KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BLOKOVANIE V KYBERNETICKEJ BEZPEČNOSTI

Meno a priezvisko

XX.XX.XXXX

KCKB UPJS CSIRT UPJS

OBSAH

1) Všeobecne o blokovaní
2) Zásah do základných práv a slobôd
3) Riziká spojené s blokovaním
4) Blokovanie v kontexte autorských práv
5) Blokovanie podľa zákona o hazardných hrách
6) Blokovanie na úrovni vládnej siete GOVNET
7) Blokovanie podľa zákona o kybernetickej bezpečnosti

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VŠEOBECNE O BLOKOVANÍ

BLOKOVANIE

- blokovanie webových stránok možno definovať ako **opatrenie, ktorým oprávnený subjekt (najčastejšie súd alebo správny orgán) uloží poskytovateľovi internetovej siete, prípadne inému sprostredkovateľovi pripojenia, povinnosť technickými prostriedkami znemožniť prístup používateľov k určitému obsahu;** podstata spočíva v prerušení dátového toku medzi koncovým používateľom a serverom, na ktorom sa nachádza obsah, ktorý má byť zneprístupnený (Mesarčík, Právny obzor 6/2025)

BLOKOVANIE PODĽA ROZSAHU ZÁSAHU

1) **PLOŠNÉ**
   - zneprístupnenie celej domény alebo IP adresy bez ohľadu na to, či je celý obsah nezákonný
2) **CIELENÉ**
   - zameranie sa na konkrétny nezákonný obsah (napr. konkrétna URL), čím sa minimalizuje riziku nadmerného blokovania

METÓDY BLOKOVANIA

1) **STATICKÉ**
   - statické blokovanie sa opiera o zoznam konkrétnych identifikátorov (IP adresa, názov domény, URL), ktoré sa aktualizuje manuálne
   - jednoduchý, predvídateľný mechanizmus, ktorý je však málo flexibilný pri rýchlo sa meniacom obsahu
2) **DYNAMICKÉ**
   - dynamické blokovanie umožňuje automatizované rozširovanie blokovaného obsahu na nové „zrkadlové“ weby alebo subdomény, ktoré vzniknú po zablokovaní pôvodného zdroja
   - najmä pri nelegálnom streamovaní

BLOKOVACIE TECHNIKY

- Blokovanie domén druhej úrovne na úrovni správcu TLD
- Blokovanie konkrétnych doménových mien na úrovni ISP
- Blokovanie IP adresných rozsahov pomocou BGP
- Blokovanie IP adresných rozsahov pomocou firewallových pravidiel
- Blokovanie IP, protokolu a portu pomocou firewallových pravidiel
- Blokovanie IP adresných rozsahov, domén, URL a mailových adries publikovaním zoznamu, bez udania spôsobu blokovania
- Blokovanie konkrétnych URL na webových serveroch
- Blokovanie konkrétnych URL na proxy serveroch
- Blokovanie prístupu koncového uzlu, resp. používateľa
- Blokovanie prostriedkami endpoint security (firewall, antivírus, antimalware a podobne)
- Blokovanie e-mailového účtu na príslušnom poštovom serveri
- Blokovanie e-mailovej adresy na relay serveroch a iných poštových serveroch

PRÍKLADY

Štát	Blokovanie	Objekt blokovania
Argentína	Áno	hazardné hry, zločiny, drogy, zbrane, UBER - ako ilegálna forma dopravy
Arménsko	Nie	
Austrália	Áno	porušenia autorských práv
Bangladéš	Áno	pornografia, hazardné hry, nelegálny obchod so zbraňami a drogami, zločiny, politické dôvody, nenávistné a diskriminačné prejavy, zásahy do súkromia
Belgicko	Áno	každý obsah, ktorý je pri vyšetrovaní verejnej autority vyhodnotený ako ilegálny
Brazília	Áno	zločiny, drogy, zbrane, phishing, ohrozovanie detí
Česká republika	Áno	hazardné hry bez povolenia
Estónsko	Áno	hazardné hry, iné ilegálne aktivity môžu byť blokované pomocou DNS podľa uváženia registra, ak je takáto aktivita nahlásená verejnými orgánmi na presadzovanie práva alebo CERTom
Filipíny	Áno	pornografia, najmä detská pornografia
Francúzsko	Áno	obhajovanie, schvaľovanie a nabádanie k terorizmu, detská pornografia
Holandsko	Áno	porušovanie autorských práv
Izrael	Áno	pornografia, pedofília

PRÍKLADY

Štát	Blokovanie	Objekt blokovania
India	Áno	pornografia, hazardné hry, zločiny, drogy, zbrane, porušovanie hospodárskej súťaže, porušovanie autorských práv, politické dôvody, nenávistné a diskriminačné prejavy, čokoľvek, čo nariadi súd
Južná Kórea	Áno	pornografia, hazardné hry, zločiny, drogy, zbrane, porušovanie autorských práv, zásahy do súkromia, politické dôvody, nenávistné a diskriminačné prejavy
Kanada	Nie	
Litva	Áno	hazardné hry
Lotyšsko	Áno	hazardné hry, nelicencované online televízie, objekty súvisiace s bezpečnosťou informačných technológií
Nemecko	Áno	porušovanie autorských práv
Nórsko	Áno	pornografia, porušovanie autorských práv
Poľsko	Áno	hazardné hry
Slovinsko	Áno	hazardné hry, daňové úniky
Švédsko	Nie	
Veľká Británia	Áno	pornografia - blokované sú pornografické stránky, ktoré neobsahujú overenie veku používateľov, takisto sú blokované stránky s detskou pornografiou, porušovanie autorských práv, zásahy do súkromia

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ZÁSAH DO ZÁKLADNÝCH PRÁV A SLOBÔD

SLOBODA PREJAVU

Čl. 10 Dohovoru o ochrane ľudských práv a základných slobôd

Sloboda prejavu

1. Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov a bez ohľadu na hranice. Tento článok nebráni štátom, aby vyžadovali udeľovanie povolení rozhlasovým, televíznym alebo filmovým spoločnostiam.
2. Výkon týchto slobôd, pretože zahŕňa povinnosti aj zodpovednosť, môže podliehať takým formalitám, podmienkam, obmedzeniam alebo sankciám, ktoré stanovuje zákon, a ktoré sú nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, územnej celistvosti alebo verejnej bezpečnosti, na predchádzanie nepokojom alebo zločinnosti, ochranu zdravia alebo morálky, ochranu povesti alebo práv iných, zabránenia úniku dôverných informácií alebo zachovania autority a nestrannosti súdnej moci.

Článok 11 Charty základných práv Európskej únie

Sloboda prejavu a právo na informácie

1. Každý má právo na slobodu prejavu. Toto právo zahŕňa slobodu zastávať názory a prijímať a rozširovať informácie a myšlienky bez zasahovania orgánov verejnej moci a bez ohľadu na hranice.
2. Rešpektuje sa sloboda a pluralita médií.

Článok 26 Ústavy Slovenskej republiky

1. Sloboda prejavu a právo na informácie sú zaručené.
2. Každý má právo vyjadrovať svoje názory slovom, písmom, tlačou, obrazom alebo iným spôsobom, ako aj slobodne vyhľadávať, prijímať a rozširovať idey a informácie bez ohľadu na hranice štátu. Vydávanie tlače nepodlieha povoľovaciemu konaniu. Podnikanie v odbore rozhlasu a televízie sa môže viazať na povolenie štátu. Podmienky ustanoví zákon.
3. Cenzúra sa zakazuje.
4. Slobodu prejavu a právo vyhľadávať a šíriť informácie možno obmedziť zákonom, ak ide o opatrenia v demokratickej spoločnosti nevyhnutné na ochranu práv a slobôd iných, bezpečnosť štátu, verejného poriadku, ochranu verejného zdravia a mravnosti.
5. Orgány verejnej moci majú povinnosť primeraným spôsobom poskytovať informácie o svojej činnosti v štátnom jazyku. Podmienky a spôsob vykonania ustanoví zákon.

BLOKOVANIE

- blokovanie obsahu predstavuje zásah do základných práv a slobôd jednotlivca, najmä do jeho **slobody prejavu a práva na informácie**
- obmedzenie týchto základných práv a slobôd je **prípustné, ale podmienené splnením určitých predpokladov**
  1. **právny základ v aplikovateľnej právnej úprave**
  2. **sledovanie legitímneho cieľa**
  3. **reagovanie na naliehavú spoločenskú potrebu**
  4. **dodržanie zásady proporcionality**
  5. **záruky proti zneužitiu v podobe notifikácie vopred, rovnosti zbraní, transparentnosti a nezávislého dohľadu**
     - **rovnosť zbraní -** blokovaný subjekt by mal mať k dispozícii nástroje, ktorým môže blokovanie efektívne zvrátiť resp. dať preskúmať nezávislému orgánu

ESĽP: Ahmet Yildrim v. Turecko

Skutkový stav vo veci:

- Sťažovateľ vlastní a prevádzkuje webové sídlo, na ktorom zverejňuje rôzne dokumenty týkajúce sa jeho akademickej práce
- toto webové sídlo bolo vytvorené pr. služby Google Sites
- prvostupňový súd v trestnej veci nariadil blokovanie iného webového sídla (neodkladné opatrenie) (v r. 2009)
- neskôr tento súd nariadil blokovanie prístupu k službe Google Sites ako takej
- v dôsledku uvedeného stratil Sťažovateľ prístup k svojmu webovému sídlu, ktoré nemalo žiadny súvis s webovým sídlom, ktoré malo byť blokované v dôsledku jeho nezákonného obsahu
- Sťažovateľ sa obrátil na príslušné súdy so žiadosťou o zastavenie blokovania, jeho žiadostiam nebolo vyhovené
- Sťažovateľ sa nedokázal prihlásiť na svoje webové sídlo ani v r. 2012, a to aj napriek tomu, že trestné konanie v pôvodnej veci bolo zastavené už v marci 2011

ESĽP: Ahmet Yildrim v. Turecko

Právne posúdenie ⇨ porušenie čl. 10 Dohovoru:

- blokovanie pôvodného webového sídla, na ktorom sa nachádzal nezákonný obsah, bolo zákonné
- to ale neplatilo vo vzťahu k webovému sídlu Sťažovateľa alebo službe Google Sites ako takej, voči ktorým neboli začaté žiadne súdne konania pre nezákonnosť obsahu
- vnútroštátne právo neposkytovalo právny základ pre blokovanie prístupu k službe ako takej, a to napriek tomu, že bolo možné založiť zodpovednosť poskytovateľa tejto služby za nezákonnosť obsahu, ktorý hosťovala
- neexistovala ani informácia o tom, že by Google Sites bola informovaná o tom, že hosťuje nezákonný obsah, alebo o tom, že odmietla konať v súlade s neodkladným opatrením týkajúcim sa webového sídla, ktoré bolo predmetom trestného konania
- vnútroštátna úprava udeľovala Telekomunikačnému úradu rozsiahle právomoci týkajúce sa blokovania, nakoľko tento úrad mohol požiadať o predĺženie rozsahu pôsobnosti príkazu napriek absencii akéhokoľvek konania v súvislosti s webovou stránkou alebo doménou, a nebola preukázaná žiadna skutočná potreba takéhoto rozsiahleho blokovania
- také rozsiahle blokovanie spôsobilo nedostupnosť veľkého množstva informácií, podstatne obmedzujúc práva používateľov internetu

ESĽP: CENGIZ A INÍ v. TURECKO

Skutkový stav vo veci:

- v r. 2008 súd uložil príkaz plošného blokovania stránky YouTube z dôvodu, že obsah 10 stránok na tejto platforme porušoval zákaz urážky pamiatky Ataturka
- Sťažovatelia, aktívni používatelia platformy, namietli toto rozhodnutie
- právna úprava, na ktorej bolo súdne rozhodnutie založené, bola na základe skutkového stavu prípadu zmenená tak, aby umožňovala vydanie všeobecného príkazu na zablokovanie celej internetovej stránky a nielen sporného obsahu

ESĽP: CENGIZ A INÍ v. TURECKO

Právne posúdenie ⇨ porušenie čl. 10 Dohovoru:

- pôvodná právna úprava platná v čase uloženia príkazu neumožňovala vydanie príkazu na plošné blokovanie celej webovej stránky z dôvodu prítomnosti nezákonného obsahu na niektorej zo stránok, ktoré hosťovala
- príkaz na blokovanie mohol byť uložený iba s ohľadom na konkrétny obsah, ak existovalo dôvodné podozrenie, že predstavuje trestný čin
- uvedený príkaz tak nespĺňal požiadavku zákonnosti

ESĽP: OOO FLAVUS v. RUSKO

Skutkový stav vo veci:

- Sťažovatelia na svojich stránkach publikovali rôzne správy a komentáre, poskytovali priestor pre blogy a analýzy týkajúce sa spoločenských a politických otázok, pričom množstvo z nich bolo kritických k ruskej vláde
- v r. 2013 bol novelizovaný ruský informačný zákon, ktorý umožnil generálnemu prokurátorovi označovať webové stránky, ktoré obsahovali známky podnecovania k masovým nepokojom, extrémistické činnosti alebo účasť na nepovolených zhromaždeniach, a to **bez súdneho príkazu**
- generálny prokurátor mohol podať **návrh na zablokovanie webovej stránky** Telekomunikačnému úradu, ktorý následne informoval poskytovateľa webhostingu pre danú stránku, ktorý prístup k webstránke zablokoval a o uvedenom informoval jej vlastníkov
- vo vzťahu k sťažovateľom došlo k plošnému zablokovaniu ich webových stránok z dôvodu, že dielčie stránky nachádzajúce sa na týchto doménach boli označené ako podnecujúce k extrémistickým aktivitám (podpora protestov, kritika obsadenia Krymu)

ESĽP: OOO FLAVUS v. RUSKO

Právne posúdenie ⇨ porušenie čl. 10 Dohovoru:

- opatrenie, ktoré znemožnilo používateľom prístup na stránky Sťažovateľov, predstavovalo **zásah orgánu verejnej moci do práva prijímať a rozširovať informácie,** nakoľko čl. 10 Dohovoru chráni právo rozširovať informácie ako aj právo verejnosti tieto informácie prijímať
- **k zákonnosti:**
  - právna úprava vyžadovala, aby oznámenie Telekomunikačného úradu odkazovalo na URL adresu konkrétnej webovej stránky za účelom možnosti identifikácie nezákonného obsahu
  - oznámenie v prípade sťažovateľov však odkazovalo iba všeobecne na webovú doménu, nešpecifikovalo konkrétnu problematickú webovú stránku
  - to sťažovateľom neumožnilo určenie problematického obsahu a znemožnilo im napraviť domnelé porušenie odstránením protiprávneho obsahu
  - tým, že ruské orgány neuviedli URL adresu dielčích webových stránok, ktoré považovali za nezákonné, jednali svojvoľne, čím sťažovateľom zabránili v informovanej voľbe medzi odstránením alebo zmenou konkrétneho obsahu a formulovaním námietky proti návrhu generálneho prokurátora

ESĽP: OOO FLAVUS v. RUSKO

Právne posúdenie ⇨ porušenie čl. 10 Dohovoru:

- **k legitímnemu cieľu a nevyhnutnosti v demokratickej spoločnosti**
  - vnútroštátne orgány nepostupovali podľa zákona, tzn. **nenaplnili podmienku zákonnosti**
  - keďže však došlo k zablokovaniu celých webových stránok sťažovateľov, ESĽP sa rozhodol preskúmať, či tieto zásahy sledovali legitímny cieľ a boli nevyhnutné v demokratickej spoločnosti
  - ESĽP zdôraznil, že **plošné zablokovanie celého webu predstavuje extrémne opatrenie**, ktoré možno prirovnať k zákazu publikačnej činnosti novín nebo vysielaniu televíznych staníc; takéto plošné opatrenie zámerne stiera rozdiely medzi zákonnými a nezákonnými informáciami, ktoré webová stránka obsahuje, a zamedzuje prístup i k obsahu, ktorý nebol identifikovaný ako nezákonný (*Ahmet Yıldırım proti Turecku*)
  - podľa ESĽP tak rozhodnutie o plošnom blokovaní webových stránok bolo založené na falošných dôvodoch či priamo ľubovôli

ESĽP: OOO FLAVUS v. RUSKO

Právne posúdenie ⇨ porušenie čl. 10 Dohovoru:

- **k legitímnemu cieľu a nevyhnutnosti v demokratickej spoločnosti**
  - aj keby existovali výnimočné okolnosti odôvodňujúce blokovanie nelegálneho obsahu, znemožnenie prístupu na celé webové stránky musí byť zdôvodnené samostatne, zvlášť a oddelene od odôvodnenia pôvodného zákazu smerujúceho voči nezákonnému obsahu a s odkazom na kritériá stanovené ESĽP
  - blokovanie prístupu k legálnemu obsahu nikdy nemôže byť automatickým dôsledkom iného širšieho opatrenia, ako tomu bolo v tomto prípade
  - tzn. **v prípade nebol sledovaný legitímny cieľ**

ESĽP: OOO FLAVUS v. RUSKO

Právne posúdenie ⇨ porušenie čl. 10 Dohovoru:

- **k zárukám proti zneužitiu:**
  - opatrenia prijaté pred vydaním súdneho rozhodnutia predstavujú predbežné obmedzenia publikovania, ktoré si vyžadujú čo najopatrnejší prieskum zo strany ESĽP a sú odôvodnené iba za výnimočných okolností
  - podmienkou je právna úprava, ktorá zabezpečuje **prísnu kontrolu nad rozsahom zákazu a účinný súdny prieskum**
  - podľa ESĽP ruská právna úprava neposkytovala sťažovateľom **žiadne procesné záruky**, ktorými by ich ochránila pred svojvoľným zásahom podľa informačného zákona
    - právna úprava nepočítala so žiadnou účasťou vlastníkov webu v konaní o jeho zablokovaní
    - všetky opatrenia boli prijaté bez predchádzajúceho upozornenia sťažovateľov
    - nevyžadovalo sa posúdenie dopadov opatrenia ani odôvodnenie ich neodkladnosti
    - blokovanie nebolo schválené súdom ani iným nezávislým súdnym orgánom
    - nevyžadovalo sa odôvodnenie nutnosti a primeranosti zásahu do slobody prejavu alebo zváženie, či by nebolo možné rovnaký cieľ dosiahnuť aj inými, menej obmedzujúcimi prostriedkami

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

RIZIKÁ SPOJENÉ S BLOKOVANÍM

RIZIKO VZNIKU ŠKÔD

1) **blokovaním prístupu na IP adresu dochádza k zamedzeniu prístupu k všetkým službám, ktoré sú na danej IP adrese prevádzkované**
   - napr. blokovanie IP adresy webového servera nutne spôsobí znefunkčnenie iných webových stránok, ktoré zdieľajú tú istú IP adresu
   - napr. blokovanie IP adresy alebo domény veľkého portálu alebo cloudovej služby môže znefunkčniť e-mailovú komunikáciu pre všetkých klientov
2) **spôsobenie škody subjektu, ktorý nie je priamo zodpovedný za infraštruktúru šíriacu škodlivý obsah**
   - napr. prevádzkovateľ služby web hostingu zablokuje prístup na stránky svojho zákazníka a zákazník nezaplatí poplatok za dané obdobie na základe nedodania objednanej služby

ĎALŠIE RIZIKÁ

1) **blokovaním dôjde k znefunkčneniu služieb, ktoré majú dopad na život, zdravie a majetok občanov**
   - napr. znefunkčnenie tiesňovej linky prevádzkovanej cez IP telefóniu
   - napr. znefunkčnenie bezpečnostných systémov - kamera, senzor, alarm
2) **blokovanie je nastavené príliš široko**
   - pri blokovaní celého prístupu na doménu druhej úrovne budú zneprístupnené všetky URL, ktoré daná doména poskytuje, ako aj iné typy služieb ako služba, ktorá má byť zablokovaná
3) **nesprávne alebo neoprávnené blokovanie**
   - niektoré udalosti vyhodnotené ako útok môžu byť v skutočnosti objednané penetračné testy alebo plošné skenovanie národného kybernetického priestoru bezpečnostnými výskumníkmi, ktorí sa snažia identifikovať problémy za účelom informovania a lepšej ochrany koncových používateľov; tieto prípady nie je možné systematicky odlíšiť od skutočnej škodlivej aktivity, pretože blokovanie ako také nie je automatizovanou činnosťou a rozhodnutie vykonáva človek, môže dôjsť k zablokovaniu takého obsahu, ktorý nie je škodlivý - napríklad preklep v názve domény, blokovanie inej IP z dôvodu omylu v číslach a podobne
4) **jednoduché obchádzanie blokovania** - dobre motivovaný útočník dokáže nájsť spôsob ako obísť blokovaciu techniku a škodlivý obsah šíriť ďalej

ĎALŠIE RIZIKÁ

5) neželaná podpora používateľov v hľadaní spôsobov ako blokovanie obísť

- pri blokovaní obsahu, ktorý je používateľmi žiadaný, je možné predpokladať rozširovanie využitia anonymizačných služieb, čo má z dlhodobého hľadiska negatívny dopad na schopnosť chrániť používateľov pred škodlivým obsahom

6) blokovanie neodstraňuje škodlivý obsah

- to, že IP adresa alebo doména so škodlivým obsahom budú zablokované nerieši reálnu existenciu tohto obsahu a potrebu jeho odstránenia

7) **strata dôvery v transparentnosť a slobodu**

- používatelia môžu vnímať zablokovanie, aj keď škodlivého obsahu, ako narušenie slobody internetu alebo svojich vlastných osobných slobôd

8) **možné narušenie súkromia**

- niektoré spôsoby blokovania si vyžadujú zásah alebo nazeranie do prenášaných informácií používateľov, čo zvyšuje riziko narušenia súkromia a slobody používateľov na internete

Z PRAVIDIEL BLOKOVANIA NBÚ:

Zamedzenie prístupu k škodlivému obsahu alebo na doménu, ktorá šíri škodlivý obsah, však nemožno považovať za zásah do práv a slobôd občanov, ale za nevyhnutné kroky, ktoré zamedzujú týmto používateľom prístup k obsahu, ktorý by im mohol škodiť alebo priamo škodí.

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BLOKOVANIE V KONTEXTE AUTORSKÝCH PRÁV

PRÁVNY ZÁKLAD PRE ULOŽENIE SÚDNYCH PRÍKAZOV *(INJUNCTIONS)*

Čl. 8 ods. 3 Smernice 2001/29/ES o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti (InfoSoc Directive):

*„Členské štáty zabezpečia, aby nositelia práv mali možnosť žiadať o **súdny zákaz** proti sprostredkovateľom, ktorých služby využívajú tretie strany na porušovanie autorského práva alebo s ním súvisiaceho práva.“*

Čl. 11 Smernice 2004/48/ES z 29. apríla 2004 o vymožiteľnosti práv duševného vlastníctva

*Členské štáty zabezpečia, aby v prípade, ak bolo prijaté súdne rozhodnutie vyslovujúce porušenia práva duševného vlastníctva, mohli súdne orgány vydať proti porušovateľovi **súdny príkaz** zakazujúci ďalšie porušovanie. Ak to umožňuje vnútroštátne právo, za nedodržanie príkazu možno v prípade v prípade potreby opakovane uložiť pokutu, aby sa zabezpečilo jeho dodržiavanie. Členské štáty tiež zabezpečia, aby vlastníci práv mali možnosť navrhnúť vydanie súdneho príkazu proti sprostredkovateľom, ktorých služby využíva tretia strana na porušovanie práva duševného vlastníctva; tým nie je dotknutý článok 8 ods. 3 smernice 2001/29/ES.*

POVAHA CHRÁNENÝCH PRÁV

- oprávnenie nositeľov práv požiadať o uloženie súdneho zákazu proti sprostredkovateľom, ktorých služby sú využívané tretími stranami **za účelom porušovania autorského práva**
- konkrétne porušovanie **práva verejného prenosu a práva sprístupňovania predmetov ochrany verejnosti** ⇨ autori majú „*výlučné právo udeliť súhlas alebo zakázať akýkoľvek verejný prenos ich diel, či po drôte alebo bezdrôtovými prostriedkami vrátane sprístupňovania ich diel verejnosti takým spôsobom, aby verejnosť k nim mala prístup z miesta a v čase, ktoré si sama zvolí.*“

VEREJNÝ PRENOS

- predpoklady:
  1) **prenos diela** (*act of communication of a work*)
     - súhlas autora sa vyžaduje pre každý prenos diela
     - na splnenie predpokladu postačuje sprístupnenie diela verejnosti takým spôsobom, ktorý umožňuje získanie prístupu k dielu verejnosťou, bez ohľadu na to, či verejnosť túto možnosť skutočne využije alebo nie
     - extenzívny výklad – v zásade každý akt, ktorým používateľ poskytne pri plnej znalosti veci prístup svojim zákazníkom k chráneným dielam
  2) **verejný prenos diela** (*communication of a work to a public*)

OBMEDZENIA

1) potreba **nájdenia spravodlivej rovnováhy** medzi právom nositeľov práv na ochranu ich duševného vlastníctva a právom iných strán dotknutých takýmto zákazom (sloboda podnikania, sloboda prejavu a právo na informácie, ochrana osobných údajov)
2) podľa čl. 3 Smernice 2004/48/ES musia byť prijaté opatrenia, postupy a prostriedky právnej nápravy:
   a) **spravodlivé a nestranné**
   b) **nesmú byť zbytočne zložité alebo nákladné alebo mať za následok príliš dlhé lehoty alebo neoprávnené prieťahy**
   c) **účinné, primerané a odradzujúce**
   d) **musia sa uplatňovať takým spôsobom, aby sa predišlo vytváraniu prekážok zákonného obchodu**
   e) **musia stanovovať záruky proti ich zneužívaniu**
3) **súlad s princípom proporcionality -** čl. 52 ods. 1 Charty základných práv EÚ pripúšťa obmedzenia práv a slobôd vymedzených v charte iba v prípade, „*ak je to nevyhnutné a skutočne to zodpovedá cieľom všeobecného záujmu, ktoré sú uznané Úniou, alebo ak je to potrebné na ochranu práv a slobôd iných*.“

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

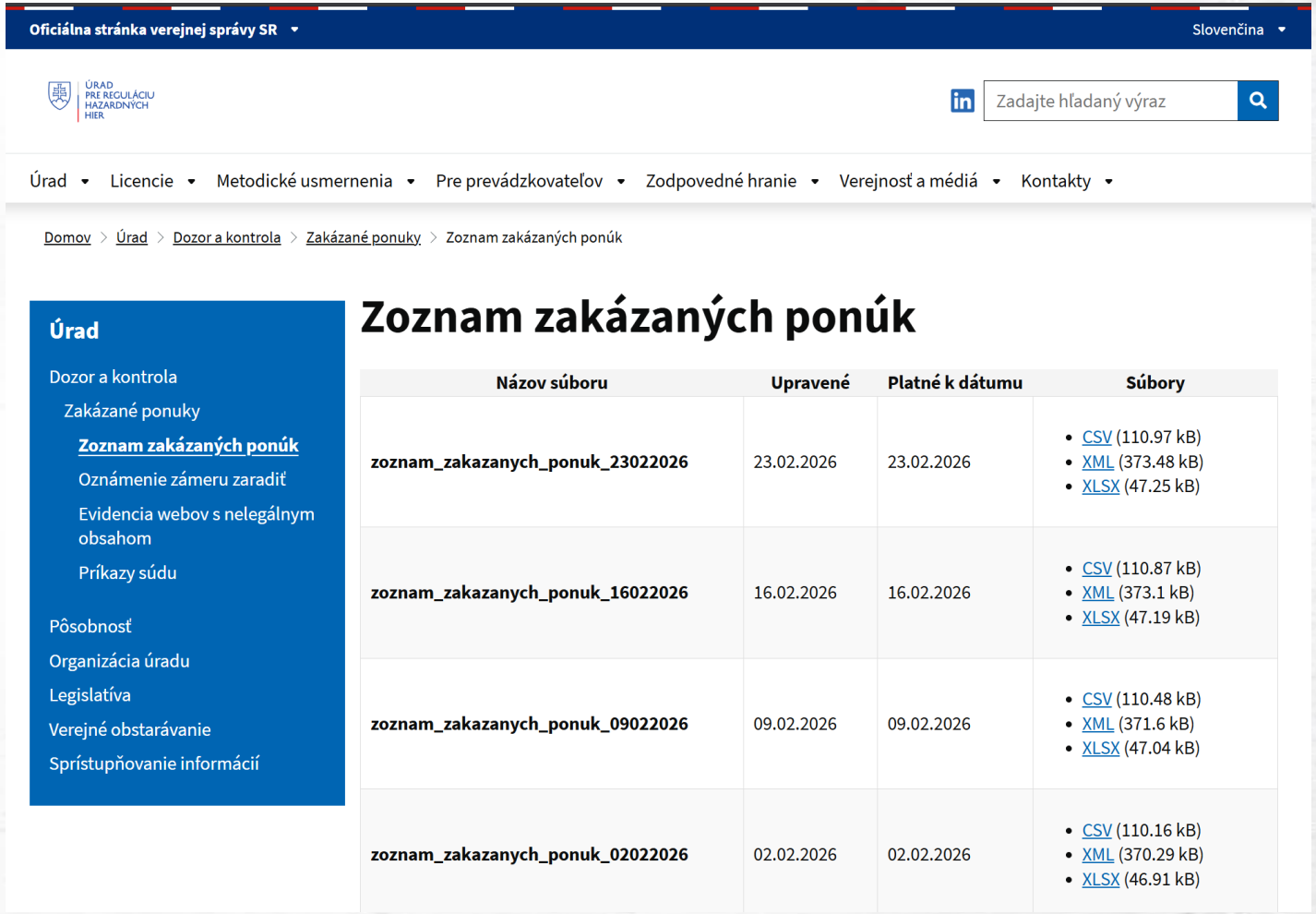
BLOKOVANIE PODĽA ZÁKONA O HAZARDNÝCH HRÁCH

POSKYTOVANIE ZAKÁZANEJ PONUKY

- § 2 písm. aa) ZoHH - poskytovaním zakázanej ponuky sa rozumie **prevádzkovanie hazardnej hry alebo propagovanie hazardnej hry dostupnej na území Slovenskej republiky bez licencie** v latinskej abecede a v latinkovom systéme písma **prostredníctvom elektronickej komunikačnej siete alebo elektronickej komunikačnej služby** vrátane nabádania a podnecovania k využívaniu takých nástrojov a prostriedkov umožňujúcich prístup k účasti na takejto hazardnej hre, ktoré obchádzajú geografickú blokáciu a iné zamedzenia uskutočnené zo strany prevádzkovateľa takejto hazardnej hry alebo ktoré obchádzajú zamedzenia prístupu k webovému sídlu uskutočnené zo strany poskytovateľa elektronických komunikačných sietí a elektronických komunikačných služieb,
  - **geografická blokácia** = také zamedzenie prístupu k webovému sídlu, ktoré neumožňuje prístup k webovému sídlu z územia SR
  - hazardná hra dostupná na území SR = hazardná hra, na ktorej sa možno zúčastniť na území alebo z územia SR najmä zaplatením vkladu, uskutočnením stávky alebo vyplatením výhry

ZOZNAM ZAKÁZANÝCH PONÚK

- dozor vykonáva **Úrad pre reguláciu hazardných hier**, ktorý
  1. vyhľadáva prípady poskytovania zakázaných ponúk
  2. zostavuje, aktualizuje a zverejňuje **zoznam zakázaných webových sídiel** a mobilných aplikácií, prostredníctvom ktorých sú poskytované zakázané ponuky (obsahové náležitosti - § 85 ods. 3 ZOHH)



BLOKOVANIE PODĽA ZoHH

- **právny základ blokovania:** § 85 ZoHH
- § 85 ods. 12 ZoHH ukladá:
  a) osobe, ktorá poskytuje elektronické komunikačné siete a elektronické komunikačné služby, **povinnosť** na základe zoznamu zakázaných ponúk **zamedziť prístup k webovému sídlu**, ktoré je zapísané v zozname zakázaných ponúk a prostredníctvom ktorého sa poskytuje zakázaná ponuka
  b) poskytovateľovi platobných služieb **povinnosť** na základe zoznamu zakázaných ponúk **zamedziť vykonaniu platobnej operácie alebo inej platobnej služby v prospech účtu, ktorý je zapísaný v zozname zakázaných ponúk** a ktorý používa osoba poskytujúca zakázanú ponuku na účely prijímania vkladu pri poskytovaní zakázanej ponuky a vo vzťahu k obchodníkovi, ak sa na účely prijímania vkladu pri poskytovaní zakázanej ponuky uskutočňujú platobné transakcie prostredníctvom obchodníka
- využíva sa technika **blokovania konkrétnych doménových mien na úrovni ISP**
- nesplnenie povinnosti = **iný správny delikt** ⇨ možnosť uloženia pokuty vo výške 10 000 – 500 tisíc € právnickej osobe, ktorá je dozorovaným subjektom

BLOKOVANIE PODĽA ZoHH

- do 1. januára 2026 sa na vznik povinností podľa § 85 ods. 12 ZoHH vyžadoval aj **príkaz súdu** vydaný na základe žiadosti Úradu pre reguláciu hazardných hier
  - proti príkazom súdov **nebol prípustný opravný prostriedok**
  - táto požiadavka bola novelou ZoHH **vypustená**

https://www.urhh.sk/urad/dozor-a-kontrola/zakazane-ponuky/prikazy-sudu/

ECLI:SK:KSBA:2025:1025200511.1
IČS:1025200511.1
sp. zn. 4Ntn/23/2025

P R Í K A Z

Krajský súd v Bratislave, sudcom JUDr. Erikom Tomusom, vo veci žiadosti Úradu pre reguláciu hazardných hier č. URHH/004343/2025-171, 080419/2025, doručenej dňa 27.10.2025, dňa 03. novembra 2025 takto

r o z h o d o l :

Podľa § 85 ods. 8, ods. 11 zákona č. 30/2019 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

p r i k a z u j e m

zamedziť prístup k webovému sídlu

https://www.coincasino.com

prostredníctvom ktorého je osobám poskytujúcim elektronické komunikačné siete a elektronické komunikačné služby, poskytovaná zakázaná ponuka, ktorou je podľa § 2 písm. aa) zákona č. 30/2019 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, konkrétne v rozsahu dostupnosti internetových stránok prevádzkovaných pod doménou coincasino.com z územia Slovenskej republiky vrátane všetkých príslušných domén nižšej úrovne, a to subjektom:

P.č.	Názov	Ulica	Mesto	PSČ	IČO
1	111, s.r.o.	Dolné Rudiny 3/2956	Žilina	010 01	36407208
2	3 Start s.r.o.	Obrancov mieru 3173/13	Detva	962 12	44133634
3	3GPS s.r.o.	Vinné 5162	Vinné	072 31	47472201
4	3LOG tech s.r.o.	Andreja Kmeťa 2082/7	Michalovce	071 01	46759204
5	3net s.r.o.	Horská 1314/38	Partizánske	958 06	47916699

PROCESNÉ ASPEKTY

- povinnosť **zverejniť** na webovom sídle Úradu **oznámenie o zámere** zaradiť webové sídlo do zoznamu zakázaných ponúk
  - musí obsahovať poučenie o možnosti podať námietku proti zápisu (najneskôr do 10 dní od zverejnenia oznámenia)
- povinnosť odoslať elektronickou poštou dozorovanému subjektu **výzvu na ukončenie poskytovania zakázanej ponuky** (lehota 10 dní od odoslania výzvy)
  - bez výzvy, ak elektronická adresa nie je uvedená (najskôr po uplynutí 10 dní odo dňa zverejnenia oznámenia)
  - výzva musí obsahovať upozornenie na dôsledky neukončenia poskytovania zakázanej ponuky

PROCESNÉ ASPEKTY

- Úrad nezaradí do zoznamu zakázaných ponúk alebo vyradí zo zoznamu zakázaných ponúk webové sídlo alebo mobilnú aplikáciu, ak
  a) dozorovaný subjekt preukáže, že neposkytuje zakázanú ponuku
  b) dozorovaný subjekt preukáže, že poskytovanie zakázanej ponuky ukončil alebo
  c) pominuli dôvody pre zápis údajov do zoznamu zakázaných ponúk

POSKYTOVATEĽ PLATOBNÝCH SLUŽIEB

- je povinný poskytnúť Úradu podklady na výkon dozoru, a to **identifikáciu používateľa platobných služieb** a **ďalšie informácie o používateľovi platobných služieb**, ktorý je dozorovaným subjektom

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BLOKOVANIE NA ÚROVNI VLÁDNEJ SIETE GOVNET

BLOKOVANIE NA ÚROVNI VLÁDNEJ SIETE GOVNET

- blokovanie škodlivého obsahu a indikátorov kompromitácie (IP adresy, domény, e-mailové adresy a podobne) prebieha aj na úrovni vládnej siete GOVNET, ktorú má v správe Národná agentúra pre sieťové a elektronické služby (NASES)
- blokovanie je zamerané **výlučne na ochranu vládnej siete a jej používateľov** pred škodlivým obsahom a útokmi a prebieha na základe zistení z bezpečnostného monitoringu, ktorý vykonávajú jednotky CSIRT v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu
- na základe výstupov a odporúčaní tejto CSIRT jednotky sú jednotlivé škodlivé indikátory alebo obsah zablokované len na úrovni vládnej siete a ovplyvňujú komunikáciu z/do uzlov v sieti GOVNET
- podobné blokovanie prebieha na úrovni viacerých organizácií z rôznych sektorov

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

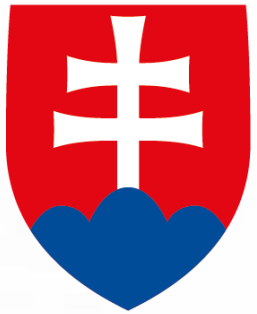
PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BLOKOVANIE PODĽA ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

PÔSOBNOSŤ

- § 5 ods. 1 písm. af) ZoKB: Národný bezpečnostný úrad (NBÚ) v oblasti KB **rozhoduje o blokovaní škodlivého obsahu alebo škodlivej aktivity, ktorá smeruje do kybernetického priestoru SR alebo z kybernetického priestoru SR (ďalej len „blokovanie“) a zabezpečuje vykonanie tohto rozhodnutia alebo vykonáva blokovanie na základe žiadosti**



NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

BLOKOVANIE PODĽA ZoKB

- § 27b ods. 1 ZoKB: **Úrad z vlastnej iniciatívy rozhoduje o blokovaní, spôsobe blokovania a vykonáva blokovanie,** ak § 27c neustanovuje inak.
- **predmet blokovania:**
  - **škodlivý obsah** ⇨ programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident
  - **škodlivá aktivita** ⇨ akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov alebo citlivých údajov, závažné dezinformácie a iné formy hybridných hrozieb

ŠKODLIVÝ OBSAH

- podľa taxonómie, ktorú používa pri klasifikácii incidentov SK-CERT (Národná jednotka CSIRT), je možné škodlivý obsah a s ním spojenú infraštruktúru rozdeliť do týchto kategórií:
  a) škodlivý kód (vírus, malvér, ransomvér)
  b) infraštruktúra, umožňujúca
     - rozosielanie nevyžiadanej pošty
     - neoprávnené získavanie informácií: skenovanie sietí, odpočúvanie, sociálne inžinierstvo, phishing
  c) podporný software, údaje a infraštruktúra umožňujúca pokusy o prienik, DoS, DDoS útoky alebo iné aktívne útoky, vrátane
     - riadiacich serverov (command and control servery)
     - uzlov siete botnet
     - obsahu, zneužívajúceho prostriedky používateľov bez ich vedomia (crypto minery)
  d) verejne prístupné citlivé údaje ako sú heslá, šifrovacie kľúče, čísla kreditných kariet, osobné údaje

DÔVODY BLOKOVANIA

Z Pravidiel blokovania vyplývajú nasledujúce dôvody blokovania:

1) **ochrana používateľov napadnutých služieb a nevedomých používateľov podvodných služieb** - ak je na šírenie škodlivého obsahu, vylákanie údajov alebo na ilegálne aktivity zneužitá legitímna doména alebo služba, zablokovanie obsahu alebo konkrétneho URL zabezpečí ochranu používateľov, ktorí túto službu alebo doménu využívajú
2) **zmiernenie alebo zamedzenie škodlivých následkov** - blokovaním domén a IP adries so škodlivým obsahom či phishingom je možné takisto dosiahnuť zmierňovanie následkov v podobe menšieho dopadu na potenciálne obete, resp. zasiahnutých používateľov. Takisto včasným blokovaním možno zabezpečiť úplné zamedzenie škodlivých následkov, pretože nemusí dôjsť napríklad k stiahnutiu škodlivého obsahu alebo k dokončeniu všetkých fáz phishingovej kampane.
3) **zastavenie šírenia škodlivého obsahu** - najmä šírenie malvéru, existenciu riadiacich serverov pre botnety, phishingové stránky a podobne. Domény a IP adresy s takýmto obsahom sú využívané útočníkmi na nelegitímne ciele a ich blokovanie zamedzuje ďalšiemu šíreniu takéhoto škodlivého obsahu.

ROZHODNUTIE O BLOKOVANÍ

- povinné minimálne obsahové náležitosti rozhodnutia (§ 27b ods. 2 ZoKB):
  a) identifikácia NBÚ
  b) identifikácia osoby, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať
  c) identifikácia škodlivého obsahu alebo škodlivej aktivity
  d) dôvod blokovania
  e) spôsob blokovania
  f) lehota na vykonanie blokovania, trvanie blokovania a možnosti jeho odblokovania
  g) poučenie
- Úrad rozhodne o spôsobe blokovania **podľa pravidiel blokovania** tak, aby bolo účinné, účelné a primerané vo vzťahu k možným rizikám spojeným s blokovaním
  - cieľom pravidiel blokovania je zaviesť pravidlá pre blokovanie útokov za účelom zvýšenia obranyschopnosti SR voči kybernetickým útokom na významné informačné systémy z externého prostredia (internetu), najmä voči šíreniu škodlivého kódu zo sietí infikovaných počítačov a šíreniu škodlivej aktivity z IP adresného rozsahu SR.
- rozhodnutím o blokovaní nie sú dotknuté postupy riešenia KBI a postupy OČTK
- je **preskúmateľné súdom; správna žaloba nemá odkladný účinok**

VYKONANIE BLOKOVANIA

- blokovanie vykonáva:
  a) **osoba, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať**
     - na základe rozhodnutia NBÚ
  b) **NBÚ**

ČASOVÁ LIMITÁCIA

- § 27b ZoKB: Rozhodnúť o blokovaní škodlivého obsahu alebo škodlivej aktivity možno **len s platnosťou do 30. septembra 2022.**
- **zoznam blokovaných subjektov:**

Blokované webové sídllo (URL)	Rozhodnutie prijaté na základe	Dôvod	Účinnosť do
hlavnespravy.sk	§ 27b ZoKB	škodlivá aktivita	30.6.2022
armadnymagazin.sk	§ 27b ZoKB	škodlivá aktivita	30.6.2022
hlavnydennik.sk	§ 27b ZoKB	škodlivá aktivita	30.6.2022
infovojna.bz	§ 27b ZoKB	škodlivá aktivita	30.6.2022

Zoznam blokovaných subjektov

Momentálne nie je v platnosti žiadne rozhodnutie o blokovaní v zmysle zákona o kybernetickej bezpečnosti.

POSÚDENIE PRÁVNEJ ÚPRAVY BLOKOVANIA V ZoKB

Požiadavka	Právna úprava v ZoKB
Zákonný základ	Čiastočne existuje, avšak detaily blokovania sú ponechané na iný právny akt.
Legitímny cieľ	Existuje, avšak je nedostatočne odôvodnený.
Naliehavá spoločenská pot reba	Existuje.
Proporcionalita	Čiastočne §27b (4) a § 27c (5) vyžadujúce účinné, účelné a primerané vykonani e blokovania.
Notifikácia vopred	Nie je upravená.
Rovnosť zbraní	Nie je upravená.
Transparentnosť	Nie je upravená.
Nezávislý dohľad	Nie je upravený.

(Zdroj: Mesarčík, Právny obzor 6/2025)

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

laura.rozenfeldova@upjs.sk

https://cyberawareness.sk