**Dôvodová správa**

1. ***Všeobecná časť***

Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov predkladajú do Národnej rady Slovenskej republiky poslanci za politickú stranu Kotlebovci – Ľudová strana Naše Slovensko Marian Kotleba, Martin Beluský a Peter Krupa.

**Predložený návrh zákona má za cieľ odstrániť zneužiteľnosť nedemokratického nástroja blokovania informácií, ktorý bol delegovaný Národnému bezpečnostnému úradu SR novelou zákona prijatého vo februári 2022 Národnou radou Slovenskej republiky.**

Situácia na východnej hranici Slovenska si vyžiadala nutnosť urýchleného prijatia viacerých zákonov v skrátenom legislatívnom konaní, ktoré boli prijaté v balíku pod názvom návrh zákona o niektorých opatreniach v súvislosti so situáciou na Ukrajine. Vojna prirodzene vyústila do masovej migrácie cudzincov aj na naše územie. V dôsledku toho bolo potrebné realizovať opatrenia hospodárskej mobilizácie, a to najmä vecné plnenia s ohľadom na potrebu zabezpečenia ubytovania cudzincov, organizáciu dopravného zabezpečenia, organizáciu zdravotníckeho zabezpečenia a podobne. Tak isto sa umožnilo vláde Slovenskej republiky vyhlásiť poskytovanie dočasného útočiska aj bez rozhodnutia Rady Európskej únie.

V skrátenom legislatívnom konaní bola však prijatá aj novela zákona o kybernetickej bezpečnosti, ktorej cieľom malo byť zamedziť šíreniu škodlivého obsahu na internete prostredníctvom nového inštitútu „blokovania“. V ňom sa za škodlivú aktivitu zadefinovalo aj šírenie závažných dezinformácií a iné forma hybridnej vojny.

Pritom 29. júna 2021 bola v Národnej rade Slovenskej republiky schválená novela zákona o kybernetickej bezpečnosti, v ktorej na návrh koaličných poslancov bol inštitút blokovania vyradený. Tento zákona s parlamentnou tlačou 441 prešiel riadnym medzirezortným pripomienkovým konaním a bol schválený aj legislatívnou radou vlády. Výsledkom konsenzu sa v tomto zákone škodlivá aktivita definovala ako akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, ako podvodná činnosť, odcudzenie osobných údajov alebo citlivých údajov.

Celospoločenskou diskusiou neprešiel návrh, aby sa ako škodlivá aktivita definovalo aj šírenie závažných dezinformácií alebo iné formy hybridnej vojny. Bez riadnej odbornej diskusie a jasnej definície vznikol v právnom poriadku Slovenskej republiky inštitút a nástroj, ktorý by sa dal jednoducho politicky zneužiť. Súčasná vládna koalícia tak do právneho poriadku zaviedla precedens, podľa ktorého si môže ktokoľvek, kto bude aktuálne pri moci, zadefinovať šírenie závažných dezinformácií podľa svojho úsudku a zablokovať tak kritické alebo znepriatelené médiá.

Ako argument neprejde ani fakt, že inštitút blokovania je možné využiť podľa súčasne platného zákona do 30. júna 2022. Obnovenie tohto inštitútu bude na rozhodnutí vládnej koalícii, a tá si ho bude môcť aktivovať jednoduchou novelou zákona o kybernetickej bezpečnosti.

Inštitút blokovania ako celok by sa podľa navrhovateľov tohto zákona nemal vypnúť úplne. V pôvodnom znení návrhu zákona o niektorých opatreniach v súvislosti so situáciou na Ukrajine sa navrhovalo, aby rozhodnutie o blokovaní škodlivej aktivity, ktorou je závažná dezinformácia alebo iná forma hybridných hrozieb bolo možné len s platnosťou do 31. decembra 2022. To znemená, že sa pôvodne navrhovalo iba dočasné využívanie blokovania závažných dezinformácií a iných foriem hybridnej vojny, avšak ostatné škodlivé aktivity a škodlivý obsah by bolo možné blokovať aj naďalej. Slovensko je a bude aj naďalej vystavené kybernetickým bezpečnostným incidentom, a preto by štát prostredníctvom Národného bezpečnostného úradu SR mal mať naďalej nástroj na jeho odstránenie.

Škodlivých aktivít na internete z roka na rok pribúda. Zároveň rastie sofistikovanosť útokov a s neustále prebiehajúcou informatizáciou spoločnosti aj riziká spojené s úspešne vykonanými útokmi. Reakcie na rôzne typy škodlivých aktivít spadajú do kompetencie rôznych štátnych orgánov. Množstvo útokov je vykonávaných buď plošne (napr. phishingové kampane lákajúce veľké množstvo používateľov kliknúť na rozoslaný link), alebo na svoju činnosť využíva identifikovateľný škodlivý obsah alebo sieťovú infraštruktúru (napr. riadiace servery botnet sietí, DNS servery k nim smerujúce, zariadenia vykonávajúce DDOS útoky a pod.). Z tohto dôvodu mnohé krajiny zavádzajú legislatívne podmienky a technické prostriedky na blokovanie nežiadúceho obsahu, IP adries, domén, URL, súborov a podobne.

Blokovanie infikovaných domén a IP adries je nutné považovať za reaktívne opatrenie vedúce k zamedzeniu prístupu k škodlivému obsahu. Dôvody, prečo využiť tento prostriedok, je možné zhrnúť do niekoľkých bodov:

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 takisto možné dosiahnuť zmiernenie následkov v podobe menšieho dopadu na potenciálne obete, resp. zasiahnutých používateľov. Rovnako aj 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 - v tomto bode ide najmä o šírenie malvéru, existenciu riadiacich serverov pre botnety, phishingové stránky a pod. Domény a IP adresy s takýmto obsahom sú využívané útočníkmi na nelegitímne ciele a ich blokovanie bráni ďalšiemu šíreniu takéhoto škodlivého obsahu.

Samozrejme, ide o krajný prostriedok, nástroj, ktorý predstavuje zásah do práv subjektov, ale zároveň predstavuje aj riešenie kybernetického bezpečnostného incidentu v prípade, kedy sú iné nástroje neúčinné a protiprávna, resp. škodlivá aktivita naďalej pokračuje a ohrozuje konečného užívateľa.

Národný bezpečnostný úrad SR od prijatia novely zákona o kybernetickej bezpečnosti využil (informácia aktuálna k 31. marcu 2022) inštitút blokovania s cieľom zamedzenia šírenia závažných dezinformácií v 4 prípadoch:

|  |  |  |  |
| --- | --- | --- | --- |
| **Názov** | **Rozhodnutie podľa** | **Dôvod** | **Platnosť do** |
| hlavnespravy.sk | zákon č. 69/2018, § 27b | škodlivá aktivita | 30. 06. 2022 |
| armadnymagazin.sk | zákon č. 69/2018, § 27b | škodlivá aktivita | 30. 06. 2022 |
| hlavnydennik.sk | zákon č. 69/2018, § 27b | škodlivá aktivita | 30. 06. 2022 |
| infovojna.bz | zákon č. 69/2018, § 27b | škodlivá aktivita | 30. 06. 2022 |

 zdroj: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/zoznam-blokovanych-subjektov/index.html>

Podľa § 32 písm. j) zákona č. 69/2018 o kybernetickej bezpečnosti je NBÚ povinný ustanoviť všeobecne záväzným predpisom pravidlá blokovania. Všetky 4 weby však boli zablokované v čase, kedy ešte vyhláška NBÚ nebolo platná, čo spôsobilo problém v kontrole vykonania týchto rozhodnutí, keďže neexistovali podrobnejšie pravidlá a inštitúty, ktoré by bol NBÚ povinný využiť pred samotným blokovaním.

Vzhľadom na všetky uvedené informácie prichádzajú navrhovatelia s novelou zákona o kybernetickej bezpečnosti, ktorá zavádza nasledovné hlavné zmeny:

1. V § 3 sa pridávajú nové definície, najmä čo sa rozumie pod pojmom hybridná hrozba a závažná dezinformácia.
2. V § 27b (blokovanie) sa škodlivá aktivita definuje ako akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, ako podvodná činnosť, odcudzenie osobných údajov alebo citlivých údajov a hybridná hrozba.
3. Zavádza sa nový odsek, ktorý určuje postup NBÚ pred využitím samotného blokovania, najmä umožnenie držiteľovi alebo prevádzkovateľovi infraštruktúry odstránenie škodlivého obsahu z dotknutej domény v určenej lehote, ktorá nesmie byť kratšia ako 72 hodín.
4. Využitie inštitútu blokovania hybridnej hrozby bude možné až po súhlase vecne príslušného krajského súdu.
5. Zavádza sa povinnosť NBÚ rozhodnutie o blokovaní zverejniť na svojom webovom sídle.

Návrh zákona je v súlade s Ústavou Slovenskej republiky, ústavnými zákonmi, inými zákonmi, nálezmi Ústavného súdu Slovenskej republiky, medzinárodnými zmluvami a inými medzinárodnými dokumentmi, ktorými je Slovenská republika viazaná a s právom Európskej únie.

Prijatie návrhu zákona nebude mať žiadny vplyv na rozpočet verejnej správy, žiadny vplyv na podnikateľské prostredie, na informatizáciu spoločnosti, sociálne vplyvy, vplyvy
na životné prostredie, na služby verejnej správy pre občana a na manželstvo, rodičovstvo
a rodinu.

Účinnosť návrhu zákona sa so zohľadnením dostatočnej legisvakačnej lehoty navrhuje od 1. júla 2022.

1. ***Osobitná časť***

**Čl. I**

K bodu 1

Zavádzajú sa nové definície pojmov hybridná hrozba, závažná dezinformácia a kritická infraštruktúra, ktoré v pôvodnom zákone chýbali.

K bodu 2

Novelizuje sa § 27b a zavádzajú sa nové zmeny:

1. Škodlivá aktivita sa definuje ako akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, ako podvodná činnosť, odcudzenie osobných údajov alebo citlivých údajov a hybridná hrozba.
2. Zavádza sa nový odsek, ktorý určuje postup NBÚ pred využitím samotného blokovania, najmä umožnenie držiteľovi alebo prevádzkovateľovi infraštruktúry odstránenie škodlivého obsahu z dotknutej domény v určenej lehote, ktorá nesmie byť kratšia ako 72 hodín.
3. Využitie inštitútu blokovania hybridnej hrozby bude možné až po súhlase vecne príslušného krajského súdu.
4. Zavádza sa povinnosť NBÚ rozhodnutie o blokovaní zverejniť na svojom webovom sídle.
5. Odstraňuje sa dočasné využívanie inštitútu blokovania.

K bodu 3

 Táto zmena v § 27c súvisí s predchádzajúcou zmenou v § 27b. Tento § upravuje blokovanie na základe žiadosti iného subjektu. Spresňuje sa, ktoré odseky § 27b sa použijú primerane.

**Čl. II**

Ustanovuje sa účinnosť tohto zákona na 1. júla 2022.