Bezpečnost přímého bankovnictví

Používání moderních prostředků komunikace se velmi rychle rozšiřuje. Vliv na tuto skutečnost nemají již jen soukromoprávní subjekty, ale i státy a integrační celky, které podporují elektronickou komunikaci nejen tvorbou právních předpisů.

Vláda České republiky schválila dne 31. května 1999 ve svém usnesení č. 525 dokument Státní informační politika – cesta k informační společnosti, jehož obsahem je prezentace vizí a strategií pro vznik a fungování informační společnosti.
Dalším dokumentem v oblasti informační společnosti, který byl schválen usnesením vlády ČR č. 265 dne 24. března 2004, a jehož obsahem je strategie rozvoje informační společnosti do roku 2006, je Státní informační a komunikační politika.[1)] Uvedený dokument v podstatě spojuje myšlenky Státní informační politiky - cesta k informační společnosti a Národní telekomunikační politiky a reaguje tak na širší oblast služeb, které náležejí pod pojem *„elektronická komunikace“*, nikoliv jen telekomunikace.

PŘÍMÉ BANKOVNICTVÍ

V bankovnictví se významně rozvíjí užívání tzv. přímého bankovnictví, což *„jsou služby, které umožňují komunikaci banky a klienta bez toho, aby klient musel banku navštívit. Vše se děje pomocí buď telefonu (a to i mobilního) nebo počítače a Internetu“*. [2)]
V souvislosti s tématem bezpečnosti přímého bankovnictví provádím rozbor platné právní úpravy, forem přímého bankovnictví a budu se věnovat zajištění bezpečnosti přímého bankovnictví a bezpečnosti z pohledu trestního práva. Dané téma je nutné hodnotit jak v oblasti právní, tak i kybernetické, neboť není možné posuzovat je zcela bez kontextu kybernetického pohledu.

PLATNÁ PRÁVNÍ ÚPRAVA ELEKTRONICKÉHO PODPISU A PŘÍMÉHO BANKOVNICTVÍ

Směrnice Evropského parlamentu a Rady č. 1999/93/ES o zásadách Společenství pro elektronické podpisy (dále jen *„směrnice o elektronickém podpisu“*) byla implementována do českého práva zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen *„zákon o elektronickém podpisu“*).
Výše uvedená směrnice doplňuje směrnici Evropského parlamentu a Rady č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, která se promítla do českého práva § 40 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.
Pro smluvní právo je ze směrnice o elektronickém podpisu podstatné zmínit článek 1, který ukládá členským státům, aby za stanovených podmínek uznaly elektronické podpisy a přiznaly jim stejné právní účinky jako vlastnoručním podpisům připojeným pod písemnou formu textu. Elektronické podpisy vyhovující požadavkům směrnice mají stejný význam jako *„klasické“* podpisy včetně podpisů ověřených notáři či orgány veřejné zprávy (tzv. legalizace), a tudíž se mohou za stanovených předpokladů použít jako důkaz před soudem (článek 5 směrnice o elektronickém podpisu).
Zákon č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů (dále jen „*občanský soudní řád*“), v této souvislosti uvádí v § 125, že za důkaz mohou sloužit všechny prostředky, jimiž lze zjistit stav věci, zejména výslech svědků, znalecký posudek, zprávy a vyjádření orgánů, fyzických a právnických osob, notářské nebo exekutorské zápisy a jiné listiny, ohledání a výslech účastníků. Pokud není způsob provedení důkazu předepsán, určí jej soud.

Pro hodnocení provedených důkazů platí zásada volného hodnocení důkazů (§ 132 občanského soudního řádu).
Otázkou je, jak věrohodně zajistit identifikaci a autentizaci, je-li právní úkon učiněn elektronickými prostředky. Odpovědí na tuto otázku je v českém platném právu zákon o elektronickém podpisu účinný od 1. října 2000.
Zákon o elektronickém podpisu vychází z existence dvou typů podpisů: elektronického podpisu a zaručeného elektronického podpisu. Elektronickým podpisem lze rozumět údaje v elektronické podobě, které jsou připojené k datové zprávě, například i naskenovaný podpis. Zaručený elektronický podpis vyžaduje existenci certifikátu, tzn. datové zprávy, kterou vydává poskytovatel certifikačních služeb, a která spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu.
S účinností od 1. května 2005 platí nový zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů (dále jen *„zákon o elektronických komunikacích“*), který zrušil zákon č. 151/2000 Sb., o telekomunikacích a o změně dalších zákonů.
Právní úprava pro elektronické komunikace je výhradně zaměřena na služby přenosu signálů na území České republiky, nevztahuje se na obsah služeb poskytovaných prostřednictvím sítí elektronických komunikací jako je obsah finančních služeb (§ 1 odst. 2 zákona o elektronických komunikacích).
Komplexní zákonná právní regulace přímého bankovnictví v českém právním řádu neexistuje. Smluvní vztah mezi bankou a klientem o poskytování a využívání služeb přímého bankovnictví se řídí § 269 odst. 2 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, dále obchodními podmínkami pro vydávání a užívání elektronických platebních prostředků, které jsou s určitými odchylkami stejné jako Vzorové obchodní podmínky pro vydávání a užívání elektronických platebních prostředků České národní banky, a také se mohou řídit tzv. technickými podmínkami pro uživatele služeb přímého bankovnictví.
Kromě právně závazných předpisů se banky řídí i nezávaznými pravidly ve formě kodexů nebo standardů aj.

FORMY PŘÍMÉHO BANKOVNICTVÍ

Mezi formy přímého bankovnictví patří: samoobslužná zóna, telefonní bankovnictví, GSM banking a internetové bankovnictví. Banky kombinují mezi formami přímého bankovnictví nebo je spojují, tzn. že požadovanou informaci či výsledek zadané služby pomocí jedné formy přímého bankovnictví obdrží klient jinou formou (i prostřednictvím tradičních prostředků komunikace jako jsou fax nebo *„klasická“* pošta).

SAMOOBSLUŽNÁ ZÓNA

Samoobslužná zóna (terminál) se považuje za první formu přímého bankovnictví. Je zpravidla umístěna na pobočce banky a bývá neomezeně časově přístupná. Pro přístup do prostoru samoobslužné zóny lze použít platební kartu a pro operace platební kartu v kombinaci s heslem. Jejím prostřednictvím lze většinou vybírat peníze (jako u klasického bankomatu), zadávat platební příkazy, získávat informace o stavu na účtu nebo si dokonce vytisknout výpis z účtu. Dále je možné získávat informace o produktech banky. Některé banky spojují funkce samoobslužné zóny a bankomatu do jediného technického prostředku.

TELEFONNÍ BANKOVNICTVÍ

Telefonní bankovnictví se označuje také jako telebanking nebo phonebanking.
Pomocí telefonního bankovnictví může klient provádět operace na svém běžném účtu. Le je rozdělit na pasivní a aktivní.

Pasivní operace jsou chráněné informace z bankovního informačního systému i veřejně dostupné informace o bankovních produktech. Mezi pasivní operace patří zejména zjišťování zůstatku na účtu, informace o pohybech na účtu, informace o zadaných a z různých důvodů neprovedených transakcích, informace o produktech a službách banky, úrokové sazby, kurzovní lístek aj.
Aktivní operace zahrnují vlastní provádění bankovních operací (transakcí). Mezi aktivní operace řadíme zejména příkaz k úhradě, trvalý příkaz k úhradě, příkaz k inkasu, trvalý příkaz k inkasu, zahraniční platební styk atd.
Klient může provádět bankovní operace pomocí pevné telefonní linky nebo mobilního telefonů. Zavolá obvykle na bezplatnou linku telefonního bankovnictví, komunikuje s automatickým telefonním systémem (u této varianty služby je nutné mít telefon s tónovou volbou) anebo s telefonním bankéřem. Nevýhodou je, že mimo obvyklou pracovní dobu bank se může většinou využívat jen část služby, a to automatického telefonního systému.

GSM BANKING

GSM banking se poskytuje ve třech variantách. První variantou je SIM Toolkit. Na bankovní SIM kartu vašeho mobilního telefonu, která podporuje GSM banking, nahraje banka aplikaci, která se objeví v menu vašeho telefonu. Stejně jako pracuje klient banky s menu telefonu, ovládá i menu bankovní aplikace a vybírá požadovanou položku, tzn. službu, kterou chce provést. Klient může provádět pasivní a aktivní operace na účtu. Nevýhodou je, že pro (minimální) část komunikace s bankou se používají zvláštní znaky, například pomlčka (-) mezi předčíslím a číslem bankovního účtu se nahrazuje křížkem (#) nebo hvězdičkou (*) apod.
Druhou variantou je WAP (Wireless Application Protocol)[3)] banking, který umožňuje spojení s bankou prostřednictvím mobilního telefonu vybaveného technologií WAP. Pomocí WAP lze provádět již několikrát zmiňované pasivní a aktivní operace.
Nemá-li klient mobilní telefon se SIM Toolkit, ani s WAP (nebo jen nemá WAP aktivován), může využívat GSM banking prostřednictvím standardních SMS (Short Message Service).[4)]

INTERNETOVÉ BANKOVNICTVÍ

Internetové bankovnictví zahrnuje opět tři varianty. Buď je vázáno na konkrétní počítač nebo je přístupné z jakéhokoliv počítače připojeného k internetu. Třetí varianta využívá e-mail.
První varianta se označuje jako homebanking. Klient si na počítač nainstaluje speciální (bezpečnostní) software. Počítač by měl být pro některé operace připojen k internetu. Klient může provádět běžné pasivní a aktivní operace. Výhodou je, že tyto produkty bank jsou často kompatibilní s účetními programy,[5)] což usnadňuje práci, zejména podnikatelům. Nevýhodou je, že je omezena mobilita na počítač, na kterém je software nainstalován.
Vlastní internetové bankovnictví je služba, která umožňuje komunikaci s bankou z jakéhokoliv počítače s internetem. Na webové stránce banky, ve které má klient účet, klikne na položku internetové bankovnictví a obrazně vyjádřeno se dostane na svůj účet a může provádět nejrůznější pasivní a aktivní operace.
Třetí variantou internetového bankovnictví je získávání informací prostřednictvím e-mailu. Klient tak může získat informace o aktuálním zůstatku účtu v předdefinovaný čas a den, dosažení určitého zůstatku na účtu, zaúčtování platby tuzemského i zahraničního platebního styku, podání platebního příkazu nebo vyřazení platebního příkazu z kartotéky, výběru hotovosti na pobočce, neprovedení platebního příkazu z důvodu nedostatku finančních prostředků na účtu, autorizaci transakce platební kartou, zbývajícím limitu platební karty, ukončení platnosti platební karty, elektronickém výpisu z účtu a kurzovního lístku.

NOVÉ MOŽNOSTI PŘÍMÉHO BANKOVNICTVÍ

Novinkou, která byla zavedena na trhu služeb přímého bankovnictví v květnu loňského roku je spojení telefonního bankovnictví a internetového bankovnictví. Podstatou služby je datový přenos prostřednictvím mobilního telefonu podporující Java,[6)] který spojuje klienta s bankou on-line.[7)]

Další novou službu přímého bankovnictví je PDA banking. PDA je kapesní počítač, na který není třeba většinou instalovat žádný speciální program, je třeba mít internetový prohlížeč, který podporuje SSL (Secure Socket Layer)[8)] protokol a připojení k internetu prostřednictvím HSCSD (High Speed Circuit Switched Data)[9)] nebo GPRS (General Packet Radio Service)[10)] protokolu, případně synchronizací přes osobní počítač a klient může provádět běžné pasivní i aktivní operace. PDA banking je také funkční na kapesních počítačích s mobilním telefonem.

PLATEBNÍ KARTA JAKO FORMA PŘÍMÉHO BANKOVNICTVÍ?

Otázkou je, zda do oblasti přímého bankovnictví patří i forma platební karty. Bankovní praxe odpovídá na tuto otázku *„ne“*. Prostřednictvím platební karty totiž většinou nelze uskutečňovat jiné transakce než platbu za zboží a služby v kamenných obchodech a výběr z bankomatu (nebereme-li v úvahu doplňkové služby k platebním kartám, například odblokování platební karty pro platby zboží a služeb přes internet), takže se nepokládá za formu přímého bankovnictví.

Je třeba dodat, že banky nabízejí virtuální platební kartu (nikoliv ve tvaru plastikové platební karty) k nákupu běžného zboží přes internet (ale ne služeb).

ZAJIŠTĚNÍ BEZPEČNOSTI PŘÍMÉHO BANKOVNICTVÍ

Zajištění bezpečnosti je jedním z nejdůležitějších bodů, který banky řeší, a který v podstatě může být řešen permanentně, protože bohužel neexistuje žádný zabezpečovací systém, který je stoprocentní.

Na zajištění bezpečnosti přímého bankovnictví je možné nahlížet z pohledu klienta nebo z pohledu banky, jehož součástí je otázka bezpečnosti vlastního informačního systému banky a otázka zajištění dostupnosti informačního systému v případě jeho narušení.

Pro zajištění ochrany dostupnosti systému se v současnosti služba poskytuje na všech serverech najednou, čímž získá vyšší dostupnost i vyšší výkon, takže při poruše si většina klientů výpadku nemusí vůbec všimnout, poněvadž provoz se velmi rychle přepojí jinam.

Třetí okruh otázek tvoří zajištění bezpečnosti přenášených dat, které mezi bankou a klientem probíhá (až na výjimky) šifrovaně – standardně se využívá 128bitové šifrování.

Podrobněji se otázkami zajištění dostupnosti informačního systému v případě jeho narušení zabývat nebudeme, stejně jako zajištěním bezpečnosti přenášených dat, poněvadž se jedná o otázky převážně z oblasti odborné, informační, která není hlavním předmětem tohoto článku.

V Kodexu chování mezi bankami a klienty (dále jen *„Kodex“*)[11)] je mezi právy klientů ve vztahu k bankám zakotveno právo na informaci a doporučení, jak chránit přístup ke svému účtu a prostředkům na něm uloženým. Dále má klient právo na informaci o tom, jak se lze, dle názoru banky, co nejlépe chránit před zneužitím platebních prostředků, které mu banka v rámci svých služeb poskytuje, či mu jejich poskytnutí zprostředkovává (bod 2.3.3 Kodexu).

Pro klienta banky je důležité si uvědomit, že pro zajištění alespoň minimální bezpečnosti je třeba dodržovat určité zásady.

Bezpečnost telefonního bankovnictví je zajištěna minimálně dvouúrovňovým systémem ochrany. Klient zadává své identifikační údaje (identifikační číslo, klientské číslo nebo klient volá z rozpoznaného telefonního čísla mobilního telefonu, které bylo sjednáno ve smlouvě apod.) a po úspěšné identifikaci následuje autentizace (autentizační kód, PIN, heslo, záložní

otázky, ověření prostřednictvím elektronického klíče nebo prostřednictvím čipové karty apod.). Dalším bezpečnostním prvkem je autorizace každé aktivní operace prostřednictvím jednorázového hesla.
Technologie GSM SIM Toolkit je chráněna v případě neoprávněného použití mobilního telefonu zvláštním bankovním PIN, který se označuje jako BPIN.[12)]
WAP banking je chráněn elektronickým klíčem anebo v současnosti i elektronickým podpisem, (který je založen na obdobném principu jako zaručený elektronický podpis podle zákona o elektronickém podpisu) připojením přes internet.
Zajištění bezpečnosti homebanking se rozděluje do dvou stupňů. Pro vstup do aplikace se používají přístupová hesla, v druhé fázi aktivní operace využívají elektronický podpis (obdobný zaručenému elektronickému podpisu).
Služba internetového bankovnictví je zajištěna při přihlášení pomocí identifikačního čísla, PIN a čipové karty. Čipová karta je chráněna pomocí PIN (odlišného od přihlašovacího PIN). Autorizace aktivních operací využívá elektronický podpis (obdobný zaručenému elektronickému podpisu) nebo jednorázový autorizační kód.
Nastavením limitu (denní, týdenní) pro převádění peněžních prostředků je další formou ochrany služeb přímého bankovnictví.

PRAVIDLA K ZAJIŠTĚNÍ BEZPEČNOSTI PŘÍMÉHO BANKOVNICTVÍ

Zabezpečení vlastního informačního systému banky reguluje Česká národní banka v opatření č. 2 ze dne 3. února 2004 (dále jen *„opatření“*), ve kterém dle § 12, § 14 a § 15 zákona č. 21/1992 Sb., o bankách, ve znění zákona č. 126/ 2002 Sb., a § 24 písm. a) zákona č. 6/1993 Sb., o České národní bance, ve znění zákona č. 127/ 2002 Sb., stanovila požadavky na vnitřní řídicí a kontrolní systém banky včetně požadavků na interní audit a řízení rizik.
V příloze č. 4 opatření definuje požadavky na informační systémy, které se týkají řízení informačních systémů, analýzy rizik spjatých s informačními systémy, bezpečnost přístupu k informacím a bezpečnost komunikačních sítí (banky a vnější komunikační sítě), fyzické bezpečnosti informačních systémů a provozování informačních systémů.
Banka přijme bezpečnostní politiku informačních systémů a zabezpečí, aby se strategie rozvoje a bezpečnostní politika informačních systémů pravidelně vyhodnocovaly a případně upravovaly. Banka musí provést analýzu rizik spjatých s informačními systémy. V ní definuje aktiva informačních systémů,[13)] hrozby, které na ně působí, zranitelná místa informačních systémů, pravděpodobnost realizace hrozeb a odhad jejich následků a protiopatření. Na základě analýzy rizik zavede banka opatření pro fyzickou ochranu aktiv informačních systémů. Připojení sítě, která je pod kontrolou banky, k vnější komunikační síti, která není pod kontrolou banky, musí být zabezpečeno tak, aby se minimalizovala možnost průniku do informačních systémů. V provozovaných informačních systémech se může používat pouze otestované programové vybavení, u kterého výsledky testů prokázaly, že bezpečnostní funkce jsou v souladu s bezpečnostní politikou informačních systémů. Banka zabezpečí zálohování informací a programového vybavení informačních systémů významných pro její fungování. Zálohované informace a programové vybavení musejí být uloženy tak, aby byly zabezpečeny proti poškození, zničení a krádeži.
Dále se v oblasti bezpečnosti informačních systémů aplikují technické předpisy na základě § 3 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů (dále jen *„zákon o technických požadavcích“*).
Technickým předpisem se pro účely zákona rozumí právní předpis, obsahující technické požadavky na výrobky, popřípadně pravidla pro služby nebo upravující povinnosti při uvádění výrobku na trh, při jeho používání nebo při poskytování nebo zřizování služby nebo

zakazující výrobu, dovoz, prodej či používání určitého výrobku nebo používání, poskytování nebo zřizování služby.
Českou technickou normou je dle § 4 zákona o technických požadavcích dokument pro opakované nebo stálé použití vytvořený podle zákona a označený písmenným označením ČSN.
Česká technická norma není obecně závazná, a proto její nedodržení není v rozporu se zákonem. Avšak stanoví-li právní předpis dodržovat ČSN, nedodržení ČSN bude porušením právního předpisu.[14)] Je tedy třeba, aby vznikl zákon o zajištění bezpečnosti informačních systémů, [1] který bude odkazovat na ČSN a použití norem bude tudíž povinné. Prozatím se používají nezávazně.
Kromě ČSN zákon o technických požadavcích zmiňuje harmonizované české technické normy, harmonizované evropské normy[15)], tzv. určené normy[2] a zahraniční technické normy.
V systému řízení bezpečnosti informačních systémů se nejen v bankovním sektoru významně prosazuje norma ČSN ISO/IEC[16)] BS 7799-2:2004 – Systém managementu bezpečnosti informací – Specifikace a s návodem pro použití. Dále se používá norma ČSN ISO/IEC 17799:2005 – Informační technologie – Soubor postupů pro management bezpečnosti informací, která nahradila pět let starou normu nesoucí stejný název. Nová norma z roku 2005 obsahuje přesnější definice obsahu bezpečnostních opatření a definice požadavků na jejich implementaci.
V současné době je uznávaným standardem v zajištění bezpečnosti bankovních systémů ČSN ISO/IEC 15408 (tzv. Common Criteria for Information Technology Security Evaluation).
V případě, že nastanou problémy, je vždy snaha je rychle a efektivně minimalizovat bez poškození dobrého jména banky nebo bez porušení právních předpisů,[17)] neboť zcela se jim vyhnout je prakticky nemožné.

BEZPEČNOST Z POHLEDU TRESTNÍHO PRÁVA

Původně byla počítačová kriminalita (computer crime) zaměřena proti fyzické podstatě počítače (například poškozování cizí věci, krádež atd.). Přes první útoky na *„obsah“* počítače (obvykle s úmyslem spáchat podvod bankovní, fakturační aj.) a tzv. softwarové pirátství[18)] se vývoj trestné činnosti v oblasti výpočetní techniky dostává do tzv. nové doby počítačového zločinu,[19)] která se vyznačuje nástupem osobních počítačů a vznikem počítačových sítí a vzdáleného přístupu, zejména internetu. Objevuje se tzv. distanční trestná činnost a další specifická trestná činnost – informační delikty a ryze internetové delikty.
Platná právní úprava českého trestního práva hmotného stanovuje v § 249b zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů (dále jen „*trestní zákon*“), ve zvláštní části mezi trestnými činy proti majetku v hlavě deváté trestný čin neoprávněného držení platební karty. Dalším trestným činem týkajícím se přímého bankovnictví je trestný čin poškození a zneužití záznamu na nosiči informací (§ 257a trestního zákona).

---

[1] V oblasti veřejné správy nabývá s výjimkami účinnosti dne 1. ledna 2007 zákon č. 81/2006 Sb., který novelizuje zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, a který klade důraz na větší bezpečnost všech informačních systémů. Měl by být vydán prováděcí předpis, který bude upravovat zajištění bezpečnosti informačních systémů veřejné správy.

[2] Pro specifikaci technických požadavků na výrobky, vyplývajících z nařízení vlády nebo jiného příslušného technického předpisu, může Úřad pro technickou normalizaci, metrologii a státní zkušebnictví po dohodě s ministerstvy a jinými ústředními správními úřady, jejichž působnosti se příslušná oblast týká, určit české technické normy, další technické normy nebo technické dokumenty mezinárodních, popřípadě zahraničních organizací, nebo jiné technické dokumenty, obsahující podrobnější technické požadavky (§ 4a odst. 1 věta druhá zákona o technických požadavcích).

Nepřijatý[20)] nový trestní zákoník (dále jen „návrh zákona“) reflektoval na novou dobu počítačového zločinu zavedením skutkových podstat vycházejících z Úmluvy o počítačové kriminalitě ze dne 23. listopadu 2001 a z požadavků praxe: neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací (§ 205 návrhu zákona), opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 206 návrhu zákona) a poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 207 návrhu zákona).
Novodobá počítačová kriminalita se soustřeďuje především na nelegální získávání nehmotných statků, přesto se útokům na vlastní hardware (zařízení) nevyhneme (uvedené krádeže, poškozování cizí věci atd.).
K vyššímu a dokonalejšímu zajištění bezpečnosti se začíná uplatňovat i biologická identifikace (biometrie), tzn. identifikace na základě váhy, výšky, hloubky hlasu, otisku prstu, tetování apod.
Dlouholetou tradici má biometrie v kriminalistice. V současnosti se prosazuje i v občanské sféře, např. vydávání biometrických pasů v zemích EU a USA.[21)]
Otázkou je, zda-li biometrie pronikne i do přímého bankovnictví a případně za jak dlouho.

ZÁVĚR

Značná část požadavků na zajištění bezpečnosti přímého bankovnictví náleží do oblasti veřejnoprávní regulace (veřejné bankovní právo, trestní právo aj.). Ze soukromoprávní oblasti práva nelze ale otázku zajištění bezpečnosti zcela eliminovat, poněvadž mezi bankou a jejími klienty, kteří mají u banky běžný účet ovládaný prostřednictvím přímého bankovnictví, existuje soukromoprávní vztah a v případě nefunkčnosti informačního systému klienti apelují na banku, aby ho opět uvedla do provozu. Narušení bezpečnosti klientských účtů (nikoliv vinou klienta) může být porušením dohodnutých povinností ze strany banky a může vzniknout protiprávní vztah, s nímž právo spojuje sankční následky.
Domnívám se, že bezpečnost přímého bankovnictví nutně souvisí s vytvořením de lege ferenda zákona o zajištění bezpečnosti informačních systémů[1] zahrnující úpravu týkající se služeb přímého bankovnictví a kodifikací nových trestných činů, protože jakákoliv zcela neupravená oblast je nekontrolovatelná a může vést k nezřízenému užívání i nepostižitelnému zneužívání.
Základem kvalitního rozvoje v oblasti přímého bankovnictví jsou, dle mého názoru, zákony, na základě kterých lze ukládat povinnosti. Předpisy, které by ovšem neměly působit jako omezující prvek vývoje (tzv. přiměřenost práva), měly by naopak flexibilně reagovat na dynamický vývoj informačních a komunikačních technologií[22)] a pomáhat tak dotvářet fungující společnost, nejen v oblasti bankovních služeb.

Poznámky:

[1)] Ministerstvo informatiky České republiky zveřejnilo dne 22. června 2006 na své webové stránce http://www.micr.cz/scripts/detail.php?id=3583 Vyhodnocení Státní informační a komunikační politiky a první Výroční zprávu o evropské informační společnosti.

[1] V oblasti veřejné správy nabývá s výjimkami účinnosti dne 1. ledna 2007 zákon č. 81/2006 Sb., který novelizuje zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, a který klade důraz na větší bezpečnost všech informačních systémů. Měl by být vydán prováděcí předpis, který bude upravovat zajištění bezpečnosti informačních systémů veřejné správy.

[2)] Přímé bankovnictví [citováno 21. února 2006]. Dostupný z: http://www.finance.cz/home/bankovnictvi/prime_b/.
[3)] Bezdrátový aplikační protokol lze zjednodušeně vyjádřeno přirovnat k webovým stránkám, které se zobrazují na displeji mobilního telefonu.
[4)] Služba krátkých textových zpráv.
[5)] Např. dle § 4 odst. 4 věta první zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, jsou účetní jednotky povinny vést účetnictví jako soustavu účetních záznamů; přitom mohou použít technických prostředků, nosičů informací a programového vybavení.
[6)] Programovací jazyk umožňující vytvářet snadno spustitelné programy určené zejména pro spolupráci s webovými stránkami.
[7)] Hauptová, H., Mobilní bankovnictví nové generace, vystoupení na mezinárodní odborné konferenci Fórum eTime 2005, Praha – hotel Andel´s ve dnech 16. – 17. května 2005.
[8)] Relace prostřednictvím klíčů a šifrovaní, která zajišťuje bezpečnou komunikaci.
[9)] Vysokorychlostní přepínané datové okruhy jsou zdokonaleným přenosem GSM. GPRS je druhým způsobem datových přenosů v síti GSM.
[10)] Předchází technologii třetí generace UMTS. UMTS je technologie třetí generace, jejímž cílem je stejně kvalitní přenos obrazu jako hlasu v reálném čase.
[11)] Česká bankovní asociace (dále jen „ČBA“) vydala 16. prosince 2005 Standardy bankovních aktivit č. 19/2005 – Kodex chování mezi bankami a klienty, který má metodický charakter, tzn. že k dodržování Kodexu se členské banky ČBA přihlašují, konkrétně písemným prohlášením, které je v závěru Kodexu. Kodex je výsledkem jednání bank a Ministerstva financí České republiky, které usilovalo o větší vyrovnanost vztahů mezi bankami a jejich klienty a zvýšení přehlednosti a dostupnosti informací o poskytovaných bankovních službách. Kodex se zabývá právy klientů a bank k sobě navzájem a řešením vzájemných sporů. Práva klientů ve vztahu k bankám zahrnují rady a informace, obchodní podmínky, informace o vedení účtu a prováděných službách, ceny a oznamování jejich změn, zacházení s informacemi o klientovi, pomoc banky v mimořádných situacích a postup banky v případě prodlení klienta.
[12)] Osobní identifikační číslo pro bankovní aplikaci neboli bankovní PIN.
[13)] Aktivem informačního systému je dle ustanovení § 2 písm. o) opatření informační technologie, informace uložené v informačním systému banky a dokumentace informačního systému.
[14)] Smejkal, V. Informační systémy veřejné správy ČR. 1. vydání. Praha: nakl. Oeconomica, 2003, s. 75.
[15)] Česká technická norma se stává harmonizovanou českou technickou normou, přejímá-li plně požadavky stanovené evropskou normou nebo harmonizačním dokumentem, které uznaly orgány Evropského společenství jako harmonizovanou evropskou normu, nebo evropskou normou, která byla jako harmonizovaná evropská norma stanovena v souladu s právem Evropských společenství společnou dohodou notifikovaných osob (§ 4a odst. 1 věta první zákona o technických požadavcích).
[16)] ISO – Mezinárodní normalizační organizace; IEC – Mezinárodní elektrotechnická komise.
[17)] Např. zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, při úniku dat s osobními údaji klientů banky.
[18)] Tzv. softwarové pirátství znamená neoprávněné užívání počítačových programů.
[19)] Smejkal, V. Jaké zločiny a jak je stíhat?, vystoupení na mezinárodní konferenci Kyberprostor 2005, Brno – Masarykova univerzita, Právnická fakulta ve dnech 7. – 8. listopadu 2005.
[20)] Dne 21. března 2006 Poslanecká sněmovna Parlamentu České republiky nepřijala (tisk 744/5) vládní návrh nového trestního zákoníku, který byl zamítnut Senátem Parlamentu České republiky.

[21)] Špinar, P. Biometrie a ověřování osob. Convergence, 2006, č. 5/2006, s. 6 an.
[22)] Informační a komunikační technologie (angl. Information and Communication Technology, ICT) jsou prostředky (zařízení) výpočetní techniky, u kterých je důležitý prvek komunikace.