

WORKSHOPY

Materiály a dokumentácia



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

OPIS

Workshopy vznikli s ambíciou priblížiť zložité právne, technologické a etické otázky spôsobom, ktorý je zrozumiteľný, no zároveň si zachováva odbornú poctivosť. Cieľom workshopov nie je zjednodušovať realitu digitálneho sveta, ale vysvetliť ju v súvislostiach, ktoré umožnia čitateľovi lepšie porozumieť vlastnému postaveniu v kybernetickom priestore. Právo tu nevystupuje ako abstraktný systém pravidiel, ale ako nástroj, ktorý má pomáhať chrániť jednotlivca aj spoločnosť pred rizikami spojenými s technologickým pokrokom.

Z historického hľadiska je vývoj kybernetickej bezpečnosti úzko spätý s rozvojom našej spoločnosti. Pôvodne decentralizovaná a relatívne dôveryhodná sieť sa postupne transformovala na globálnu infraštruktúru s obrovskou koncentráciou dát a moci. Tento vývoj priniesol nielen nové príležitosti, ale aj nové formy zraniteľnosti. Kybernetické útoky sa stali nástrojom ekonomickej kriminality, politického nátlaku aj hybridných konfliktov. Právo na túto realitu reaguje postupne, často ex post, čo kladie vysoké nároky na jeho adaptabilitu a schopnosť predvídať budúce riziká.

Kybernetická bezpečnosť sa v súčasnosti stala jednou z kľúčových tém moderného práva, verejnej politiky aj každodenného života jednotlivcov. Digitálna transformácia spoločnosti spôsobila, že informačné technológie a sieťové systémy prenikli do takmer všetkých oblastí fungovania štátu, hospodárstva aj súkromnej sféry. Kybernetický priestor už dávno nie je len technickým prostredím určeným pre odborníkov, ale stal sa miestom, kde sa realizujú základné ľudské práva, ekonomické aktivity, verejná správa aj sociálne vzťahy. Hoci ide o prostredie nehmotné a bez geografických hraníc, jeho dôsledky sú veľmi konkrétne a reálne. Útok na informačný systém môže viesť k finančným stratám, ohrozeniu súkromia, narušeniu poskytovania verejných služieb alebo dokonca k ohrozeniu základných funkcií štátu. Kybernetická bezpečnosť preto predstavuje súbor opatrení, ktorých cieľom je zabezpečiť, aby informačné systémy a údaje zostali dôverné, presné a dostupné aj v podmienkach rastúcich hrozieb. Práve preto je nevyhnutné, aby otázky kybernetickej bezpečnosti neboli vnímané výlučne ako technický problém, ale ako komplexná spoločenská a právna výzva, ktorej porozumenie musí byť prístupné aj širokej verejnosti. Osobitný dôraz sa preto kladie na vzdelávanie a prevenciu. Kybernetická bezpečnosť nie je stav, ale proces, ktorý si vyžaduje neustále prispôbovanie sa novým hrozbám. Vzdelávanie širokej verejnosti zohráva v tomto

procesu kľúčovú úlohu. Informovaný používateľ je menej zraniteľný a dokáže aktívne prispieť k ochrane digitálneho prostredia.

V tomto prostredí zohráva čoraz významnejšiu úlohu umelá inteligencia. Otázky kybernetickej bezpečnosti a umelej inteligencie už dávno presiahli rámec odborných diskusií a stali sa súčasťou každodenného života. Digitálne technológie ovplyvňujú spôsob, akým ľudia komunikujú, pracujú, vzdelávajú sa a uplatňujú svoje práva. Zároveň však vytvárajú nové riziká, ktoré nemožno účinne riešiť bez základného porozumenia ich právnym a spoločenským súvislostiam. Umelá inteligencia predstavuje technológiu, ktorá umožňuje strojom vykonávať činnosti, ktoré boli tradične spájané s ľudskou inteligenciou, ako je učenie sa zo skúseností, rozpoznávanie vzorcov, rozhodovanie alebo spracúvanie jazyka.

Kybernetická bezpečnosť v ére umelej inteligencie patrí medzi najvýznamnejšie výzvy súčasnej spoločnosti, pretože sa dotýka samotných základov fungovania moderného štátu, hospodárstva aj každodenného života jednotlivcov. Právo sa v tomto kontexte ocitá pred náročnou úlohou. Musí reagovať na technologický vývoj, ktorý je rýchlejší než tradičné legislatívne procesy, a zároveň chrániť základné hodnoty demokratickej spoločnosti. Kybernetická bezpečnosť sa tak stáva priestorom, kde sa prelínajú prvky verejného práva, súkromnoprávnej zodpovednosti, ústavnoprávnej ochrany základných práv a etických princípov. Ide o oblasť, v ktorej už nepostačuje len represívne pôsobenie práva, ale čoraz väčší význam nadobúdajú preventívne a vzdelávacie nástroje.

Z právneho hľadiska je dôležité zdôrazniť, že umelá inteligencia nie je autonómnym subjektom práva, ale nástrojom vytvoreným človekom, za ktorého vývoj, nasadenie a používanie nesú zodpovednosť konkrétne fyzické alebo právnické osoby. V oblasti kybernetickej bezpečnosti sa umelá inteligencia často prezentuje ako nevyhnutná odpoveď na rastúcu komplexnosť hrozieb. Automatizované systémy dokážu analyzovať správanie používateľov, sieťovú komunikáciu či systémové logy v rozsahu, ktorý ďaleko presahuje ľudské možnosti. Táto technologická výhoda však zároveň posúva hranice zásahov do súkromia a vyvoláva otázku primeranosti. Právo tu musí hľadať rovnováhu medzi legitímnym cieľom ochrany bezpečnosti a ochranou individuálnych práv, čo je jedna z najnáročnejších úloh súčasnej regulácie. Napriek tomu však jej schopnosti zásadne menia spôsob, akým sa pristupuje ku kybernetickej bezpečnosti. Umelá inteligencia zásadne mení tradičné predstavy o kontrole, predvídateľnosti a zodpovednosti v digitálnom prostredí.



Algoritmické systémy sú schopné autonómne sa učiť a optimalizovať svoje správanie, čo znižuje mieru priameho ľudského zásahu. Z právneho hľadiska to vyvoláva otázky, ktoré presahujú klasické kategórie zavinenia a príčinnej súvislosti.

Na jednej strane sa umelá inteligencia stáva mimoriadne účinným nástrojom ochrany. Vďaka schopnosti analyzovať obrovské množstvo dát v reálnom čase dokáže identifikovať neobvyklé správanie v sieťovej prevádzke, predvídať potenciálne útoky a automatizovať reakcie na bezpečnostné incidenty. To výrazne zvyšuje rýchlosť a efektívnosť obrany, najmä v prostredí, kde ľudský faktor už nestačí reagovať na komplexnosť a dynamiku hrozieb. Umelá inteligencia tak prispieva k posilneniu odolnosti informačných systémov a k znižovaniu rizika rozsiahlych bezpečnostných incidentov.

Na druhej strane však umelá inteligencia prináša aj nové riziká. Rovnaké technológie, ktoré možno využiť na obranu, môžu byť zneužitú na útok. Generatívne systémy umelej inteligencie umožňujú vytvárať mimoriadne presvedčivé podvodné správy, falošné audiovizuálne záznamy či automatizované útoky, ktoré sú pre bežného používateľa len ťažko rozpoznateľné. Zvyšuje sa tým miera neistoty a narúša sa dôvera v digitálne prostredie. Právna otázka zodpovednosti za škody spôsobené takýmito technológiami sa tak dostáva do popredia a stáva sa predmetom intenzívnej odbornej diskusie. Právny rámec kybernetickej bezpečnosti reaguje na tieto výzvy prostredníctvom kombinácie preventívnych povinností, regulačných mechanizmov a sankčných nástrojov. Na európskej úrovni sa vytvára jednotný prístup, ktorý kladie dôraz na riadenie rizík, oznamovanie bezpečnostných incidentov a posilňovanie spolupráce medzi verejným a súkromným sektorom. Národné právne poriadky tieto princípy implementujú do konkrétnych povinností pre orgány verejnej moci, podnikateľské subjekty aj ďalšie organizácie. Dôležité však je, že právne dôsledky kybernetickej bezpečnosti sa nevyhýbajú ani jednotlivcom, ktorí môžu svojím nezodpovedným správaním prispieť k vzniku bezpečnostného incidentu. Významnou témou je aj otázka zodpovednosti. V prostredí, kde rozhodnutia prijímajú komplexné algoritmické systémy, sa tradičné právne koncepty stretávajú s novými výzvami. Kto nesie zodpovednosť za škodu spôsobenú autonómnym systémom? Ako rozdeliť zodpovednosť medzi vývojára, prevádzkovateľa a používateľa? Vedecko-populárna publikácia umožňuje tieto otázky vysvetliť bez zbytočného formalizmu, pričom poukazuje na aktuálne trendy v právnej teórii aj legislatívnom vývoji.

Osobitnú pozornosť si zasluhujú etické aspekty využívania umelej inteligencie v oblasti bezpečnosti. Automatizované rozhodovanie, masové spracúvanie údajov a prediktívne systémy



vyvolávajú otázky ochrany súkromia, spravodlivosti a transparentnosti. Ak má byť dôvera verejnosti v digitálne technológie zachovaná, je nevyhnutné, aby používanie umelej inteligencie rešpektovalo základné práva a slobody jednotlivca. Právo v tomto kontexte neplní len represívnu funkciu, ale má aj normatívnu a hodnotovú úlohu, keď stanovuje hranice technologického rozvoja. V spleti právnych predpisov, technických štandardov a etických princípov môže byť orientácia v oblasti kybernetickej bezpečnosti pre bežného používateľa mimoriadne náročná. Práve tu nachádza svoje uplatnenie právny dizajn ako moderný prístup, ktorý sa snaží sprístupniť právo jeho adresátom. Právny dizajn možno chápať ako most medzi abstraktným normatívnym svetom práva a každodennou skúsenosťou jeho adresátov.

Právny dizajn predstavuje moderný prístup k právu, ktorý vychádza z presvedčenia, že právne normy a pravidlá nemajú byť len formálne správne, ale aj zrozumiteľné, použiteľné a orientované na človeka, ktorému sú určené. V tradičnom ponímaní je právo často sprostredkované prostredníctvom jazyka a štruktúr, ktoré sú pre širokú verejnosť ťažko prístupné. Zložité formulácie, technické pojmy a abstraktné konštrukcie môžu viesť k tomu, že adresáti práva jeho obsah nepochopia, prípadne ho vnímajú ako vzdialený a neosobný systém, s ktorým nemajú reálny kontakt. Právny dizajn sa snaží tento stav prekonať tým, že kladie dôraz na spôsob, akým je právo komunikované a uplatňované v praxi.

Podstatou právneho dizajnu nie je zjednodušovanie práva na úkor jeho presnosti, ale hľadanie takých foriem a nástrojov, ktoré umožnia lepšie porozumenie jeho zmyslu a účelu. Ide o proces, v ktorom sa právo prekladá do jazyka každodennej skúsenosti bez toho, aby stratilo svoju normatívnu silu. V oblasti kybernetickej bezpečnosti má tento prístup mimoriadny význam, pretože ide o oblasť, kde sa právne pravidlá stretávajú s technicky zložitým a rýchlo sa meniacim prostredím. Ak má právna regulácia v digitálnom priestore fungovať, jej adresáti musia rozumieť nielen tomu, čo sa od nich vyžaduje, ale aj prečo sú tieto požiadavky dôležité.

Význam právneho dizajnu spočíva v jeho schopnosti prepájať právne normy s reálnym správaním jednotlivcov. Právo je v tomto ponímaní vnímané nie ako súbor príkazov a zákazov, ale ako nástroj, ktorý má podporovať zodpovedné rozhodovanie a bezpečné správanie. V kontexte kybernetickej bezpečnosti to znamená vytvárať právne informácie a pravidlá tak, aby jednotlivcom pomáhali lepšie sa orientovať v digitálnom prostredí, rozpoznávať riziká a predchádzať škodám. Právny dizajn tak prispieva k prevencii a posilňovaniu celkovej digitálnej odolnosti spoločnosti.



Osobitne dôležité je uplatnenie právneho dizajnu vo vzdelávacích aktivitách určených širokej verejnosti. Workshop ako forma vzdelávania vytvára priestor, v ktorom možno princípy právneho dizajnu uplatniť v plnej miere. Umožňuje overovať zrozumiteľnosť právnych informácií v priamom kontakte s účastníkmi a reagovať na ich otázky, skúsenosti a nejasnosti. Právny dizajn sa tu neprejavuje len v obsahu výkladu, ale aj v jeho štruktúre, spôsobe prezentácie a vo výbere príkladov, ktoré vychádzajú z reálnych situácií digitálneho života.

V rámci workshopu právny dizajn podporuje aktívne zapojenie účastníkov a posilňuje ich schopnosť aplikovať právne poznatky v praxi. Právo prestáva byť vnímané ako vzdialený a abstraktný systém a začína fungovať ako praktický nástroj orientácie v digitálnom priestore. Tento prístup je mimoriadne dôležitý najmä pre širokú verejnosť, ktorá sa s právnymi normami často stretáva bez hlbšieho porozumenia ich mechanizmom a dôsledkom.

Z dlhodobého hľadiska právny dizajn prispieva k budovaniu dôvery v právo a inštitúcie, ktoré ho vytvárajú a uplatňujú. Ak je právo komunikované zrozumiteľne a s ohľadom na potreby jeho adresátov, zvyšuje sa ochota ho rešpektovať a dodržiavať. V oblasti kybernetickej bezpečnosti a umelej inteligencie má tento aspekt zásadný význam, pretože dôvera je jedným zo základných predpokladov fungovania digitálnej spoločnosti. Právny dizajn tak zapadá do workshopového vzdelávania nielen ako doplnkový prvok, ale ako jeho koncepčný základ, ktorý prepája právo, technológie a každodennú skúsenosť jednotlivca do zrozumiteľného a funkčného celku.

Práve v tomto bode zohráva kľúčovú úlohu forma workshopu ako špecifického nástroja vzdelávania. Workshop predstavuje priestor, v ktorom sa odborný právny a technologický výklad prepája s praktickou skúsenosťou účastníkov. Na rozdiel od klasickej prednášky umožňuje aktívnu účasť, kladenie otázok a spoločnú reflexiu problémov, s ktorými sa ľudia stretávajú v každodennom digitálnom živote. Pre širokú verejnosť je tento prístup mimoriadne dôležitý, pretože umožňuje pochopiť právne pravidlá nie ako abstraktné normy, ale ako súčasť bežného správania v digitálnom priestore. Z teoretického hľadiska možno workshopové vzdelávanie chápať ako formu mäkkej regulácie, ktorá dopĺňa tradičné právne nástroje. Ide o spôsob pôsobenia práva, ktorý nestavia na sankciách, ale na porozumení, dobrovoľnom prijatí pravidiel a zodpovednosti jednotlivca. V digitálnom prostredí, kde je vynucovanie práva často obmedzené technickými a jurisdikčnými hranicami, má takýto prístup mimoriadny význam. Právo sa tu prejavuje nielen ako systém príkazov a zákazov, ale ako rámec, ktorý formuje správanie prostredníctvom vzdelávania a

kultivácie spoločenských hodnôt. Metodologický význam workshopu spočíva v prepojení teórie a praxe. Účastníci sú vedení k tomu, aby si uvedomili, ako ich vlastné rozhodnutia ovplyvňujú úroveň ich bezpečnosti a aké právne dôsledky môže mať nezodpovedné správanie. Analýza konkrétnych situácií a prípadov umožňuje lepšie pochopiť riziká spojené s používaním digitálnych technológií a umelej inteligencie. Zároveň sa tým posilňuje kritické myslenie a schopnosť rozlišovať medzi legitímnym využívaním technológií a ich potenciálnym zneužitím.

Empirická skúsenosť s workshopovým vzdelávaním ukazuje, že takýto prístup má reálne dopady na správanie účastníkov. Ľudia, ktorí lepšie rozumejú kybernetickým rizikám a právnym súvislostiam, pristupujú k digitálnym technológiám obozretnejšie, kritickejšie hodnotia informácie a sú ochotnejší meniť svoje návyky. Hoci nejde o okamžitú a úplnú zmenu správania, postupné zvyšovanie povedomia má dlhodobý pozitívny vplyv na celkovú úroveň kybernetickej bezpečnosti v spoločnosti. Tento efekt je o to významnejší, že bezpečnosť v digitálnom priestore je do veľkej miery kolektívnym javom, závislým od správania jednotlivcov. Rozmer workshopov poukazuje na ich potenciál ako stabilnej súčasti verejných politík v oblasti digitálnej bezpečnosti. Ich ukotvenie v akademickom prostredí alebo v spolupráci s verejnými inštitúciami zvyšuje dôveryhodnosť obsahu a umožňuje systematické vyhodnocovanie ich prínosov. Zároveň vytvára priestor na prepojenie výskumu, výučby a praxe, čím sa zabezpečuje, že vzdelávacie aktivity reagujú na aktuálne výzvy technologického vývoja.

Pre širokú verejnosť majú takéto workshopy význam nielen ako zdroj informácií, ale aj ako priestor na dialóg o budúcnosti digitálnej spoločnosti. Umožňujú ľuďom lepšie porozumieť úlohe práva v regulácii technológií a posilňujú ich schopnosť aktívne sa zapájať do verejnej diskusie. Kybernetická bezpečnosť a umelá inteligencia sa tak prestávajú javiť ako témy vyhradené úzkemu okruhu odborníkov a stávajú sa súčasťou širšieho spoločenského vedomia. Dlhodobý prínos workshopového vzdelávania spočíva aj v jeho schopnosti podporovať kritické myslenie. V prostredí presýtenom informáciami, automatizovanými rozhodnutiami a rýchlo sa meniacimi technológiami je schopnosť kriticky hodnotiť digitálny obsah jednou zo základných kompetencií.

Záverom možno konštatovať, že kybernetická bezpečnosť v ére umelej inteligencie predstavuje komplexnú výzvu, ktorú nemožno riešiť izolovane ani výlučne prostredníctvom právnych noriem. Ide o oblasť, v ktorej sa stretávajú technológie, právo, etika a spoločenské správanie, pričom každá z týchto rovín má zásadný vplyv na celkový výsledok. Ak má byť digitálne prostredie bezpečné a dôveryhodné, je nevyhnutné vnímať ho ako spoločný priestor zodpovednosti, v ktorom má svoje

miesto štát, odborná verejnosť aj jednotlivci. Práve vzájomná interakcia týchto aktérov určuje mieru odolnosti spoločnosti voči kybernetickým hrozbám a schopnosť reagovať na technologické zmeny, ktoré prináša rozvoj umelej inteligencie. Právo v tomto kontexte neplní len úlohu formálneho regulátora, ale stáva sa súčasťou širšieho spoločenského procesu, ktorého cieľom je vytvárať rámec pre bezpečné a zodpovedné používanie digitálnych technológií. Jeho účinnosť však závisí od miery porozumenia a prijatia zo strany jeho adresátov. Bez aktívnej účasti verejnosti a bez rozvoja právneho a digitálneho povedomia zostávajú aj najprecíznejšie právne normy len čiastočne funkčné. Z tohto pohľadu je zrejmé, že kybernetická bezpečnosť nemôže byť dosiahnutá len prostredníctvom sankcií a povinností, ale vyžaduje si systematickú prevenciu a vzdelávanie. Ak má byť technologický pokrok vnímaný ako legitímny a prospešný, musí byť sprevádzaný dôverou, že jeho využívanie podlieha jasným pravidlám a hodnotovým hraniciam. Práve tu sa ukazuje význam prepojenia právnej regulácie s verejnou diskusiou. Spoločnosť, ktorá rozumie digitálnym rizikám, dokáže ich lepšie predvídať a zvládať ich dôsledky. Vzdelávanie, otvorená komunikácia a zrozumiteľné sprostredkovanie právnych pravidiel zohrávajú v tomto procese kľúčovú úlohu. Posilňujú schopnosť jednotlivcov orientovať sa v digitálnom prostredí a zároveň prispievajú k stabilite a dôveryhodnosti inštitúcií.

V konečnom dôsledku možno povedať, že workshopy zamerané na kybernetickú bezpečnosť, umelú inteligenciu a právny dizajn predstavujú dôležitý nástroj budovania spoločenskej odolnosti. Umožňujú postupne vytvárať prostredie, v ktorom sú technológie vnímané nielen ako zdroj efektivity, ale aj ako oblasť vyžadujúca zodpovednosť a reflexiu. Informovaní a digitálne gramotní občania sú lepšie pripravení zapájať sa do diskusie o regulácii technológií, o hraniciach využívania umelej inteligencie a o ochrane základných práv v digitálnom priestore. Kybernetická bezpečnosť sa tak stáva nielen technickou a právnou otázkou, ale aj súčasťou verejnej debaty o smerovaní modernej spoločnosti. Práve prostredníctvom takéhoto prístupu je možné smerovať k digitálnemu priestoru, ktorý bude nielen inovatívny, ale aj bezpečný, spravodlivý a dôveryhodný pre všetkých jeho používateľov.