

**cesnet**  
"...."

# § TADY, § TAM, § VŠUDE KAM SE PODÍVÁM

**Jan Kolouch**  
CESNET

---

**8. března 2022**

**Seminář o bezpečnosti sítí a služeb**



- **O právu...**
- **Kybernetické bezpečnosti**
  - EU scope
  - Právo
  - Reálný dopad
- **GDPR**
  - A kybernetická bezpečnost
  - Rozhodnutí soudů
- **Potírání terorismu**
- **Banu webů**
- **Černobílé slepotě**

cesnet  
"...."

# FUNKCE PRÁVA?



- **Regulace společenských vztahů** prostřednictvím právních norem
- **Prevence a řešení konfliktů**
- Trestání při porušení pravidel

**Vytváření prostředí „právní jistoty“**



- **podmínky pro to, aby** objektivní **právo bylo dlouhodobě stabilní**, jednotné, **relativně jednoduché a předvídatelné** a aby byla dodržována subjektivní práva všech.
- Nikdo nesmí být zkrácen na svých právech než způsobem stanoveným zákonem.
- Každý, kdo porušuje právní povinnosti, musí být postižen způsobem, který stanoví zákon.
- **Tím je naplňováno legitimní očekávání fyzických i právnických osob.**

\* Za tento symbol si doplňte svoji vlastní preferenci (typicky OS, app. aj.)

1. **V \* věřiti budeš.**
2. **Nepohaniš \*.**
3. **Udatuj.**
4. **Cti Google, Microsoft, Apple, Meta, \*, abys dlouho živ byl a dobře se ti vedlo v kyberprostoru.**
5. **Nezabiješ jinak než ve hře.**
6. **Nesesmilníš...offline.**
7. **Nepokradeš...Jinak si pro tebe přijde ČPU, IFPI aj.**
8. **Nepromluvíš křivého svědectví proti bližnímu svému...WTF?**
9. **Nepožádáš manželky bližního svého...Seriously? Viděli jste ty fotky a video? MILF's rules!**
10. **Aniž požádáš statku jeho. Ale ne...vlastnictví je přeceňovaný a zastaralý konstruk nefungující v digitálním prostředí. Tedy jen do okamžiku, kdy nejde o moje věci...to pak...**



# A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE

Vlády Průmyslového světa, vy znavení obři z masa a oceli, přicházím z Kyberprostoru, nového domova Mysli. **Jménem budoucnosti vás žádám, abyste nás vy, lidé minulosti, nechali na pokoji.** Nejste mezi námi vítáni. Vaše svrchovanost nesahá do míst, kde se scházíme...

...V Číně, Německu, Francii, Rusku, Singapuru, Itálii a Spojených státech se snažíte zahnat virus svobody **budováním strážných věží na hranicích Kyberprostoru.** Ty sice nákazu mohou na krátkou chvíli zadržet, jenže budou k ničemu ve světě, který brzy zaplaví bitonosná média.

Váš zastarávající informační průmysl se bude snažit upevnit svou pozici navrhováním zákonů, v Americe i jinde, podle kterých by každé slovo na celém světě bylo jejich majetkem. **Tyto zákony prohlásí všechny myšlenky jen za další průmyslový výrobek, o nic ušlechtlejší než surové železo.** V našem světě se veškeré výtvořiny lidské mysli dají neomezeně reprodukovat a šířit s nulovými náklady. Globální výměna myšlenek se teď obejde bez vašich továren...

**...V Kyberprostoru vytvoříme civilizaci Mysli. Necht' je lidštější a spravedlivější než svět, který v minulosti vytvořily vaše vlády.**

Davos, Švýcarsko 8. února 1996 BARLOW, Perry, John.

cesnet  
"...."

# KYBERNETICKÁ BEZPEČNOST A PRÁVO





**Ajay Grewal** • 3. a více  
CCIE Security#55637 | CEH  
1 týden • Upraveno

InfoSec 1990: You need AntiVirus

InfoSec 1998: You need honeypots

InfoSec 2004: You need DLP

InfoSec 2007: You need IPS/IDS

InfoSec 2010: You need behavior blocking

InfoSec 2013: You need Sandboxing , Threat extraction,  
emulation

InfoSec 2015: You need ATP/APT

InfoSec 2017: You need machine learning

The entire time: Maybe patch your stuff first? InfoSec: Nah,  
that's boring.



SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148

ze dne 6. července 2016

o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN>

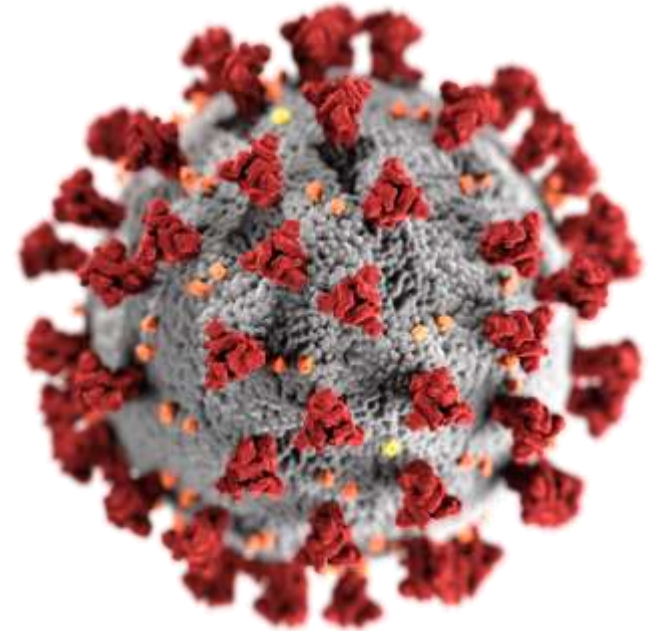
Směrnice o bezpečnosti sítí a informací:

- 1) přispěla ke zlepšení schopností v oblasti kybernetické bezpečnosti** na úrovni členských států, neboť vyžadovala, aby **členské státy přijaly národní strategie** kybernetické bezpečnosti **a určily orgány pro kybernetickou bezpečnost;**
- 2) zvýšila spolupráci členských států** na úrovni Unie zřízením různých fór usnadňujících výměnu strategických a operačních informací a
- 3) zlepšila kybernetickou odolnost veřejných a soukromých subjektů v sedmi konkrétních odvětvích** (energetika, doprava, bankovníctví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastruktura) **a ve třech oblastech digitálních služeb** (on-line tržiště, internetové vyhledávače a služby cloud computingu) tím, že požadovala, aby členské státy zajistily, že provozovatelé základních služeb a poskytovatelé digitálních služeb zavedou požadavky kybernetické bezpečnosti a budou hlásit incidenty.

Hodnocení fungování směrnice NIS, poukázalo na tyto problémy:

- 1) nízká úroveň kybernetické odolnosti podniků v EU;**
- 2) nestejná odolnost** členských států a odvětví a
- 3) nízká úroveň společného situačního povědomí** a nedostatečná společná reakce na krize.

- Digitální transformace společnosti;
- zvýšená digitalizace vnitřního trhu;
- přesun do on-line světa
- **nárůst kybernetických bezpečnostních hrozeb a útoků;**
- stále sofistikovanější útoky vycházejí z celé řady zdrojů v EU i mimo ni.



<https://cs.wikipedia.org/wiki/Covid-19>

## ■ 4 pilíře:

- **ochrana údajů,**
- **základní práva,**
- **bezpečnost a**
- **kybernetickou bezpečnost**

jako nezbytné předpoklady pro posílení společnosti díky využívání údajů.

## NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

ze dne 27. dubna 2016

o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS>



## Rozsudek SDEU C-311/18

<https://curia.europa.eu/juris/liste.jsf?num=C-311/18>

Obecné nařízení o ochraně osobních údajů (GDPR) stanoví, že **k předávání takových údajů do třetí země může dojít v zásadě jen tehdy, pokud dotyčná třetí země zajistí odpovídající úroveň ochrany těchto údajů.**

Schrems tvrdil, že právní předpisy a praxe v USA neposkytují dostatečnou ochranu před přístupem orgánů veřejné moci k osobním údajům předávaným do této země.

Soudní dvůr má za to, že **omezení ochrany osobních údajů, která plynou z vnitrostátních právních předpisů Spojených států** upravujících přístup k takovým údajům předávaným z Unie do této třetí země a jejich použití orgány veřejné moci USA a která Komise posuzovala v rozhodnutí 2016/1250, **nejsou upravena takovým způsobem, aby odpovídala požadavkům, které jsou v zásadě rovnocenné požadavkům vyžadovaným v unijním právu zásadou proporcionality, protože sledovací programy prováděné na základě těchto předpisů se neomezují na to, co je nezbytně nutné.**

Doporučení: **Rozsudek SDEU C-311/18 (Schrems II)** a jeho důsledky (<https://www.uoou.cz/rozsudek-sdeu-c-311-18-schrems-ii-a-jeho-dusledky/ds-6338>)

- Začátek: 2020
- **Uživatel...**
- stránka věnující se zdravotnictví...
- skrze analytický nástroj odeslána Googlu, který tak o něm získal informace, které si uživatel nepřál předat.
- **IP adresy, cookies, reklamní identifikátory apod.** spadají pod evropskou legislativou, **lze je považovat za osobní údaje.**



### Austrian DSB: Use of Google Analytics violates "Schrems II" decision by CJEU.

In a groundbreaking decision, the Austrian Data Protection Authority ("Datenschutzbehörde" or "DSB") has decided on a model case by *noyb* that the continuous use of Google Analytics violates the GDPR. This is the first decision on the **101 model complaints** filed by *noyb* in the wake of the so-called "Schrems II" decision. In 2020, the Court of Justice (CJEU) decided that the use of US providers violates the GDPR, as US surveillance laws require US providers like Google or Facebook to provide personal details to US authorities. Similar decisions are expected in other EU member states, as regulators have cooperated on these cases in an EDPB "task force". It seems the Austrian DSB decision is the first to be issued.

<https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal>



AUTORITEIT  
PERSOONSgegevens

- AP prošetřuje **dvě stížnosti na používání Google Analytics v Nizozemsku**. Po dokončení tohoto vyšetřování, bude AP moci říci, zda je Google Analytics nyní povolena, nebo ne.
- AP se zaměřuje konkrétně na Google Analytics, protože se jedná o **nejpoužívanější analytickou službu na webových stránkách v Nizozemsku**.

Gebruikt u Google Analytics, dan verwerkt u met de analytische cookies persoonsgegevens van uw websitebezoekers. Dat heeft dus gevolgen voor hun privacy. U moet hierbij in principe zowel voldoen aan de Telecommunicatiewet (uw bezoekers informeren en om toestemming vragen) als aan de Algemene verordening gegevensbescherming (AVG).

Let op: gebruik Google Analytics mogelijk binnenkort niet toegestaan

De Oostenrijkse privacytoezichthouder rondde in januari 2022 een onderzoek af naar het gebruik van Google Analytics door een Oostenrijkse website. Google Analytics blijkt volgens de Oostenrijkse toezichthouder in dit onderzochte geval niet aan de AVG te voldoen.

De AP onderzoekt op dit moment twee klachten over het gebruik van Google Analytics in Nederland. Na afronding van dat onderzoek, begin 2022, kan de AP zeggen of Google Analytics nu is toegestaan of niet.

Google Analytics privacyvriendelijk instellen

Maar zorgt u ervoor dat de cookies geen of geringe gevolgen hebben voor de privacy van uw websitebezoekers? Dan hoeft u geen toestemming meer te vragen voor de cookies. U kunt hiervoor de Handleiding privacyvriendelijk instellen Google Analytics van de Autoriteit Persoonsgegevens (AP) gebruiken. In 6 stappen leert u hoe u Google Analytics zo instelt dat u de privacy van uw bezoekers zo goed mogelijk beschermt.

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies#hoe-kan-ik-bij-google-analytics-de-privacy-van-mijn-websitebezoekers-beschermen-4898>

- Společnost Meta Platforms znovu pohrozila, že **pokud nebude mít možnost uchovávat data uživatelů na serverech v USA, znemožní, aby lidé z Evropské unie mohli používat její služby**, jako jsou Facebook nebo Instagram.

- **Privacy shield II. ?**

- **Backup your data!**

Vypneme v Evropě Facebook, Instagram nebo WhatsApp, hrozí Zuckerberg

REDAKCE | 8. 2. 2022

PŘIDEJTE NÁZOR  



Autor: Depositphotos

<https://www.pcworld.cz/clanky/vypneme-v-evrope-facebook-instagram-nebo-whatsapp-hrozi-zuckerberg/>

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2018/1972

ze dne 11. prosince 2018,

kterou se stanoví evropský kodex pro elektronické komunikace

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32018L1972&from=CS>

- Standardně užívaný **princip opt-out**
- Novela zák. č. 127/2005 Sb., o elektronických komunikacích - **účinná od 1.1.2022**
- správci webových stránek mohou shromažďovat osobní údaje návštěvníků těchto stránek pouze na základě jejich prokazatelného souhlasu (**princip opt-in**)
- **Princip opt-in se netýká technických cookies, které jsou nezbytné pro přenos zpráv a poskytování služeb, včetně zajištění bezpečné komunikace.**
- možnost získat souhlas prostřednictvím nastavení prohlížeče, ovšem za podmínky, že souhlas splňuje požadavky obecného nařízení.

<https://www.uoou.cz/cookies-od-zacatku-roku-2022-pouze-se-souhlasem/d-53646>

<https://www.cesnet.cz/zpracovani-osobnich-udaju/cookies/>

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2019/881

ze dne 17. dubna 2019

o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“)

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32019R0881&from=EN>

cesnet  
"...."

**Co nás čeká?**





Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0823&from=EN>

- **NIS předpokládal, že některé organizace nejsou závislé na ICT**
- Současná odvětví jsou zachována a jsou **přidána odvětví další**
- **Identifikace a regulace dopadne na organizaci jako celek**, nikoli na systém, na němž je závislé fungování základní služby

NIS covered sectors



Finance



Health



Energy



Banking



Transport



Water



Digital Infrastructure



Digital Service Providers

NIS2 expanded scope



Providers of public electronic communications networks or services



Digital services such as social networking service platforms and data centre services



Waste water and waste management



Space



Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)



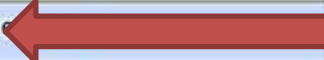
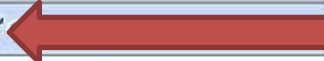
Postal and Courier Services



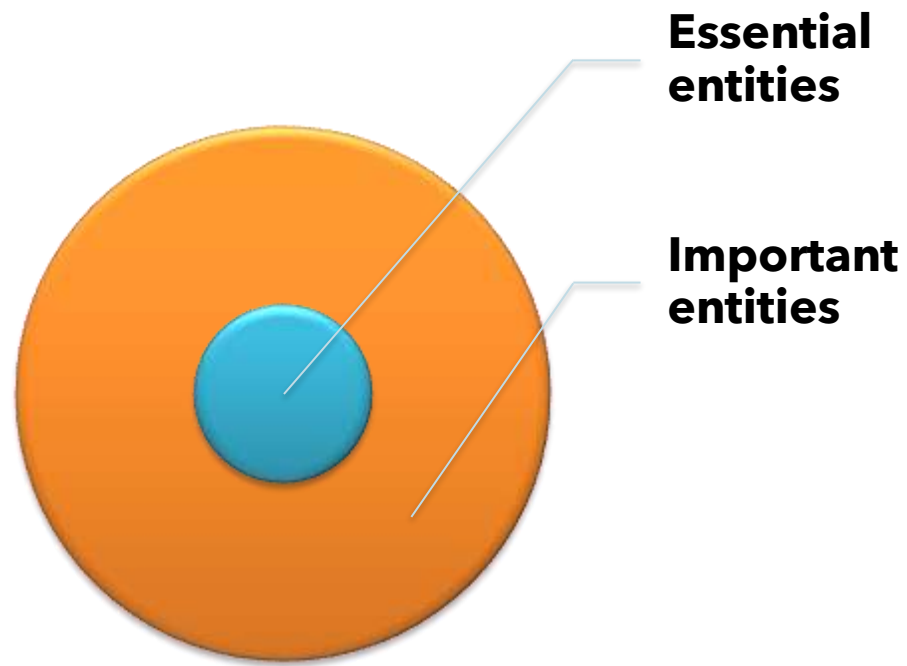
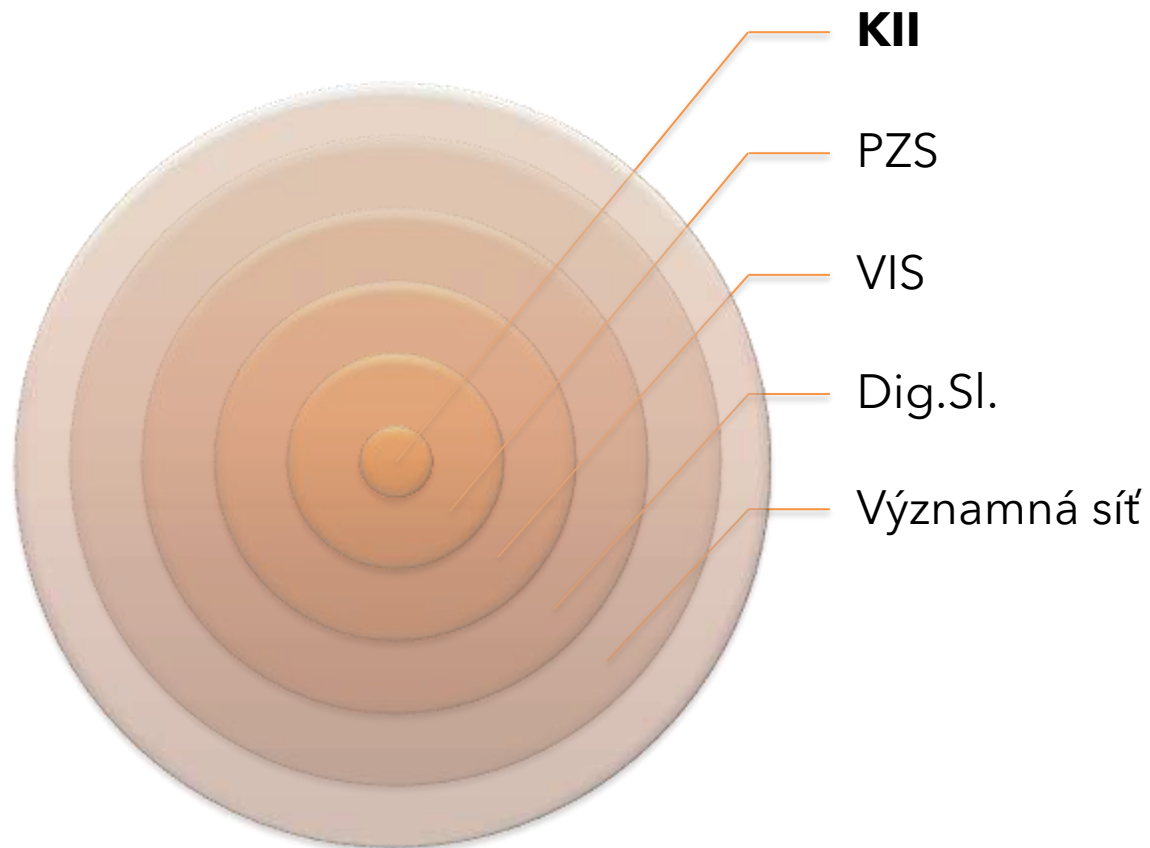
Foods



Public administration

Sectors covered by NIS 1	Sectors covered by NIS 2 proposal
"Operators of essential services" category	"Essential entities" 
	<i>All sectors from NIS 1</i>
Healthcare providers	Additional health-related services - including pharma, some medical device manufacturers, researchers
Digital infrastructure - (IXPs, DNS services, TLD registries)	Additional digital infrastructure services - cloud computing services, data centers, CDNs, network providers
Drinking water	Waste water
Transport	Space
Financial market infrastructure	Public Administration
Energy	
Banking	
"Digital service providers" category	"Important entities" 
Online marketplaces	Online marketplaces
Online search services	Online search services
Cloud services	Social networking services
	Food production & distribution
	Postal services
	Waste management
	Chemical manufacturers
	Manufacturing - medical devices, electronic products and equipment, machinery, vehicles and transport equipment

<https://www.rapid7.com/blog/post/2021/04/20/overview-of-the-eus-draft-nis-2-directive/>



- **Povinné vzdělávání managementu, větší míra odpovědnosti managementu**
- Minimální bezpečnostní standard
- Hlášení relevantních událostí a hrozeb, sdílení informací o zranitelnostech (registr ENISA)
- Řešení bezpečnosti dodavatelských vztahů
- **Způsob identifikace povinné osoby**
- Rozsah regulovaných systémů
- Povinné certifikace kybernetické bezpečnosti
- Vyšší pokuty (inspirace GDPR) aj.

# **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vyzývá odbornou veřejnost k zasílání návrhů na změny zákona č. 181/2014 Sb., o kybernetické bezpečnosti**

24. září 2021

<https://www.nukib.cz/cs/infoservis/aktuality/1748-narodni-urad-pro-kybernetickou-a-informacni-bezpecnost-nukib-vyzyva-odbornou-verejnost-k-zasilani-navrhu-na-zmeny-zakona-c-181-2014-sb-o-kyberneticke-bezpecnosti/>

cesnet  
“...”

**Kdo bude regulován?**

**5000-6000**







cesnet  
"...."

**CER**

**- CRITICAL ENTITIES RESILIENCE**

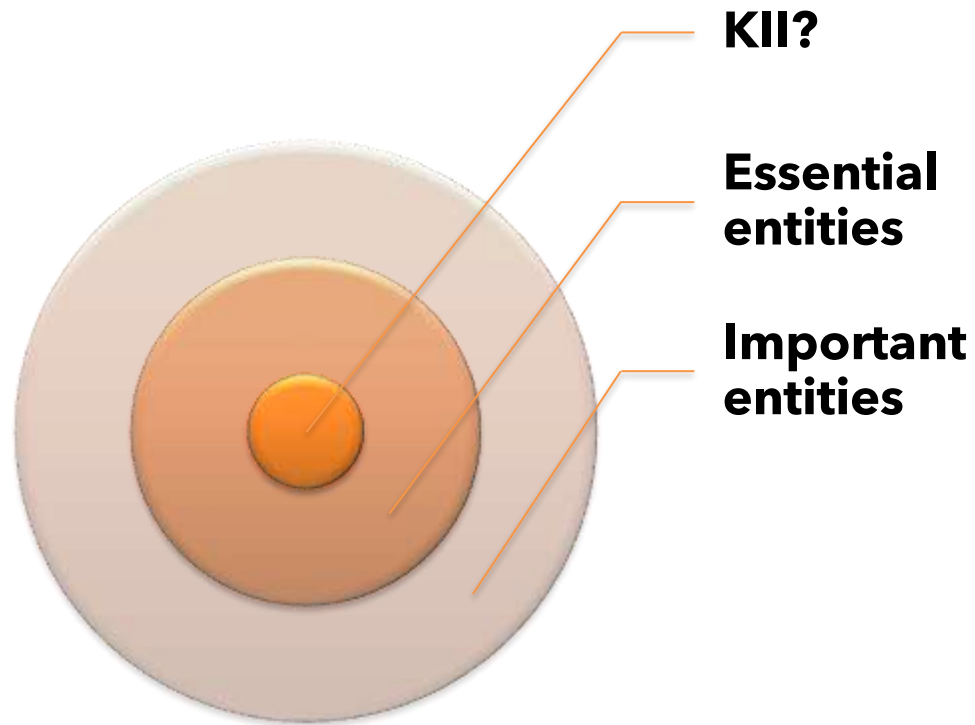
Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY  
o posílení odolnosti kritických subjektů

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0829&from=EN>

## ■ 2020

- **Potřeba soudržnějšího a jednotnějšího přístupu mezi směrnici o evropských kritických infrastrukturách a směrnici (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.**
- **zajistit, aby příslušné orgány** podle obou právních aktů **přijímaly vzájemně se doplňující opatření a podle potřeby si vyměňovaly informace** týkající se kybernetické i nekybernetické odolnosti a aby zejména klíčoví provozovatelé v odvětvích, která jsou podle tohoto návrhu považována za „základní“, podléhali také obecnějším povinnostem zaměřeným na posilování odolnosti s důrazem na nekybernetická rizika.



**Každý členský stát vytvoří seznam určených kritických subjektů a zajistí, aby tyto kritické subjekty byly informovány o svém určení** jako kritických subjektů do jednoho měsíce od tohoto určení, přičemž budou rovněž informovány o svých povinnostech podle kapitol II a III a o datu, od kterého se na ně ustanovení těchto kapitol vztahují.

## NIS2 - kybernetické hrozby

z. č. 480/2004  
Sb., ZSIS

z. č. 181/2014  
Sb., ZKB

z. č. 127/2005  
Sb., ZoEK

GDPR

eIDAS

## Hybridní hrozby

## CER - fyzické hrozby

Doprava

energetika

Telekomunikace

Bankovnictví

Infrastruktura  
finančních trhů


Digitální  
infrastruktura

Veřejná správa

Zdraví

Pitná a odpadní  
voda

Vesmír

- Poskytovatelé **výměnného uzlu internetu** [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
  - Poskytovatelé **služeb DNS** [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
  - Registry internetových domén nejvyšší úrovně (registry **TLD**) [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
  - Poskytovatelé **cloudových služeb** [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
  - Poskytovatelé **služeb datového střediska** [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
  - Poskytovatelé **sítí pro doručování obsahu** [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
  - Poskytovatelé **služeb vytvářejících důvěru** ve smyslu čl. 3 bodu 19 nařízení (EU) č. 910/2014
  - Poskytovatelé **veřejné sítě elektronických komunikací** ve smyslu čl. 2 bodu 8 směrnice (EU) 2018/1972 nebo poskytovatelé služeb elektronických komunikací ve smyslu čl. 2 bodu 4 směrnice (EU) 2018/1972, pokud jsou jejich služby veřejně dostupné
- 
- A decorative horizontal bar at the bottom of the slide, consisting of a series of small blue squares of varying heights and widths, creating a pixelated or digital effect.

cesnet  
"...."

**NIS2 A CER...kdy?**





2025



- **Subjekty se mnohdy překrývají** (KII, ISVS, PZS, VIS aj.)
- Opuštění definice prvku kritické infrastruktury jako jednotlivé věci a změnu definice na množinu aktiv, která zajišťují předem vytyčenou a pro stát kritickou službu.
- **Nevhodně nastavená kritéria pro určení KI v některých odvětvích**
- **Určování služby jako celku**
- Odlišnost procesu určování prvku na základě toho, zda subjekt je nebo není organizační složkou státu.
- Proces určování „soukromého“ subjektu pomocí **opatření obecné povahy**
- Změny povahy prováděcího právního předpisu z nařízení vlády na vyhlášku

LIDÉ



Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0595&from=EN>

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o jednotném trhu digitálních služeb (akt o digitálních službách) a o  
změně směrnice 2000/31/ES

[https://eur-lex.europa.eu/legal-  
content/CS/TXT/HTML/?uri=CELEX:52020PC0825&from=CS](https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0825&from=CS)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví (akt o digitálních trzích)

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

cesnet  
“...”

# Potírání terorismu



NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2021/784

ze dne 29. dubna 2021

o potírání šíření teroristického obsahu online

<https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32021R0784&from=CS>



1. **Poskytovatel hostingových služeb vystavený teroristickému obsahu podle odstavce 4 v příslušných případech zahrne do svých podmínek ustanovení týkající se zneužívání jeho služeb k veřejnému šíření teroristického obsahu a tato ustanovení uplatňuje.**

Učiní tak řádným, přiměřeným a nediskriminačním způsobem a za všech okolností s patřičným ohledem na základní práva uživatelů a vezme přitom v úvahu zejména zásadní význam svobody projevu a informací v otevřené a demokratické společnosti, s cílem vyhnout se odstranění jiného než teroristického obsahu.

2. **Poskytovatel** hostingových služeb vystavený teroristickému obsahu podle odstavce 4 **přijme zvláštní opatření na ochranu svých služeb proti veřejnému šíření teroristického obsahu.**

O zvláštních opatřeních rozhoduje poskytovatel hostingových služeb. Takováto opatření mohou zahrnovat jedno nebo více z těchto opatření:

- a) **vhodná technická a provozní opatření nebo kapacity, jako například odpovídající personál nebo technické prostředky pro identifikaci a rychlé odstraňování teroristického obsahu** nebo znemožnění přístupu k němu;
- b) snadno dostupné a uživatelsky vstřícné **mechanismy, jejichž prostřednictvím mohou uživatelé poskytovateli hostingových služeb oznamovat** nebo označovat domnělý teroristický obsah;
- c) jakékoli jiné **mechanismy ke zvýšení informovanosti o teroristickém obsahu** v rámci jeho služeb, jako jsou mechanismy uživatelského moderování;
- d) jakékoli jiné opatření, které poskytovatel hostingových služeb považuje za vhodné pro potírání dostupnosti teroristického obsahu v rámci svých služeb.

4. **Poskytovatel hostingových služeb je vystaven teroristickému obsahu, pokud příslušný orgán členského státu**, v němž má tento poskytovatel hlavní provozovnu nebo v němž má bydliště nebo je usazen jeho právní zástupce,

a) **přijal rozhodnutí založené na objektivních faktorech, například na skutečnosti, že poskytovatel hostingových služeb v předchozích dvanácti měsících obdržel dva nebo více pravomocných příkazů k odstranění**, kterým konstatuje, že poskytovatel hostingových služeb je vystaven teroristickému obsahu a

b) oznámil rozhodnutí uvedené v písmenu a) poskytovateli hostingových služeb.

5. Po obdržení rozhodnutí uvedeného v odstavci 4 nebo případně v odstavci 6 oznámí poskytovatel hostingových služeb příslušnému orgánu zvláštní opatření, která přijal a která hodlá přijmout k zajištění souladu s odstavci 2 a 3.

## ZÁKON

ze dne ..... 2022

proti šíření teroristického obsahu online

<https://komora.cz/legislation/16-22-navrh-zakona-proti-sireni-teroristickeho-obsahu-onlinet10-3-2022/>

## § 2

### Příkaz k odstranění

(1) **Policie České republiky** (dále jen „policie“) **může** po posouzení skutečného účelu veřejného šíření teroristického obsahu **příkázat odstranění teroristického obsahu nebo znemožnění přístupu k němu**, a to prostřednictvím formuláře podle přílohy I nařízení Evropského parlamentu a Rady (EU) 2021/784 (dále jen „nařízení“); přitom přihlédne zejména k povaze a znění výroku nebo projevu, ke kontextu, ve kterém byl učiněn, a k míře, ve které mohou přivodit škodlivé důsledky, pokud jde o bezpečnost a ochranu osob.

- **„Stanovit podrobnější pravidla proti zneužívání hostingových služeb k veřejnému šíření teroristického obsahu online...“**
  - obecná právní úprava stanoví odpovědnost poskytovatele hostingových služeb za obsah informací uložených uživatelem je stanovena v ustanovení **§ 5 zákona č. 480/2004 Sb.**, o některých službách informační společnosti.
- **„Přezkum přeshraničních příkazů k odstranění. Nařízení kvůli rychlé a účinné reakci na teroristický obsah umožňuje, aby orgány členských států vydávaly příkazy k odstranění i vůči poskytovatelům hostingových služeb, kteří jsou usazeni v jiném členském státě.“**
  - **Absence podmínek**, jakož i stanovení toho v jakém režimu budou přeshraniční příkazy sloužící k znepřístupnění teroristického obsahu online vydávány.
- **V návrhu není nikterak upraveno, jakým způsobem může Česká republika, resp. pověřený orgán žádat o odstranění teroristického obsahu nacházejícího se v zahraničí.**
  - Tím vzniká významná **disproporce v možnosti redukce teroristického obsahu on-line ze strany České republiky.**

- **rezignace na zapracování vazeb na platné a účinné právní předpisy**
- nové pravomoci Policii ČR, ale pravomoc není nedoplněna žádnými stanovenými pravidly, která jsou obsažena v zákoně o Policii a v trestním řádu.
- **na adresáty** normy **budou dopadat režimy** k odstraňování obsahu **plynoucím z několika právních předpisů** (navržená právní norma, z. 480/2004 Sb., z. 141/1961 Sb.)
- Reálně tak v praxi může vzniknout situace, kdy poskytovatel hostingových služeb bude úkolován různými subjekty v různých řízeních k vykonání těchto

cesnet  
"...."

**Ban webů**





# Jak blokujeme nepovolené hazardní weby

31. 7. 2017

1. ledna 2022 došlo ke změnám v právním rámci, pro aktuální informace se prosím podívejte nejprve [sem](#).

Ačkoli kontroverzní [zákon č. 186/2016 Sb](#) o hazardních hrách, který v [§ 82](#) nařizuje *poskytovatelům připojení k internetu* zamezení v přístupu ke stránkám s nepovolenými hazardními hrami, platí už od prvního ledna letošního roku, teprve 26. července byl zveřejněn první seznam nepovolených her. Nyní běží 15denní lhůta, ve které by měly všechny povinné subjekty zahájit blokování *internetové stránky* `1xbet.com`. V tomto příspěvku si představíme způsob, jakým zákonné blokování implementujeme v e-infrastruktúře CESNET.

## Blokujeme pomocí DNS

<https://www.cesnet.cz/2017/07/jak-blokujeme-nepovolene-hazardni-weby/>

**Státní ústav pro kontrolu léčiv** jako orgán výkonu státní správy v oblasti humánních léčiv **vede od 1.1.2022** v souladu s ustanovením § 13 odst. 3 písm. s) zákona č. 378/2007 Sb., zákon o léčivech a o změnách některých souvisejících zákonů (zákon o léčivech) (dále jen „zákon o léčivech“) **seznam internetových stránek nabízejících léčivé přípravky v rozporu s tímto zákonem** (dále jen "seznam stránek s nelegální nabídkou léčivých přípravků") **a zveřejňuje ho na svých internetových stránkách.**

<https://www.sukl.cz/farmaceuticky-prumysl/seznam-stranek-s-nelegalni-nabidkou-lecivych-pripravku>

<https://opendata.sukl.cz/?q=katalog/seznam-stranek-s-nelegalni-nabidkou-lecivych-pripravku>

- Nejsme-li schopni se domluvit právu válečném, resp. jej akceptovat...
- **...jsme schopni definovat a dodržovat právo v kyberprostoru?**

# Rusko se chce údajně odpojit od světového internetu. Už si to vyzkoušelo

7. března 2022



Zatím nepotvrzená informace zpravodajského serveru Nexta uvádí, že by se Ruská federace měla odpojit od světového internetu a vytvořit si vlastní, státem kontrolovaný internet. Ten je znám pod označením Runet.



Ruský internet - ilustrační foto | foto: Profimedia.cz

[https://www.idnes.cz/technet/internet/internet-runet-vyputi-internet-rusko.A220306\\_213449\\_sw\\_internet\\_vse](https://www.idnes.cz/technet/internet/internet-runet-vyputi-internet-rusko.A220306_213449_sw_internet_vse)

<https://www.cnews.cz/rusko-hlasi-ze-po-odchodu-zapadnich-sofwarovych-firem-legalizuje-piratstvi/>

# Rusko hlásí, že po odchodu západních softwarových firem legalizuje pirátství

Od Radomír Kejdůš - 4.3.2022



Facebook



Twitter



LinkedIn



ilustrační obrázek - Zdroj: Depositphotos

Ruské úřady v reakci na stažení západních softwarových firem ze země navrhuji legalizovat pirátství. Ruským ajťákům také odloží vojnu. Jde o součást balíku opatření a některé jeho části se již začaly realizovat. Mělo by jít jen o ty softwarové produkty, kde neexistuje ruská varianta.

**"Si vis pacem, para bellum"**





DAILYMAIL.CO.UK | OD DAILY MAIL

**Japan's minister of cybersecurity has NEVER used a computer**



**cesnet**  
"...."

**DĚKUJI ZA POZORNOST  
MÁTE NĚJAKÉ DOTAZY?**

**doc. JUDr. Jan Kolouch, Ph.D.**  
[jan.kolouch@cesnet.cz](mailto:jan.kolouch@cesnet.cz)