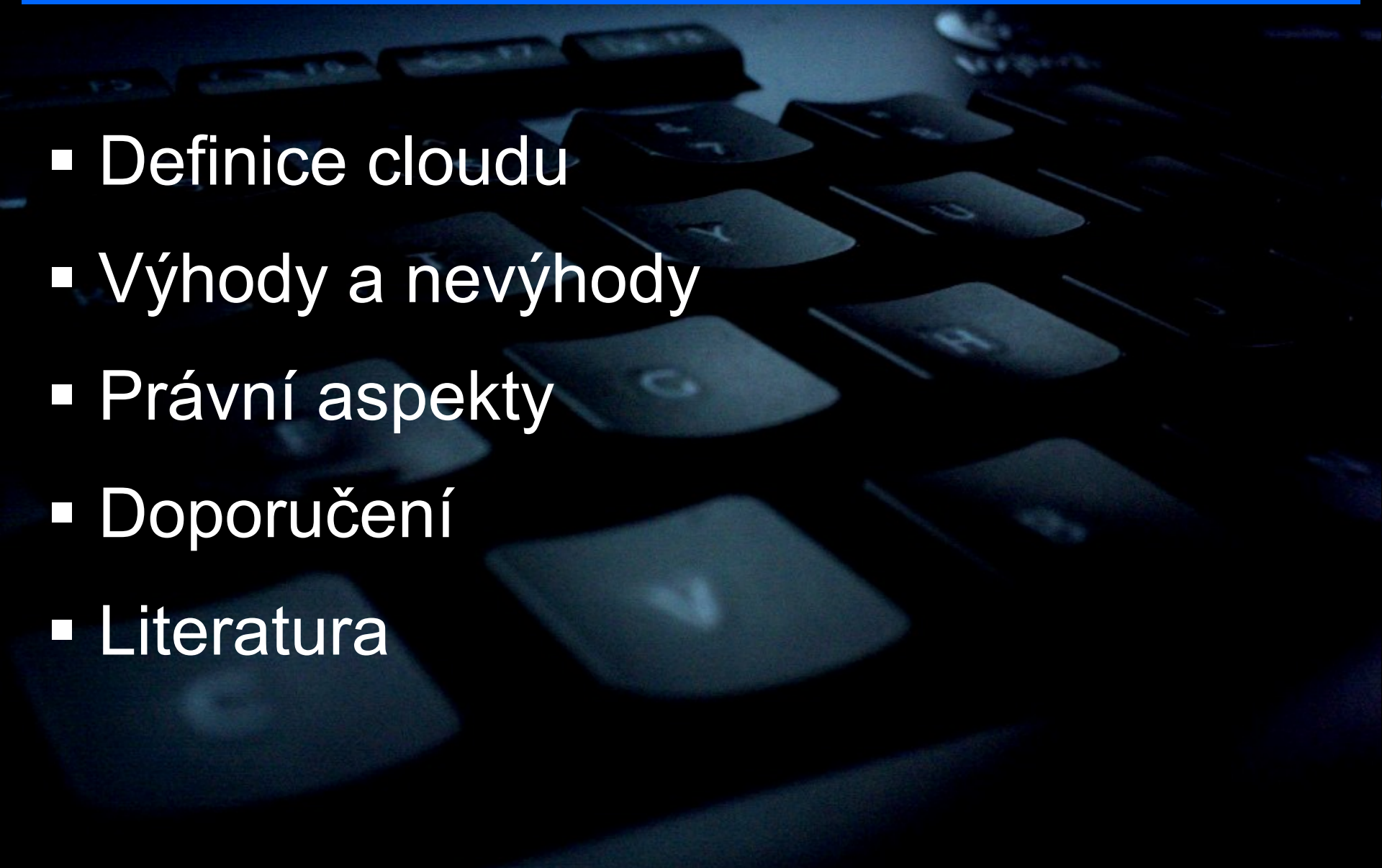
Právní aspekty a rizika Cloud Computingu

Prof. Ing. Vladimír Smejkal, CSc. LL.M.
člen Legislativní rady vlády ČR
soudní znalec
Vysoké učení technické v Brně
Masarykova univerzita v Brně

O čem budeme hovořit?



- Definice cloudu
- Výhody a nevýhody
- Právní aspekty
- Doporučení
- Literatura

Víme, co to je „cloud“?

Co si lze koupit?

V oblasti IT lze definovat poskytování plnění, tj. služeb IT (zhotovitelem a/nebo jeho subdodavatelem) na řadě úrovní:

- Aplikace;
- Prostředí pro běh aplikace (.NET, JVM…) + web server;
- Operační systém;
- Hypervizor (v případě virtualizace);
- Hardware;
- Síťová konektivita, elektřina, klimatizace aj. technologie;
- Budova atd.

Proč cloud?

Uživatel kupuje SW a HW, který sám provozuje

…typicky podnikové IS

Uživatel si nechává poskytovat nějakou službu

…hodně často OVM (např. DS, důchody apod.)

Dnes se poskytovatelé služeb snaží minimalizovat náklady (na HW, SW, provoz) jejich přesouváním do cloudu různé úrovně.

Proč cloud?

- Mezi výhody cloudu patří zejména škálovatelnost služeb, nižší mzdové náklady na ICT pracovníky, nezávislost na místě, čase a platformě.

+ přenesení investičních nákladů (CAPEX) a odpovědnosti za provoz při daném SLA.

…o nevýhodách si řekneme podrobněji za chvíli.

Definování pojmu „cloud computing“

- Základním principem cloud computingu je to, že uživatel odebírá službu, která může být definována různým způsobem – podle typu cloudu, typu služby apod., a to ze vzdáleného centra vlastněného a spravovaného poskytovatelem cloudu prostřednictvím Internetu, obvykle pro větší počet externích zákazníků.

Definování pojmu „cloud computing“

Druhy cloudových služeb:

- Software as a Service (SaaS) – software jako služba.
- Platform as a Service (PaaS) – platforma jako služba.
- Infrastructure as a Service (IaaS) – infrastruktura jako služba.
- a další, jako např. Desktop as a Service, Security as a Service, Database as a Service, Information as a Service, Process as a Service atd.

Cloud podle funkce

…dovedu si
představit
i další služby
poskytované
s cloudem:

(asi by to také mohlo být označeno jako SaaS)

Hlavní druhy

IaaS zahrnuje celé výpočetní prostředí včetně serverů, pamětí, komunikační infrastruktury a podpůrných nástrojů pro vysokou dostupnost, jako je load ballancing apod. Po poskytování a implementaci těchto služeb jsou v široké míře využívány virtualizační technologie, stejně jako gridy či klastry (cluster). V tomto případě se jedná pouze o přeprodávání výpočetní kapacity.

Hlavní druhy

PaaS poskytuje platformu pro vytváření a provoz aplikací, např. prostředí pro běh programů (runtime), aplikační (webový) server, a to případně včetně mechanismů jako autentizace, autorizace a session management.

Zpravidla je poskytováno:

- vývojové prostředí (development),
- testovací prostředí (testing, Q&A),
- produkční prostředí (production).

Hlavní druhy

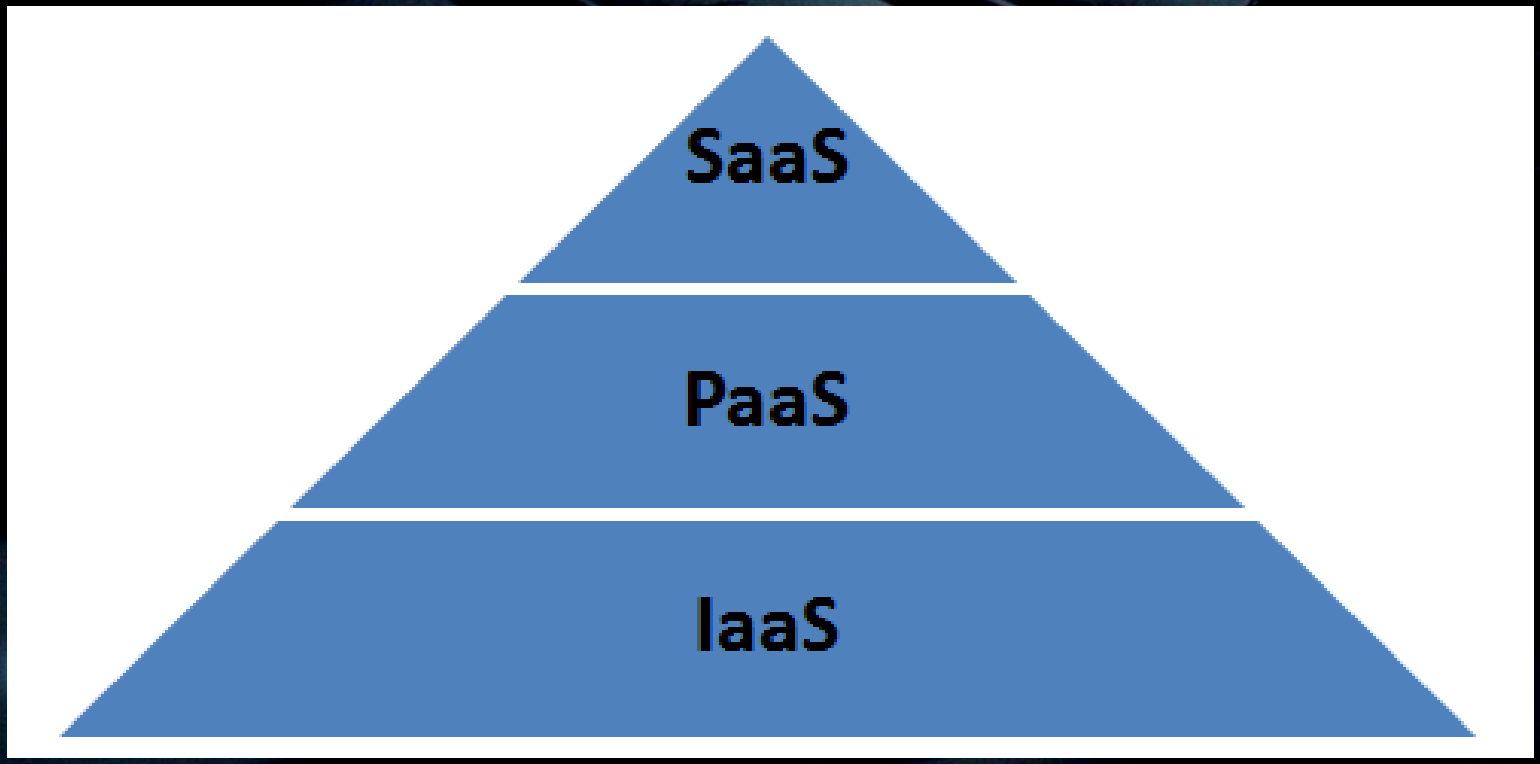
- **SaaS** poskytuje kompletní funkcionalitu dle požadavků zákazníků. V tomto případě se jedná o službu z hlediska zákazníků nejtransparentnější, kdy zákazník získává funkcionalitu zajišťovanou určitou aplikací (PaaS) v rámci určité výpočetní kapacity (IaaS).
- Zjednodušeně lze říci, že si zákazník pronajme k využívání určitý software.

Hlavní druhy

- Odběratel služby cloud computing nemusí být koncovým zákazníkem, ale využívat např. úroveň Platform as a Service (PaaS) k tomu, aby na ní provozoval vlastní aplikační software a svému zákazníku (resp. jeho koncovým uživatelům) poskytoval službu na úrovni Software as a Service (SaaS).
- Lze ale nad to nadřadit i další stupeň, např. Process as a Service či Information as a Service…

Hierarchie

Podle poskytovaných služeb můžeme definovat nejen druh cloudu, ale i hierarchii mezi nimi:



Riziko

- Nejasné vlastnické struktury, odpovědnosti, právní vztahy atd.

…časovaná bomba cloudu!

Koho je cloud?

Můžeme rozlišit zásadně dva druhy:

Private cloud (soukromý, interní cloud) – organizace má svojí ICT infrastrukturu konfigurovanou do podoby cloudu, platí veškeré své investice do ICT, ale udržuje si přímou kontrolu nad infrastrukturou.

Může být provozován IT oddělením organizace nebo dodavatelem IT služeb (outsourcing kombinovaný s cloudem).

Není podstatné, zda se jedná o organizaci soukromoprávní, nebo ze sféry orgánů veřejné moci.

Koho je cloud?

Public cloud (veřejný cloud) – veřejně dostupný cloud pro předem nespecifikované široké pole zákazníků; organizace využívá cloud externího poskytovatele, platí jen za služby, ale nemá přímou kontrolu nad infrastrukturou.

Existují i **Komunitní cloud** nebo **Hybrid cloud** (hybridní cloud) – kombinace private a public cloudu.

…čím obtížněji uchopitelný vlastník a odpovědný provozovatel, tím rizikovější!

Rizika

Pokud se jedná o private cloud provozovaný interně, pak hrozí stejná právní rizika, jako v případě jakéhokoliv jiného uspořádání podnikové ICT infrastruktury. A rovněž v případě jeho outsourcování budeme hovořit o stejných rizicích, jako v případě outsourcingu – odvíjejících se od základní otázky, **kdo má kontrolu nad infrastrukturou a nad daty.**

…otázka smlouvy a výběru dodavatele.

Nevýhody externího cloudu

1) Data jsou fyzicky uložena u poskytovatelů služeb – díky čemuž nejsou pod přímou kontrolou zákazníků cloudu.
2) Data mohou být fyzicky uložena v jiné zemi – u velkých poskytovatelů jsou obvykle využívána technologická centra po celém světě. Tato skutečnost může představovat určité právní problémy, například v oblasti zpracování osobních nebo citlivých údajů, autorských práv, jakož i z hlediska rozdílných právních úprav z hlediska odpovědnosti za škodu a její náhradu, limitace škody nebo vymahatelnosti práva vůbec.

Nevýhody externího cloudu

3) Značná závislost na poskytovateli služby a jeho řešení – použité softwarové a hardwarové řešení je dáno poskytovatelem a obvykle je nemůžeme ovlivnit.

Poskytovatel služby cloud computingu rozhoduje o všem, co se s hardware, software a dalšími složkami cloudového systému děje, včetně migrací, update a upgrade, odstávek apod.

Změna poskytovatele služby může být u některých variant cloud computingu komplikovaná a nákladná, až nemožná.

Nevýhody externího cloudu

4) Vyšší provozní náklady na konektivitu k Internetu – vzhledem k podstatě cloud computingu, kdy jsou služby poskytovány prostřednictvím Internetu, přirozeně roste objem přenesených dat a současně se zvyšují požadavky na přenosovou rychlost a latenci spojení.

Cloud pro OVM

- V případě externího cloudu použitého pro informační systém veřejné správy se jeví rizika ještě daleko větší: **orgán veřejné moci by měl mít plnou kontrolu nad daty, neboť má také plnou odpovědnost za obsah a jeho důvěrnost, integritu a ochranu před zneužitím.**
- Bezpečnostní rizika jsou v případě poskytnutí údajů, které obvykle podléhají různým druhům tajemství (od utajovaných skutečností, přes osobní údaje až po neveřejnost v případě soudních či správních řízení) příliš vysoká.

Cloud pro OVM

- Další otázkou je nutnost atestace provozovaného informačnímu systému podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy.
- Zatímco v oblasti subjektů soukromého práva je použití externího cloudu otázkou komplexního manažerského posouzení (náklady vs. rizika), **v případě informačních systémů veřejné správy je možné připustit použití externího cloudu pouze na území České republiky** a i v tomto případě po důkladné analýze rizik vzhledem k agendám, které by měly být takto zpracovávány.
-

Co je třeba mít na paměti

Víme, kde se cloud nachází
a kdo jej provozuje?
Co by nás mělo zajímat:

- teritorium a jeho poltické,

a ekonomické vlastnosti a rizika,

- provozovatel a jeho vlastnosti,
- právní řád a vymožitelnost práva,
- znění smlouvy, jurisdikce,

způsob řešení sporů,
odpovědnost za škodu atd.

Většina rizik vyplývá ze špatných smluv!

…ale co je vám platná úžasná smlouva, když se nedovoláte spravedlnosti,

nebo prosoudíte kalhoty (zahraniční spory).

Klíčové otázky věcné i smluvní

Zajištění věrohodnosti původu dat, neporušitelnosti obsahu, čitelnosti a bezpečnosti dat.

Identifikace, autentizace a autorizace transakcí.

Dlouhodobé úložiště a dokazování.

…co se stane, když?

Co dělat, když se vyskytnou problémy

1. nekomunikovat s protistranou, dokud problém nezanalyzujete a nezkonzultujete s právníkem a expertem;
2. vyhledat odbornou pomoc dříve, než máte na stole žalobu; ideální je mimosoudní řešení – dohoda o narovnání, rozhodčí řízení… cokoliv kromě soudu; výjimkou může být spor, kde jde spíše o právní, nežli věcné otázky a v tom případě je „mnohoinstančnost“ soudního řízení výhodou;

Co dělat, když se vyskytnou problémy

3. mnoho kuchařů přesolí polévku – vyberte si jednoho poradce či právníka a tomu věřte; právní zástupce by měl mít zkušenosti s předmětem sporu (důležité v jakékoliv speciální oblasti – od IT po zdravotní péči),
4. přeshraniční spor chce místního právního zástupce!

Co dělat, když se vyskytnou problémy

A hlavně:

CLOUD NENÍ SPASITELEM, BA DOKONCE VÁS MŮŽE ÚPLNĚ POHŘBÍT.

ROZHŘEŠENÍ

- ✓ Interní cloud … proč ne
- ✓ Externí cloud tuzemský … lze, ale pozor na MATRJOŠKY
- ✓ Externí cloud zahraniční, zejména mimo EU … vysoké riziko (nebezpečí ztráty soukromí uživatelů, závislosti na poskytovateli, nevymožitelnosti ničeho)

…pro OVM je zahraniční cloud v rozporu se zájmy a povinnostmi státu!

UPOZORNĚNÍ NA ZÁVĚR

Problematice se věnují ochránci osobních údajů:

- Podrobněji se všem aspektům cloud computingu věnuje Stanovisko Pracovní skupiny pro ochranu údajů zřízené podle směrnice 95/46/ES ke cloud computingu (dokument WP 196) přijaté dne 1. 7. 2012 a dostupné na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_cs.pdf#h2-2,

UPOZORNĚNÍ NA ZÁVĚR

Problematice se věnují ochránci osobních údajů:

- u nás dokument „K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb“, viz http://www.uoou.cz/files/k_pravni_ochrane_ou_pri_predavani_v_ramci_cloudovych_sluzeb.pdf

UPOZORNĚNÍ NA ZÁVĚR

Požaduje se:

- identifikovat, kam jsou OÚ předávány (EU/non EU ale Úmluva RE č.108/bez ochrany/USA – „Safe Harbour“ List),
- podle toho odpovídající úroveň ochrany,
- nejvhodnějšími nástroji jsou standardní smluvní doložky a závazná podniková pravidla (BCR).

UPOZORNĚNÍ NA ZÁVĚR

Smluvní doložky jsou přílohou rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES.

UPOZORNĚNÍ NA ZÁVĚR

Závazná podniková pravidla (Binding Corporate rules, dále jen „BCR“) jsou vhodná pro předávání údajů zpracovatelem dílčím zpracovatelům v rámci téže korporace a na základě pokynů správce, aniž by bylo zapotřebí uzavřít s každým novým dílčím zpracovatelem zvlášť smlouvu o zpracování.

Zpracovatel musí BCR předložit ke schválení vedoucímu dozorovému úřadu v EU, který řídí celý schvalovací proces a následně garantuje, že BCR mohou být považována za nástroj poskytující odpovídající ochranu.

Literatura

Smejkal, V., Rais, K.:
Řízení rizik ve firmách a jiných organizacích.
4. vydání. GRADA,
Praha 2013.
Cca 450 stran.
(www.grada.cz)

Literatura – vyjde příští týden!

Mates, V., Smejkal, V.

E-government v České republice.

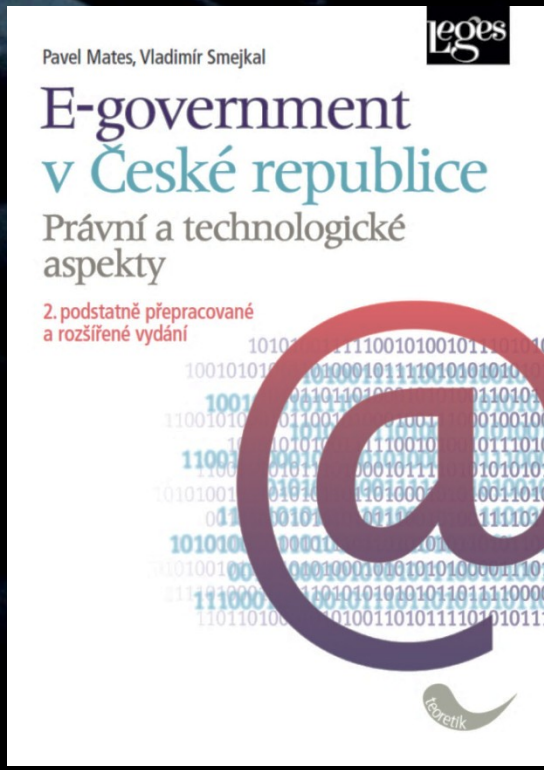
Právní a technologické aspekty.

2. podstatně přepracované a rozšířené vydání

500 stran

Nakladatelství Leges

(www.leges.cz)



Děkuji za pozornost.

Kontakt:

smejkal@znalci.cz

www.znalci.cz

www.kompetence.cz