11. Právo a bezpečnost v IT

Trestní zákon a IT

Trestní zákon (**zákon č. 40/2009 Sb.**, stále platný v červnu 2025) obsahuje ustanovení týkající se trestných činů souvisejících s informačními technologiemi a kybernetickou bezpečností. Například **§ 230 – Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému**, § 231 až 232 se zabývají opatřeními a šířením prostředků umožňujících neoprávněný přístup do počítačového systému.

Zákon o kybernetické bezpečnosti a vyhlášky

V zákoně **č. 181/2014 Sb.** (stále platný v červnu 2025) o kybernetické bezpečnosti se stanovují povinnosti týkající se bezpečnosti informačních systémů a sítí.

Vyhláška **č. 82/2018 Sb.** definuje bezpečnostní opatření a postupy, které se musí dodržovat s cílem minimalizovat rizika spojená s kybernetickými útoky. Tento zákon a vyhláška jsou klíčové pro ochranu kritické informační infrastruktury země.

Autorský zákon z hlediska IT

Zákon č. 121/2000 Sb. o autorském právu chrání autorská práva k dílům v digitální podobě včetně softwaru a databází. Tento zákon upravuje i udělování licencí na software a ochranu práv vývojářů a uživatelů.

eIDAS

Nařízení **EU č. 910/2014** o elektronické identifikaci, autentifikaci a důvěryhodných službách (eIDAS) upravuje elektronickou identifikaci a důvěryhodné služby pro elektronické transakce v rámci EU. Stanovuje jednotné technické i právní požadavky na důvěryhodnost elektronických transakcí.

Digitální podpis a certifikační autority

Digitální podpis je elektronický ekvivalent vlastnoručního podpisu, který zajišťuje pravost a integritu elektronických dokumentů. Certifikační autority (CA) jsou důvěryhodné třetí strany, které vydávají digitální certifikáty na ověření identity uživatelů a zařízení. Tyto certifikáty jsou potřebné k vytváření a ověřování digitálních podpisů.

Časové razítko

Elektronický údaj, který potvrzuje čas vytvoření nebo změny dokumentu. Slouží k prokázání existence dokumentu v daném čase a ochraně proti zpětným změnám.

Elektronická pečeť

Elektronická pečeť je nástroj podobný digitálnímu podpisu, který se používá k zajištění pravosti a integrity dokumentů v elektronické podobě. Používají ji zejména organizace k ověřování pravosti svých elektronických dokumentů.

Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce

Upravuje poskytování služeb, jako jsou **elektronické podpisy, pečeti, časová razítka a autentifikace**.

Implementuje eIDAS do českého právního systému.

Elektronické podatelny

Systémy pro příjem a zpracování **elektronických podání** (žádostí, dokumentů) vůči úřadům a organizacím. Zajišťují bezpečnost, evidenci a archivaci elektronické komunikace.

Komunikace se státní správou a samosprávou

Probíhá pomocí datových schránek a elektronických formulářů. Zajišťuje rychlou, bezpečnou a doložitelnou výměnu informací bez nutnosti fyzické návštěvy úřadu.

Komunikace se zdravotními pojišťovnami a jejich zabezpečení

Elektronická komunikace (například výkazy, faktury) probíhá přes zabezpečené systémy. Cílem je ochrana citlivých údajů před neoprávněným přístupem a zneužitím.

Zálohování, podpis a další náležitosti elektronické zdravotní dokumentace

Elektronické zdravotní záznamy se pravidelně zálohují a chrání proti ztrátě nebo poškození dat. Používají se elektronické podpisy, pečeti a šifrování na ochranu integrity a pravosti záznamů.

Ochrana osobních a citlivých údajů v IT

Ochrana údajů v IT zahrnuje šifrování, anonymizaci, kontrolu přístupu a pravidelné bezpečnostní audity. Organizace musí zavést technická a organizační opatření na ochranu údajů před neoprávněným přístupem a zneužitím.

Zákon o ochraně osobních údajů v současném znění, GDPR

Zákon č. 110/2019 Sb. o zpracování osobních údajů je českou adaptací **GDPR (General Data Protection Regulation)**, které harmonizuje ochranu osobních údajů v rámci EU. GDPR stanovuje pravidla zpracování osobních údajů, práva dotčených osob a povinnosti správců a zpracovatelů.

Ochrana soukromí na pracovišti vzhledem k IT

Týká se monitorování zaměstnanců, používání pracovních IT prostředků a přístupu k osobním údajům zaměstnanců. Zaměstnavatelé musí respektovat práva zaměstnanců a informovat o rozsahu monitorování.

Ochrana soukromí a IT

Zajišťuje, že osobní údaje jsou zpracovávány zákonně, transparentně, v minimálním rozsahu a bezpečně. Typicky zahrnuje šifrování, anonymizaci a omezení přístupu.

Úřad pro ochranu osobních údajů

Nezávislý dozorový orgán pro oblast ochrany osobních údajů.

Poskytuje metodickou pomoc, vyřizuje stížnosti a může ukládat sankce za porušení právních předpisů o ochraně údajů.

Právní aspekty outsourcingu

Outsourcing IT služeb zahrnuje smluvní ujednání mezi klientem a poskytovatelem služeb. Právní aspekty zahrnují ochranu duševního vlastnictví, bezpečnost údajů, dodržování předpisů a odpovědnost za případné škody způsobené outsourcingovým partnerem.

Zákon č. 365/2000 Sb. – o informačních systémech veřejné správy a o změně některých dalších zákonů

Zákon o informačních systémech veřejné správy upravuje povinnosti a práva při používání informačních systémů ve veřejné správě. Zákon stanovuje standardy interoperability, bezpečnosti a ochrany údajů v systémech veřejné správy.

Zákon č. 480/2004 Sb. – o některých službách informační společnosti

Zákon o některých službách informační společnosti upravuje poskytování elektronických komunikačních služeb a ochranu osobních údajů v online prostředí.

Upravuje poskytování elektronických služeb (např. e-maily, newslettery).

Řeší také pravidla pro zasílání obchodních sdělení (antispam).

Webové stránky, obsah webu a související zákony

Webové stránky podniků musí obsahovat **identifikační údaje** dle **§ 435 občanského zákoníku** a **§ 7 zákona o obchodních korporacích**.

Musí plnit i povinnosti týkající se ochrany osobních údajů podle GDPR a zákona o službách informační společnosti.

Ochrana soukromí u webových stránek

Povinnost **informovat návštěvníky** o zpracování osobních údajů a získat souhlas s cookies.

Je třeba zavést vhodná opatření pro ochranu údajů shromážděných přes web.