AKTUALITY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Správa (november – december 2025)

Financované Európskou úniou Next Generation EU prostredníctvom
Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-0002.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

ÚVOD

Vážení čitatelia, od vydania poslednej správy ubehli vyše dva mesiace. Za ten čas sa v oblasti kybernetickej bezpečnosti stihlo udiať mnoho. Na týchto stranách sa však dočítate nielen o aktuálnom dianí, ale aj čo to o kľúčových reguláciách vrátane pripravovaných, a rovnako tak si rozoberieme vybrané rozhodnutia súdov. Taktiež budete mať možnosť dozvedieť sa niečo o aktuálnych kurzoch a výskume, ktoré formujú rýchlo sa meniacu oblasť kybernetickej bezpečnosti vrátane ochrany súkromia a kybernetickej kriminality.

ČO JE NOVÉ V OBLASTI KYBERNETICKEJ BEZPEČNOSTI?

Kybernetické útoky

Portál ANY.RUN sa v rámci októbra 2025 venoval kľúčovým kybernetickým útokom. Identifikoval ich viacero, pričom sa podľa neho útoky čoraz viac integrujú do legitímnych cloud služieb a využívajú ich dôveru (Google, ClickUp, Figma). Ako kľúč pre ich odhalenie označuje namiesto statických IOC skôr interaktívnu analýzu (sandboxing) a behaviorálnu detekciu. Nižšie uvádzame identifikované kľúčové útoky:

- *Phishing kampane s využitím dôveryhodných cloud služieb*
  Útočníci stále sofistikovanejšie zneužívajú legitímne platformy (napr. Google Careers, ClickUp) na maskovanie phishingových tokov. Kampane kombinujú viacero presmerovaní cez dôveryhodné služby a Cloudflare Turnstile CAPTCHA, aby prešli tradičnými bezpečnostnými filtrami a ukradli firemné prihlasovacie údaje.

- *Zneužitie Figma na phishing*
  Phishingové útoky teraz často hostujú phishing stránky priamo na figma.com, kde sa obeť presmeruje z e-mailu do „dizajnu", ktorý následne vyzve k zadaniu prihlasovacích údajov, typicky najmä do Microsoft účtu. Tieto kampane obchádzajú URL reputačné filtre, lebo používajú dôveryhodnú doménu.

- *LockBit 5.0 — nová generácia ransomware*
  Rodina LockBit sa vyvinula do verzie 5.0, ktorá už cieli nielen na Windows, ale aj na Linux a VMware ESXi, teda priamo na virtualizované servery a kritickú infraštruktúru. Tento ransomvér obsahuje silnejšiu obfuskáciu a anti-analytické techniky, čo sťažuje detekciu a reakciu.

- *ClickUp ako phishing redirect hostiteľ*
  Útočníci zneužívajú ClickUp dokumenty a stránky ako prvý krok redirect reťazca — potom presmerujú obete cez dôveryhodné služby (napr. Microsoft microdomény, Azure Blob Storage) na phishing login stránky. Takýto reťazec vyzerá legitímne pre používateľov aj bezpečnostné nástroje.

- *TyKit – nový phishing kit*
  Objavil sa nový phishing kit TyKit, ktorý skrýva škodlivý JavaScript v SVG obrázkoch a používa niekoľko krokov (obfuskácia, CAPTCHA) na získanie údajov Microsoft 365 účtov.

Tento kit napádal firmy naprieč regiónmi a odvetviami a je ťažší na detekciu statickými pravidlami.

Za pozornosť tiež stoja útoky, ktoré si všimol denník Guardian. Viaceré miestne orgány v Londýne (Royal Borough of Kensington and Chelsea, Westminster City Council a London Borough of Hammersmith and Fulham), zasiahla vlna vážnych kybernetických útokov. Tie narušili interné IT systémy vrátane telefónnych liniek a online služieb. Mestá okamžite aktivovali plány núdzovej reakcie a business continuity, obmedzili prevádzku viacerých systémov a začali spolupracovať s národnými bezpečnostnými orgánmi, vrátane National Crime Agency (NCA) a National Cyber Security Centre (NCSC), na vyšetrovaní a obnove služieb. Úrady zároveň vyšetrujú, či pri incidente došlo k neoprávnenému prístupu alebo úniku údajov, a poskytujú obyvateľom informácie o možných dopadoch na ich dáta. Incident ovplyvnil služby, ktoré denne využíva viac než pol milióna obyvateľov Londýna. Presné detaily o technike útoku či motíve útočníkov však nebol zverejnený.

Ochrana súkromia

Európske centrum pre digitálne práva NOYB oznámilo, že podalo trestné oznámenie voči americkej firme Clearview AI a jej vedeniu, obviňujúc ju z nelegálneho zhromažďovania fotografií a videí obyvateľov Európskej únie na vytvorenie databázy pre technológiu rozpoznávania tvárí, čo sú podľa noyb vážne porušenia GDPR.

Cybersecuritynews si všimli rozsiahly únik údajov spoločnosti Mercedes-Benz USA. Aktér známy pod prezývkou „zestix" ktorý sa prihlásil k zodpovednosti tvrdí, že exfiltroval 18,3 GB citlivých právnych a zákazníckych údajov. Dataset bol ponúknutý na predaj na fóre darknetu, pričom kompletný archív je ocenený na 5 000 USD. Podľa zverejneného inzerátu únik zahŕňa široké spektrum interných dokumentov vrátane aktívnych aj uzavretých súdnych spisov zo 48 štátov USA. Údajne išlo o údaje, ktoré ľudia zadali na webových stránkach spoločnosti a jej predajcov v rokoch 2014 až 2017, vrátane čísiel vodičských preukazov, sociálnych zabezpečení, údajov o kreditných kartách a dátumov narodenia. V čase zverejnenia tejto správy spoločnosť Mercedes-Benz USA nevydala oficiálne vyhlásenie potvrdzujúce pravosť týchto údajov.

Európska komisia pripravuje návrh tzv. omnibusového balíka EÚ, ktorým sa usiluje o zmiernenie pravidiel GDPR a ePrivacy s cieľom podporiť inovácie v oblasti umelej inteligencie. Konkrétne ide o zjednodušenie a zosúladenie povinností, ktoré sa dnes prekrývajú medzi GDPR, ePrivacy, AI Act, DSA/DMA a kyberbezpečnostnými pravidlami. Návrh predpokladá zníženie duplicít, teda firmy nebudú plniť tú istú povinnosť viackrát podľa rôznych nariadení. Zároveň má dôjsť ku jasnejším pravidlám pre AI a to najmä pri tréningu modelov, využívaní dát a anonymizácii.
Kritici majú obavy, že ochrana súkromia by mohla byť oslabená a vo výsledku v prospech záujmov veľkých technologických spoločností, na čo komisia reaguje tvrdeniami o právnej istote a efektivite.

Autonómne vozidlá

Španielsko sa potichu stalo jednou z najotvorenejších jurisdikcií v Európe pre testovanie autonómnych vozidiel, keď udelilo povolenia, ktoré okamžite umožnili rozšírené testovanie systému Full Self-Driving (FSD) spoločnosti Tesla. Tento regulačný impulz je významný, pretože prelamuje európsku zotrvačnosť v oblasti autonómie a naznačuje, že kontinent sa definitívne vydal na cestu k nasadeniu „robotaxi" v rokoch 2026 alebo 2027. Hoci nejde o plné komerčné schválenie, krok Španielska má okamžité dôsledky nielen na mobilitu ale napríklad aj na poisťovníctvo či

logistiku, keďže tieto odvetvia núti prispôsobiť sa modelom zodpovednosti založeným na softvéri a flotilách vozidiel.

Tím ICS CERT zo spoločnosti Kaspersky na konferencii Security Analyst Summit 2025 predstavil výsledky auditu, ktorý odhalil kritické zraniteľnosti v telematickom systéme výrobcu áut. Tieto chyby by umožnili útočníkom získať neautorizovaný prístup k prepojeným vozidlám a potenciálne ich úplne ovládnuť, vrátane manipulácie s kľúčovými funkciami ako zmena prevodovky či vypnutie motora počas jazdy. Audit ukázal na kritickú zraniteľnosť typu zero-day SQL injekcie a to v aplikácii dodávateľa, ktorá poskytovala prístup k citlivým údajom a konfiguráciám telematickej infraštruktúry. Následne mohli experti získať prístup k interným serverom a dokonca modifikovať firmware jednotky telematického riadenia (TCU), čím sa otvorila cesta k ovládaniu systému vozidla cez jeho CAN zbernicu.

Európska únia

Organizácia TechPolicy.press zmapovala, ako Európska komisia zvažuje zaradenie ChatGPT pod Akt o digitálnych službách (DSA). Komisia momentálne posudzuje, či by ChatGPT mal byť formálne klasifikovaný ako „Very Large Online Search Engine" (VLOSE) podľa pravidiel DSA. Ide o kategóriu, ktorá sa vzťahuje na služby s viac ako 45 miliónmi mesačných používateľov v EÚ a podlieha prísnym povinnostiam vrátane správy systémových rizík, transparentnosti a auditu. ChatGPT totiž podľa údajov OpenAI dosiahol priemerne viac než 120 miliónov mesačných používateľov v EÚ pre svoju vyhľadávaciu funkciu, čo výrazne prekračuje prah pre takéto označenie. Kľúčovým problémom je to, či má ChatGPT fungovať ako nezávislá vyhľadávacia služba alebo ako súčasť širšieho chatbotu. Na základe toho sa má posúdiť aplikácia DSA. Ak by bol zaradený ako VLOSE, musel by OpenAI napríklad robiť ročné hodnotenia rizík, poskytovať väčšiu transparentnosť ohľadom moderovania obsahu a správy dát, a sprístupňovať informácie o rizikách nezávislým výskumníkom. Podľa organizácie TechPolicy by išlo bezprecedentný krok, pretože by viedol k situácii, keď generatívne AI chatboty budú podliehať rovnako prísnym pravidlám EÚ ako veľké vyhľadávače, čím sa už len samotné generovanie odpovedí dostáva pod regulačný dohľad.

Európska komisia uložila platforme X pokutu 120 miliónov eur za porušenie požiadaviek na transparentnosť podľa Aktu o digitálnych službách (DSA), a to po dvojročnom vyšetrovaní. Ide o prvé rozhodnutie o nezhode od spustenia DSA, v rámci ktorého regulátor zistil, že X porušila povinnosti týkajúce sa transparentnosti a zverejňovania informácií online, a to najmä v oblasti reklám a verejného prístupu k údajom. Konkrétne išlo o porušenia v podobe klamlivého označovania „modrého overovacieho odznaku", ktoré môže zavádzať používateľov, keďže umožňuje overenie len na základe platby bez skutočnej identity overovateľa, nedostatočnej transparentnosti reklamnej databázy, ktorá nespĺňa požiadavky DSA na prístupnosť a vyhľadávanie, a ktorá neobsahuje kľúčové informácie o obsahu a platených zadávateľoch reklám. A na záver porušenie v podobe obmedzeného prístupu výskumníkov k verejným dátam platformy, čo bráni nezávislému skúmaniu systémových rizík a podvodov.

Európska komisia začala práce na kódexe postupov pre označovanie a štítkovanie obsahu generovaného umelou inteligenciou. Tento krok zahŕňa sedemmesačný proces zahŕňajúci nezávislých odborníkov a zúčastnené strany, ktorý má viesť k vypracovaniu dobrovoľného nástroja pomáhajúceho poskytovateľom a používateľom generatívnych AI systémov efektívne plniť povinnosti transparentnosti, vrátane označovania syntetického textu, obrazov, videí a deepfake obsahu tak, aby bol ľahko identifikovateľný a detekovateľný, čím sa má okrem iného znížiť riziko šírenia dezinformácií a podvodov. Obsah by mal byť jasne označený v strojovo čitateľnom formáte.

Povinnosti týkajúce sa označovania a transparentnosti by mali nadobúdať účinnosť od augusta 2026, pričom Kódex má doplniť existujúce pravidlá EÚ o vysokorizikových AI systémoch a všeobecných AI modeloch.

LEGISLATÍVA A SÚDNE ROZHODNUTIA

Ako už názov vypovedá, v tejto časti si rozoberieme novinky z oblasti legislatívy a súdnych rozhodnutí ktoré rezonovali v rámci kybernetického sektora. V prvom rade však poukážeme na legislatívne návrhy viacerých štátov vrátane iniciatív Európskej únie.

Legislatíva

Európska komisia spustila verejnú konzultáciu s cieľom zhromaždiť podklady a názory k návrhu budúceho EU Quantum Act, ktorý sa očakáva v roku 2026 ako nástroj na podporu rozvoja kvantových technológií v EÚ. Táto iniciatíva nadväzuje na Quantum Europe Strategy resp. strategický rámec EÚ, ktorého cieľom je urobiť z Európy svetového lídra v oblasti kvantových technológií do roku 2030. Medzi hlavné ciele pripravovaného zákona patrí posilnenie výskumu a inovácie v oblasti kvantových technológií, zvýšenie priemyselnej kapacity, vrátane zavádzania pilotných liniek a dizajnérskych zariadení, posilnenie odolnosti dodávateľských reťazcov a správy strategických komponentov. EU Quantum Act má dopĺňať ďalšie dôležité európske iniciatívy v oblasti technológií, ako sú Chips Act, EuroHPC alebo infraštruktúra EuroQCI pre zabezpečené kvantové komunikácie

Nemecko prijalo „NIS-2-Umsetzungsgesetz", teda zákon o implementácii európskej NIS 2 smernice do národného práva. Zákon ktorý nadobudol účinnosť 6. decembra 2025, novelizuje BSI-Gesetz (zákon o bezpečnosti informácií) a zároveň *rozširuje rozsah pôsobnosti kybernetických bezpečnostných predpisov* v Nemecku. Nemecko sa tak definitívne zaradilo medzi členské štáty implementujúce NIS 2 do vnútroštátneho právneho poriadku. Zákonom sa pritom rozširuje pôsobnosť predpisov ďaleko za doteraz regulované kritické infraštruktúry a prináša nové povinnosti v oblasti riadenia rizík, hlásenia incidentov a implementácie technických a organizačných opatrení pre značný počet podnikateľských subjektov. Implementácia predstavuje reakciu na zvýšené kybernetické riziká a to najmä tým, že určuje povinnosť dodržiavať najnovšie štandardy bezpečnosti, pričom sa posilňuje rola BSI ako národného orgánu dohľadu nad kybernetickou bezpečnosťou.

Obdobne aj Rakúska vláda predložila do parlamentu návrh ktorým chce implementovať európsku smernicu NIS 2 do rakúskeho právneho poriadku a posilniť národnú kybernetickú bezpečnosť. Konkrétne ide o *Netz- und Informationssystemsicherheitsgesetz 2026* – nový zákon o kybernetickej bezpečnosti. Tento nový zákon má komplexne upraviť rámec pre zabezpečenie sietí a informačných systémov, zavádza tiež povinnosti pre „wesentliche a wichtige Einrichtungen" (kľúčové a významné subjekty) a definuje štruktúru národnej kybernetickej autority vrátane CSIRT a kontrolných mechanizmov.

Nezaháľa ani Poľsko, ktoré realizovalo do 3. decembra 2025 verejné konzultácie k návrhu zákona o spravodlivom prístupe k údajom. Cieľom zákona je preniesť do národného práva ustanovenia Európskeho Aktu o údajoch (2023/2854), ktorý je zameraný na harmonizáciu pravidiel spravodlivého prístupu k údajom a ich využívaniu medzi podnikmi, spotrebiteľmi a verejnými orgánmi.

Britská vláda spustila tzv. *call for evidence* na vývoj regulačného rámca pre automatizované vozidlá. Ministerstvo dopravy Spojeného kráľovstva spolu s Centre for Connected and Autonomous Vehicles dňa 4. decembra 2025 zverejnilo verejnú výzvu (call for evidence*)* na zasielanie podnetov a názorov, ktorá má pomôcť pri tvorbe sekundárnej legislatívy, usmernení a politík pre reguláciu samo-riaditeľských (self-driving) vozidiel na britských cestách. Ide o súčasť implementácie legislatívneho rámca Automated Vehicles Act 2024, ktorý má podporiť bezpečné nasadenie autonómnych vozidiel, zlepšiť dostupnosť mobility, posilniť bezpečnostné štandardy, chrániť údaje a osobnú bezpečnosť a zároveň udržať Spojené kráľovstvo konkurencieschopné v oblasti rozvoja tejto technológie. Dokument je rozdelený do dvoch hlavných častí:

- „Getting AVs on the road" – otázky týkajúce sa schvaľovania typu vozidiel, autorizačných procesov, postavenia človeka v kabíne (User-in-Charge), prechodu medzi autonómnym a manuálnym režimom, licencovania prevádzkovateľov a poistenia.
- „Once AVs are on the road" – otázky týkajúce sa prevádzky vozidiel, vyšetrovania incidentov, kybernetickej bezpečnosti, sankcií a ďalších aspektov ich používania na cestách.

Čo sa týka nadnárodnej legislatívy, Európska komisia dňa 28. novembra 2025 vydala Implementačné nariadenie (EÚ) 2025/2392, ktoré obsahuje technické definície a popisy kategórií produktov s digitálnymi prvkami považovaných za dôležité alebo kritické podľa *Cyber Resilience Act* (Nariadenie EÚ 2024/2847). Tieto definície sú kľúčové pre to, aby výrobcovia vedeli, ktoré produkty podliehajú prísnym kybernetickým požiadavkám a hodnoteniu zhody pred uvedením na jednotný európsky trh. Presnejšie Nariadenie 2025/2392 uvádza, ktoré konkrétne typy produktov spadajú do vyšších rizikových kategórií, ako sú napríklad samostatné prehliadače, firewally, heslové manažéry, tamper-resistant mikroprocesory či smart karty, čím poskytuje istotu pri uplatňovaní povinností CRA

Európska agentúra pre kybernetickú bezpečnosť (ENISA) vydala „NIS2 Technical Implementation Guidance", ktorá poskytuje praktické technické usmernenie pre implementáciu Smernice NIS 2 pre subjekty zapojené do digitálnej infraštruktúry a poskytovania ICT služieb v celej EÚ. Dokument nadväzuje na Nariadenie (EÚ) 2024/2690, ktoré definuje povinné bezpečnostné opatrenia pre tieto organizácie. Usmernenie vysvetľuje technické a metodologické požiadavky na riadenie kybernetických rizík podľa NIS 2 a poskytuje konkrétne rady, príklady dôkazov a odporúčania, ako tieto povinnosti uviesť do praxe. Aj keď nejde o právne záväzný dokument, má zladiť právne požiadavky smernice NIS 2 s praktickými krokmi pre zlepšenie kybernetickej bezpečnosti a odolnosti organizácií.

V novembri bolo Európskym parlamentom a Radou prijaté Nariadenie 2025/2509 o bezpečnosti hračiek a o zrušení smernice 2009/48/ES. Akt potvrdzuje, že moderné digitálne riziká spojené s hračkami, vrátane tých, ktoré vyplývajú z rádiových funkcií a pripojenia na internet, budú primárne upravené osobitnými právnymi predpismi EÚ, a nie samotným nariadením o bezpečnosti hračiek. Podľa bodov odôvodnenia (14) a (15) musia hračky využívajúce umelú inteligenciu spĺňať požiadavky Aktu o umelej inteligencii (Nariadenie 2024/1689) a digitálne prepojené hračky musia dodržiavať Akt o kybernetickej odolnosti (CRA, Nariadenie 2024/2847).Za pozornosť stojí, že hračky s bezpečnostnými komponentmi AI sú klasifikované ako vysokorizikové systémy AI, čo si podľa Aktu o umelej inteligencii vyžaduje prísne posudzovanie zhody treťou stranou.

Súdne rozhodnutia

Ústavný súd Českej republiky dňa 1. decembra 2025 v konaní I. ÚS 3004/25 popri rozhodovaní o ústavnej sťažnosti podanej proti uzneseniu Najvyššieho správneho súdu ČR, uložil právnemu zástupcovi sťažovateľa poriadkovú pokutu vo výške 25 000 Kč, pretože ústavná sťažnosť obsahovala množstvo nezmyselných tvrdení a citácií neexistujúcich rozhodnutí Ústavného súdu a Európskeho súdu pre ľudské práva. Podľa súdu tým zástupca hrubo zaťažil priebeh konania, pričom časť citovaných rozhodnutí vôbec neexistuje a ďalšie boli hrubo dezinterpretované, čo znemožnilo efektívny priebeh konania pred Ústavným súdom.

Nemecký súd v Mníchove v utorok 11. novembra 2025 rozhodol, že OpenAI porušila autorské práva. Súd sa tak priklonil na stranu nemeckej organizácie na ochranu autorských práv GEMA, ktorá žalovala americkú spoločnosť OpenAI za neautorizované použitie chránených textov piesní pri trénovaní modelov ChatGPT. Súd konštatoval, že jazykový model AI reprodukoval texty chránené autorským právom, čím došlo k porušeniu autorského zákona. Medzi použitými dielami boli texty deviatich nemeckých skladieb, ktoré ChatGPT dokázal generovať takmer identicky, čo súd považoval za dôkaz ich zahrnutia do tréningových dát bez licencie. OpenAI naopak argumentovala, že modely iba učia vzory a neukladajú ani neukazujú priamo tréningové dáta, a že pri generovaní výstupov je zodpovedný používateľ, ktorého prompt text vyvolal. Súd však tieto argumenty odmietol a rozhodol, že memorovanie a reprodukcia textov predstavujú porušenie autorských práv.

V Spojených štátoch amerických, presnejšie na Floride, došlo k historickej sankcii ktorú nariadil federálny sudca Leibowitz. Túto sankciu vo výške 85 567,75 USD uložil právnemu zástupcovi žalobcov v prípade *Byoplanet International, LLC v. Johansson a Gilstrap* (č. 24-cv-60630, S.D. Fla. 1. augusta 2025). Tento vysoký trest bol uložený za rozsiahle zneužívanie generatívnej umelej inteligencie, ktoré viedlo k predloženiu vymyslených (halucinovaných) prípadov a sfalšovaných citácií. Súd rozhodol o priznaní plnej výšky trov konania, ktoré požadovala žalovaná strana, čím tento prípad upevnil ako popredné varovanie pred finančnými dôsledkami nesprávneho spoliehania sa na umelú inteligenciu v právnych podaniach. Právny zástupca žalobcov, James Martin Paul, podal sériu žalôb a návrhov v ôsmich súvisiacich prípadoch (na štátnej aj federálnej úrovni). Pri ich príprave sa spoliehal na generatívnu AI (pravdepodobne ChatGPT alebo podobný model), ktorú použil na vyhľadávanie judikatúry a koncipovanie textov. Kľúčovým problémom nebolo samotné použitie AI, ale absencia akejkoľvek kontroly výstupov (verifikácie). To, čo tento prípad odlišuje od obyčajnej nedbanlivosti, je reakcia advokáta na upozornenia. Protistrana (obhajoba) podala návrh na zamietnutie žaloby, v ktorom explicitne upozornila, že citované prípady sú falošné. Napriek tomu advokát Paul v následných odpovediach súdu a v ďalších podaniach naďalej používal AI bez overenia, a dokonca generoval nové falošné citácie na svoju obhajobu. Súd toto konanie vyhodnotil nie ako omyl, ale ako subjektívnu zlú vieru (v preklade: subjective bad faith) a pokus o podvod na súde. Tento prípad predstavuje jeden z najvýznamnejších a najprísnejších rozsudkov týkajúcich sa zneužitia umelej inteligencie v súdnej sieni od známej kauzy *Mata v. Avianca* z roku 2023.

KURZY A EVENTY

Escar Europe 2025 predstavuje vedúcu konferencia o kybernetickej bezpečnosti v automobilovom priemysle. 23. ročník escar Europe sa uskutočnil **5. až 6. novembra 2025** vo **Frankfurte nad Mohanom** (Nemecko) ako hybridná konferencia zameraná na automotive cybersecurity. Podujatie poskytlo fórum pre spoluprácu priemyslu, akademickej obce a vládnych orgánov pri riešení hrozieb, zraniteľností a mitigácie rizík v oblasti bezpečnosti vozidiel.

- **viac informácií / program na:** https://escar.info/escar-europe/program

Medzinárodná asociácia odborníkov na ochranu súkromia (International Association of Privacy Professionals – IAPP) usporiadala 14. ročník **Europe Data Protection Congress**, ktorý sa konal 19. až 20. novembra 2025 **v Bruseli** (Belgicko). Podujatie privítalo tisíce profesionálov z oblasti ochrany osobných údajov, AI governance a kyberbezpečnosti, aby diskutovali o kľúčových trendoch a praktických riešeniach v európskom i globálnom kontexte. Aktuálne prebieha výzva na predkladanie návrhov na diskusiu pre ďalší ročník 2026.

- **výzva dostupná na:** https://iapp.org/conference/iapp-europe-congress

Dňa 3. decembra 2025 usporiadala CONNECT University (DG CONNECT) virtuálne podujatie s názvom ***"CRAzy About Product Cybersecurity: From Compliance to Confidence"*,** ktoré sa sústredilo na pochopenie nových pravidiel Európskej únie v oblasti produktovej kybernetickej bezpečnosti pod Cyber Resilience Act (CRA). Prednášky a diskusie vysvetlili cieľ, rozsah a praktické dôsledky CRA, ktorý zavádza horizontálne kybernetické požiadavky pre produkty s digitálnymi prvkami tak, aby bezpečnosť bola integrovaná už pri návrhu produktov.

- **link na online záznam:** https://www.youtube.com/live/QRLWcU_Yx18?si=Sv9WOm7rgKmGH_UW

Europa Institute pri **Leiden University** organizuje v akad. roku 2025/2026 interdisciplinárnu **prednáškovú sériu s názvom *Humanity in the Automated State***, ktorá skúma, ako automatizované systémy a algoritmické riadenie menia vzťah medzi občanmi a štátom, legislatívne koncepcie a základné hodnoty humanistického právneho poriadku. Série sa zúčastnia viacerí medzinárodní odborníci z oblasti práva, verejnej správy, manažmentu a technológií. Séria sa začala **20. novembra 2025** otvorenou prednáškou Prof. Christine Moser (Vrije Universiteit Amsterdam), ktorá diskutovala o naratívoch okolo AI a ich vplyve na spoločnosť a organizácie. Ďalšie plánované prednášky zahŕňajú vystúpenia odborníkov ako **Aya Rizk (12. januára 2026), Sofia Ranchordás (29. januára 2026), Madalina Busuioc (12. februára 2026)** a ďalších, ktoré sa uskutočnia osobne aj online.

- **viac informácií na:** https://www.universiteitleiden.nl/en/law/institute-of-public-law/europa-institute/events/lecture-series-humanity-in-the-automated-state#format-and-location

Európsky dozorný úrad pre ochranu údajov (European Data Protection Supervisor – EDPS) spolu s Radou Európy (CoE) organizuje jednodňové podujatie **Data Protection Day 2026** na tému *„Reset or refine?"*, ktoré sa uskutoční **28. januára 2026** v budove Charlemagne, Európska komisia, **Brusel**. Podujatie je otvorené osobne aj online a je venované diskusii o nových výzvach a príležitostiach v oblasti ochrany osobných údajov v kontexte GDPR, Conventione 108+ a rýchlo sa meniacich technológií vrátane umelej inteligencie.

- **viac informácií / registrácia na:** https://www.edps.europa.eu/webform/data-protection-day-2026_en

LITERATÚRA

Správa International Transport Forum (ITF/OECD s názvom: **AI, Machine Learning and Regulation: The Case of Automated Vehicles** skúma regulačné výzvy automatizovaných vozidiel v kontexte použitia umelej inteligencie a strojového učenia v dopravných systémoch. Dokument, publikovaný 21. februára 2025, vznikol na základe diskusií z okrúhleho stola ITF a poskytuje komplexný prehľad otázok spojených s dôveryhodnosťou, bezpečnosťou a spoločenskými dopadmi AVs (Automated Vehicles).

- **Dostupná TU**

Článok ***„Rethinking Cybersecurity Research Governance: Lessons from the Act on Digital Services?"*** analyzuje právny rámec pre kyberbezpečnostný výskum v EÚ. Autori **Michal Rampášek** a **Matúš Mesarčík** v článku publikovanom v *European Journal of Risk Regulation* skúmajú, ako súčasné európske právne predpisy upravujú postavenie a činnosť kyberbezpečnostných výskumníkov, najmä v prostredí mimo formálnych inštitúcií. Text sa zameriava na ambície a limity *Digital Services Act (DSA)* v oblasti prístupu k dátam a auditov na veľkých online platformách (VLOPs), a porovnáva ich s inými právnymi nástrojmi ako *Cyber Resilience Act (CRA)* a *Smernica NIS2.*

- **Dostupné TU**

Kniha **CIPP/C Study Guide: CANADA DATA PROTECTION LAW** je podrobným sprievodcom kanadskou legislatívou o ochrane osobných údajov, koncipovaným najmä pre uchádzačov o certifikáciu **Certified Information Privacy Professional/Canada (CIPP/C)**. Publikácia vyšla **8. apríla 2024** nezávislým vydavateľstvom a obsahuje 380 strán textu v angličtine, ktoré sa venujú kľúčovým právnym princípom a rámcom v oblasti kanadskej ochrany súkromia. Kniha slúži nielen ako príprava na certifikačné skúšky, ale aj ako praktický nástroj pre porozumenie komplexnej kanadskej ochrany osobných údajov.

- **Dostupná TU**

Kniha **„CIPP/CN Study Guide 2024: Hong Kong, Singapore, India..."** *(sprievodca pre ochranu údajov a prípravu na skúšky)* predstavuje komplexný študijný materiál zameraný na globálne právne rámce ochrany osobných údajov, s dôrazom na jurisdikcie ako Hongkong, Singapur a India. Kniha je navrhnutá ako praktický návod pre uchádzačov skúšok CIPP/A a CIPP/CH, ale zároveň slúži ako prehľad právnych princípov správy osobných údajov v týchto regiónoch.

- **Dostupná TU**

European Data Protection Supervisor (EDPS) vydala 11. novembra 2025 správu ***"Guidance for Risk Management of Artificial Intelligence Systems"***. Správa predstavuje technické usmernenie pre identifikáciu a riadenie rizík spojených s používaním umelej inteligencie (AI) pri spracovaní osobných údajov v inštitúciách EÚ. Dokument poskytuje 55-stranový rámec založený na ISO 31000:2018 a je určený predovšetkým pre EÚ inštitúcie, orgány, úrady a agentúry, ktoré pôsobia ako správcovia údajov a vyvíjajú, obstarávajú alebo nasadzujú AI systémy. EDPS upozorňuje, že

táto príručka nenahrádza úplnú compliance analýzu, ale slúži ako praktický doplnok pre kontrolu a riadenie rizík v súlade so Všeobecným nariadením o ochrane údajov pre inštitúcie EÚ – EUDPR (Regulácia 2018/1725)

- **Dostupná TU**

European Data Protection Supervisor (EDPS) publikoval tiež **TechSonar Report 2025-2026**, ktorý predstavuje prehľad šiestich kľúčových technologických trendov s potenciálnym dopadom na súkromie a ochranu údajov v nasledujúcich rokoch. TechSonar je strategická iniciatíva EDPS na monitorovanie vznikajúcich technológií z pohľadu práva a základných práv, pričom sa zameriava na predikciu vzostupných trendov a ich možných rizík či prínosov pre jednotlivcov a spoločnosť.

- **Dostupné TU**

Článok ***"Key Safety Design Overview in AI-driven Autonomous Vehicles"*** od **Vikas Vyas** a **Zheyuan Xu** publikovaný na *arXiv* predstavuje prehľad kľúčových princípov bezpečnostného dizajnu pre autonómne vozidlá využívajúce umelú inteligenciu, najmä úrovní SAE 3 a 4, kde AI softvér zohráva rozhodujúcu úlohu. Autori identifikujú hlavné konštrukčné výzvy v oblasti softvéru a hardvéru, vrátane integrácie AI/ML systémov s vysokými bezpečnostnými nárokmi a bezpečnostných mechanizmov fail-safe pre kritické situácie. Stratégie uvedené v práci sa zameriavajú na analýzu porúch, mitigáciu rizík a návrh systémovej architektúry, ktorá podporuje spoľahlivosť AI systémov počas celého životného cyklu dát a prevádzky.

- **Dostupné TU**

V preprintovej práci ***"A Criminology of Machines"*** autor **Gian Maria Campedelli** navrhuje nové paradigmy pre štúdium kriminality v ére autonómnych AI systémov. Campedelli tvrdí, že so stúpajúcou prítomnosťou autonómnych AI agentov, ktorí dokážu samostatne vnímať, rozhodovať a interagovať, je potrebné rozšíriť tradičné kriminologické rámce, ktoré sa doposiaľ sústreďovali na ľudí, o štúdium samotných strojov ako aktérov so sociálnou a právnou agentúrou.

- **Dostupné TU**

V decembri vyšiel tiež článok od autorov ***Nathan Genicot & Thiago Guimaraes Moraes*** názvom ***„Exploring the boundaries of AI regulatory sandboxes under the AI Act: Flexibility and real-world testing"***. V článku autori poukazujú na kritické nezrovnalosti v Akte EÚ o umelej inteligencii. Odhaľujú v ňom zložitý a protirečivý vzťah medzi „regulačnými sandboxmi" (pieskoviskami), ktoré ponúkajú právny dialóg a podmienečné oslobodenie od pokút, a „testovaním v reálnych podmienkach", ktorého cieľom je odstrániť trhové bariéry. V závere článku sa uvádza, že Európska komisia musí poskytnúť urýchlené objasnenie, aby sa zabezpečila efektívna a konzistentná implementácia týchto nových nástrojov na experimentovanie s AI.

- **Dostupné TU**