Finanční arbitr České republiky
Washingtonova 25, 110 00 Praha 1
Tel. 221 674 660, e-mail: arbitr@finarbitr.cz

Publikační číslo:
P/5/1/2005

N á l e z

Finanční arbitr České republiky rozhodl v souladu s ust. § 15 zákona č. 229/2002 Sb., o finančním arbitrovi, v platném znění ve sporu navrhovatelky N, bytem ..... proti instituci Q se sídlem ....., o zaplacení částky 300 000 Kč

t a k t o :

Instituce – Q je povinna vrátit navrhovatelce odčerpané peněžní prostředky ve výši 200 000 Kč s 3% úrokem z prodlení ročně od 28.12.2004 do zaplacení a ve výši 100 000 Kč s 3% úrokem z prodlení ročně od 29.12.2004 do zaplacení, a to vše do 15 dnů od právní moci tohoto nálezu.

O d ů v o d n ě n í :

Návrhem ze dne 28.2.2005 se navrhovatelka domáhala proti instituci vrácení odčerpaných peněžních prostředků v celkové výši 300 000 Kč, včetně úroků z účtu navrhovatelky č. 123456789/1111. Navrhovatelka odůvodnila svůj návrh tím, že si dne 2.1.1995 založila u instituce účet č. 123456789/1111. Tento účet si navrhovatelka založila z toho důvodu, že do instituce nastoupila jako zaměstnanec a bylo nutné mít účet, na který bude zasílána výplata. Navrhovatelka je dosud zaměstnancem instituce a s účtem neměla nikdy problémy, vše bylo v pořádku. K tomuto účtu navrhovatelka uzavřela dne 21.3.2001 Smlouvu o poskytnutí telefonního bankovnictví Q, kterou po výše uvedeném sporu zrušila.

Dále navrhovatelka uvedla, že dne 29.12.2004 zjistila, že z jejího účtu byla postupně neoprávněně převedena částka v celkové výši 300 000 Kč ve prospěch účtu č. 12-987654321/1111. Majitelem účtu je osoba jménem N.J. Transakce byly provedeny přes telefonní bankovnictví Q. Navrhovatelka osobně nikdy nedala souhlas k převodům peněz, ani je neprovedla. Proto ihned o tomto informovala vedení instituce a Policii ČR, která následně provedla opatření a pachatele při výběru peněz zadržela. Zároveň navrhovatelka podala dne 29.12.2004 reklamaci v instituci, přičemž předpokládala, že došlo k chybě ze strany jejího pracovníka a proto požadovala vrácení peněz na svůj účet. Na toto instituce reagovala tak, že ona při postupu nepochybila a odmítla navrhovatelce peníze vrátit. Navrhovatelka je však přesvědčena o tom, že někdo z instituce musel informovat pachatele o tom, jakým způsobem manipulovat prostřednictvím telefonního bankovnictví Q s účtem navrhovatelky. Musel tedy znát číslo účtu navrhovatelky, rodné číslo, PIN (osobní identifikační číslo), heslo, přístupové kódy a další důvěrné informace. Tyto údaje získal buď ze složky klienta instituce, případně ze systému instituce, neboť navrhovatelka sama nikomu tyto údaje neposkytla (doklady

neztratila, ani jí nebyly odcizeny a ani osobní údaje nikomu nesdělovala). Prostřednictvím telefonního bankovnictví Q může s účtem nakládat pouze navrhovatelka, nikdo jiný k tomuto nemá oprávnění.

Navrhovatelka ve svém návrhu dále uvedla, že v tomto sporu spatřuje zásadní nedostatek v tom, že instituci svěřila svá osobní data a následně i peněžní prostředky. Přestože je instituce povinna tyto informace chránit dle zákona č. 101/2000 Sb., tyto neochránila a v důsledku toho došlo k neoprávněnému nakládání s jejím účtem a ke škodě ve výši 300 000 Kč. Jelikož navrhovatelka svěřila své peněžní prostředky instituci (nikoli panu J.), trvá na tom, aby ji instituce tyto prostředky vrátila na její účet a v žádném případě nepřistupuje na možnost vymáhat spornou částku na panu J. cestou občanskoprávního sporu.

Instituce ve svém vyjádření navrhuje zamítnout požadavek navrhovatelky na vrácení částky 300 000 Kč s příslušenstvím, protože při provádění sporných transakcí postupovala zcela v souladu s platnými právními předpisy, resp. s dohodami uzavřenými s navrhovatelkou. Dále instituce uvádí, že při transakcích, kterými došlo k převodu částky v celkové výši 300 000 Kč, byly použity PIN a heslo zvolené navrhovatelkou. Tyto bezpečnostní prvky jsou známy pouze klientovi (zde navrhovatelka) služby telefonního bankovnictví a instituce není odpovědná za případné zneužití bezpečnostních prvků.

Dále z vyjádření instituce vyplynulo, že dle Podmínek Q pro poskytnutí a využívání telefonního bankovnictví Q (dále i jen „Podmínky“), které jsou nedílnou součástí Smlouvy o poskytnutí telefonního bankovnictví Q, je klient povinen pečovat o to, aby se jiná osoba neseznámila s využívanými bezpečnostními prvky. Instituce dále uvádí, že z protokolu o výslechu svědka ze dne 10.1.2005, který je přiložen k návrhu na zahájení řízení, je velice pravděpodobné, že dcera navrhovatelky zná jeden z bezpečnostních prvků, konkrétně heslo, což je možné považovat za nedodržení závazku klienta vyplývajícího z Podmínek. Dle Podmínek byl dále klient povinen v případě, že zjistí, že jeho bezpečnostní prvky zná neoprávněná osoba, o tom ihned informovat instituci, která by po dohodě s klientem zablokovala přístup k telefonnímu bankovnictví (dále i jen „TB“). Tento závazek nebyl navrhovatelkou dodržen.

Instituce dále ve svém vyjádření podrobně popisuje proces zabezpečení ochrany klientů TB, resp. proces aktivace služby TB. Institucí popsaný proces zabezpečení zvolený navrhovatelkou používá jako bezpečnostní prvky PIN a heslo. Dále jsou ve vyjádření instituce popsány jednotlivé kroky, které při zřizování a aktivaci služby TB zajišťují skutečnost, že žádná další osoba kromě klienta nemůže přijít do styku se všemi bezpečnostními prvky potřebnými pro aktivaci a vlastní používání služby. Dále jsou také popsány jednotlivé kroky, ze kterých se skládá bezpečnostní procedura při vlastním využívání služeb TB s ohledem na skutečnost, zda je klient identifikován automatickým hlasovým systémem IVR nebo přímo telefonním bankéřem.

Z vyjádření instituce vyplynulo také organizačně technické zabezpečení dat, kdy telefonní bankéři mohou provádět veškeré transakce klienta pouze pomocí bankovní aplikace tzv. TSS/3 a to pouze v průběhu hovoru. Telefonní bankéři mají možnost přehrávat si pouze vlastní hovory a to pouze s časovým omezením jedné hodiny zpět. Přístup do delší historie nahrávek hovorů má pouze úzká skupina vedení telefonního centra instituce a pracovníci podpory, kteří řeší reklamace klientů. K vyhledání hovorů je nutno znát kontaktní historii klienta, kterou lze získat v aplikaci TSS/3; přístup k ní je logován. Hovory klientů s hlasovým systémem (IVR) nejsou nahrávány. Loguje se pouze přístup klienta v kontaktní historii TSS/3. Na systému IVR se provádí celá identifikace a část autentizace (PIN) – to neplatí pro případ, že klient nepoužije systém IVR. Dále veškeré bezpečnostní údaje klienta (PIN, heslo

atd.) jsou uloženy v lokální databázi TSS/3 v telefonním centru instituce a jsou šifrovány. Pro žádného pracovníka instituce neexistuje přímá možnost zobrazení všech bezpečnostních prvků klienta nutných pro provedení účetní transakce prostřednictvím služby TB a telefonní bankéř nikdy v systému nevidí veškeré potřebné údaje pro provedení transakce.

Dále instituce ve vyjádření popsala stručně historii kontaktů (od září roku 2004) mezi navrhovatelkou, resp. narušitelem - osobou používající bezpečnostní identifikační údaje, a institucí. V závěru vyjádření instituce poukazuje na skutečnost, že veškeré relevantní informace poskytla Obvodnímu státnímu zastupitelství pro Prahu X.

V průběhu důkazního řízení při podání vysvětlení navrhovatelkou finanční arbitr zjistil heslo navrhovatelky. Z toho lze dovodit zcela jasně, že ten, kdo by příp. odposlouchával telefonické hovory navrhovatelky, příp. dodatečně hovory zaznamenané institucí, zjistí velmi jednoduchým způsobem již po třech posleších tajné heslo.

Z odborného posudku, který byl vypracován na základě požadavku finančního arbitra Mgr. O., finanční arbitr zjistil, že smluvní odpovědnost instituce ve vztahu ke službě TB je upravena ve Smlouvě o poskytnutí telefonního bankovnictví Q. V čl. 10 této smlouvy se uvádí, že instituce nenese odpovědnost za škody vzniklé z příčin mimo její kontrolu nebo zneužitím TB bez zavinění jejích pracovníků. Dále v Podmínkách v čl. VI odst. 3 se uvádí, že klient musí pečovat o to, aby se žádná jiná osoba neseznámila s využívanými bezpečnostními prvky. Pokud se tak stane, riziko zneužití těchto prvků spojené s realizací požadovaných služeb nese v plné výši klient. Článek VI odst. 13 týchž Podmínek pak ještě uvádí, že TB je realizována prostřednictvím veřejných telefonních linek, které neprovozuje instituce ani jiný subjekt pod její kontrolou. Tyto veřejné telefonní linky nejsou žádným zvláštním způsobem chráněny proti zneužití tajemství přepravovaných zpráv. Instituce tak nemůže ovlivnit případný vznik škody na straně klienta v důsledku zneužití tohoto tajemství. Odborník se ve svém posudku domnívá, že čl. VI odst. 3 Podmínek je neplatný, neboť představuje neplatné vyloučení odpovědnosti dle § 374 obchodního zákoníku. Domnívá se také, že toto ustanovení je taktéž v rozporu s § 13 zákona č. 101/2000 Sb., ve znění pozdějších předpisů (zákon o ochraně osobních údajů), ze kterého instituci vyplývají určité povinnosti, v souvislosti s nimiž nelze uvádět takovéto liberačními důvody. Ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. stanoví, že správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů. Zároveň § 21 téhož zákona stanoví, že v otázkách tímto zákonem neupravených se použije obecná úprava odpovědnosti za škodu.

Dále z odborného posudku vyplynulo, že služba TB je kombinovanou službou, zahrnující jak aspekt finanční služby, tak aspekt služby elektronických komunikací. Služba elektronických komunikací je služba, spočívající zcela nebo z podstatné části v přenosu signálů neboli dat. V tomto případě by se jednalo o přenos dat od navrhovatelky do instituce a opačně, probíhající prostřednictvím telefonní linky. Příkladem podobné právní otázky by mohlo být francouzské soudní rozhodnutí z tohoto roku. Francouzský soud rozhodl, že firma Yahoo!, která kromě jiného provozuje po celém světě dostupné on-line aukce, poskytuje kombinovanou službu. Yahoo! je podle francouzského soudu jak poskytovatelem hostingových služeb (tedy služeb elektronických komunikací, spočívající v zajištění provozu internetového portálu, na němž mohou třetí strany prodávat a kupovat nejrůznější zboží v rámci on-line aukcí), tak služeb vydavatelských, spočívajících v přípravě a stanovení pravidel on-line aukcí a klasifikace produktů, jež jsou předmětem těchto aukcí. Přestože se jedná o jednu službu, z právního

pohledu je třeba ji rozdělit na dva různé komponenty a oba posuzovat zvlášť, podle zvláštních pravidel platných pro tyto služby. Na základě výše uvedeného by instituce měla splňovat ve vztahu ke službě elektronického bankovnictví při ochraně osobních údajů požadavky kladené jak na poskytovatele finančních služeb, tak služeb elektronických komunikací. Povinnosti ochrany osobních údajů v rámci sektoru elektronických komunikací byly v rámci práva EU podrobněji rozpracovány ve směrnici č. 2002/58/EC (tzv. Directive on privacy and electronic communications) z roku 2002. Tato směrnice uvádí následující odpovědnost poskytovatelů služeb elektronických komunikací. Poskytovatel veřejně dostupných služeb elektronických komunikací musí přijmout vhodná technická a organizační opatření, aby zajistil bezpečnost svých služeb, v případě nutnosti i v součinnosti s provozovatelem veřejné komunikační sítě s ohledem na bezpečnost sítě. Se zřetelem na technikou a nákladovou stránku jejich provádění je třeba, aby tato opatření zajišťovala úroveň bezpečnosti odpovídající stávajícímu riziku. Existuje-li zvláštní riziko, že bude narušena bezpečnost sítě, musí poskytovatel veřejně dostupných služeb elektronických komunikací informovat účastníky o takovém riziku a pokud toto riziko přesahuje rozsah opatření, která má přijmout poskytovatel služeb, musí účastníky informovat o veškerých možných opatřeních k nápravě, včetně stanovení pravděpodobných souvisejících nákladů. Pro tento spor je významné, že poskytovatelé služeb musí informovat své zákazníky o rizicích, která z jejich služeb mohou vyplynout. Konkrétně, musí informovat o specifických rizicích porušení bezpečnosti elektronické komunikace ve vztahu k ochraně osobních údajů. Pokud tato rizika přesahují rozsah opatření přijímaných poskytovatelem, musí informovat své zákazníky o postupu, kterým by tato rizika minimalizovali. To však v tomto případě instituce, jak se zdá, neučinila. Obdobná povinnost, tj. povinnost upozornit na hrozící rizika a doporučit případná opatření na straně klienta, jsou obsahem obecné prevenční povinnosti předcházet hrozící škodě ve smyslu § 415 občanského zákoníku.

V této souvislosti upozorňuje odborník ve svém posudku na rozhodnutí Spolkového soudního dvora v Německu (č. IIIZR 96/03), popsaný panem JUDr. Radimem Polčákem z Právnické fakulty Masarykovy Univerzity v Brně v časopise Jurisprudence, číslo 3/2005. V tomto soudním rozhodnutí Spolkový soud rozhodl, že provozovatel telefonní sítě a nikoliv majitel přípojky nese riziko utajené instalace automatického volacího programu (tzv. dialeru) do počítače, který pro průměrného uživatele nepozorovaně naváže spojení v internetu přes číslo s vyšší cenou, pokud za něj uživatel připojení neodpovídá, a dále, že uživatel připojení nemá povinnost učinit preventivní opatření proti tzv. dialeru, pokud nic konkrétního nepoukazuje na případné zneužit. Odborník se domnívá, že toto soudní rozhodnutí je v řadě ohledů významné také pro tento spor. Jak je uvedeno výše, instituce v čl. VI odst. 13 Podmínek sice upozorňuje klienta na to, že služba TB je provozována prostřednictvím veřejných telefonních linek, které nejsou žádným způsobem chráněny proti tajemství přepravovaných zpráv, avšak nijak klienta neinformuje o prostředcích, jak by mohl výsledná rizika omezit. Instituce ani výslovně na tato rizika neupozorňuje (např. v tom smyslu, že jde o aspekt služby, který není bezpečný). Jak uvedl německý soud, je to poskytovatel služby a nikoliv příjemce služby, kdo je v prvé řadě odpovědný za bezpečnost poskytované služby. Povinnosti klienta k preventivním opatřením nastupují až poté, co se systém, prostřednictvím kterého klient službu přijímá, začne chovat nestandardně. Pokud se systém chová standardně, nelze na klientovi chtít, aby prováděl preventivní opatření proti možným ohrožením, pokud k tomu není specificky zavázán ve smlouvě. Smlouva instituce takové specifické závazky klienta neobsahuje. Stanovisko německého spolkového soudu podle názoru odborníka vyjadřuje převažující právní stanovisko bankovních regulátorů v západní Evropě. Např. v Lucembursku a ve Velké Británii, pravděpodobně i v jiných státech EU, vydaly regulační orgány doporučení pro banky, jak postupovat při zabezpečení on-line finančních služeb. Tato pravidla obsahují také povinnosti informovat klienty o rizicích a možných preventivních opatřeních. V rámci

uzavírané smlouvy mezi bankou a klienty potom dochází k dohodě o „rovnováze specifických povinností“ při zabezpečení příslušné služby. Z vyjádření instituce je zřejmé, že si byla vědomá toho, že (1) poskytuje kombinovanou službu, jejíž jedna součást spočívá v zabezpečení komunikace, a (2) že služba obsahuje specifická rizika. Přesto instituce o těchto specifických rizicích a o odpovídajících bezpečnostních opatřeních na straně klienta své klienty neinformovala a spokojila se se smluvním ujednáním, kterým je klient odpovědný za veškeré zneužití bezpečnostních prvků.

K odpovědnosti navrhovatelky odborník ve svém posudku uvádí, že také na navrhovatelku se vztahuje obecná prevenční povinnost předcházet škodě. Z vyjádření instituce vyplývá, že spatřují porušení povinnosti navrhovatelky v tom, že je velice pravděpodobné, že dcera navrhovatelky zná jeden z bezpečnostních prvků, konkrétně heslo. Odborník se v této souvislosti domnívá, že primární důkazní břemeno v tomto sporu nese instituce a nikoliv navrhovatelka. Důvodem je výše uvedená povinnost zabezpečit ochranu osobních údajů, obsažená v zákoně o ochraně osobních údajů. Ze smluvních dokumentů, specificky z článku VI odst. 3 Podmínek („Klient musí pečovat o to, aby se žádná jiná osoba neseznámila s využívanými bezpečnostními prvky. Pokud se tak stane, riziko zneužití těchto prvků spojené s realizací požadovaných služeb nese v plné výši klient.“) vyplývá obecná povinnost chránit hesla a PIN. Navrhovatelka však uvádí, že tyto bezpečnostní prvky chránila v rodinném trezoru, a instituce neprokázala vyzrazení bezpečnostních prvků navrhovatelkou.

V závěru odborného posudku se odborník domnívá, že instituce nemůže vyloučit svou odpovědnost při zneužití PIN a hesla či při prozrazení bezpečnostních údajů, které jsou sdělovány prostřednictvím nezabezpečení veřejné telefonní sítě, a že služba TB je kombinovanou službou (finanční i elektronických komunikací), což sama instituce potvrzuje (čl. VI odst. 13 Podmínek), a vztahuje se proto na ni povinnost ochrany osobních údajů dle §13 zákona č. 101/2000 Sb., stejně jako obecná prevenční povinnost předcházet škodám. Tímto instituce nedostála své zákonné obecné povinnosti předcházet škodám, specifické povinnosti k ochraně osobních údajů svých klientů a proto je odpovědná za škodu, jež navrhovatelce vznikla. S tímto názorem se ztotožnil i finanční arbitr.

Na základě provedeného dokazování dospěl finanční arbitr k závěru, že návrh ze dne 28.2.2005 je důvodný a instituce je v tomto případě odpovědna za škodu podle § 415 (resp. § 420) občanského zákoníku, neboť je prokázána příčinná souvislost mezi konáním (či spíše nekonáním) instituce a vznikem škody. Proto finanční arbitr rozhodl tak, jak je uvedeno ve výroku tohoto nálezu.

P o u č e n í : Proti tomuto nálezu lze podat do 15 dnů ode dne jeho doručení písemně odůvodněné námitky k finančnímu arbitrovi ČR.
Práva podat námitky se lze vzdát.
Námitky mají odkladný účinek.

V Praze dne 22. července 2005

finanční arbitr