AI & TECHNOLÓGIE: MALÝ SLOVNÍK POJMOV

...ALEBO ČO VEDIEŤ, KEĎ IT HOVORÍ O AI

G. Lehnert
LAWYERS WITH INTEGRITY

TENTO SLOVNÍK JE MALÝ MOSTÍK... LEBO IT JEDNODUCHO CHODÍ NA INÉ RAŇAJKY AKO COMPLIANCE.

G. Lehnert, s. r. o.
Budova ORBIS, Rajská 7, SK-811 08 Bratislava
lehnert@lehnert.sk | www.lehnert.sk

AI (ARTIFICIAL INTELLIGENCE) / UMELÁ INTELIGENCIA

Systémy, ktoré vykonávajú úlohy vyžadujúce ľudský úsudok — rozpoznávanie textu, analýza dát, rozhodovanie. Nie je to mágia. Je to matematika na veľkých dátach. **Kľúčová otázka:** Vieme presne, ktoré AI systémy v našej firme fungujú a kto za ne zodpovedá?

AI AGENT / AGENTICKÁ AI

AI, ktorá nielen odpovedá, ale koná — prehľadáva weby, píše e-maily, spúšťa procesy. Vyšší výkon, vyššie riziko. **Kľúčová otázka:** Kto nesie zodpovednosť za jej rozhodnutia? Máme definované, čo môže AI robiť samostatne a kde musí rozhodovať človek?

ALGORITMUS

Sada pravidiel, podľa ktorých AI (alebo akýkoľvek softvér) rozhoduje. „Algoritmus to rozhodol“ znamená: systém podľa nastavených pravidiel vyhodnotil situáciu. **Kľúčová otázka:** Poznáme kritériá, podľa ktorých naše kľúčové systémy rozhodujú?

API (APPLICATION PROGRAMMING INTERFACE)

„Konektor“ medzi dvoma systémami. Keď IT hovorí „napojíme to cez API“, znamená to automatickú výmenu dát medzi aplikáciami — bez manuálneho exportu. **Kľúčová otázka:** Vieme, ktoré naše systémy si vymieňajú dáta navzájom a s kým externe?

AUDIT TRAIL & AUDIT LOG

Záznam o tom, čo AI systém urobil, kedy a na základe čoho. Nevyhnutné pre compliance a prípadné vyšetrovania. Ak to systém nezaznamenáva — nie je auditovateľný. **Kľúčová otázka:** Vieme spätne doložiť, kto alebo čo urobil akékoľvek kľúčové rozhodnutie v systéme?

BIAS / ZAUJATOSŤ AI

AI zdedí predsudky z tréningových dát. Ak boli historické rozhodnutia diskriminačné, AI ich zopakuje — a zosilní. Kritické pri HR, úveroch, poistení. **Kľúčová otázka:** Testovali sme, či naše AI nástroje nerozhodujú diskriminačne?

CHATBOT

Automatizovaný systém konverzácie, ktorý odpovedá na otázky používateľov. Základný chatbot funguje podľa pravidiel, pokročilý používa AI (LLM). Dnes štandardná súčasť zákazníckej podpory aj interných HR procesov. **Kľúčová otázka:** Vieme, aké dáta chatbot zbiera a kam ich posiela?

CLOUD / ON-PREMISE / HYBRID

Cloud = dáta bežia na serveroch dodávateľa (napr. Microsoft, Amazon). On-premise = vlastné servery vo firme. Hybrid = kombinácia. Pre compliance: vždy vedzte, kde sú vaše dáta. **Kľúčová otázka:** Vieme, kde fyzicky sídlia naše firemné dáta?

COPILOT

Marketingový termín (Microsoft) pre AI asistenta zabudovaného do bežných nástrojov — Word, Excel, Outlook, Teams. Pomáha, ale stále potrebuje ľudský dohľad. **Kľúčová otázka:** Majú naši zamestnanci pravidlá, čo môžu a nemôžu cez Copilot zdieľať?

DATA GOVERNANCE / SPRÁVA DÁT

Kto vlastní dáta, kto k nim má prístup, ako sa uchovávajú a mažú. Základ pre akýkoľvek AI projekt. Bez data governance nie je možný zodpovedný AI. **Kľúčová otázka:** Máme stanovené, kto vlastní ktoré dáta a kto má k nim prístup?

DATA LAKE & DATA WAREHOUSE

Úložiská veľkého množstva dát. Data Lake = surové, netriedené dáta. Data Warehouse = štruktúrované, pripravené na analýzu. AI modely sa z nich učia. **Kľúčová otázka:** Vieme, aké dáta o nás a našich klientoch uchovávame a ako dlho?

DATA RESIDENCY & DATA SOVEREIGNTY

Kde fyzicky sídlia vaše dáta — v ktorej krajine, na akom serveri. Kľúčové pre GDPR a regulačné požiadavky. „Uložené v cloude“ nestačí — pýtajte sa: v ktorej krajine? **Kľúčová otázka:** Máme písomne potvrdené, v ktorej krajine sídlia naše dáta u každého dodávateľa?

DEEP LEARNING

Poddruh strojového učenia inšpirovaný štruktúrou ľudského mozgu (neurónové siete). Umožňuje rozpoznávanie obrazu, hlasu alebo textu s vysokou presnosťou. **Kľúčová otázka:** Ak používame systém na báze deep learningu, vieme vysvetliť jeho rozhodnutia regulátorovi?

ENCRYPTION / ŠIFROVANIE

Prevod dát do nečitateľnej podoby bez správneho kľúča. Základný štandard ochrany dát. Ak to váš dodávateľ neponúka, je to červená vlajka. **Kľúčová otázka:** Sú všetky citlivé dáta — v pohybe aj v úložisku — šifrované?

EU AI ACT

Európska regulácia AI účinná od 2024–2026. Delí AI systémy do rizikových kategórií (nízke, stredné, vysoké, neprijateľné riziko). Pre compliance officers: toto je váš nový GDPR. **Kľúčová otázka:** Identifikovali sme, ktoré naše AI systémy spadajú do kategórie vysokého rizika?

EXPLAINABILITY / VYSVETLITEĽNOSŤ AI

Schopnosť vysvetliť, prečo AI dospela k danému rozhodnutiu. Regulátor aj súd sa môžu pýtať. Čierna skrinka nestačí — najmä pri high-risk AI systémoch. **Kľúčová otázka:** Dokážeme vysvetliť, prečo náš systém prijal konkrétne rozhodnutie — napríklad zamietnutie žiadosti?

FINE-TUNING

Doladenie existujúceho AI modelu na špecifické firemné dáta alebo odvetvie. Nákladnejšie ako RAG, ale model je potom „odborníkom“ na danú oblasť. **Kľúčová otázka:** Ak dolaďujeme AI model na firemných dátach, vieme, aké dáta sme mu dali a aké riziká z toho plynú?

GDPR (GENERAL DATA PROTECTION REGULATION)

Európske nariadenie o ochrane osobných údajov platné od 2018. Základ pre všetky compliance povinnosti v oblasti spracovania dát fyzických osôb. Každý AI systém spracúvajúci osobné údaje musí byť v EÚ GDPR-kompatibilný. **Kľúčová otázka:** Máme zdokumentovaný súhlas alebo právny základ pre každé spracovanie osobných údajov vrátane AI systémov?

GENERATÍVNA AI (GENAI)

AI, ktorá netriedi ani neklasifikuje — ale tvorí nový obsah: text, obrázky, kód, tabuľky. ChatGPT, Claude, Gemini. To je ten zásadný posun oproti staršej AI. **Kľúčová otázka:** Majú zamestnanci jasné pravidlá, čo môžu generovať pomocou AI a čo musia vždy overiť?

HALLUCINÁCIA (HALLUCINATION)

Keď AI s istotou tvrdí niečo, čo je nepravda — vymýšľa citácie, zákony, fakty. Pre compliance kľúčové riziko. Výstup AI treba vždy overovať ľudským okom. **Kľúčová otázka:** Máme nastavený proces, kto a ako overuje výstupy AI pred ich použitím?

HIGH-RISK AI

Podľa EU AI Act: AI systémy v oblastiach ako HR (nábor), úvery, zdravotníctvo, kritická infraštruktúra. Podliehajú prísnejším požiadavkám na transparentnosť a audit. **Kľúčová otázka:** Vieme, ktoré naše AI systémy podliehajú prísnejšej regulácii podľa EU AI Act?

HUMAN IN THE LOOP

Princíp, že pri dôležitých rozhodnutiach musí byť v procese ľudský dohľad — AI navrhuje, človek schvaľuje. Regulačný štandard pre high-risk AI systémy. **Kľúčová otázka:** Máme definované, pri ktorých rozhodnutiach musí byť vždy prítomný človek?

IAM (IDENTITY AND ACCESS MANAGEMENT)

Systém riadenia toho, kto má prístup k akým systémom a dátam. „Princíp minimálnych oprávnení“: každý má prístup len k tomu, čo skutočne potrebuje. Základ firemnej bezpečnosti. **Kľúčová otázka:** Vieme v reálnom čase, kto má prístup k akým systémom — a odoberiete prístup okamžite pri odchode zamestnanca?

KYBERBEZPEČNOSŤ (CYBERSECURITY)

Ochrana digitálnych systémov, sietí a dát pred neoprávneným prístupom a útokmi. V ére AI sa kyber útoky stávajú sofistikovanejšími — a compliance musí držať krok s IT. **Kľúčová otázka:** Kedy sme naposledy testovali odolnosť našich systémov voči útoku?

LARGE LANGUAGE MODEL (LLM)

Model trénovaný na obrovskom množstve textu, ktorý vie generovať, prekladať a analyzovať jazyk. ChatGPT, Claude, Gemini sú príklady LLM. **Kľúčová otázka:** Vieme, aké dáta LLM, ktoré používame, vidí a či ich dodávateľ využíva na ďalší tréning?

MACHINE LEARNING (ML) / STROJOVÉ UČENIE

AI sa neučí z pravidiel napísaných programátorom, ale z dát. Čím viac dát, tým „inteligentnejší“ model. Pozor: učí sa aj zo zlých a zaujatých dát. **Kľúčová otázka:** Monitorujeme výkonnosť ML modelov v čase — a vieme, kedy a prečo sa ich výstupy menia?

MFA (MULTI-FACTOR AUTHENTICATION) / VIACFAKTOROVÉ OVERENIE

Prihlásenie vyžadujúce viac než len heslo — napr. heslo + kód z telefónu. Základný bezpečnostný štandard. Ak vaša firma MFA nepoužíva, je to zraniteľnosť, ktorú regulátor nezanedbá. **Kľúčová otázka:** Je viacfaktorové overenie povinné pre všetkých zamestnancov, vrátane manažmentu?

MODEL RISK MANAGEMENT (MRM)

Riadenie rizík spojených s AI/ML modelmi — ich validácia, monitoring a dokumentácia. Dlhoročný štandard v bankovníctve, ktorý sa rozširuje do ďalších odvetví. **Kľúčová otázka:** Máme zdokumentované, validované a monitorované všetky modely, ktoré ovplyvňujú naše rozhodovanie?

NEURÓNOVÁ SIEŤ (NEURAL NETWORK)

Matematická štruktúra inšpirovaná ľudským mozgom, ktorá tvorí základ modernej AI. Spracúva dáta vo vrstvách a učí sa rozpoznávať vzory. **Kľúčová otázka:** Ak rozhodnutie urobila neurónová sieť, vieme ho napadnúť alebo revidovať?

NIS2 (NETWORK AND INFORMATION SECURITY DIRECTIVE 2)

Európska smernica o kybernetickej bezpečnosti účinná od 2024. Rozširuje povinnosti na širší okruh firiem vrátane dodávateľských reťazcov. Compliance a IT musia spolupracovať — toto nie je len IT záležitosť. **Kľúčová otázka:** Sme si istí, že naša firma — a naši kľúčoví dodávatelia — spĺňajú požiadavky NIS2?

NLP (NATURAL LANGUAGE PROCESSING)

Oblasť AI zameraná na porozumenie a generovanie ľudského jazyka. Základ chatbotov, automatického prekladu či analýzy dokumentov. **Kľúčová otázka:** Ak systém číta a vyhodnocuje texty (zmluvy, sťažnosti, e-maily), vieme, čo s nimi robí a kde sa ukladajú?

OPEN SOURCE AI

AI modely a kód voľne dostupné na použitie, úpravu a distribúciu (napr. Meta Llama). Nižšie náklady, ale vyššia zodpovednosť — bezpečnosť a regulačný súlad nikto iný za vás nekontroluje. **Kľúčová otázka:** Ak používame open source AI, kto u nás zodpovedá za jej bezpečnosť a aktualizácie?

PHISHING

Podvodný pokus získať citlivé údaje (heslá, prístupy) prostredníctvom falošných e-mailov alebo webstránok. S AI sa phishingové útoky stávajú presvedčivejšími a ťažšie odhaliteľnými. **Kľúčová otázka:** Kedy sme naposledy testovali, koľko percent zamestnancov klikne na phishingový e-mail?

PRIVACY BY DESIGN

Princíp, že ochrana súkromia musí byť zabudovaná do systémov od začiatku — nie pridaná dodatočne. Požiadavka GDPR aj EU AI Act. Opak: „zabezpečíme to neskôr“ — čo zvyčajne nenastane. **Kľúčová otázka:** Je ochrana osobných údajov súčasťou každého nového projektu od začiatku, nie až po spustení?

PROMPT / PROMPTOVANIE

Pokyn alebo otázka, ktorú zadáte AI. Kvalita odpovede závisí od kvality promptu — preto existuje „prompt engineering“ ako samostatná odbornosť. **Kľúčová otázka:** Vieme, aké informácie naši zamestnanci vkladajú do AI nástrojov pri každodennej práci?

RAG (RETRIEVAL-AUGMENTED GENERATION)

AI, ktorá pred odpoveďou vyhľadá relevantné dokumenty z internej databázy — nie len zo svojho tréningu. Vhodné na „naučenie“ AI firemných smerníc a interných dát. **Kľúčová otázka:** Ak AI pracuje s našimi internými dokumentmi, vieme, ktoré dokumenty vidí a či sú aktuálne?

RANSOMWARE

Škodlivý softvér, ktorý zašifruje firemné dáta a žiada výkupné za ich odomknutie. Jeden z najčastejších a najnákladnejších kybernetických útokov. Prevencia: zálohy, MFA, školenia. **Kľúčová otázka:** Máme otestovaný plán obnovy — a vieme, za koľko hodín by sme obnovili prevádzku po útoku?

RPA (ROBOTIC PROCESS AUTOMATION)

Softvéroví „roboti“, ktorí automatizujú opakujúce sa manuálne úlohy (napr. spracovanie faktúr, kopírovanie dát medzi systémami). Predchodca AI agentov — menej inteligentný, ale overený a predvídateľný. **Kľúčová otázka:** Máme prehľad o všetkých softvérových robotoch v prevádzke a kto ich spravuje?

SAAS (SOFTWARE AS A SERVICE)

Softvér, ku ktorému pristupujete cez prehliadač a platíte predplatné — bez inštalácie. Salesforce, Microsoft 365, väčšina AI nástrojov. Dáta sú u dodávateľa. **Kľúčová otázka:** Máme zmapované všetky SaaS nástroje, ktoré zamestnanci používajú — vrátane tých bez súhlasu IT?

SHADOW AI

Zamestnanci používajú AI nástroje bez vedomia IT a compliance — napr. kopírujú citlivé dáta do ChatGPT. Jedno z najväčších skrytých rizík dnes v každej firme. **Kľúčová otázka:** Vieme, ktoré AI nástroje zamestnanci používajú bez vedomia firmy?

TOKENIZÁCIA (TOKENIZATION)

V AI: rozkladanie textu na menšie jednotky (tokeny), s ktorými model pracuje. V bezpečnosti: nahradenie citlivých údajov nečitateľným identifikátorom. Jeden termín, dve použitia — vždy sa opýtajte, ktoré. **Kľúčová otázka:** Sú naše najcitlivejšie dáta (napr. osobné údaje klientov) tokenizované — teda nečitateľné bez kľúča?

VENDOR LOCK-IN

Situácia, keď ste natoľko závislí od jedného dodávateľa, že prechod by bol extrémne nákladný. Dôležité zvažovať pri výbere AI nástrojov a cloudových platforiem. **Kľúčová otázka:** Ak by sme zajtra museli opustiť nášho kľúčového technologického dodávateľa, čo by to stálo?

ZERO TRUST

Bezpečnostný model, ktorý predpokladá, že nikto — ani interný zamestnanec — nie je automaticky dôveryhodný. Každý prístup sa overuje. Opak starého modelu: „vnútri firewallu = bezpečné“. **Kľúčová otázka:** Overujeme identitu a oprávnenia každého prístupu k systémom — aj interného?

G. Lehnert
LAWYERS WITH INTEGRITY

G. Lehnert, s. r. o.
Budova ORBIS, Rajská 7, SK-811 08 Bratislava
lehnert@lehnert.sk | www.lehnert.sk