AKTUALITY V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Správa (február a marec 2026)

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,

predkladáme vám správu v oblasti aktualít kybernetickej bezpečnosti, ktorá prináša komplexný prehľad kľúčových udalostí a trendov za mesiace február a marec 2026. V období, kedy sa hranice medzi fyzickým a digitálnym svetom čoraz viac stierajú, sa kybernetická bezpečnosť, ochrana súkromia a boj proti kyberkriminalite stávajú piliermi stability modernej demokratickej spoločnosti.

Cieľom tejto správy je poskytnúť odbornému publiku, akademickej obci a zainteresovaným subjektom hĺbkový pohľad na dynamicky sa vyvíjajúce regulačné prostredie. Zameriavame sa nielen na publikované texty nových právnych predpisov, ale aj na pripravované legislatívne iniciatívy, prelomové súdne rozhodnutia a najnovšie výsledky vedeckého výskumu, ktoré spoločne formujú globálnu architektúru digitálnej dôvery.

Aktuálne sledované obdobie bolo poznačené najmä intenzívnou diskusiou o praktickej implementácii európskeho Aktu o umelej inteligencii (AI Act) a hľadaním rovnováhy medzi technologickou inováciou a ochranou základných práv jednotlivcov. Čelíme novým výzvam v oblasti autonómnej mobility, kde sa bezpečnosť systémov stretáva s prísnymi nárokmi na ochranu osobných údajov, a zároveň sme svedkami neustáleho zdokonaľovania techník kybernetických útočníkov, čo si vyžaduje proaktívny a koordinovaný prístup na nadnárodnej úrovni.

Správa je štruktúrovaná tak, aby mapovala kľúčové piliere našej expertízy:
Aktuality a technologické trendy: Analýza najnovších incidentov a inovácií, ktoré menia bezpečnostnú paradigmu.
Legislatívny rámec: Prehľad noriem EÚ a globálnych štandardov (ISO, OSN), ktoré nastavujú pravidlá pre digitálnu budúcnosť.
Judikatúra: Rozbor súdnych sporov, ktoré definujú hranice zodpovednosti za algoritmy
a autorskoprávnu ochranu diel vytvorených AI.
Vzdelávanie a vedecký diskurz: Pozvánky na odborné fóra a reflexia najnovšej literatúry v oblasti strategickej komunikácie a boja proti manipulácii.

Veríme, že tento súhrn poznatkov prispeje k lepšej orientácii v zložitej problematike práva kybernetickej bezpečnosti a posilní odolnosť našich informačných systémov voči súčasným aj budúcim hrozbám.

ČO JE NOVÉ V OBLASTI KYBERNETICKEJ BEZPEČNOSTI?

Automatizované systémy na rozpoznávanie evidenčných čísiel vozidiel (ALPR) vyvolávajú výrazné diskusie o ochrane súkromia, keďže policajné oddelenia rozširujú ich využívanie na sledovanie trestnej činnosti a vyhľadávanie odcudzených vozidiel. Kritici tvrdia, že táto technológia vytvára „plošný sledovací systém", ktorý monitoruje každodenný pohyb občanov bez dostatočného dohľadu a ochrany údajov. Tento konflikt viedol niektoré miestne samosprávy k pozastaveniu zavádzania týchto kamier s cieľom riešiť obavy z masového sledovania a možného zneužitia údajov.

Autonómna nákladná doprava prechádza od úplného riadenia vozidla k modelu, v ktorom ľudskí vodiči fungujú ako „riadiaci letovej prevádzky", dohliadajúci na flotily poháňané autonómnou inteligenciou a tzv. decision surface physics. Táto zmena presúva vodiča od volantu k strategickému dohľadu, pričom využíva údaje v reálnom čase na riadenie komplexného logistického prostredia s vyššou presnosťou.

Nový systém Behavioural ADAS (BADAS) od spoločnosti Nexar využíva rozsiahly dataset 10 miliárd kilometrov z reálnej premávky na identifikáciu jemných behaviorálnych vzorcov, ktoré predchádzajú dopravným nehodám ešte pred ich vznikom. Presunom od reaktívneho brzdenia k prediktívnemu predvídaniu má tento systém ambíciu prekonať tradičné vizuálne modely pri detekcii kritických hraničných situácií, ktoré predstavujú výzvu pre autonómne vozidlá.

Európska komisia oficiálne nestihla termín 2. februára na poskytnutie kľúčových usmernení k vysokorizikovým systémom umelej inteligencie podľa Aktu o umelej inteligencii EÚ. Toto oneskorenie vyvolalo obavy medzi podnikmi z hľadiska právnej istoty, čo viedlo k návrhu tzv. „Digital Omnibus", ktorý by mohol posunúť účinnosť niektorých pravidiel pre vysokorizikové systémy až o 16 mesiacov. Regulátori v súčasnosti zapracúvajú mesiace spätnej väzby od priemyslu, aby zabezpečili technickú realizovateľnosť štandardov pred ich konečným prijatím.

Holandský telekomunikačný gigant Odido utrpel rozsiahle narušenie bezpečnosti. Spoločnosť Odido, najväčší mobilný operátor v Holandsku, potvrdila 12. februára 2026, že kybernetický útok na systém zákazníckej podpory odhalil osobné údaje 6,2 milióna ľudí. Ukradnuté informácie zahŕňajú mená, IBAN účty a identifikačné doklady, čo viedlo k okamžitým varovaniam pred vysoko cielenými phishingovými

útokmi. Spoločnosť incident nahlásila holandskému úradu na ochranu údajov (AP), pričom vyšetrovanie nad'alej prebieha.

Masívna kampaň škodlivých rozšírení odhalila ohrozenie 37 miliónov používateľov. Bezpečnostní výskumníci odhalili rozsiahlu sieť viac ako 300 škodlivých rozšírení prehliadača Chrome, ktoré boli spolu stiahnuté viac ako 37 miliónkrát. Tieto rozšírenia, často maskované ako neškodné nástroje na produktivitu alebo prispôsobenie, odosielali históriu prehliadania, výsledky vyhľadávania a citlivé osobné údaje na nezabezpečené siete alebo zberné servery. Tento objav poukazuje na významnú „slepú škvrnu" v bezpečnosti prehliadačov, keďže mnohé z týchto nástrojov prešli počiatočným schvaľovaním v online obchode pred tým, ako boli aktualizované škodlivým kódom.

LEGISLATÍVA A SÚDNE ROZHODNUTIA

Už tradične si v tejto časti uvedieme novú legislatívu a zaujímavé súdne rozhodnutia ktoré rezonovali v rámci kybernetického sektora.

Legislatíva

Európska komisia navrhla nový balík kybernetickej bezpečnosti s cieľom posilniť odolnosť EÚ voči narastajúcim kybernetickým a hybridným hrozbám prostredníctvom zjednodušenia certifikačných procesov a zabezpečenia dodávateľských reťazcov IKT. Iniciatíva zahŕňa revíziu Aktu o kybernetickej bezpečnosti a cielené zmeny smernice NIS2, pričom cieľom je zjednodušiť dodržiavanie predpisov pre tisíce spoločností a zároveň posilniť úlohu agentúry ENISA pri riadení strategických rizík. Tento krok má zabezpečiť, aby digitálne produkty boli bezpečné už od návrhu a chránili technologickú suverenitu Únie a základné služby.

Organizácia Spojených národov pripravila prelomový právny rámec na harmonizáciu bezpečnostných štandardov a schvaľovania typu pre systémy automatizovaného riadenia vozidiel (ADS) naprieč takmer 60 krajinami. Nahradením fragmentovaných národných právnych úprav jednotným globálnym štandardom má táto regulácia odstrániť hlavné prekážky pre rozsiahle nasadenie autonómnych vozidiel. Rámec, ktorý pokrýva oblasti ako riadenie bezpečnosti a monitorovanie počas prevádzky, má byť prijatý v júni 2026.

Prehľad časovej osi:

- Január 2026: Schválenie finálneho návrhu pracovnou skupinou GRVA
- 22. – 26. jún 2026: Plánované formálne prijatie Svetovým fórom pre harmonizáciu predpisov pre vozidlá (WP.29) na jeho 199. zasadnutí

- Začiatok roka 2027: Očakávaná účinnosť (približne šesť mesiacov po prijatí)

Norma ISO/TS 5083:2025 zavádza komplexný bezpečnostný rámec pre systémy automatizovaného riadenia (ADS), pričom nahrádza ISO/TR 4804:2020 a rozširuje usmernenia o bezpečnostných prípadoch a rizikách špecifických pre umelú inteligenciu. Norma obsahuje 16 bezpečnostných princípov a zdôrazňuje potrebu „zrozumiteľných" bezpečnostných argumentov, ktoré majú preklenúť priepasť medzi komplexným vývojom AI a prísnou regulačnou validáciou.

Riešenie vAnonymize od spoločnosti Vector je nástroj využívajúci umelú inteligenciu, ktorý zabezpečuje anonymizáciu video dát v reálnom čase priamo na zariadení (on-premise), najmä so zameraním na tváre a evidenčné čísla vozidiel, aby sa zabezpečil súlad s GDPR pri vývoji ADAS a autonómnych vozidiel. Lokálne a offline spracovanie dát umožňuje firmám bezpečne inovovať a zdieľať dataset-y pri zachovaní potrebných metadát a vizuálnej kvality na ďalšiu technickú analýzu.

TEXAS zavádza poradný výbor pre reguláciu autonómnych vozidiel (AVRAC)

Rada Texaského ministerstva motorových vozidiel (TxDMV) oficiálne prijala konečné pravidlá (43 TAC §§206.101–.102) na vytvorenie poradného výboru pre reguláciu autonómnych vozidiel (AVRAC).

- **Mandát:** AVRAC bude pôsobiť ako špecializovaný poradný orgán poskytujúci odborné odporúčania v oblasti regulácie autonómnych vozidiel a riešenia kľúčových otázok ochrany spotrebiteľa.
- **Regulačný dohľad:** Výbor má zefektívniť riadenie bezpečného zavádzania autonómnych systémov a zabezpečiť, aby regulačný rámec držal krok s technologickým vývojom, najmä pokiaľ ide o „minimálne rizikové stavy" a dodržiavanie dopravných predpisov.
- **Dopad:** Tento krok centralizuje odborné kapacity na úrovni štátu, poskytuje štruktúrovaný rámec pre priemyselné subjekty a zabezpečuje kontinuitu prístupu Texasu k autonómnej doprave minimálne do roku 2031.

Akčný plán EÚ pre bezpečnosť dronov a proti-dronové opatrenia (COM(2026) 81)

Dňa 11. februára 2026 Európska komisia predstavila prelomový akčný plán na vytvorenie jednotného európskeho prístupu proti škodlivému využívaniu dronov a hrozbám z veľkých výšok. Tento plán posúva zameranie EÚ smerom k proaktívnemu „balíku bezpečnosti dronov", ktorý je plánovaný na

tretí štvrťrok 2026 a zásadne prispôsobí regulačný rámec pre civilné drony súčasným bezpečnostným výzvam.

Implementácia ochrany mladistvých v kľúčových právnych aktoch EÚ

Nová štúdia komisie SEDEC (január 2026) hodnotí, ako miestne a regionálne orgány implementujú ustanovenia zamerané na ochranu maloletých v rámci hlavných regulácií EÚ:

- **Digital Services Act (DSA):** dôraz na článok 28, ktorý vyžaduje vysokú úroveň ochrany súkromia a bezpečnosti pre maloletých a zakazuje reklamu založenú na profilovaní.
- **Audiovisual Media Services Directive (AVMSD):** posilnenie opatrení na ochranu mládeže pred škodlivým obsahom prostredníctvom technických filtrov a časových obmedzení.
- **GDPR a rodičovský súhlas:** harmonizácia pravidiel v rámci EÚ týkajúcich sa veku, od ktorého môžu deti samostatne súhlasiť so spracovaním osobných údajov.

Čína: novelizovaný zákon o kybernetickej bezpečnosti (CSL) nadobúda plnú účinnosť

Od začiatku februára 2026 začala mať prvá významná aktualizácia čínskeho zákona o kybernetickej bezpečnosti od roku 2017 dopad aj na medzinárodných operátorov. Novela výrazne zvyšuje pokuty – až do výšky 10 miliónov RMB pri „mimoriadne závažných" porušeniach – a rozširuje právomoci vlády sankcionovať zahraničné subjekty, ktorých činnosť ohrozuje kritickú informačnú infraštruktúru Číny.

Súdne rozhodnutia

NAJVYŠŠÍ SÚD SPOJENÝCH ŠTÁTOV – V prípade Thaler v. Perlmutter (2026) generálny advokát USA podal podanie, v ktorom vyzval Najvyšší súd, aby odmietol napadnutie požiadavky ľudského autorstva pri autorskom práve. Vláda argumentovala, že text autorského zákona – ktorý obsahuje pojmy ako „život", „smrť" a „vdovy" – jasne predpokladá, že autorom je človek. Zároveň poukázala na to, že keďže Stephen Thaler výslovne vylúčil akýkoľvek ľudský tvorivý vklad pri svojom diele generovanom AI, takéto dielo nie je spôsobilé na ochranu. Toto podanie strategicky zužuje predmet sporu na čisto autonómnu tvorbu strojom a ponecháva otvorené zložitejšie právne otázky týkajúce sa diel vytvorených v spolupráci človeka a umelej inteligencie.

NAJVYŠŠÍ SÚD SPOJENÉHO KRÁĽOVSTVA vydal prelomové rozhodnutie vo veci Emotional Perception AI Ltd v Comptroller General of Patents, ktoré prináša dlho očakávané objasnenie patentovateľnosti umelej inteligencie. Rozhodnutie signalizuje priaznivejšie prostredie pre inovátorov v oblasti AI v Spojenom kráľovstve tým, že znižuje počiatočné bariéry pre patentovú

ochranu softvérových riešení. Rozsudok zároveň približuje britský prístup európskym štandardom a rieši dlhodobú diskusiu o tom, či AI „myslí", alebo iba spracúva údaje ako počítačový program.

Nemecký súd rozhodol o tréningových dátach AI spoločnosti Meta

Vyšší krajinský súd v Kolíne nad Rýnom rozhodol, že spoločnosť Meta môže trénovať svoje AI modely na základe údajov z verejných používateľských profilov bez potreby predchádzajúceho výslovného súhlasu. Súd dospel k záveru, že takýto postup nepredstavuje zakázané „spájanie údajov" podľa Aktu o digitálnych trhoch (DMA). Toto rozhodnutie predstavuje významný precedens pre využívanie verejných dát sociálnymi sieťami na účely strojového učenia v rámci EÚ.

KURZY A EVENTY

- Dňa 16. marca 2026 usporiadala Univerzita v Groningene seminár „Regulácia umelej inteligencie v trestnej justícii", ktorý sa zameral na právne a etické dôsledky využívania AI v presadzovaní práva a trestnom práve. Odborníci z Europolu, akademickej sféry a národných policajných zložiek diskutovali o súlade s Aktom o AI, policajných praktikách a vyvíjajúcej sa úlohe digitálnych dôkazov.
- Automated Mobility Summit, organizovaný Swiss Association for Autonomous Mobility (SAAM) a PAVE Europe, otvoril registráciu na svoje hlavné podujatie v máji 2026 v Zürichu. Summit bude zahŕňať živé ukážky autonómnych vozidiel od viacerých výrobcov na súkromných testovacích plochách a poskytne praktický pohľad na budúcnosť medzinárodnej autonómnej dopravy.
- Letná škola 2026: Digitálne bojiská
  Centrum pre medzinárodné humanitárne a operačné právo oznámilo druhý ročník letnej školy v Olomouci, ktorá sa uskutoční od 13. do 24. júla 2026.
  Zameranie: kybernetická a informačná vojna v medzinárodnom práve, suverenita v kyberpriestore, atribúcia a použitie sily
  Program: intenzívna výučba kombinujúca prednášky a prípadové štúdie vrátane exkurzie do sídla OSN vo Viedni
- Hackathon: Legal Design a Data Science pre vysvetliteľnú AI
  Univerzita v Bologni pod vedením prof. Moniky Palmirani oznámila špecializovaný hackathon v rámci výskumného projektu „Legal Design and Data Science for Explicable AI in Legal Domain".
  Účastníci budú pracovať na riešeniach zahŕňajúcich LegalXML, veľké jazykové modely (LLMs), vysvetliteľnú AI (XAI) a rozvíjajúci sa rámec práv umelej inteligencie.

Cieľ: prepojiť komplexné právne dáta s používateľsky orientovaným dizajnom a podporiť tvorbu transparentných a zrozumiteľných AI systémov v právnej oblasti

Ocenenia: 1 800 € (1. miesto), 1 200 € (2. miesto), 700 € (3. miesto)

Prihlášky: otvorené pre výskumníkov a študentov so záujmom o právo a informatiku

- Data Takes Flight: Ochrana súkromia na letiskách

  Dňa 12. februára 2026 usporiadal Európsky dozorný úradník pre ochranu údajov (EDPS) odborné podujatie v Bruseli zamerané na výzvy ochrany súkromia pri biometrickom sledovaní v letectve. Diskusia sa sústredila na rovnováhu medzi pohodlím cestujúcich a prísnymi požiadavkami transparentnosti podľa GDPR a Aktu o umelej inteligencii. Podujatie predstavuje predstupeň nových celoeurópskych usmernení týkajúcich sa využívania rozpoznávania tváre v dopravných uzloch.

LITERATÚRA

Gundars Bergmanis-Korāts, Tetiana Haiduchyk, Bohdan Smolts: Social Media Manipulation for Sale: 2025 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement

Dostupné tu.

V novom experimente z roku 2025 testovalo Centrum excelentnosti strategickej komunikácie NATO schopnosť hlavných sociálnych platforiem identifikovať a odstraňovať neautentickú interakciu. Štúdia odhalila, že napriek aktualizovaným politikám je stále jednoduché zakúpiť si falošné lajky, zdieľania a komentáre, čo poukazuje na pretrvávajúce slabiny v obrane platforiem proti organizovanej manipulácii. V nasledujúcich odsekoch prinášame zhrnutie záverov a odporúčaní v uvedenom dokumente:
Platformy sociálnych médií v poslednom období preukázali určitý pokrok v boji proti spamovým aktivitám. Hoci miera blokovania vytvárania nových účtov zostáva približne na rovnakej úrovni ako v predchádzajúcom hodnotenom období, citeľne sa zlepšilo odstraňovanie už existujúcich účtov a obmedzovanie ich škodlivej činnosti. Napriek tomu však manipulácia ostáva relatívne jednoduchá na realizáciu a finančne nenáročná, a to aj v podmienkach rozšíreného experimentálneho skúmania. Aj keď náklady na manipuláciu zostávajú nízke, efektívnosť moderácie a odhaľovania sa zvyšuje, čo znamená, že aktéri musia vynakladať väčšie zdroje na dosiahnutie rovnakého účinku ako v minulosti.

Zaujímavým trendom je aj posun v tematickom zameraní botmi generovaného obsahu. Po volebnom roku 2024 sa pozornosť presunula z politických otázok na vojenské témy, pričom analýza naznačuje výrazné posilňovanie pročínskeho obsahu. Manipulácia prostredníctvom reklamy na sociálnych sieťach

síce predstavuje vyššie náklady v porovnaní s bežnými formami manipulácie, no stále zostáva dostupná. Existencia trhu s manipulačnými službami je zrejmá, pričom nákup účtov schopných prevádzkovať reklamy je jednoduchý a ich následné využitie umožňuje prostredníctvom nástrojov založených na umelej inteligencii efektívnu distribúciu obsahu naprieč viacerými platformami.
Významnú úlohu v tomto ekosystéme zohrávajú kryptomeny, ktoré slúžia ako hlavný platobný mechanizmus pre poskytovateľov manipulačných služieb. Ich výhodou je rýchlosť, cezhraničný charakter a obmedzená možnosť kontroly. Finančné prostriedky sú často presúvané cez custodial peňaženky a vysokorizikové burzy, čím vzniká odolná a ťažko sledovateľná infraštruktúra. Bežnou praktikou je využívanie tzv. „hot wallets", kde dochádza k miešaniu prostriedkov viacerých používateľov, čo výrazne sťažuje sledovanie transakcií. Empirické zistenia ukazujú, že len menšia časť transakcií je plne vysledovateľná, no aj tie, ktoré sa podarilo analyzovať, potvrdzujú stabilnú a vysokú úroveň finančnej aktivity, čo poukazuje na rozsah a kontinuitu tohto trhu. Súčasne vznikajú aj právne a regulačné riziká, najmä v súvislosti s možným porušovaním sankčných režimov Európskej únie, napríklad pri využívaní veľkých kryptomenových búrz na výber finančných prostriedkov.

Z hľadiska technologického vývoja možno pozorovať výrazný nárast sofistikovanosti týchto operácií. Siete využívajúce umelú inteligenciu vytvárajú falošné profily, ktoré pôsobia psychologicky realisticky a napodobňujú správanie skutočných používateľov. Využívajú pritom dôveryhodné vizuálne prvky, lokalizovaný jazyk a prirodzené časovanie komunikácie. Kľúčovou zmenou je, že tieto siete už nefungujú len ako nástroje na masové šírenie obsahu, ale aktívne sa integrujú do online komunít. Budovaním dôvery a simulovaním autenticity získavajú prístup k diskusiám, kde sa formujú názory, a následne dokážu nenápadne ovplyvňovať verejný diskurz. Tento posun od kvantity k kvalite predstavuje zásadnú výzvu pre existujúce mechanizmy moderácie obsahu a hodnotenia rizík.

Dostupnosť takýchto sofistikovaných manipulačných nástrojov na komerčnej báze predstavuje vážnu hrozbu pre autenticitu online priestoru. Možnosť ich globálneho využitia narúša integritu digitálnej komunikácie a zároveň komplikuje ochranu informačného prostredia. Sociálne siete sa tak ocitajú v situácii, keď musia riešiť nielen tradičné formy spamu, ale aj komplexné a adaptívne formy manipulácie, ktoré zasahujú do základných princípov slobody prejavu a dôvery v informácie.
V reakcii na tieto výzvy je potrebné prehodnotiť existujúce prístupy k detekcii a prevencii manipulácie. Dôležité je presunúť pozornosť od analýzy samotného textu k sledovaniu behaviorálnych vzorcov, ako sú koordinované časovanie, tón komunikácie či vzťahové interakcie medzi účtami. Rovnako je nevyhnutné zaviesť kontinuálne a kontextové monitorovanie, ktoré umožní sledovať vývoj naratívov v čase a identifikovať ich prenikanie do autentických diskusií. Analýza by sa mala zamerať aj na úroveň

celých konverzácií, nie len jednotlivých príspevkov, čo umožní odhalit' falošné profily integrované do reálnych komunít.

Neoddeliteľnou súčast'ou analýzy by malo byt' aj sledovanie finančných tokov, keď'že investície do manipulačných služieb môžu signalizovat' širšie strategické operácie. Súčasne je potrebné uplatňovat' tzv. red-team prístup, ktorý spočíva v aktívnom skúmaní zraniteľností systému a identifikácii fungovania šedej ekonomiky manipulačných služieb. Na základe týchto poznatkov by mali byt' informovaní tvorcovia politík aj samotné platformy, pričom poskytovatelia takýchto služieb by mali čelit' sankciám. Zároveň je nevyhnutné priebežne aktualizovat' stratégie narušovania týchto aktivít v súlade s najnovším výskumom a technologickým vývojom.