty navázány. Rozhodující je – obdobně jako u porušování domovní svobody – že v okamžiku, kdy pachatel tohoto způsobu narušení soukromí využívá, ví, že do toho důvěrného prostoru vstupuje neoprávněně, a je s tímto následkem přinejmenším srozuměn. Za překonání „bezpečnostního opatření“ ve smyslu § 230 odst. 1 trestního zákoníku je proto možno považovat i využití duplikátu telefonní SIM karty, na kterou jsou tyto soukromé účty vázány, s jejichž využitím lze do důvěrného prostoru vstupovat přímo, nebo za pomoci nově vygenerovaných hesel.

Autor: JUDr. Vladimír Janošek, ARROWS

www.epravo.cz, 11. března 2021

Právo subjektu údajů na přístup k osobním údajům nejen ve veřejné správě

GDPR[1] jako obecné nařízení přiznává každému ze subjektu údajů práva, která mu mají sloužit k ochraně jeho osobních údajů. Cílem tohoto článku je přiblížit jedno z práv subjektu údajů, které mu GDPR přiznává, a to konkrétně právo na přístup k osobním údajům, tj. právo na sdělení informace o tom, zda jsou osobní údaje subjektu údajů správcem zpracovávány a případně dalších informací s tím souvisejících.

Oproti původní právní úpravě ochrany osobních údajů, posiluje nyní GDPR práva subjektu údajů, a to například vytvořením nového práva na přenositelnost údajů nebo změnou stávajících práv. Právo na přístup k osobním údajům bylo v minulosti zakotveno v čl. 12 Směrnice 95/46/ES[2] a v § 12 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOÚ“). Zatímco dříve § 12 ZOOÚ stanovoval, že má správce subjektu údajů poskytnout na základě jeho žádosti určité informace o zpracování osobních údajů, nově čl. 15 GDPR stanovuje, že má požadované informace poskytnout a současně musí poskytnout i přímo konkrétní osobní údaje, tj. např. formou kopie smluv apod. Nová úprava obsažená v GDPR tedy přinesla zejména rozšíření rozsahu informací, které jsou poskytovány a také právo na bezplatné poskytnutí

[1] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

[2] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY č. 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

jedné kopie osobních údajů. V čl. 15 GDPR dále najdeme i taxativní výčet informací, které musí být poskytnuty. Seznam zahrnuje zejména informace, které je povinen správce vést v záznamech o zpracování dle čl. 30 GDPR, např. účely zpracování, kategorie osobních údajů, příjemce atd. V zájmu větší informovanosti musí správce subjektu údajů sdělit i dobu, po kterou bude uchovávat osobní údaje, nebo minimálně kritéria, na základě kterých to bude možné určit.[3]

Právo na přístup k osobním údajům zahrnuje právo subjektu údajů na přístup ke všem zpracovávaným osobním údajům, tj. nejen k takovým, které byly poskytnuty subjektem údajů správci.[4] Správce by měl vždy posuzovat ze široka, zda se osobní údaje subjektu údajů týkají či nikoliv.

Před poskytnutím osobních údajů je nutné, aby správce neměl pochybnosti o totožnosti žadatele. Správce si může dle čl. 12 odst. 6 GDPR při pochybnostech o totožnosti žadatele vyžádat dodatečné informace nezbytné k potvrzení jeho totožnosti (ověřený podpis na žádosti, připojení elektronického podpisu apod.). Poskytnutí osobních údajů subjektu údajů jiné fyzické či právnické osobě by mohlo mít za následek velké riziko pro práva a svobodu fyzické osoby, o které byly osobní údaje poskytnuty, a to se všemi právními důsledky, včetně sankcí.

Právo na přístup k osobním údajům mají také nezletilé děti. Pokud dítě není dostatečně rozumově vyspělé na to, aby právo na přístup k osobním údajům mohlo uplatnit u správce samo, je možné, aby toto právo za něj uplatnil zákonný zástupce. GDPR přitom nevyžaduje, aby ohledně výkonu práv nezletilých subjektů údajů byl informovaný druhý zákonný zástupce, nebo aby k tomu musel udělit souhlas. Jedná se o práva, které náleží dítěti, jako subjektu údajů a zákonný zástupce v takovém případě jedná pouze ve prospěch dítěte, tudíž by tím neměl sledovat své vlastní zájmy, ale pouze zájmy dítěte.

Jak je uvedeno výše, na rozdíl od předchozí úpravy musí dle GDPR správce poskytnout informace podle čl. 13 a 14 GDPR a provádět veškerá sdělení a opatření dle čl. 15 až čl. 22 GDPR zásadně bezplatně. Výjimkou z tohoto uvedeného obecného pravidla je možnost vyúčtovat subjektům údajů dle čl. 15 odst. 3 poplatky na administrativní náklady, a to v případě poskytování další kopie zpracovávaných osobních údajů nebo v případě, kdy je žádost zjevně nedůvodná či nepřiměřená. Dříve bylo možné dle § 12 odst. 3 ZOOÚ požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace.

Každé další poskytnutí buď po delším časovém úseku, kdy je důvodné očekávat změny v údajích a jejich zpracování, nebo po každé takové změně, by mělo být bezplatné.

Pokud by subjekt údajů toto právo zneužíval (například prostřednictvím opakovaných žádostí uplatňovaných krátce po sobě) je možné takovým žádostem nevyhovět, případně za ně požadovat přiměřený poplatek za vynaložené administrativní náklady. Při stanovování přiměřeného poplatku za poskytnutí informací či učinění požadovaných úkonů dle GDPR lze analogicky použít sazebník stanovený pro účely zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon o svobodném přístupu k informacím“), nicméně lze jistě doporučit stanovení sazebníku úhrad nákladů v souvislosti se zpracováním žádosti subjektu údajů o uplatnění práva subjektu údajů podle nařízení GDPR, a to zejména pro správce, kteří sazebník dle zákona o svobodném přístupu k informacím nemají.

Podle čl. 12 odst. 1 GDPR se kopie osobních údajů poskytují písemně nebo jinými prostředky, ve vhodných případech i v elektronické formě. Vhodným případem pro použití elektronické formy je v souladu s odst. 4 tohoto článku situace, kdy subjekt údajů žádá v elektronické formě a zároveň nepožádá o to, aby ho správce informoval jiným způsobem. Vyhovuje-li správce žádosti elektronickou formou, využívá formát, který se běžně užívá, a není tedy povinen převádět informace do neobvyklých formátů dle požadavků subjektu údajů, zejména pokud je elektronický systém, do kterého subjekt údajů požaduje přístup nepřístupný neoprávněným osobám a není možné mu oprávnění poskytnout v jím žádaném rozsahu bez ohrožení práv třetích osob..

Při poskytování kopií dokumentů musí být vždy dbáno na ochranu práv třetích osob. Dle bodu 63 odůvodnění GDPR jde zejména o ochranu autorského práva, obchodního tajemství či duševního vlastnictví, tj. tedy informací, které mohou tvořit know-how správce. Dále je také třeba chránit práva dalších subjektů údajů, avšak při ochraně práv třetích osob nesmí být odepřen přístup ke všem osobním údajům žadajícího subjektu údajů, ale může být poskytnut užší rozsah údajů.[5]

Pokud správce zpracovává velké množství osobních údajů žadatele, např. u zaměstnance územně samosprávného celku a současně občana, může správce před poskytnutím informací požádat subjekt údajů, aby uvedl, jaké konkrétní informace požaduje. Po subjektu údajů obecně nelze požadovat, aby zúžil rozsah své žádosti o přístup k osobním údajům. Právo na přístup však nemůže být omezeno ani odepřeno, a pokud by tedy subjekt údajů blíže nespécifikoval svou žádost, je nezbytné mu vyhovět v plném rozsahu.

Nicméně při posuzování žádosti lze jako nedůvodnou či nepřiměřenou vyhodnotit jen část žádosti, např. žádost lze považovat za nedůvodnou a nepřiměřenou v rozsahu, ve kterém subjekt údajů (bývalý zaměstnanec) požaduje sdělení osobních údajů z emailové korespondence, protože je zřejmé, že se může jednat o nespočetné množství emailů, které navíc pocházejí

[3] NULÍČEK, M., DONÁT, J., NONNEMAN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017 str. 203 - 204

[4] Srov. např. právo na přenositelnost dle čl. 20 GDPR

[5] NULÍČEK, M., DONÁT, J., NONNEMAN, F., LICHNOVSKÝ, B., TOMÍŠEK, J., GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. Praha: Wolters Kluwer ČR, 2017 str. 206

z výkonu zaměstnání, tj. informace v nich obsažené jsou subjektu údajů, jako zaměstnanci s ohledem na výkon jeho zaměstnání pravděpodobně známé. Takovou žádost lze v této části dle čl. 12 odst. 5 písm. b) odmítnout.

O zpracování osobních údajů ve smyslu čl. 2 odst. 1 GDPR se dále nejedná, pokud je v emailové korespondenci, nebo i v jiných obdobných dokumentech, uvedeno pouze jméno fyzické osoby, která není odesílatelem ani adresátem dané korespondence. Takové údaje tedy nemusí být poskytnuty podle čl. 15 GDPR.

Důležitou otázkou při vyřizování žádosti o informace ve veřejné správě je použití či nepoužití zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“). K tomuto vydalo Ministerstvo vnitra ČR stanovisko, ve kterém uvedlo, že *zákon č. 110/2019 Sb. o zpracování osobních údajů, ve znění pozdějších předpisů, výslovně vztah ke správnímu řádu neupravuje. Existují ovšem výjimky, kdy se správní řád použije, a to při uplatnění práva na námitku nebo jiného prostředku ochrany proti zpracování osobních údajů, kdy se použijí obdobně ustanovení správního řádu o stížnosti. Předmětná úprava se však vztahuje k ochraně proti zpracování osobních údajů, nikoliv k právnímu režimu přístupu k informacím podle čl. 15 GDPR (byť získání těchto informací nepochybně může mít význam pro ověření zákonnosti zpracování osobních údajů a pro úsudek subjektu údajů o případném využití navazujících prostředků ochrany zejména podle čl. 21 GDPR).*[6]

Podobné informační právo subjektu údajů jako v GDPR bylo obsaženo rovněž v § 12 ZOOÚ. Tento zákon rovněž výslovně neřešil vztah ke správnímu řádu.

K předmětné úpravě v zákoně č. 101/2000 Sb. se nicméně vyjádřil několikrát zvláštní senát mj. v usnesení ze dne 14. 6. 2012 č. j. Konf 10/2012 – 6 a v usnesení ze dne 6. 11. 2014 č. j. Konf 7/2014 – 12, kde šlo o spor o poskytnutí informace o všech osobních údajích, které jsou o žalobci zpracovávány finančním úřadem. V obou dovodil zvláštní senát příslušnost soudu rozhodujícího v občanském soudním řízení. Na základě závěrů soudní judikatury má MVČR za to, že *„předmětné postupy nepředstavují výkon veřejné moci, a to ani v případě, že k samotnému shromažďování osobních údajů dochází při výkonu veřejné moci – např. v souvislosti s vedením správních řízení. Domníváme se, že při vyřizování žádosti o informace podle čl. 15 GDPR se nepostupuje podle správního řádu, neboť se nejedná o výkon působnosti v oblasti veřejné správy ve smyslu § 1 odst. 1.“*[7]

Vzhledem k zažitému institutu žádosti o informace dle zákona o svobodném přístupu k informacím, můžou subjekty údajů chybně podat žádost o osobní údaje dle zákona o svobodném přístupu k informacím. Na to pamatuje § 2 odst. 3 zákona o svobodném přístupu k informacím, který uvádí, že se nevztahuje na poskytování informací, pokud zvláštní zákon upravuje jejich poskytování, zejména vyřízení žádosti včetně náležitostí a způsobu podání žádosti, lhůt, opravných prostředků a způsobu poskytnutí informací, tj. že se tento obecný předpis neuplatní tam, kde existuje komplexní speciální právní úprava.

Pokud bude tedy obsahově žádost podaná chybně na základě zákona o svobodném přístupu k informacím (tj. je označena jako žádost dle zákona o svobodném přístupu k informacím), vyhodnocena jako žádost dle čl. 15 GDPR, bude žádost vyřizovat správce v rámci režimu stanoveném GDPR, a to včetně delší lhůty k vyřízení. Správce ale bude muset nejdříve žádost odmítnout v režimu zákona o svobodném přístupu k informacím, a to dle § 15 odst. 1 (s odkazem na ustanovení § 2 odst. 3) a následně bude požadavek řešit podle ustanovení GDPR. Povinnost vydat i v těchto případech rozhodnutí o odmítnutí podle ustanovení § 15 odst. 1 zákona o svobodném přístupu k informacím vychází z judikatury.[8]

Aby nebyla správcem zbytečně prodlužována doba pro poskytnutí informací, stanovuje GDPR v čl. 12 odst. 3, že správce poskytne subjektu údajů na jeho žádost bez zbytečného odkladu a v každém případě do 1 měsíce od obdržení žádosti. Lhůtu je možno prodloužit, a to s ohledem na složitost a počet žádostí, a to maximálně o dva měsíce. Do jednoho měsíce od obdržení žádosti, ale musí správce subjekt údajů vyzkoušet o tom, že bude lhůta prodloužena a současně s tím správce uvede důvody takového prodloužení.

V případě nesplnění dotčených povinností správcem má subjekt údajů možnost podat stížnost u dozorového úřadu a žádat o soudní ochranu dle čl. 12 odst. 4 GDPR.

Závěrem lze tedy říct, že nová úprava posílila práva subjektu údajů a přinesla trochu více povinností pro správce osobních údajů, zvýšila administrativu při vyřizování žádostí o přístup k osobním údajům a znemožnila správcům si vyúčtovat vzniklé náklady, což v případě veřejného subjektu má za následek menší hospodárnost při vynakládání finančních prostředků.

Autorka: Mgr. Lenka Feberová, LL.M.

www.epravo.cz, 18. března 2021

[6] Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR Ministerstvo vnitra České republiky [online]. Dostupné z: Výkladová stanoviska – Ochrana osobních údajů (mvcr.cz) str. 1

[7] Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR Ministerstvo vnitra České republiky [online]. Dostupné z: Výkladová stanoviska – Ochrana osobních údajů (mvcr.cz) str. 3

[8] Rozsudek Nejvyššího správního soudu ze dne 26. 6. 2009 č. j. 2 As 44/2008 - 72 (potvrzený rozsudkem Nejvyššího správního soudu ze dne 27. 6. 2012 9 Ans 7/2012 - 56 a rozsudkem Nejvyššího správního soudu ze dne 10. 10. 2013 č. j. 9 As 78/2013 - 26)