MPSV

ÚSTAV STÁTU A PRÁVA
Akademie věd ČR

VÚBP VÝZKUMNÝ ÚSTAV BEZPEČNOSTI PRÁCE

WORKSHOP
DIGITALIZACE V PRACOVNÍM PRÁVU II

Praha
2024

TYP VÝSLEDKU

☒ W ☐ M

ČÍSLO VÝZKUMNÉHO ÚKOLU

01-S4-2023-VUBP

NÁZEV VÝZKUMNÉHO ÚKOLU V ČJ

Nové fenomény pracovněprávního prostředí zasahující do kvality zajišťovaných pracovních podmínek zaměstnanců s přesahem do problematiky bezpečnosti a ochrany zdraví

NÁZEV VÝZKUMNÉHO ÚKOLU V AJ

New phenomena in the labor law environment affecting the quality of provided working conditions for employees with implications for safety and health protection issues.

HLAVNÍ ŘEŠITEL

Výzkumný ústav bezpečnosti práce, v. v. i.

VÚBP je otevřené multidisciplinární pracoviště, které spolupracuje s ostatními výzkumnými a odbornými organizacemi, vysokými školami i individuálními odborníky v širokém spektru svých aktivit, a to jak na domácí, tak i na mezinárodní úrovni. Zřizovatelem je MPSV. Ve své činnosti se věnuje vědě a výzkumu, vzdělávání, zkoušení osobních ochranných prostředků, poradenství a osvětě v oblasti prevence pracovních rizik a bezpečnosti a ochrany zdraví při práci (BOZP). VÚBP hraje také nezastupitelnou úlohu v prevenci závažných havárií.

SPOLUŘEŠITEL

Ústav státu a práva Akademie věd ČR, v. v. i.

Ústav uskutečňuje vědecký výzkum v oblasti práva a právní informatiky, přispívá ke zvyšování úrovně poznání a vzdělanosti, využívá výsledků vědeckého výzkumu; získává, zpracovává a rozšiřuje vědecké informace; poskytuje vědecká stanoviska), posudky a doporučení. Ústav v rámci předmětu své činnosti rozvíjí mezinárodní spolupráci, pořádá konference, semináře apod., spolupracuje s dalšími institucemi, a především s vysokými školami. Vydává časopis Právník jako výrazně teoretický časopis pro otázky státu a práva, který má dlouholetou tradici (jeho první číslo vyšlo roku 1861), časopis TLQ a Časopis zdravotnického práva a bioetiky. Od 1. 1. 2007 se ústav stal veřejnou výzkumnou institucí dle zákona č. 341/2005 Sb., o veřejných výzkumných institucích (ve zkratce v. v. i.), a je zapsán v Rejstříku veřejných výzkumných institucí. Nadále má vlastní právní subjektivitu a je součástí Akademie věd ČR, která je jeho zřizovatelem.

Tento výsledek byl finančně podpořen z institucionální podpory na dlouhodobý koncepční rozvoj výzkumné organizace na léta 2023–2027 a je součástí výzkumného úkolu 01-S4-2023-VÚBP Nové fenomény pracovněprávního prostředí zasahující do kvality zajišťovaných pracovních podmínek zaměstnanců s přesahem do problematiky bezpečnosti a ochrany zdraví řešeného Výzkumným ústavem bezpečnosti práce, v. v. i., v letech 2023–2024 ve spolupráci s Ústavem státu a práva Akademie věd ČR.

DATUM KONÁNÍ

25. 11. 2024, 14:00–16:30

MÍSTO KONÁNÍ

VÚBP, v. v. i. (Jeruzalémská 1283/9, Praha 1)/ online prostřednictvím aplikace Restream živě vysílané na platformě YouTube

CÍLOVÁ SKUPINA

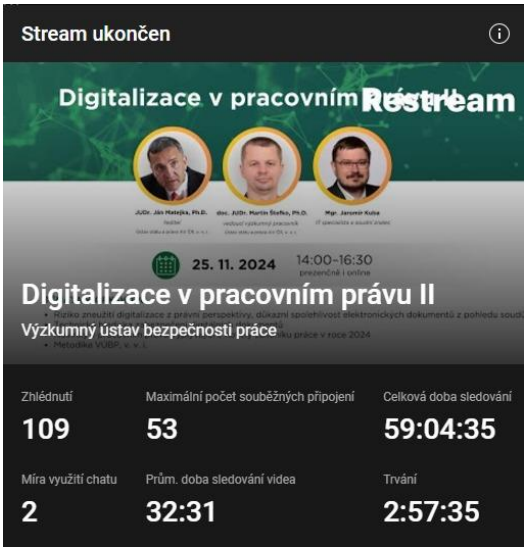
Zaměstnavatelé, personalisté, osoby odborně způsobilé v prevenci rizik a další zaměstnanci soukromého sektoru, zástupci státní správy (MPSV, Státní úřad inspekce práce, Ministerstvo vnitra)

POČET ÚČASTNÍKŮ

5 prezenčně (přednášející, zástupci VÚBP)/ 103 registrovaných pro online přenos (celkový počet zhlédnutí na YouTube k 26. 11. 2024 – 174)

Z TOHO ZE ZAHRANIČÍ 0

Podrobné statistiky průběhu Streamu:



PŘEDSTAVENÍ VÝZKUMNÉHO ÚKOLU, V RÁMCI KTERÉHO BYLA AKCE REALIZOVÁNA

Měnící se trh práce vyžaduje zvýšení tlaku na digitalizaci pracovněprávní dokumentace s dopady do dokumentace BOZP. Součástí příprav na zvýšení odolnosti společnosti je posílení právní úpravy týkající se distančního výkonu práce. Tato forma práce je z hlediska ergonomických parametrů a psychosociálních rizik velmi zátěžová a je třeba nastavit systémově tuto oblast tak, aby nezpůsobovala snížení kvality pracovních podmínek zaměstnanců a zároveň byla pro zaměstnavatele byla přínosná. Digitalizace a zjednodušení a modernizace nástrojů v této oblasti sníží tlak na obě strany jak v oblasti psychosociální, tak z hlediska administrativní zátěže zaměstnavatele. Jedná se úpravu sjednávání pracovní smluv na dálku, úpravu elektronických výplatnic, plánování směn, školení zaměstnanců k zajištění ochrany zdraví zaměstnanců a zajištění bezpečnosti práce a odškodnění zaměstnanců za úrazy či nemoci z povolání způsobené distančním výkonem práce či v souvislosti s tímto atypickým výkonem práce.

JMÉNO PŘIZVANÉHO ODBORNÉHO GARANTA VÝSLEDKU

JUDr. Jaroslav Stádník, Ph.D., DBA, LL.D.

SEZNAM PREZENTUJÍCÍCH, NÁZEV A KRÁTKÉ PŘEDSTAVENÍ PŘEDNÁŠKY

Jméno: Jana Příjmení: Ranglová Instituce: Výzkumný ústav bezpečnosti práce, v. v. i.

Název přednášky: *Úvodní slovo*

V rámci úvodního slova workshopu byl účastníkům představen výzkumný úkol Nové fenomény pracovněprávního prostředí zasahující do kvality zajišťovaných pracovních podmínek zaměstnanců s přesahem do problematiky bezpečnosti a ochrany zdraví. Účastníci byli upozorněni, že se jedná o tematicky i obsahově navazující workshop a že je možné ze záznamu shlédnout workshop, který se uskutečnil v listopadu 2023.

Příspěvek prezentuje původní výsledek výzkumu výzkumného úkolu: ☐

Jméno: Martin Příjmení: Štefko Instituce: Ústav státu a práva Akademie věd ČR, v. v. i.

Název přednášky: *Digitalizace v pracovním právu (aplikační problémy)*

Přednáška shrnula úvodní pojmy týkající se digitalizace pracovního práva, které jsou součástí připravované Metodiky digitalizace pracovněprávní dokumentace určené zaměstnavatelům. Mgr. Štefko se také věnoval z právního hlediska zejména praktickým aplikačním problémům digitalizace, již v kontextu chystané flexinovely zákoníku práce. Velká pozornost byla také věnována aktuální rozhodovací praxi soudů, které se otázkami digitalizace v posledních letech zabývaly.

Příspěvek prezentuje původní výsledek výzkumu výzkumného úkolu: ☒

Jméno: Ján Příjmení: Matejka Instituce: Ústav státu a práva Akademie věd ČR, v. v. i.

Název přednášky: *Otázky digitalizace pracovního práva, ochrany osobních údajů a využívání umělé inteligence*

Přednáška se zabývala zásadními aspekty digitalizace pracovního práva z pohledu české legislativy, které jsou součástí připravované Metodiky digitalizace pracovněprávní dokumentace určené zaměstnavatelům. Jedná se o: elektronické podpisy a jejich druhy, úpravu elektronického podepisování dle eIDAS a českého práva, problematiku ochrany osobních údajů atd. Značná pozornost byla věnována také vysoce aktuální otázce využití (resp. i zneužití) umělé inteligence a povinnosti a omezení vyplývající z AI Actu.

Příspěvek prezentuje původní výsledek výzkumu výzkumného úkolu: ☒

Jméno: Jaromír Příjmení: Kuba Instituce: Soudní znalec, IT specialista

Název přednášky: *Technická hlediska zabezpečení a průkaznosti digitálních dokumentů*

Přednáška doplnila právní pohled na problematiku digitalizace pracovního práva o technické hledisko odborníka v oblasti IT. Mgr. Kuba se zabýval především rizikem zneužití a možnými preventivními opatřeními v rámci digitalizace a nově i využívání umělé inteligence.

Příspěvek prezentuje původní výsledek výzkumu výzkumného úkolu: ☐

POZVÁNKA

PROGRAM

Jana Ranglová – Úvodní slovo, představení výzkumného úkolu

Martin Štefko – Digitalizace v pracovním právu (aplikační problémy)

Technická pauza

Ján Matejka – Otázky digitalizace pracovního práva, ochrany osobních údajů a využívání umělé inteligence

Jaromír Kuba – Technická hlediska zabezpečení a průkaznosti digitálních dokumentů

Dotazy a diskuze: průběžně

Závěr a poděkování

ZÁPIS

Workshop byl zaměřen na zejména právní aspekty digitalizace pracovního práva a byl doplněn o technické hledisko dané problematiky. Martin Štefko zdůraznil zejména praktické právní aspekty a aplikační problémy digitalizace, přičemž se věnoval i tématům plánované flexinovely zákoníku práce. Součástí výkladu byla také analýza aktuálních soudních rozhodnutí, která reflektují postupující digitalizaci v pracovněprávním kontextu.

Ján Matejka se zaměřil na zásadní aspekty digitalizace z hlediska českého práva. Představila problematiku elektronických podpisů včetně jejich různých typů a legislativní úpravy podle nařízení eIDAS a českého právního rámce. Důležitou částí byla diskuse o ochraně osobních údajů a aktuálních požadavcích v souvislosti s využíváním a regulací umělé inteligence. Zvláštní důraz byl kladen na témata spojená s AI Actem, jeho povinnostmi a riziky spojenými se zneužitím umělé inteligence.

Mgr. Kuba se věnoval rizikům zneužití technologií, zejména v oblasti využití umělé inteligence, a navrhl možná preventivní opatření pro minimalizaci těchto rizik. Přednáška spojila právní rámec s praktickými IT doporučeními, čímž doplnila celkový přehled workshopu.

Nedílnou součástí workshopu byla diskuze s účastníky, která probíhala prostřednictvím chatu živě během Streamu, případně zasláním příspěvků na email organizátorů. Účastníci během konání workshopu vznesli dotazy např. k těmto tématům: možnost zavedení evidence docházky prostřednictvím otisku prstů; nutnost vlastnoručního podpisu na prezenční listině v případě e-learningového školení BOZP a PO; pořizování fotografií/ videí z požárního cvičení ve vztahu k požadavkům GDPR; povinnost státních institucí komunikovat s fyzickými osobami prostřednictvím datových schránek; RFID čtečky zaměstnance, atd.

Záznam z workshopu: https://www.youtube.com/watch?v=8Fhzt7G1dQM

PŘÍLOHY – JEDNOTLIVÉ PREZENTACE

Příloha č. 1 – Digitalizace v pracovním právu II – společná prezentace Jána Matejky a Martina Štefka

Příloha č. 2 – Technická hlediska zabezpečení a průkaznosti digitálních dokumentů – prezentace Jaromíra Kuby

Praha, 25. 11. 2024 Workshop – Digitalizace v pracovním právu

ÚSTAV STÁTU A PRÁVA

Digitalizace v pracovním právu II

(Aplikační problémy)

Ján Matejka, Martin Štefko
Ústav státu a práva AV ČR, v. v. i.

ÚSTAV STÁTU A PRÁVA

I. Pojem a význam digitalizace v pracovním právu

Digitalizace je proces

ÚSTAV STÁTU A PRÁVA

- **Proces zavádění využívání digitálních technologií** v nejrůznějších oblastech výroby i života společnosti.
- Původně byl termín používán pouze v souvislosti s digitalizací textu (například knih nebo dokumentů). Obecně digitalizace pokrývá všechny nové možnosti postavené na digitálních technologiích, které přinášejí zefektivnění procesů a služeb.

- **Cílem** tohoto procesu je:
  - zvýšení efektivity a zlepšení fungování procesů a služeb (včetně výroby),
  - snížení ekologické zátěže,
  - zlepšení kvality života.

- **Důsledky**:
  - částečný „přenos" odpovědnosti od člověka k technologiím,
  - nový pohled na výsledky „práce", včetně regulatorních přesahů,
  - změna pracovního trhu.

Digitalizace „pracovněprávních vztahů“

ÚSTAV STÁTU A PRÁVA

- **Výkon práce prostřednictvím digitálních platforem práce** (crowdworking, aj.)
- **Flexinovela**
- **Využívání IT nástrojů podpory práce (AI asistence)**
  - **Využívání nástrojů automatizace práce (AI) při výkonu práce**
  - **Využívání generativních modelů a nástrojů big data**
- **Nároky kladené na informační systémy**
  - požadavky GDPR (zabezpečení), a kyberbezpečnosti.
- **Elektronický právní styk** mezi účastníky PP vztahů
  - možnost el. kontraktace, včetně el. doručování,
  - impl. automatizované zpracování os. údajů (GDPR)
  - otázky archivace el. písemností (EIDAS)

ÚSTAV STÁTU A PRÁVA

II. Otázky digitalizace pracovního práva, ochrany osobních údajů a využívání umělé inteligence

Změny v PP obecně

ÚSTAV STÁTU A PRÁVA

změny daňových předpisů

- změny u zdanění DPP – již schváleno (1.1.2025)

– **novely zákoníku práce**

- tzv. “flexinovela“ ZP – 1. čtení, tisk 775 (1.1.2025?)
- transpozice EU směrnice o transparentnosti – zatím není návrh (7.6.2026)

– novela zákona o zaměstnanosti a o inspekci práce

- zaměstnávání OZP a změny u přestupků – 2. čtení, tisk 743 (1.1.2025?)

– **změny ostatních předpisů**

- zrušení vstupních lékařských prohlídek – po projednání vládou (1.1.2025?)
- zrušení přísedících u pracovněprávních sporů – veto přehlasováno (1.1.2025)
- transpozice EU “women on board“ směrnice – 2. čtení (28.12.2024)

Flexinovela

- sněmovní tisk 775; projednání na schůzi od 19.11.2024
- stále se oficiálně předpokládá účinnost od 1.1.2025, ale už nereálné
- ve verzi předložené Sněmovně je pár nových/změněných bodů, např.

primární způsob výplaty na účet (zaměstnanec má právo veta) nebo vyladění

práva na „odstupné“ (od Kooperativy i při ohrožení nemocí z povolání)

- ostatní diskutované body (vč. úpravy běhu a délky výpovědní doby) zůstávají
- naopak stále chybí výpověď bez udání důvodu (ODS hlásí, že doplní ve Sněmovně) a bohužel strop pro náhradu mzdy při neplatném propuštění
- pozměňov. mlčenlivost o odměně

ÚSTAV STÁTU A PRÁVA

DPP

- režim tzv. oznámené DPP, který měl být účinný od 1.1.2025, se má zrušit

(pozměňovací návrh ministra Jurečky ke sněmovnímu tisku 743)

 od ledna nemá pouze jedna oznámená DPP zaměstnance

- oznamovací povinnosti (které jsou platné od 1.7.2024) týkající se existence DPP a povinného hlášení o výši odměny z DPP (každý měsíc) zůstanou v platnosti

 všechny DPP u více zaměstnavatelů budou osvobozené od pojistného do limitu, sčítají se pouze příjmy z více DPP u jednoho zaměstnavatele podléhat odvodům na pojistné jen pokud v daném měsíci překročí limit 25% průměrné mzdy (11.500 Kč v roce 2025); to samé i pro srážkovou daň

 pozm. návrh přináší také vyšší osvobození zdravotních benefitů

ÚSTAV STÁTU A PRÁVA

NS sp.zn. 21 Cdo 1209/2024

zaměstnanec oznámil pomocí SMS čerpání dovolené za předchozí rok (v režimu § 218/4 ZP) a následně „na papíru“ až těsně před čerpáním

NS: určení dovolené (právní jednání) SMS je nerelevantní, neboť neodpovídalo požadavkům § 337 ZP na doručování písemností

Ale:§ 337 ZP vůbec nedopadá na nařizování dovolené

ÚSTAV STÁTU A PRÁVA

Podpis písemnosti v PP

21 Cdo 2061/2021: přílohu e-mailové zprávy scan dohody o narovnání, podepsané předsedou představenstva žalované L. Š. a M. Z – závěr NS: je závazná

21 Cdo 3693/2012: **Písemnost musí být podepsána elektronickým podpisem založeným na kvalifikovaném certifikátu**

21 Cdo 2061/2021 ze dne 27. 4. 2022

V průběhu měsíce června 2019 žalobce, právní zástupkyně žalobce a žalovaná jednali (formou e-mailové korespondence) o vyřešení sporných právních vztahů. Žalovaná dne 19. 6. 2019 zaslala žalobci jako přílohu e-mailové zprávy scan dohody o narovnání, podepsané předsedou představenstva žalované L. Š. a M. Z. Zástupkyně žalobce zaslala dne 20. 6. 2019 **žalované e-mailovou zprávu – potvrzení o tom, že dohoda byla žalobcem akceptována a podepsána**.

NS: scan byl již podepsán dvěma členy statutárního orgánu + dohodnuté náležitosti + nabídku bez výhrad přijímá

ÚSTAV STÁTU A PRÁVA

21 Cdo 3411/2014-665 ze dne 19. 2. 2016,

Zec právo na náhradu škody

Přijetím takové nabídky ze strany žalobce (navíc, učiněné elektronicky na adresu žalované, aniž by listina byla podepsána elektronickým podpisem žalobce založeným na kvalifikovaném systémovém certifikátu) nemohlo dojít ke smlouvě o budoucí pracovní smlouvě účastníků

Překážky digitalizace

ÚSTAV STÁTU A PRÁVA

- **nová legislativa je použitelná, byť nikoliv bezproblémová**
  - novela umožňuje elektronické podepisování vybraných pracovněprávních dokumentů, včetně pracovních smluv, dodatků, dohod o rozvázání pracovněprávního vztahu,
  - jednostranné ukončovacích jednání jsou vázány na uznávaný elektronický podpis, lze je doručovat elektronicky,
  - rozšiřují se také možnosti využití různých digitálních nástrojů, včetně digitalizace náborů (použití vzdálené identifikace, aj.).

- **přetrvává právní (ne)jistota ohledně důvěryhodnosti digitálních písemností,**
- **riziko z transakčních nákladů a zák. limitace při zpracování dat,**
- **zpravidla chybí vzdělaný a nadšený tým, který za tento proces ponese odpovědnost,**
- **chybí podpora těchto procesů na straně zaměstnavatele,**
- **přetrvává obava z rizika ochrana (biometrických osobních údajů), kde současně dochází k přeceňování existujících rizik,**

- **relevantní právní úprava je roztříštěná, její aplikace není triviální,**

Důvěryhodnost digitálních písemností

ÚSTAV STÁTU A PRÁVA

- **V obecné rovině (soukromé) právo elektronickým písemnostem poskytuje dostatečnou míru důvěry**

- **Důkazní domněnka spolehlivosti** (§ 562/2 OZ)
  - Má se za to, že záznamy údajů o právních jednáních v elektronickém systému jsou spolehlivé, provádějí-li se systematicky a posloupně a jsou-li chráněny proti změnám. Byl-li záznam pořízen při provozu závodu a dovolá-li se jej druhá strana k svému prospěchu, má se za to, že záznam je spolehlivý.

- **Možnosti ISDS** (dle zák. č. 300/2008)
  - Nepřihlásí-li se do datové schránky osoba … lhůtě 10 dnů ode dne, kdy byl dokument dodán do datové schránky, **považuje se tento dokument za doručený posledním dnem této lhůty** (§ 18a odst. 3)
  - Úkon učiněný osobou … nebo pověřenou osobou, pokud k tomu byla pověřena, prostřednictvím datové schránky **má stejné účinky jako úkon učiněný písemně a podepsaný**, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.

- **Fikce doručení v pracovním právu je z hlediska důkazního břemene problematická (lze však prokazovat i jinak - viz diskuse)**

Ochrana osobních údajů I. (obecně)

ÚSTAV STÁTU A PRÁVA

- **Režim obecného nařízení o ochraně osobních údajů (GDPR)**
  - znalost procesů zpracování osobních údajů (vždy),
  - SW nástroje účetní či mzdové evidence, práce přesčas, apod.,
  - požadavky na zabezpečení přístupu, apod.
  - znalost procesů zpracování osobních údajů (vždy),
  - Povinnost transparentnosti
  - princip minimalizace osobních údajů (ve vztahu k pr. titulu),
  - zvážit potřebnost pověřence(?),
  - případně existenci povinnosti vést záznamy o činnostech zpracování (nad 250 zaměstnanců).

- **Nutno pamatovat na zvláštní povinnosti dle GDPR**
  - existence právního titulu (u údajů nad rámec plnění zák. povinností),
  - stanovení účelu a princip minimalizace osobních údajů.

- **Zpracování biometrických osobních údajů**
  - praktické zejména v oblasti autentizace zaměstnance/uživatele.

- **Požadavky na zabezpečení informačních systémů**
  - princip technologické neutrality, ale…

Ochrana osobních údajů II.
(zákaz automatizovaného rozhodování)

ÚSTAV STÁTU A PRÁVA

- **Omezení vyplývající z čl. 22 GDPR pro případy automatizovaného rozhodování**
  - „Subjekt údajů má právo **nebýt předmětem** žádného **rozhodnutí** založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho **právní účinky** nebo se ho obdobným způsobem **významně dotýká**."
  - jde o všeobecný zákaz, nevyžadující aktivitu člověka,
  - Výsledkem aut. rozhodnutí však může být doporučení, které přezkoumá člověk (nikoliv formálně či rutinně) s kompetencí aut. rozhodnutí změnit či upravit

- **Adaptační legislativa (§ 11 zák. č. 110/2019)**
  - na základě subsidiární výjimky lze „odložit" v nezbytném rozsahu

- **Výjimky**
  - uzavření nebo plnění smlouvy,
  - právo EU nebo členského státu a vhodná opatření,
  - souhlas.

Ochrana osobních údajů III. (povinnost zabezpečení údajů)

ÚSTAV STÁTU A PRÁVA

- **Povinnost zabezpečení údajů (čl. 32, vy. 74 - 77)**
  - ochrana před **ztrátou, zničením, neoprávněným přístupem, pozměněním, nedostupností**
  - přijetí vhodných technických a organizačních opatření **podle míry rizika pro subjekt, stavu techniky, nákladů na provedení, účelu zpracování**, apod.

- **Opatření:**
  - technická - šifrování, pseudonymizace, hesla a jejich obměna, zálohování, antivirový program
  - organizační - školení, vnitřní předpisy
- **Porušení zabezpečení a rizika pro subjekt:**
  - hlášení porušení zabezpečení ÚOOÚ, případně subjektům
  - do 72 hodin poté, co se správce dozvěděl

Využívání systémů umělé Inteligence dle AI Aktu

ÚSTAV STÁTU A PRÁVA

- Počátky regulace AI na EU úrovni: 2016
- Návrh EK: 21. 4. 2021 | Rev. EP: 14. 6. 2023 | Podpis: 13. 6. 2024
- Publikace: 12. 7. 2024
- Vstup v platnost: **1. 8. 2024**
- Použitelnost: obecně od 2. 8. 2026
  - 2. 2. 2025 - obecná ustanovení, zakázané postupy
  - 2. 8. 2025 - oznamující orgány a oznámené subjekty, obecné modely AI, správa, zachovávání důvěrnosti, sankce a jejich stanovení
  - 2. 8. 2027 - specifické vysoce rizikové systémy dle přílohy I.

Proč máme v EU regulaci AI?

ÚSTAV STÁTU A PRÁVA

- AI může zasáhnout do základních práv člověka;
  - biais,
  - feedback loop,
  - confirmation biais…
- některá užití umělé inteligence nechceme (vojenské užití!)
- pravidla musí být jednotná v celé EU
- podpora inovací v EU

Působnost AI aktu

ÚSTAV STÁTU A PRÁVA

AIA se vztahuje na:

- **poskytovatele**, kteří systémy AI **uvádějí na trh nebo do provozu** v EU
- **subjekty**, které zavádějí systémy AI a jsou usazeny nebo se nacházejí v EU
- **poskytovatele a subjekty** mimo EU, pokud se **výstup používá v EU**
- **výrobce produktů**, kteří uvádějí na trh nebo do provozu systém AI společně se svým produktem a pod svým jménem nebo ochrannou známkou
- **dotčené osoby**, které se nacházejí v EU

AIA se n**evztahuje** na:

- na oblasti **mimo oblast působnosti práva EU**
- **vojenské, obranné účely**
- systémy, vč. výstupů, které byly speciálně vyvinuty a uvedeny do provozu **výhradně za účelem vědeckého výzkumu a vývoje**
- **neprofesionální užití**
- systémy **zpřístupněné na základě bezplatných licencí s otevřeným zdrojovým kódem** kromě zakázaných systémů a systémů s omezeným rizikem

Výjimky z AI Aktu

ÚSTAV STÁTU A PRÁVA

- **Působnost:** poskytovatelé, zavádějící subjekty (efekt v EU), dovozci a distributoři, výrobci produktů, zplnomocnění zástupci, dotčené osoby

- **Výjimky z působnosti:**
  - Národní bezpečnost, vojenské a obranné účely
  - Mezinárodní spolupráce v oblasti justice a vymáhání práva
  - AI výhradně pro účely vědeckého výzkumu a vývoje
  - Žádné činnosti výzkumu, testování či vývoje AI před uvedením na trh nebo do provozu; vyjma testování v reálných podmínkách
  - FO používající AI v rámci čistě osobní neprofesionální činnosti
  - AI zpřístupněné na základě svobodných licencí a licencí s otevřeným zdrojovým kódem (s výjimkou vysoce rizikových AI, zakázaných AI nebo AI s požadavky na transparentnost)

AI Akt a jeho vztah k ochraně osobních údajů

ÚSTAV STÁTU A PRÁVA

- Rec. 10 & čl. 2 odst. 7
  - Na osobní údaje zpracovávané v souvislosti s právy a povinnostmi stanovenými v tomto nařízení se vztahuje právo Unie o ochraně osobních údajů, soukromí a důvěrnosti sdělení. Tímto nařízením nejsou dotčena nařízení (EU) 2016/679 nebo (EU) 2018/1725 ani směrnice 2002/58/ES nebo (EU) 2016/680.

- Čl. 10 odst. 5: **možnost zpracování zvláštních kategorií OÚ, pokud je to nezbytně nutné pro zajištění detekce a oprav zkreslení ve vztahu k vysoce rizikovým systémům AI**

- Čl. 59: Další zpracování osobních údajů pro účely vývoje určitých systémů AI ve veřejném zájmu v rámci regulačního sandboxu pro AI

Nový titul pro zpracování zvláštních kat. OÚ

ÚSTAV STÁTU A PRÁVA

- Možnost zpracování zvláštních kategorií OÚ, pokud je to nezbytně nutné **pro zajištění detekce a oprav zkreslení ve vztahu** k vysoce rizikovým systémům AI

- Zajištění vhodných záruk, splnění podmínek legislativy na ochranu OÚ a při kumulativním **splnění všech dalších podmínek**:
  - Nelze provést pomocí anonymizovaných, syntetických nebo jiných údajů
  - Přísné požadavky na ochranu dat a omezení přístupu
  - Odůvodnění nutnosti

- Použití na testovací data u vysoce rizikových systémů, kt. netrénují modely

Kategorie systémů umělé inteligence dle AIA

ÚSTAV STÁTU A PRÁVA

1. **Systémy s neakceptovatelným rizikem** (zakázané systémy)

2. **Systémy s vysokým rizikem**
   - Riziko pro bezpečnost a zdraví
   - Riziko pro základní práva člověka

3. **Systémy s omezeným rizikem**
   - Systémy komunikující s lidmi
   - Systémy manipulující s textem, audio, video, deep-fake

- **Redakční systémy**

- **Ostatní systémy**

1. Systémy s neakceptovatelným rizikem
Zakázané systémy (čl. 5)

ÚSTAV STÁTU A PRÁVA

- Systémy, které využívají **podprahové**, **manipulativní, klamavé techniky**
- Systémy, které využívají **zranitelnost**
- Systémy biometrické kategorizace, které mohou **dovodit rasu, sexuální orientaci, politické názory, apod.**
- ***Social-scoring***, které by mělo způsobit nepříznivé jednání s osobou nebo skupinou osob
- Systémy pro vzdálenou **biometrickou identifikaci** v reálném čase kromě výjimek
- ***Predictive policing*** kromě podpory lidského rozhodování
- Systémy pro vytváření databáze pro **rozpoznávání obličejů** za pomocí stahování fotek z internetu nebo CCTV

- Systémy pro **rozpoznávání emocí na pracovišti** a ve vzdělávacích zařízeních

2. Systémy s vysokým rizikem (čl. 6)

ÚSTAV STÁTU A PRÁVA

- **První kategorie**: AI systém je určen pro užití v rámci **bezpečnostní součástí výrobku**, nebo je přímo výrobkem na který se vztahují předpisy uvedené v příloze I, a tento výrobek prochází posouzením shody s cílem uvedení na trh.
  - **Strojní zařízení, hračky, výtahy, zdravotnické prostředky, apod**.

- **Druhá kategorie**: AI systémy uvedené v příloze III (možno měnit aktem v přenesené působnosti)
  - **Systémy biometrické identifikace na dálku**, některé systémy biometrické kategorizace, **kritická infrastruktura**, systémy používané ve **vzdělávání**, systémy používané v pracovněprávních vztazích a při náboru zaměstnanců, **systémy hodnotící nárok na dávky**, **úvěruschopnost**, míru rizika u životního a zdravotního pojištění, apod.

Systémy s omezeným rizikem (čl. 50)

ÚSTAV STÁTU A PRÁVA

- Víceúčelové AI systémy, včetně generativních modelů jako je CHATGPT, apod.
- Systémy rozpoznávání emocí a biometrické kategorizace
- Systémy, které generují deep-fake
- Systémy, které generují nebo manipulují textem pro účely informování veřejnosti o věcech veřejného zájmu

Povinnosti při používání generativní AI

ÚSTAV STÁTU A PRÁVA

- Informace o **komunikaci** s AI
- Informace o **výstupu** utvořeného AI, ne u SW pro standardní editaci (photoshop)
- Informace o **deep-fake**
- Informace o **použití AI u textu**, jenž je zveřejněn za účelem informování veřejnosti o záležitostech veřejného zájmu, nebo který s takovým textem manipuluje
  - Nevztahuje se na texty s redakční kontrolou a odpovědností konkrétní osoby

Povinnosti poskytovatelů vysoce rizikových systémů

ÚSTAV STÁTU A PRÁVA

- Vypracovat **systém řízení rizik** (čl. 9)
  - Rozumně předvídatelné riziko pro zdraví, bezpečnost (*safety*) a základní práva za předpokladu, že se systém používá k zamýšlenému účelu
  - Monitorování zbytkového rizika

- Požadavky **na data** (čl. 10)
  - Datasety pro trénování, validaci, testování AI systémů
  - Bezchybnost a úplnost, reprezentativnost

- Vedení **dokumentace** (čl. 11)

- Zaznamenávání událostí, dohledatelnost *(traceability*) (čl. 12)

- Transparentnost a informování uživatelů (čl. 13)

- Lidský dohled (čl. 14)
- Kyberbezpečnost (čl. 15)
- Certifikace (čl. 43)

Využívání velkých jazykových modelů (problémy)

ÚSTAV STÁTU A PRÁVA

Problémy s ChatGPT:

- Získávání osobních údajů **bez souhlasu** a vědomí subjektů údajů
- **Absence záruk** a nástrojů pro uživatele
- Problematický (nemožný) **výkon práva na zapomenutí**
- **Extenzivní sběr dat** o chování uživatelů
- Sdílení informací se třetími stranami
- Nedodržování principů ochrany osobních údajů (mj. přesnost údajů)
- **Produkce chybných** osobních údajů
- Náhodné zveřejnění údajů získaných ze soukromých dokumentů jiných uživatelů

Využívání velkých jazykových modelů (nebezpečí)

ÚSTAV STÁTU A PRÁVA

Možná nebezpečí:

- Obejití ochranných prvků (např. pokyn **DAN** - "do anything now")
- **Manipulace** jednotlivcem (případ sebevraždy v Belgii)
- Přístup k **citlivým** dokumentům
- **Diskriminační** obsah
- **Odposlouchávání**
- **Prozrazení** hesel
- Zjišťování nových informací o uživatelích, včetně biometrických údajů
- ... nové způsoby narušení soukromí

ÚSTAV STÁTU A PRÁVA

III. Význam podpisu v právním řádu

Obecný význam podpisu v právním řádu

ÚSTAV STÁTU A PRÁVA

Podpis v soukromém právu

- **V soukromoprávních vztazích je podpis jednající osoby předpokladem platnosti písemných právních úkonů** (§ 561 občanského zákoníku).

Podpis ve veřejném právu

- Ve vztazích veřejnoprávních jde rovněž zpravidla o **nezbytnou náležitost řádného podání.**

- **Je třeba rozlišovat** režim v oblastech veřejného (e-government – vertikální vztah) i soukromého práva (smlouvy, e-commerce – horizontální vztah). Hezký je to vidět v oblasti ISDS (§16 - §18a), případně v katastrálních předpisech (cert. MPSV, apod.)
- *Pozor na notářské, úřední či jiné ověření listiny (legalizace, vidimizace), jež má rovněž veřejnoprávní podstatu.*
- *Klíčovým pojmem je listina…*

Obecný význam podpisu v právním řádu (pojem listina)

ÚSTAV STÁTU A PRÁVA

Co je to listina?

- Legální definice listiny v právu chybí. Nejde však o vytýkatelný nedostatek současné právní úpravy a „teoretické spory kolem listiny tak nemají patrně praktického významu“.

Co je to podpis?

- Podobně jako pojem „listina“, není v právním řádu definován ani pojem podpis (vyjma elektronického). V tomto ohledu tak nemusí být vždy zřejmé, jak úplný podpis je z hlediska práva ještě dostatečný a jaký již nikoliv.

- Podpis však vždy (tradičně) plnit určitou identifikační funkci…

Absence jasných definic by však v praxi neměla činit potíže.
Důležité je však se zabývat náležitostmi konkrétního právního jednání…

ÚSTAV STÁTU A PRÁVA

IV. Forma a náležitosti písemného právního jednání

Písemné právní jednání (§ 561 ObčZ)

ÚSTAV STÁTU A PRÁVA

- § 559 Každý má právo zvolit si pro právní jednání **libovolnou** formu, není-li ve volbě formy omezen ujednáním nebo zákonem.
  - písemná
  - ústní
  - „konkludentní“

- § 560 **Písemnou formu vyžaduje právní jednání, kterým se zřizuje nebo převádí věcné právo k nemovité věci**, jakož i právní jednání, kterým se takové právo mění nebo ruší.
  - požadavek na písemnou formu tak nutno chápat jako určité “varování“,

Písemné právní jednání (§ 561 ObčZ)

ÚSTAV STÁTU A PRÁVA

- § 562/1 **Písemná forma je zachována** i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu a určení jednající osoby"

- Obsah **emailové zprávy**:
- - „Ahoj, vím, že ti to dlužím, Tomáš"
- Obsah **SMS zprávy**:
- „daruji ti svůj dům, otec", „rozvádím se", „máte výpověď"

§ 562 odst. 1 je **zvláštní úpravou platné písemnosti bez podpisu** vůči obecné úpravě písemnosti s podpisem v § 561 odst. 1 věty 1 a 3", tj. postačí určení (nikoli ověření) jednající osoby", i pouhé jméno a příjmení v e-mailu

ÚSTAV STÁTU A PRÁVA

V. Druhy podpisu v právu (obecně)

Druhy podpisu a jejich případná komparace (obecně)

ÚSTAV STÁTU A PRÁVA

Podpis

- Jde o nejméně bezpečnou variantu *(postačuje řetězec znaků)*

Vlastnoruční podpis *(autogram)*

- Jde relativně bezpečnou variantu (písmo-znalecký posudek)

Ověřený podpis *(ať již soudně, notářsky nebo úředně)*

- Tradičně považováno za nejbezpečnější variantu (veřejnoprávní povaha)

Elektronický podpis *(včetně jeho vyšších forem – viz eIDAS)*

- Jeho bezpečnost zde zcela závisí na použití konkrétního druhu (viz. jednotlivé druhy)

Další hybridní druhy podpisu

- Např. dle kvality a povahy autentizace - prostřednictvím behaviorální biometrických znaků člověka (např. dynamiky záznamu řeči, chůze, psaní na klávesnici, apod.).

ÚSTAV STÁTU A PRÁVA

VI. Úprava elektronického podepisování dle eIDAS a českého práva

Prameny el. podepisování v ČR

ÚSTAV STÁTU A PRÁVA

- Zákon č. 227/2000 Sb., **o elektronickém podpisu (ZoEP)** byl ke dni 19. 9. 2016 zrušen a nahrazen

- zákonem č. 297/2016 Sb. **o službách vytvářejících důvěru pro elektronické transakce (**ZoSVD**)**, čímž zákonodárce reagoval na

- nařízení EP a Rady (EU) č. 910/2014 ze dne 23. července 2014 o **elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (eIDAS)**

ZoSVD upravuje:
- některé **postupy** poskytovatelů služeb vytvářejících důvěru,
- některé **požadavky** na služby vytvářející důvěru,
- působnost Ministerstva vnitra oblasti služeb vytvářejících důvěru a
- sankce za porušení povinností v oblasti služeb vytvářejících důvěru.

Nařízení eIDAS má aplikační přednost a **upravuje:**
- vzájemné uznávání v EU, služby vytvářející důvěru
- elektronický podpis, elektronická pečeť
- elektronická časová značka, el. doručování, apod.

Druhy el. podpisu (obecně)

ÚSTAV STÁTU A PRÁVA

"Nařízení **eIDAS** rozlišuje několik základních druhů elektronických podpisů

- **elektronický podpis,**
- **zaručený elektronický podpis,**
- **zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis**
- **kvalifikovaný elektronický podpis.**

- **uznávaný elektronický podpis** (specifikum české úpravy)
  - zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo
  - kvalifikovaný elektronický podpis.

Druhy podpisu 1/4
(prostý elektronický podpis)

ÚSTAV STÁTU A PRÁVA

Prostý elektronický podpis (čl. 3 eIDAS)
- data v elektronické podobě, která
- jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena a která
- podepisující **osoba používá k podepsání**.

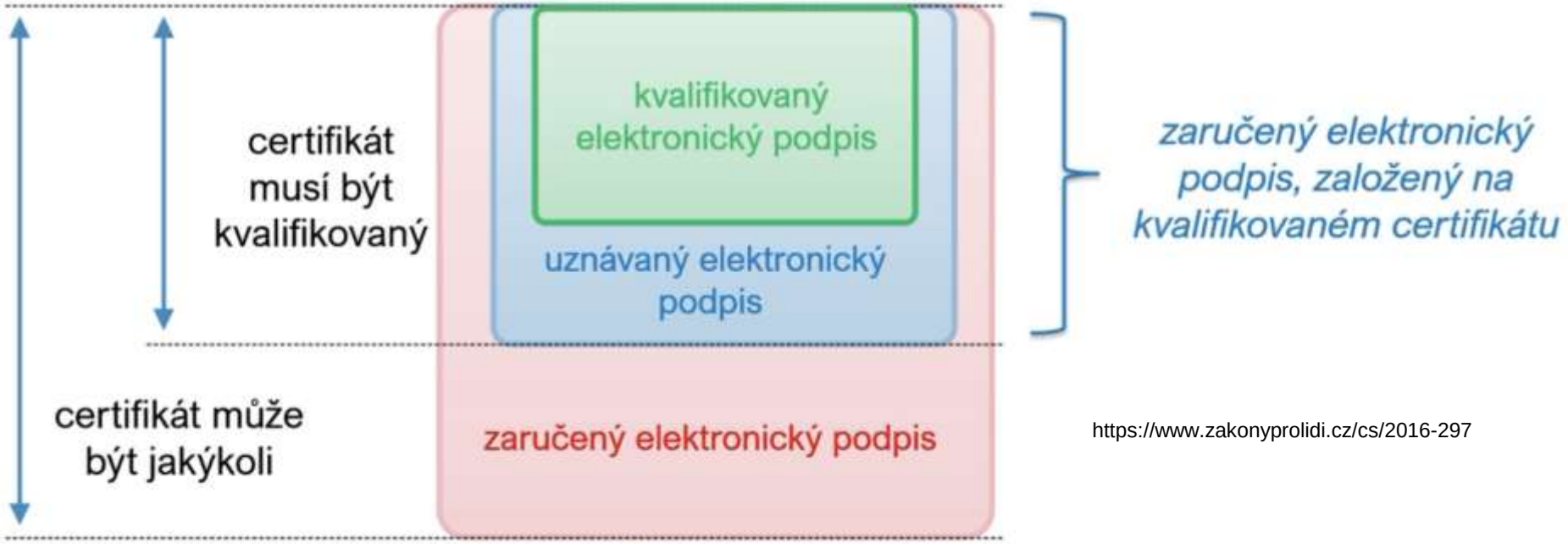
Předchozí (neplatná) úprava (§ 2 zákona č. 227/2000 Sb.) považovala za (prostý) elektronický podpis pouze:
- údaje v elektronické podobě,
- které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které
- slouží jako **metoda k jednoznačnému ověření** identity podepsané osoby ve vztahu k datové zprávě.

Existuje zde nějaký faktická změna:
- možnosti podepsat (obligatorní) písemné právní jednání dle OZ?
- sms, email, ale i např. elektronický záznam ústní komunikace...

Druhy podpisu 2/4
(zaručený elektronický podpis)

ÚSTAV STÁTU A PRÁVA

Nařízení eIDAS stanoví (čl. 26), že **zaručený elektronický podpis** musí splňovat:
a) je **jednoznačně spojen** s podepisující osobou;
b) **umožňuje identifikaci** podepisující osoby;
c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může **s vysokou úrovní důvěry použít pod svou výhradní kontrolou**; a
d) je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že **je možné zjistit jakoukoliv následnou změnu dat**.



https://www.zakonyprolidi.cz/cs/2016-297

Druhy podpisu 3/4
(zaručený elektronický podpis založený na kvalifikovaném certifikátu)

ÚSTAV STÁTU A PRÁVA

Nařízení eIDAS stanoví (čl. 3), že **zaručený elektronický podpis založený na kvalifikovaném certifikátu**:

• Musí jít o **zaručený elektronický podpis** (čl. 26), tj.
- je jednoznačně spojen s podepisující osobou;
- umožňuje identifikaci podepisující osoby;
- je vytvořen pomocí dat pro vytváření elektronických podpisů, která
- podepisující osoba může s vysokou úrovní důvěry použít pod svou
- výhradní kontrolou; a
- je k datům, která jsou tímto podpisem podepsána, připojen takovým
- způsobem, že je možné zjistit jakoukoliv následnou změnu dat.

• Musí být **založen na kvalifikovaném certifikátu**, který vydává důvěryhodný (kvalifikovaný) poskytovatel těchto služeb a musí obsahovat určité specifické informace, jako je identita podepisující osoby a informace o certifikační autoritě.

- Zaručený elektronický podpis splňující výše uvedené požadavky má stejnou právní hodnotu jako vlastnoruční podpis v rámci všech členských států EU. Kvalifikovaný elektronický podpis (nejvyšší úroveň) má přitom výhodu v tom, že má automaticky plnou právní závaznost a nemusí být dodatečně dokazován.

Druhy podpisu 4/4
(kvalifikovaný elektronický podpis)

ÚSTAV STÁTU A PRÁVA

Nařízení eIDAS stanoví (čl. 2), že **kvalifikovaný elektronický podpis** je vymezen jako:

- zaručený elektronický podpis (čl. 26), který
- je vytvořen **kvalifikovaným prostředkem** pro vytváření elektronických podpisů a který
- je založen na **kvalifikovaném certifikátu** pro elektronické podpisy.

- **Kvalifikovaným prostředkem** pro vytváření elektronických podpisů prostředek pro vytváření elektronických podpisů, který splňuje stanovené požadavky stanovené (USB token, chip, apod.);
- **Kvalifikovaným certifikátem** pro elektronický podpis je certifikát pro elektronický podpis, který je vydán kvalifikovaným poskytovatelem služeb vytvářejících důvěru a splňuje stanovené;
- **Kvalifikovaným poskytovatelem služeb vytvářejících důvěru** je poskytovatel služeb vytvářejících důvěru, který poskytuje jednu či více kvalifikovaných služeb vytvářejících důvěru a kterému orgán dohledu udělil status kvalifikovaného poskytovatele.

Druhy podpisu
(uznávaný elektronický podpis)

ÚSTAV STÁTU A PRÁVA

Dle § 6 odst. 2 ZoSVD se rozumí **uznávaným elektronickým podpisem** zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis **nebo** kvalifikovaný elektronický podpis.

- česká specialita (a podivnost);
- pojem uznávaný el. podpis **implikuje dva různé druhy el. podpisu**;
- není **to intuitivní konstrukce**, způsobuje problémy v praxi (praxe uznává jen zaručený el. podpis založený na kval. certifikátu
- princip matrjošky (ZP je obsažen v ZEP, ten pak ZEPsQC a ten zase v QEP)
- zmínka o něm je zbytečná, zákon měl normovat jen o ZEPsQC;
- v principu jde o podpis, kdy se lze důvěryhodně spoléhat na to, že patří tomu, kdo je uveden v kval. Certifikátu

- Stricto sensu **nejde o druh podpisu**, ale o zastřešující pojem pro dva jiné druhy podpisu

- **Kde má smysl a význam používat QEP?**

Právní účinky el. podpisu

ÚSTAV STÁTU A PRÁVA

- **Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.**

- **Kvalifikovaný elektronický podpis** má právní účinek rovnocenný vlastnoručnímu podpisu.

- Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě **se uznává** jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.

- **V platné právní úpravě chybí ekvivalent ověřeného podpisu pro el. podpisu**, tj. není možné provést legalizaci v el. světě, existují výjimky (ISDS, insolvenční zákona)

Specifika české úpravy: Podepisování dle ZoSVD (§ 5 – § 6)

ÚSTAV STÁTU A PRÁVA

Podepisování dokumentu

§ 5

K podepisování elektronickým podpisem **lze použít pouze** kvalifikovaný elektronický podpis, podepisuje-li elektronický dokument, kterým

a) činí úkon nebo právně jedná **stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem nebo jejich orgán anebo jiná jejich součás**t (dále jen „**veřejnoprávní podepisující**“), nebo

b) činí úkon osoba **neuvedená** v písmenu a) **při výkonu své působnosti**.

§ 6

(1) K podepisování elektronickým podpisem **lze použít pouze** uznávaný elektronický podpis, podepisuje-li se elektronický dokument, kterým se činí úkon vůči veřejnoprávnímu podepisujícímu nebo jiné osobě **v souvislosti s výkonem jejich působnosti.**

(2) **Uznávaným elektronickým podpisem** se rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis.

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

Pečetění dle ZoSVD (§ 8 - § 10)

ÚSTAV STÁTU A PRÁVA

- Může vytvářet **jen právnická osoba** (pečetící osoba) a lze ji připojit **jen na to, čeho je sama původcem**. Nejde o projev vůle, ale deklarací původu!

- Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, **veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí**.
- K pečetění elektronickou pečetí lze použít **pouze uznávanou elektronickou pečeť**, pečetí-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti. Uznávanou elektronickou pečetí se rozumí zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť.

V ostatních případech lze k pečetění použít
- zaručenou elektronickou pečeť,
- uznávanou elektronickou pečeť, případně jiný typ elektronické pečeti, pečetí-li se elektronický dokument, kterým se právně jedná

- **Co když se osoba podepíše el. pečetí?**

ÚSTAV STÁTU A PRÁVA

VII. Dokazování, důkazní spolehlivost elektronické písemnosti, aj.

Dokazování - právní prokazatelnost a odpovědnostní aspekty

ÚSTAV STÁTU A PRÁVA

Soukromé právo

- za důkaz sloužit **všechny prostředky, jimiž lze zjistit stav věci**, zejména výslech svědků, znalecký posudek, zprávy a vyjádření orgánů, fyzických a právnických osob, notářské zápisy a jiné listiny, ohledání a výslech účastníků. *(§ 125 občanského soudního řádu)*

Veřejné právo

- za důkaz v trestním řízení může sloužit **vše, co může přispět k objasnění věci**, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání (§ 89 odst. 2 trestního řádu).

Důkazní prostředky

- důkaz el. podpisem zpravidla neleží ve vzduchoprázdnu,
- Lze kombinovat s celou řadou dalších doprovodných (nepřímých důkazů), např.
  - záznam dat dle data retention (zákon o el. komunikacích)
  - znalecké posudky (lingvistiko matematická analýza textu, apod.)

Srovnání vlastnoručního a kvalifikovaného podpisu

ÚSTAV STÁTU A PRÁVA

- Na rozdíl od problematiky elektronického podepisování je u podepisování vlastní rukou řada praktických zkušeností ve všech sférách života člověka

- Vlastnoruční podpis je výsledkem **individuálního a relativně stálého písemného projevu člověk**a. Z těchto poznatků vychází např. grafologie. Posudkem soudního znalce v oboru písmoznalectví pak lze určit pravost vlastnoručního podpisu.

Existují však problémy:

- Písmoznalecké expertízy nebývají příliš jednoznačné
- Pro určení pravosti podpisu nepostačuje méně než 10 nesporně pravých podpisů
- Osoba je individuálně identifikovatelná až od 13 let věku

Srovnání vlastnoručního a kvalifikovaného podpisu

ÚSTAV STÁTU A PRÁVA

- Často dochází k záměně písmoznalectví za grafologii.
- Písmoznalectví je jedním ze znaleckých oborů, který umožňuje individuální identifikaci pisatele. Předmětem zkoumání jsou jak sporné podpisy, tak celé písemné projevy (např. závět).
- Grafologie je obor (?)psychologie, zabývající se studiem písma a jeho vztahu k lidskému chování. Z empirického pohledu jde o velmi hypotetický obor.
- Mezi písmoznalectvím a grafologií těmito dvěma obory je však značný rozdíl, písmoznalectví zjišťuje, kdo (tj. jaká osoba) co napsala, zatímco grafologie se zajímá o to, jaký je ten, kdo něco napsal. Grafologie se někdy též nazývá „psychologie písma“.

Zneužití podpisu

ÚSTAV STÁTU A PRÁVA

Útočník/podvodník	Stručný popis útoku / pokusu o podvod	EP	P
A	tvrdí, že se nepodepsal	!	*
A A	tvrdí, že text byl zaměněn A zneplatní klíč u PCS a provede transakci, dříve než PCS vydá CRL, A pak odmítne odpovědnost za škodu	!	*
A	tvrdí, že dokument, který podepsal dříve, vznikl až po zneplatnění DVEP , A se chce se zbavit odpovědnosti		
B B	tvrdí, že je podepsán A zamění část podepsaného textu	! !	* *
B	získá DVEP A po zneplatnění certifikátu, podepíše se za A a tvrdí, že dokument vznikl před zneplatněním		
A,B (domluví se)	A zneplatní klíč, než PCS vytvoří CRL , B provede transakci, škodu chce nahradit od PCS		
X	podepíše se za A	! 4	*
X	zamění text	!	*
X	získá DVEP a dále se může vydávat a podepisovat za A !!!		
X	Získá DVEP A po zneplatnění certifikátu, podepíše se za A a tvrdí, že dokument vznikl před zneplatněním (chce poškodit A)		
X	zneplatní u PCS certifikát A (poškodí A)		
X	X zachytí podepsanou zprávu (bez časového údaje), X ji odešle B znovu (cíl poškodit původního odesílatele nebo i příjemce)		
X X (má k dispozici PCSX)	Získá u PCS certifikát za někoho jiného zamění certifikát PCS za PCSX u B a tím si umožní vydávat se za A (zasláním certifikátu, který si X vydal za A a podepsal jako PCSX) - dočasný útok	3	
X	získá osobní data zákazníků PCS		
PCS PCS	zneplatní bezdůvodně certifikát A a tím jej poškodí vytvoří certifikát pro neexistující osobu		
PCS	vytvoří z dat v certifikátu A certifikát pro C (C i A mohou být poškozeny, B se totiž domnívá, že komunikuje s C nikoliv s A)		
PCS	při generaci klíčů pro A si PCS ponechá jeho DVEP		
PCS	úmyslně neuvede zneplatněný certifikát v CRL		
PCS	zneužije osobní data svých zákazníků		

Odpovědnostní důsledky zneužití podpisu

- ***platnost, resp. zdánlivost právního jednání***
- ***Přestupek***
- ***zločin, přečin, atd.***

Diskuse

Děkuji za pozornost

ÚSTAV STÁTU A PRÁVA

matejka@ilaw.cas.cz

Technická hlediska zabezpečení a průkaznosti digitálních dokumentů

rizika zneužití a možná preventivní opatření

Mgr. Jaromír Kuba

Digitalizace v pracovním právu II

Rekapitulace

- Elektronický podpis
  - Certifikáty
    - Certifikáty, privátní klíče, úložiště
    - Elektronické pečeti a časová razítka
  - Dynamický biometrický podpis
  - Prostý elektronický podpis
- Dlouhodobé uchovávání dokumentů
  - Digitální kontinuita
  - Formáty
  - Platnost podpisů, pečetí a časových razítek
  - Konverze dokumentů
- Nástroje

Navázání na předešlý workshop

- Dynamický biometrický podpis (docházka)

  Holandský dozorový úřad: Ověření 1:1 a 1:N z pohledu GDPR velmi podobné.

  Rozpoznávání obličejů Odpovědi na otázky týkající se zpracování osobních údajů při používání rozpoznávání obličeje (https://www.autoriteitpersoonsgegevens.nl/uploads/2024-05/Juridisch%20kader%20gezichtsherkenning.pdf)

- Ai Act

  Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení … (akt o umělé inteligenci)

  Identifikace: „automatizované rozpoznání…“

  Ověření (včetně autentizace): „účelem je potvrdit…“

  Hodně nových pojmů (AI Act je založený na riziku, zasahuje i do pracovní oblasti)

- Největší rizika souvisí s podvržením a zpochybněním digitálního dokumentu

  Často pomohou IT forenzní postupy (dále lehký úvod).

Doručování dokumentů

- Problém s „poslední mílí“

  Z logů našeho mail serveru vidíme jen, že mail server adresáta mail přijal

  Standardní potvrzení o doručení garantuje pouze doručení na server, ne do konkrétní schránky (antivir, antispam, zahození e-mailu z různých důvodů, přeposílání, …)

- Možná řešení

  Potvrzení o přečtení (nespolehlivé)

  Tracking pixely

  Odkazy místo příloh

  Portály pro zaměstnance (intranet atd.)

  Datové schránky

- Průkaznost doručených e-mailů

  Možno zvýšit skrz DKIM a další technologie, určené pro boj s nevyžádanou poštou.

  Elektronický podpis (kvalifikovaný) má spoustu výhod.

DKIM podpis v e-mailu

- Může pomoci v důkazní nouzi
- DKIM

  Jednoduchá forma elektronického podpisu

  Elektronicky podepisuje poštovní server odesílatele

  Cílem boj proti spamu

  Veřejný klíč dostupný (zveřejněn jako DNS záznam u domény)

- DKIM může zvýšit důkazní hodnotu e-mailu

  Pokud nám protistrana pošle e-mail, jehož obsah by později rozporovala, lze s rozumnou mírou jistoty její tvrzení napadat.

  Pomocí DKIM podpisu lze autenticitu mailu ověřit později. Platnost klíčů není technicky omezena!

  Běžný uživatel nemá přístup k privátnímu DKIM klíči velkých provozovatelů systémů pro elektronické odesílání e-mailů.

DKIM podpis v e-mailu

- DKIM záznam v DNS

  v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBC…….;

  Nutné porovnat hlavičku, co je do podpisu zahrnuto (h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;)

  Pozor na **„l=0“**! (v tomto případě je vyjmuto tělo zprávy z DKIM podpisu!

  Šikovný ajťák ověří, případně znalec

  Po úspěšném ověření e-mailu vhodné DKIM záznam z DNS stáhnout a uložit a (a uložení doložit)

  Např. programy Mailauth a Dkimverify (verze v Rustu) umí ověřit signatury dříve uložené v souboru

- Falešně negativní výsledek

  Stačí, aby poštovní systém upravil tělo zprávy. Stává se to, ačkoliv by nemělo.

SPF, DMARC, ARC

- ARC přidá mezi hlavičky v e-mailu informaci o tom, zda a s jakým výsledkem server někde „na cestě“ provedl ověření e-mailu. Podepsáno podobně jako DKIM (hlavička *ARC-Seal*).

  ARC-Authentication-Results obsahuje informace o dřívějším ověření DKIM a SPF.

- V SPF záznamu lze v řadě případů dohledat informace o poštovních serverech, přes které organizace odesílá poštu (lze namítat „my přes poštovní server, přes který Vám údajný mail od nás přišel, maily nikdy neodesíláme“).
- DMARC může rovněž napovědět, jak dopadl test SPF a DKIM během cesty e-mailu.
- Nejhůře verifikovatelný je e-mail z odeslané pošty. Minimum informací.

  U důležitých mailů přidávejte sebe sama do skryté kopie (BCC), případně mail rovnou elektronicky podepište (pomůže nějaká „sběrná schránka“).

- SPF může odkrýt skutečné IP adresy!

  Pokud jsou servery skryty např. za CDN, v SPF jsou v celé řadě případů viditelné skutečné IP adresy serverů.

Tracking pixel v e-mailu

- Obrázek většinou o velikosti 1x1 pixel, jehož URL je unikátní pro každého příjemce e-mailu.

  Není-li blokováno načítání obrázků, lze zjistit, že protistrana mail otevřela.

- Pozor na GDPR

  Dle EDPB podobné, jako analytické cookies – třeba získat souhlas!

  Informace o zpracování osobních údajů

- Průkaznost?

  „My skrz náhled do systému, který je náš a který máme ve správně tvrdíme, že jste e-mail otevře dne….“?

  Jsou logy nějak chráněné proti manipulaci???

Blockchain

- Moderní slovo, ale reálně databáze, která není jen na jednom místě.
- Jednotlivé záznamy na sebe vzájemně navazují způsobem, kdy zásahy do dřívějších záznamů jsou snadno detekovatelné.
- Decentralizace, odolnost (registr pracovních dokumentů?)
- Chytré kontrakty – „programy“ (automatizace smluvních procesů)
- Výzvy v oblasti GDPR
  - Problém minimálně v oblasti práva na výmaz
  - Zásada minimalizace – mazání již nepotřebných dat
- European Blockchain Regulatory Sandbox
  - Součástí i dozorové úřady.
  - Řada zajímavých projektů, např. decentralizovaná platforma pro freelancery.
  - Předzvěst regulatorních sandboxů v AI Actu? (hrozný překlad „regulační sandbox“)

Analýza metadat, anonymizace

- Dokumenty i obrázky obsahují celou řadu dat
  - Datum vytvoření dokumentu, autor, počet změn, kdo dokument naposledy změnil atd.
  - Datumy v souboru jsou rozdílné od data souboru.
  - ExifTool, v případě .docx lze rozbalit podobně jako ZIP a prohlížet v editoru.
- Někdy se vyplatí udělat i analýzu počítače
  - Když jsme v důkazní nouzi
  - Z analýzy může vyplývat, že v době, kdy měl e-mail vzniknout, nebyl počítač vůbec spuštěn atd., případně co z něj odešlo.
- Pozor na anonymizaci začerněním
  - Text musí být před začerněním nahrazen
  - Nové výzvy v oblasti práva na přístup

Právo na přístup

- Může být třeba anonymizovat

  Lze i zdarma (Blender, Audacity)

  AI přináší nové výzvy v oblasti anonymizace (depixelizace dnes možná i u větších kostiček, v případě videa je možné složit z velkých kostek jemnější)

  Již nemusí stači jen rozkostičkování nebo zvýšení frekvence hlasu

eIDAS 2.0, eDoklady

- Revize nařízení eIDAS (Nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024…)
- Evropské peněženky
  - Nejen doklady (potvrzení vzdělání, profesní kvalifikace, zmocnění atd.)
  - Jízdenky atd.
  - Řidičské oprávnění atd.
  - Primárně forma mobilní aplikace
  - Možné využití pro autentizaci a autorizaci
  - Bezplatné využití kvalifikovaného elektronického podpisu pro neprofesionální využití
- Služby, elektronické archivace, potvrzování atributů, elektronické knihy záznamů (zajištění integrity a přesnosti chronologického řazení, centralizovaná i decentralizovaná kniha záznamů).
- eDoklady
  - Jen občanský průkaz
  - Aplikace od DIA
  - Stále ještě omezení využitelnosti
  - Současná verze prověřena

Elektronický podpis

- Nejen certifikáty
- Smluvně ošetřit při nástupu?
- Různé formy kombinace SMS klíčů a aplikací v mobilních telefonech
- Dnes využívají i banky (v bance pozor!)
- Často možné využít stejné řešení pro vícefaktorovou autentizaci i podpis
- Nutné dobře naimplementovat (seznam IP adres lidí, co se podepsali nemá velkou vypovídací hodnotu)

- Bankovní identita

  Elektronické podepisování Bank iD

  Nahraje se PDF dokument, určí umístění podpisu v dokumentu.

  I tento druh podpisu je o dohodě obou stran.

Rizika

- Podvodníci se zlepšují
  - Umělá inteligence je všudypřítomná, od hlasu po video
  - Phishingové e-maily dnes již defakto bez chyb
  - Napodobení elektronického podpisu řešeno v minulém workshopu
  - Podvodná volání s falešným telefonním číslem volajícího
  - Novela ZEK, možná budoucí spolupráce operátorů a bank

- Falešné faktury za domény
  - Malé částky, předpoklad, že oběť zaplatí
  - Snadné zjistit registrátora a kdy byla doména naposledy zaplacena
  - Evergreenem faktury, kde je malým písmem napsáno, že jde vlastně jen o nabídku služby. Nemají problém ani posílat upomínky.

Prevence

- Učit se, učit se, učit se (~~proškolení~~ průběžné proškolování zaměstnanců)
- Pravidelné zálohy, ideálně inkrementální, šifrované a do více lokalit
- Technická řešení pro archivaci e-mailů, evidenční systémy
- Využití elektronického podpisu a šifrování
- Logy v e-mailových serverech
- Využití blockchainu pro ukládání a sledování e-mailů (informací o e-mailech)
- DKIM, SPF, ARC, DMARC
- Různé doplňky pro prohlížeče
- Využití vícefaktorové autentizace, VPN
- Využití umělé inteligence v rámci detekce anomálií

Dokumentace pomáhá

- ISO normy – proč vymýšlet už vymyšlené?

  Využití mezinárodně uznávaných standardů šetří čas a zdroje.

  ISO normy jsou výsledkem kolektivní práce odborníků z celého světa.

  Certifikace podle ISO zvyšuje důvěru klientů a partnerů.

- ISMS

  27001 - základ

  27701 – ochrana osobních údajů

  29100 - Informační technologie – Bezpečnostní techniky – Rámec soukromí

- Směrnice, informační memoranda
  - Nezapomeňte na cookies!

Řešení na klíč

- Pozor na „instantní dokumentaci s mašličkou“

  „Napiš, jak to děláš, dělej to, jak píšeš.“ – dokumentace musí sedět na firmu.

  Opatření mají být přiměřená míře rizik

  Lze se inspirovat nějakou šablonou

- „Ten šanon na tu bezpečnost“ nefunguje!

  Příběh – kontrolovaná osoba nebyla schopná doložit prohlášení o aplikovatelnosti

  Normou se lze i inspirovat, což platí i pro již neplatné normy.

- Neexistují „zázračné nástroje na GDPR / NIS 2 / AI Act / DSA / DORA / ...“

- Vyhněte se konzultantům, podle kterých je u vás všechno špatně.

  Zvláště těm, kteří tvrdí, že dle ISO 27001 musíte nutně implementovat konkrétní technická opatření.

AI Act

- Od 2.2.2025 je zakázáno např. rozpoznávání emocí na pracovišti
- Postupný náběh
  - 2.2.2025 – Zakázané postupy, obecná ustanovení
  - 2.8.2025 – Sankce, obecné modely AI, oznamující orgány, oznámené subjekty
  - 2.8.2026 – Obecně použitelné
  - 2.8.2027 – Vysoce rizikové systémy v příloze I
- Nábor, pracovně-právní vztahy, přidělování úkolů na základě chování,…

  Doporučuji zvážit, řada povinností (vysoké riziko)

Konec

- Diskuze
- Děkuji za pozornost ☺

- Jaromír Kuba
  - kuba@znal.ec
  - 774 487 670