**Trestný zákon**: Trestný zákon (zákon č. 40/2009 Z. z.) obsahuje ustanovenia týkajúce sa trestných činov súvisiacich s informačnými technológiami a kybernetickou bezpečnosťou. Napríklad § 230 sa zameriava na neoprávnený prístup do počítačového systému a na nosič informácií, zatiaľ čo § 231 až 232 sa zaoberajú opatreniami a šírením prostriedkov umožňujúcich neoprávnený prístup do počítačového systému.

**Zákon o kybernetickej bezpečnosti, vyhlášky**: V zákone č. 181/2014 o kybernetickej bezpečnosti sa stanovujú povinnosti týkajúce sa bezpečnosti informačných systémov a sietí. Vyhláška č. 82/2018 Z. z. definuje bezpečnostné opatrenia a postupy, ktoré sa musia dodržiavať s cieľom minimalizovať riziká spojené s kybernetickými útokmi. Tento zákon a vyhláška sú kľúčové pre ochranu kritickej informačnej infraštruktúry krajiny.

**Autorské právo z pohľadu IT**: Zákon č. 121/2000 Z. z. o autorskom práve chráni autorské práva k dielam v digitálnej podobe vrátane softvéru a databáz. Tento zákon upravuje aj udeľovanie licencií na softvér a ochranu práv vývojárov a používateľov.

**eIDAS**: Nariadenie č. 910/2014 o elektronickej identifikácii, autentifikácii a dôveryhodných službách (eIDAS) upravuje elektronickú identifikáciu a dôveryhodné služby pre elektronické transakcie v rámci EÚ. Toto nariadenie stanovuje jednotné normy pre elektronické podpisy, elektronické pečate, časové pečiatky a služby overovania dokumentov.

**Digitálny podpis, certifikačné autority**: Digitálny podpis je elektronický ekvivalent vlastnoručného podpisu, ktorý zabezpečuje pravosť a integritu elektronických dokumentov. Certifikačné autority (CA) sú dôveryhodné tretie strany, ktoré vydávajú digitálne certifikáty na overenie identity používateľov a zariadení. Tieto certifikáty sú potrebné na vytváranie a overovanie digitálnych podpisov.

**Časová pečiatka**: Časová pečiatka je elektronický údaj, ktorý potvrdzuje čas vytvorenia alebo odoslania dokumentu. Používa sa na zabezpečenie integrity a pravosti dokumentov zaznamenaním presného času ich existencie a akýchkoľvek zmien.

**Elektronická pečať**: Elektronická pečať je nástroj podobný digitálnemu podpisu, ktorý sa používa na zabezpečenie pravosti a integrity dokumentov v elektronickej podobe. Používajú ju najmä organizácie na overovanie pravosti svojich elektronických dokumentov.

**Zákon č. 297/2016 Z. z.**: Zákon o službách vytvárania dôvery pre elektronické transakcie upravuje poskytovanie služieb, ako sú elektronické podpisy, pečate, časové pečiatky a autentifikácia. Tento zákon je implementáciou eIDAS do českého právneho systému a stanovuje povinnosti poskytovateľov týchto služieb.

**Elektronické podateľne**: sú systémy na prijímanie a spracovanie elektronických podaní od verejnosti a organizácií. Umožňujú efektívnu a bezpečnú komunikáciu medzi občanmi a verejnými inštitúciami a zabezpečujú evidenciu a archiváciu elektronických dokumentov.

**Komunikácia so štátnou správou a samosprávou**: Elektronická komunikácia so štátnou správou a samosprávou zahŕňa využívanie dátových schránok a elektronických systémov na podávanie žiadostí, správ a iných dokumentov. Zabezpečuje rýchlu a bezpečnú výmenu informácií a minimalizuje potrebu osobných návštev úradov.

**Komunikácia so zdravotnými poisťovňami, ich zabezpečenie**: Komunikácia so zdravotnými poisťovňami zahŕňa elektronické predkladanie faktúr, výkazov a iných dokumentov prostredníctvom zabezpečených elektronických systémov. Zabezpečuje sa ochrana citlivých údajov pacientov a lekárov pred neoprávneným prístupom a zneužitím.

**Zálohovanie, podpisovanie a ďalšie prvky elektronických zdravotných záznamov**: Elektronické zdravotné záznamy sa pravidelne zálohujú a chránia pred stratou údajov. Elektronické podpisy a pečate zabezpečujú pravosť a integritu zdravotných záznamov, zatiaľ čo šifrovanie a iné bezpečnostné opatrenia chránia údaje pred neoprávneným prístupom.

**Ochrana osobných a citlivých údajov a IT**: Ochrana údajov v IT zahŕňa šifrovanie, anonymizáciu, kontrolu prístupu a pravidelné bezpečnostné audity. Organizácie musia zaviesť technické a organizačné opatrenia na ochranu údajov pred neoprávneným prístupom a zneužitím.

**Zákon o ochrane údajov, nariadenie GDPR**: Zákon č. 110/2019 Z. z. o spracúvaní osobných údajov je českou adaptáciou GDPR (General Data Protection Regulation), ktoré harmonizuje ochranu osobných údajov v rámci EÚ. GDPR stanovuje pravidlá spracúvania osobných údajov, práva dotknutých osôb a povinnosti prevádzkovateľov a sprostredkovateľov.

**Ochrana osobných údajov na pracovisku v súvislosti s IT**: Ochrana osobných údajov na pracovisku zahŕňa pravidlá týkajúce sa monitorovania zamestnancov, používania pracovných IT zdrojov a prístupu k osobným údajom. Zamestnávatelia musia rešpektovať práva zamestnancov na súkromie a informovať ich o rozsahu a metódach monitorovania.

**Ochrana súkromia a IT**: Ochrana súkromia v oblasti IT zahŕňa implementáciu technológií a politík, ktoré zabezpečujú, aby sa osobné údaje spracúvali zákonným a transparentným spôsobom. To zahŕňa šifrovanie, anonymizáciu, pravidelné audity a obmedzenie prístupu k citlivým údajom.

**Orgán na ochranu údajov**: Úrad na ochranu osobných údajov (OPDP) je nezávislý orgán, ktorý dohliada na dodržiavanie pravidiel ochrany údajov v krajine. OPDP poskytuje metodickú pomoc, vybavuje sťažnosti a môže ukladať sankcie za porušenie právnych predpisov o ochrane údajov.

**Právne aspekty outsourcingu**: Outsourcing IT služieb zahŕňa zmluvné dojednanie medzi klientom a poskytovateľom služieb. Právne aspekty zahŕňajú ochranu duševného vlastníctva, bezpečnosť údajov, dodržiavanie predpisov a zodpovednosť za prípadné škody spôsobené outsourcingovým partnerom.

**Zákon č. 365/2000 Z. z.**: Zákon o informačných systémoch verejnej správy upravuje povinnosti a práva pri používaní informačných systémov vo verejnej správe. Zákon stanovuje štandardy interoperability, bezpečnosti a ochrany údajov v systémoch verejnej správy.

**Zákon č. 480/2004 Z. z.**: Zákon o niektorých službách informačnej spoločnosti upravuje poskytovanie elektronických komunikačných služieb a ochranu osobných údajov v online prostredí. Tento zákon stanovuje pravidlá pre zasielanie obchodných oznámení a ochranu pred spamom.

**Webové stránky, webový obsah a súvisiace zákony**: Webové stránky podnikov musia obsahovať povinné identifikačné údaje podľa § 435 Občianskeho zákonníka a § 7 zákona o obchodných korporáciách. Pravidlá ochrany osobných údajov na webových stránkach vychádzajú z GDPR a zákona o niektorých službách informačnej spoločnosti.

**Ochrana osobných údajov a webové stránky**: Ochrana súkromia na webových stránkach zahŕňa transparentné informovanie návštevníkov o spracúvaní ich osobných údajov, získavanie súhlasu na používanie súborov cookie a vykonávanie opatrení na ochranu osobných údajov získaných prostredníctvom webových stránok.