

Základy regulácie kybernetickej bezpečnosti a súvisiacich oblastí

Modul 1 - Úvod do regulácie kybernetickej bezpečnosti
Časť 2

Doc. JUDr. Jozef Andraško, PhD.



Financované
Európskou úniou
NextGenerationEU

PLÁN [OBNOVY]



MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

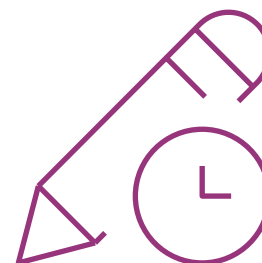


Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality CUSEC

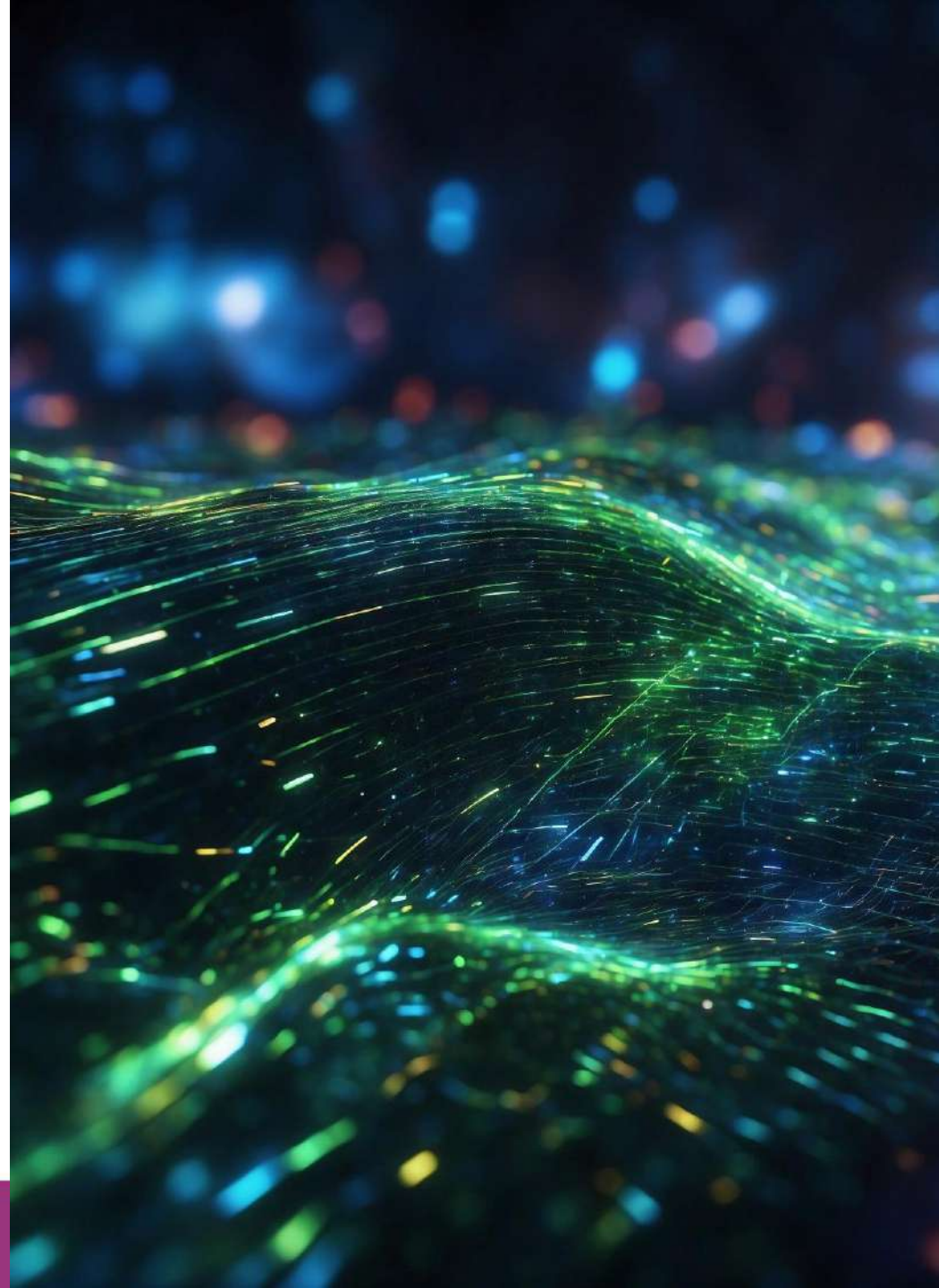


PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-VO1-00002



Čo sú základné ľudské práva a slobody?





Globálny

Všeobecná
deklarácia
ľudských práv
(OSN)



Rada Európy

Európsky
dohovor o
ochrane
ľudských práv a
základných
slobôd



Európska únia

Charta
základných práv EÚ



Národné právo

Ústava
Slovenskej
republiky (Hlava II)

Ako môžu technológie
ovplyvniť ľudské práva?









Black Mirror - Lacie Rates Coworker - Social Credit System (Nosedive S3E1)



Worldie - Network for Good
523 subscribers

Subscribe

3.6K



Share

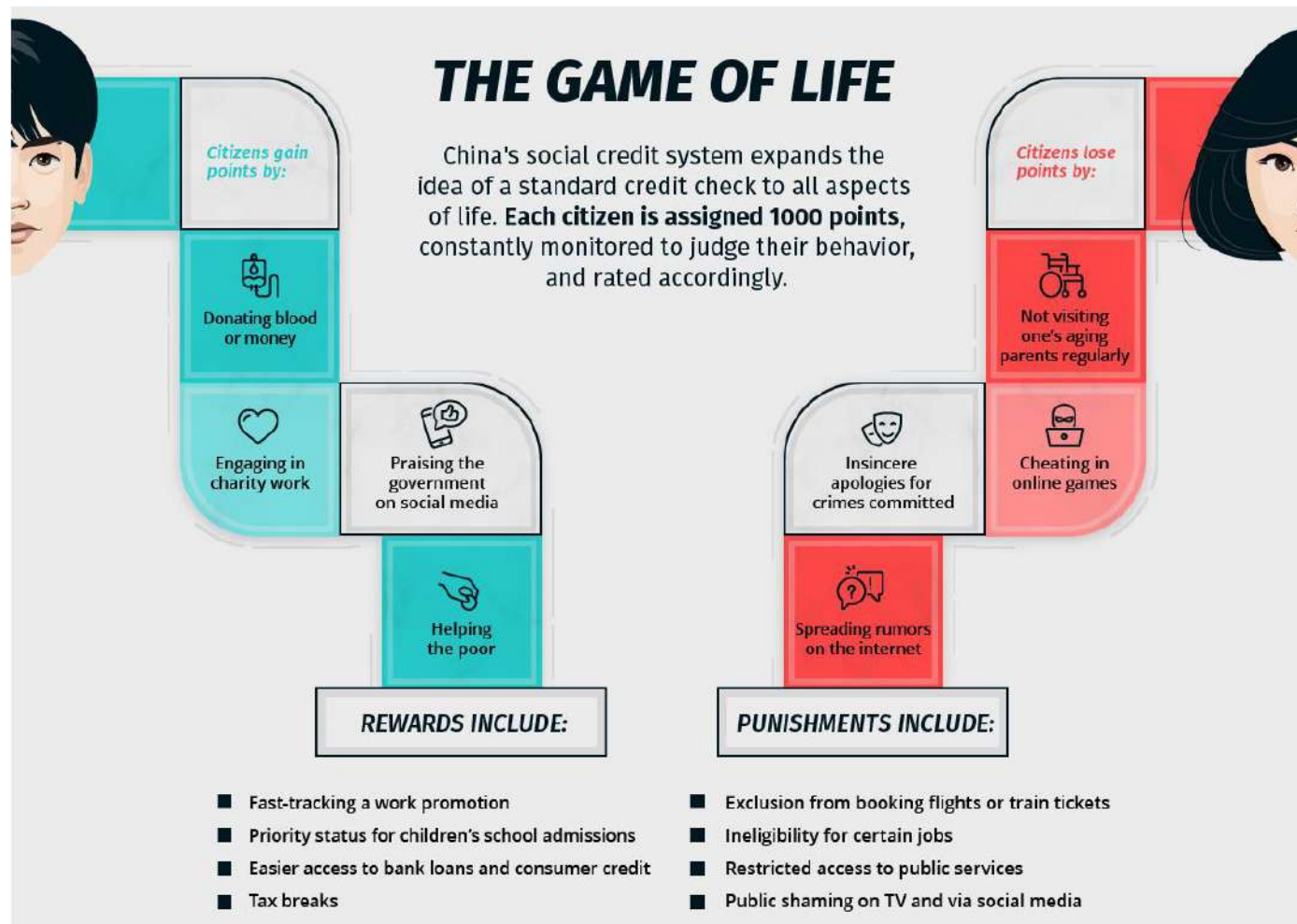
Download

Clip

Save



SOCIAL CREDIT SYSTEM



Nové digitálne práva?



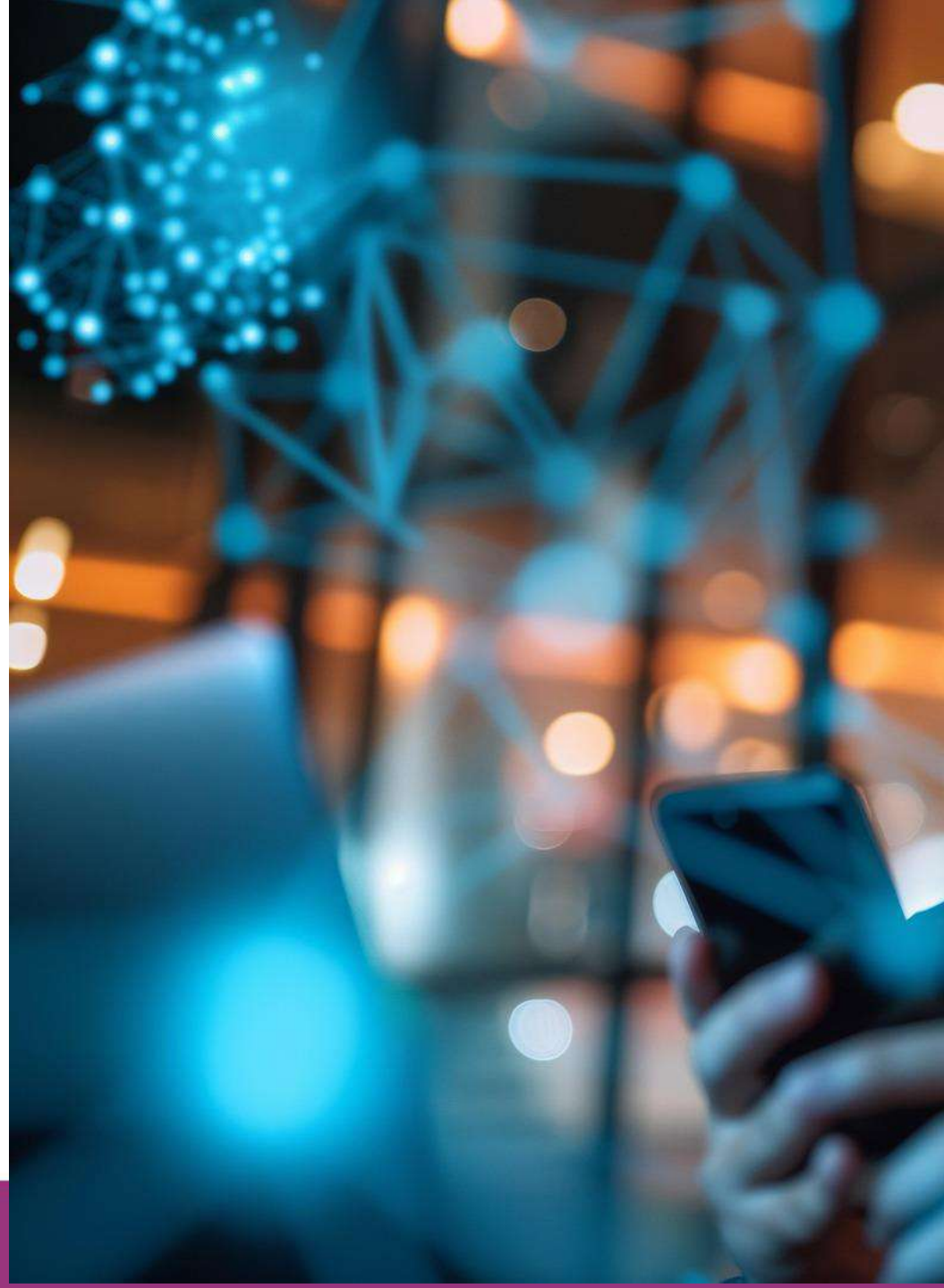


Európske vyhlásenie o digitálnych právach a zásadách v digitálnom desaťročí



#DigitalEU

Ochrana súkromia a osobných údajov



Právo na zabudnutie

SDEÚ Google Spain
SDEÚ Google v. CNIL



Plošný zber údajov

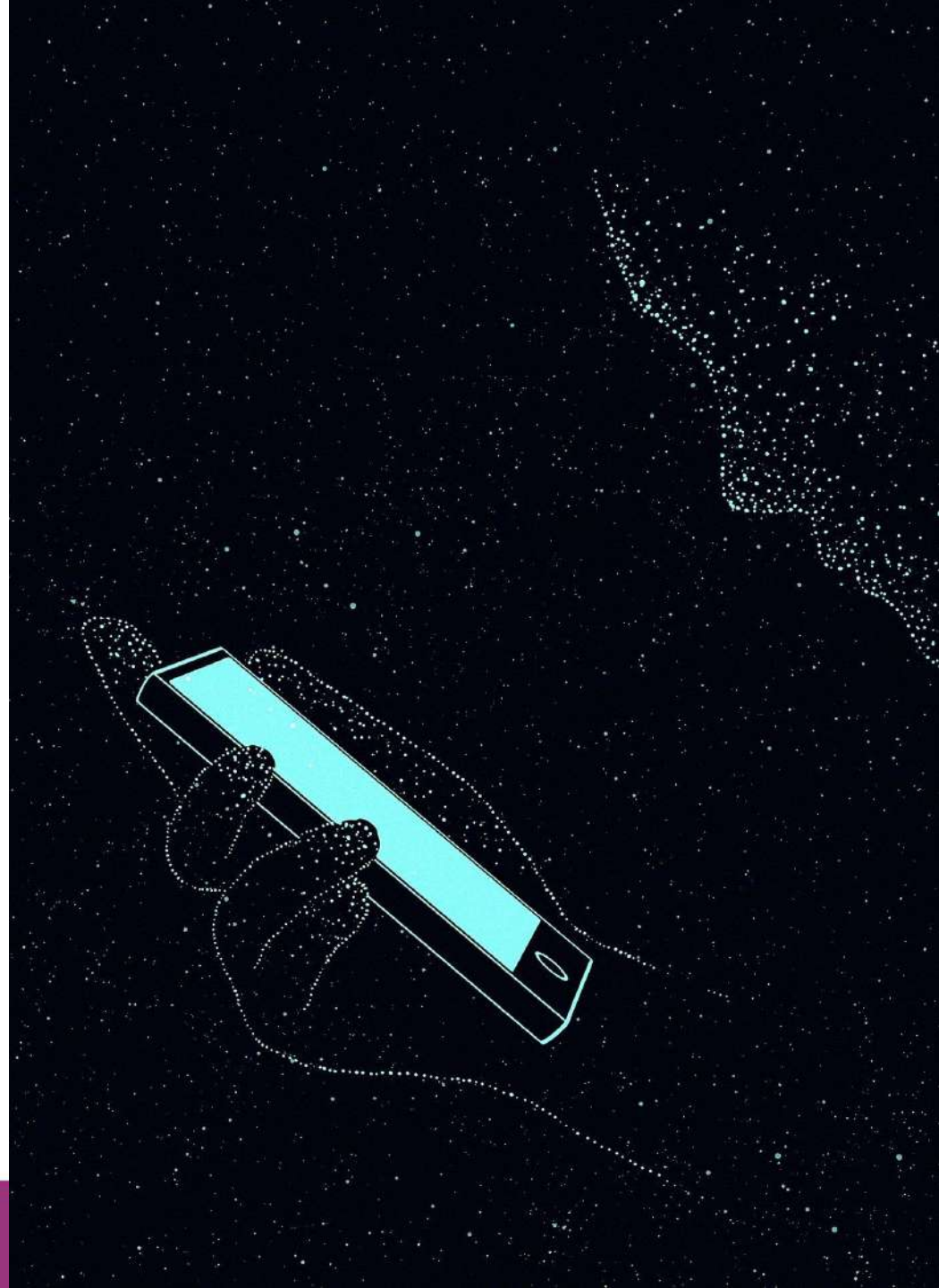
SDEÚ Digital Rights Ireland

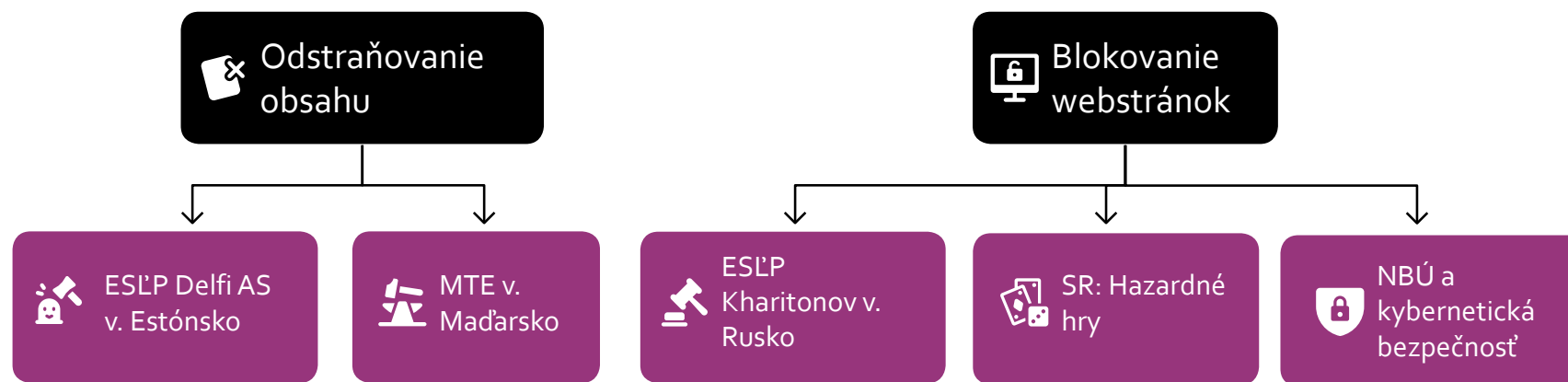


Trasovanie kontaktov počas pandémie COVID-19

PL. ÚS 13/2020-103

Sloboda prejavu







EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Anotace rozhodnutí Evropského soudu pro lidská práva

Rozsudek ze dne 23. června 2020 ve věci č. [10795/14](#) – *Kharitonov proti Rusku*

Senát třetí sekce Soudu jednomyslně rozhodl, že zablokováním internetové stránky stěžovatele, které nastalo automaticky v důsledku rozhodnutí státního orgánu o zablokování jiné k porušení článku 10, jakož i článku 13 ve spojení s článkem 10 Úmluvy.



- Stanovené zákonom
- Sleduj legitímny cieľ
- Náležitá predvídateľnosť
- Potrebný v demokratickej spoločnosti
- Záruky proti zneužitiu
 - predchádzajúce upozornenie
 - schválenie súdom/nezávislým orgánom
 - posúdenie dopadu/vedľajších účinkov
- Požiadavka transparentnosti blokačných príkazov
 - zaslanie textu blokačného príkazu (komu, opravné prostriedky)
 - informovanie tretích strán

Hmm, túto stránku sa nám nepodarilo nájsť.

Nebolo možné sa pripojiť k serveru www.hlavnespravy.sk.

Ak je táto adresa správna, môžete skúsiť nasledujúce:

- Skúsiť to znova neskôr.
- Skontrolovať svoje pripojenie k sieti.
- Ak ste pripojení pomocou firewallu, skontrolujte, či má Firefox povolený prístup na web.

Skúsiť znova



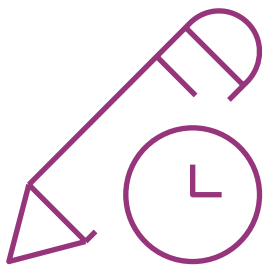
HLAVNÉ | SPRÁVY

KONZERVATÍVNY DENNÍK

- rozhoduje o **blokovaní škodlivého obsahu alebo škodlivej aktivity**, ktorá smeruje do kybernetického priestoru Slovenskej republiky alebo z kybernetického priestoru Slovenskej republiky (ďalej len „blokovanie“) a zabezpečuje vykonanie tohto rozhodnutia alebo vykonáva blokovanie na základe žiadosti.

Blokovanie podľa ZoKB

§ 27b



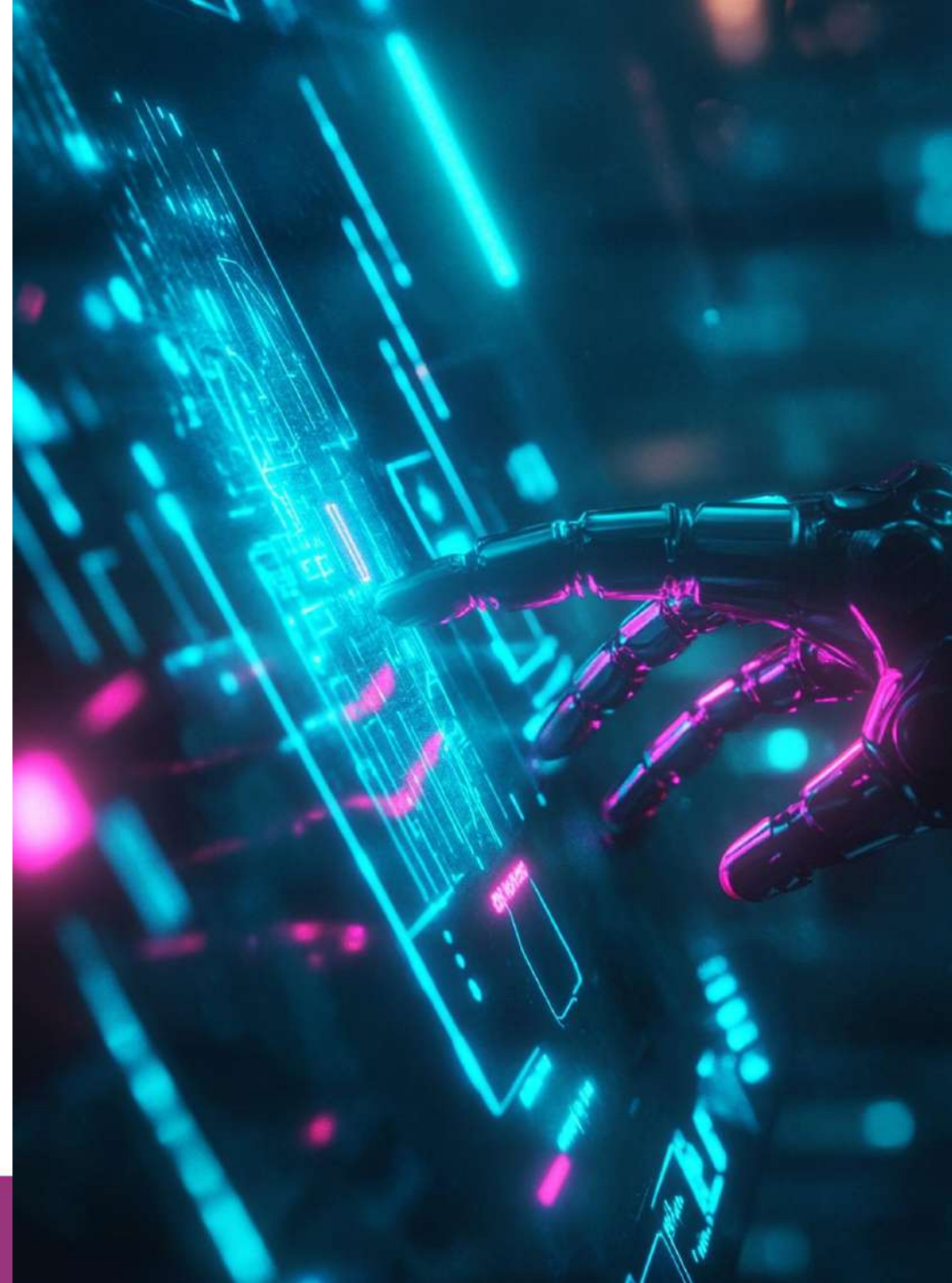
- z **vlastnej iniciatívy** rozhoduje o blokovaní, spôsobe blokovania a vykonáva blokovanie
- Škodlivým obsahom sa rozumie programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. **Škodlivou aktivitou** sa rozumie akákoľvek **činnosť**, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, podvodnú činnosť, odcudzenie osobných údajov alebo citlivých údajov, **závažné dezinformácie** a iné formy hybridných hrozieb.
- **Štátne orgány** sú povinné bez meškania oznamovať úradu škodlivý obsah a škodlivé aktivity, ktoré zistia pri svojej činnosti.
- Rozhodnúť o blokovaní škodlivého obsahu alebo škodlivej aktivity možno len s platnosťou **do 30. septembra 2022.**

- [Návrh novely zákona o KB](#)
- V § 27b odsek 1 znie:
- „(1) Úrad rozhoduje o blokovaní **len na základe doručeného odôvodneného návrhu subjektu s pôsobnosťou v oblasti bezpečnosti a obrany štátu**^{28ba)} a na základe predchádzajúceho **súhlasu súdu** a v jeho rozsahu. Žiadosť o vydanie súhlasu súdu s blokovaním **predkladá úrad písomne Najvyššiemu správne mu súdu Slovenskej republiky** s náležitosťami podľa odseku 2 písm. a) až f). Sudca Najvyššieho správneho súdu Slovenskej republiky rozhodne o vydaní súhlasu s blokovaním do 15 dní odo dňa podania žiadosti postupom podľa osobitného predpisu^{28a)} primerane. Proti rozhodnutiu Najvyššieho správneho súdu o vydaní súhlasu s blokovaním nie je prípustný opravný prostriedok. Rozhodnutie Najvyššieho správneho súdu Slovenskej republiky o vydaní súhlasu s blokovaním musí obsahovať náležitosti podľa odseku 2.“.

- V § 27b odsek 3 znie:
- „(3) Škodlivým obsahom sa rozumie činnosť, údaj alebo programový prostriedok, ktorý má alebo môže mať za následok poškodenie alebo ohrozenie bezpečnostných, zahraničnopolitických alebo hospodárskych záujmov Slovenskej republiky a je formou hybridnej hrozby.“.
- V § 27b ods. 4 sa na konci pripájajú tieto vety:
- „Úrad vykonáva blokovanie v rozsahu nevyhnutnom na dosiahnutie cieľa a spôsobom primeraným vo vzťahu k následkom na majetku, právach a právom chránených záujmoch iných osôb. Rozhodnutie o blokovaní možno vydať s platnosťou najdlhšie **na deväť kalendárnych mesiacov.**“

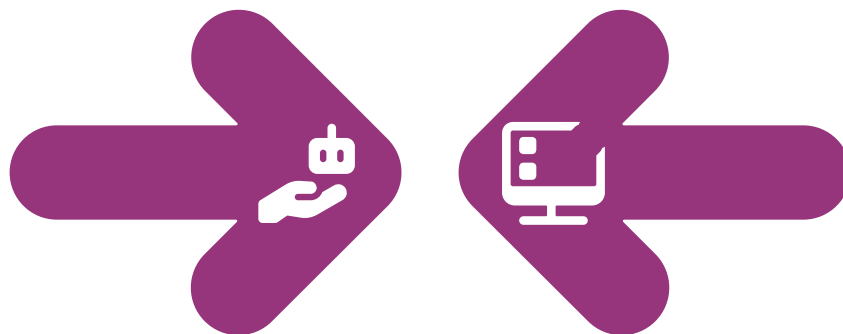
- V § 27b odsek 9 znie:
 - „(9) Úrad **zverejní rozhodnutie** o blokovaní a informáciu o zrušení blokovania na svojom webovom sídle.“.
-
- V § 5 sa odsek 1 dopĺňa písmenom ah), ktoré znie:
 - „ah) predkladá príslušnému osobitnému kontrolnému výboru Národnej rady Slovenskej republiky každoročne správu o vydaných rozhodnutiach o blokovaní podľa § 27b.“

Digitálna verejná správa



Algoritmičné rozhodovanie

Maturity
(Spojené
kráľovstvo)



Elektronická verejná správa

EURA

Poľnohospodárske pozemky



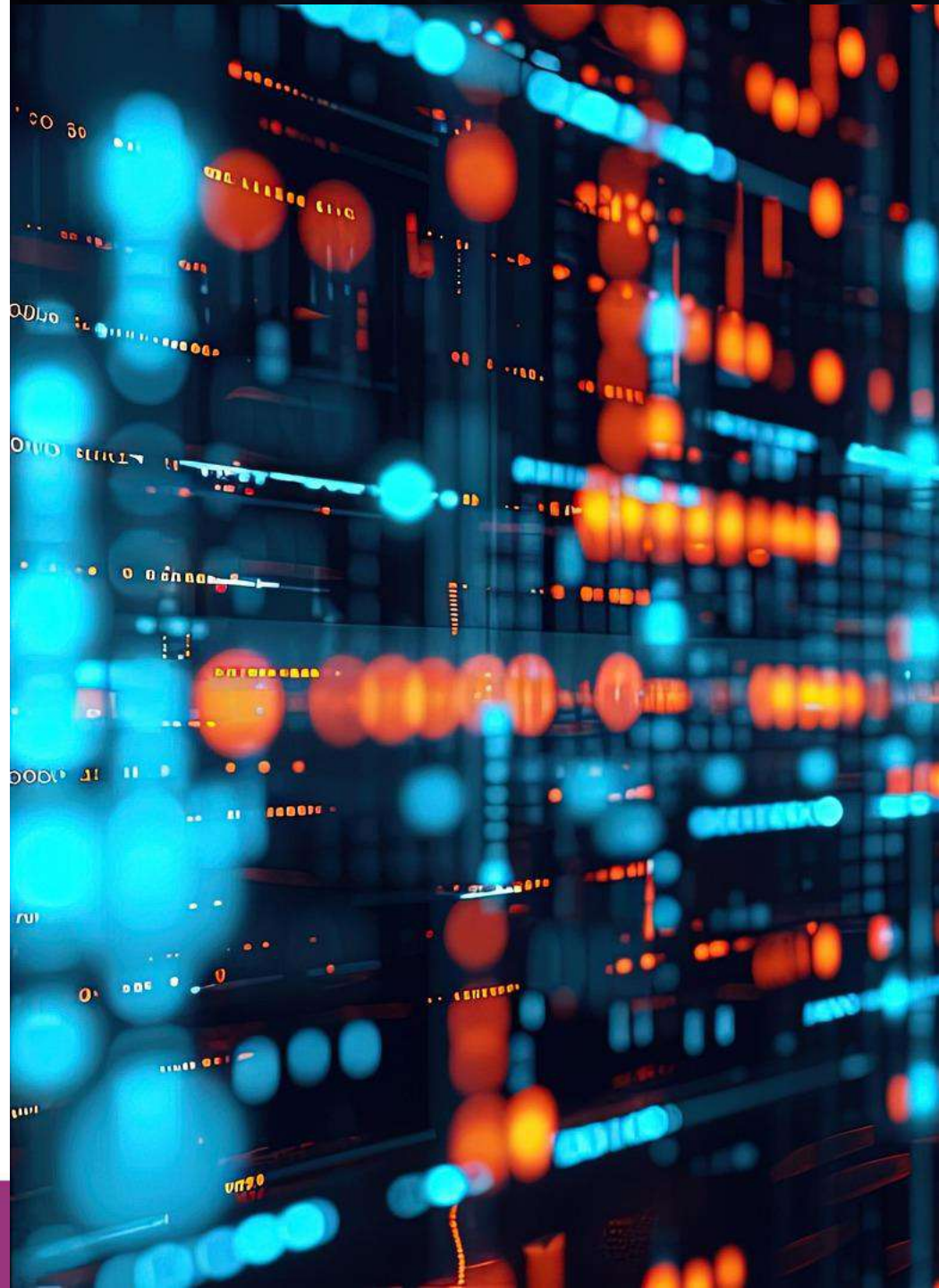
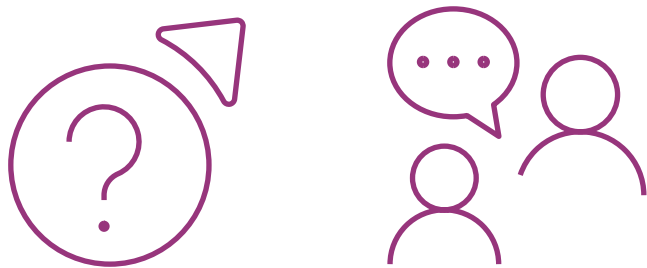
CUSEC

The vehicle was seen in (location) Pulteney Bridge, Bath on 29/07/2021 at 15:41



Bath and North East Somerset Council believes that a Penalty Charge is now payable with respect to the vehicle above, for the following alleged contravention:- 34 - Being in a bus lane (as defined in S.144(5) Transport Act 2000).

Prečo sú ľudia ochotnejší
akceptovať ľudské chyby
oproti chybám algoritmov?



Ak by sa o vašich P/PCHZ/P
rozhodovalo
automatizovane, aké práva
by ste chceli uplatniť?



Vzťah KB a základných ľudských práv a slobôd

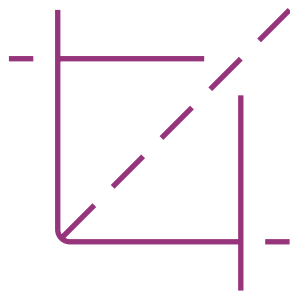




KB chráni základné
ľudské práva a
slobody



KB musí byť v súlade
s ľudsko-právnym
štandardom



KB oddelene od základných
práv a slobôd



KB chrání základné
ľudské práva a
slobody

Akt o kybernetickej bezpečnosti (nariadenie 2019/881)

Kybernetická bezpečnosť

- „činnosti potrebné na **ochranu sietí a informačných systémov, užívateľov** takýchto systémov a **iných osôb dotknutých** kybernetickými hrozbami.“

Kybernetická hrozba

- „každá potenciálna **okolnosť, udalosť alebo činnosť**, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť **siete a informačné systémy, užívateľov** takýchto systémov a **iné osoby**.“

CUSEC

SIS (NIS)

užívatelia

iné osoby

Prístup
založený na
právach

Otvorená
definícia

PLÁN [OBNOVY]

- Rec. 3
- „Rastúca digitalizácia a pripojiteľnosť zvyšujú kybernetickobezpečnostné riziká, takže spoločnosť ako celok sa stáva zraniteľnejšou z hľadiska kybernetických hrozieb a zvyšuje sa nebezpečenstvo, ktorému čelia **fyzické osoby, vrátane zraniteľných osôb, ako sú napríklad deti.**“





KB musí byť v súlade
s ľudsko-právnym
štandardom

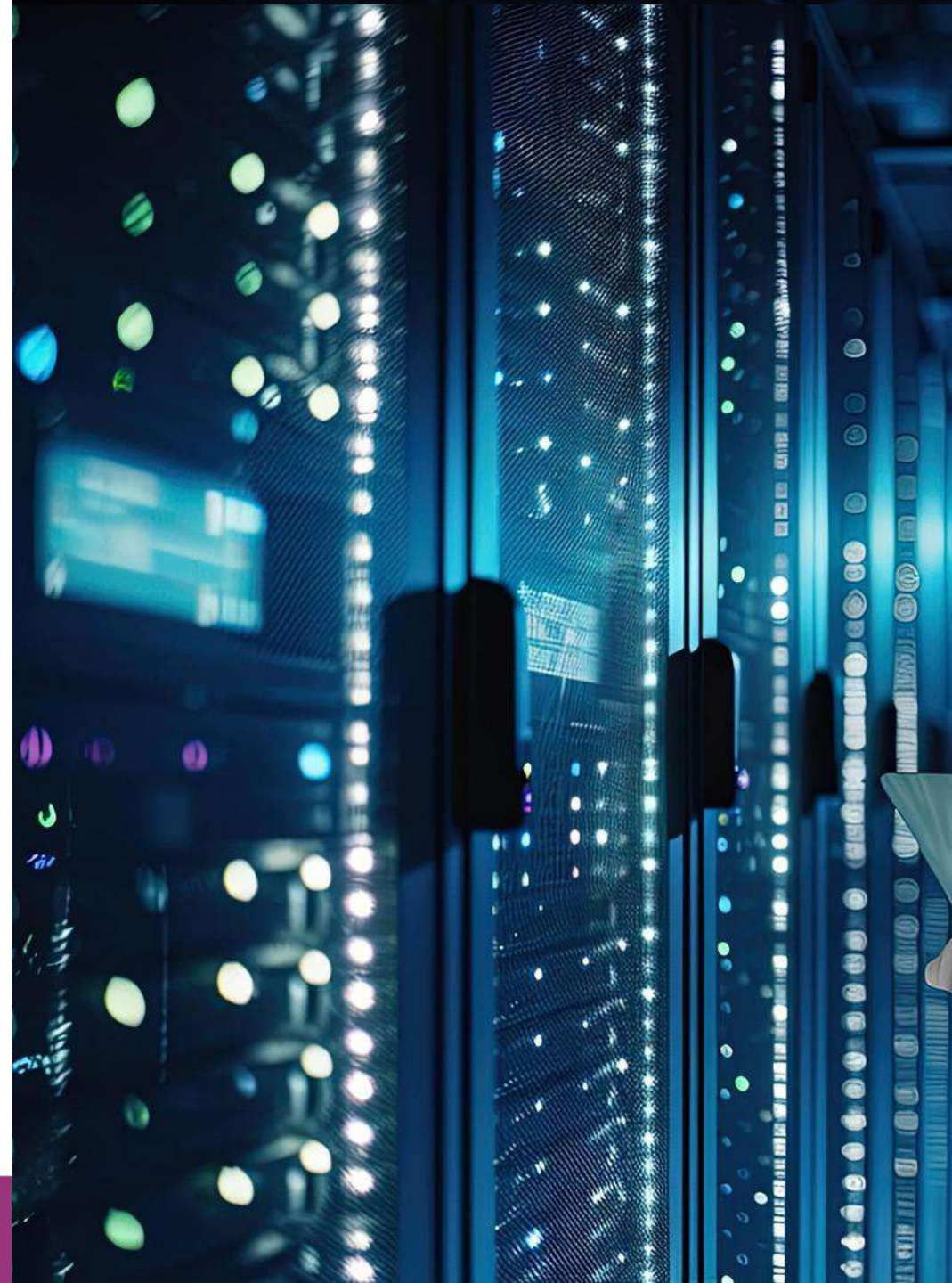
Smernica NIS 2

R 143

- V tejto smernici sa **rešpektujú základné práva a dodržiavajú zásady uznané v charte, najmä právo na rešpektovanie súkromného života a komunikácií, ochranu osobných údajov, slobodu podnikania, právo vlastniť majetok, právo na účinný prostriedok nápravy a na spravodlivý proces, prezumpcia nevinu a právo na obhajobu**. Právo na účinný prostriedok nápravy sa vzťahuje aj na príjemcov služieb poskytovaných kľúčovými a dôležitými subjektmi. Táto smernica by sa mala vykonávať v súlade s uvedenými právami a zásadami.



Právo podnikat' a vlastnické právo



Sloboda podnikania je zaručená článkom 16 Charty:

„Sloboda podnikania sa uznáva v súlade s právom Únie, vnútroštátnymi právnymi predpismi a praxou.“

+ ochrana obchodného tajomstva (SDEÚ)

Ochrana vlastníckeho práva je predmetom článku 17 Charty:

„1. Každý má právo vlastniť svoj oprávnene nadobudnutý majetok, užívať ho, nakladať s ním a odkázať ho. Nikoho nemožno zbaviť jeho majetku, s výnimkou verejného záujmu, v prípadoch a za podmienok, ktoré ustanovuje zákon, pričom musí byť včas vyplatená spravodlivá náhrada. Užívanie majetku môže byť upravené zákonom v nevyhnutnej miere v súlade so všeobecným záujmom.

2. Duševné vlastníctvo je chránené.“

- Úrad môže rozhodnutím **zakázať alebo obmedziť používanie konkrétneho produktu, procesu, služby** alebo **tretej strany** na poskytovanie služby ak zistí, že takéto používanie
 - neumožňuje alebo zásadným spôsobom **sťažuje udržanie kybernetickej bezpečnosti**, a tým ohrozuje život alebo zdravie osôb, hospodárske fungovanie štátu, verejný poriadok, bezpečnosť alebo majetok osôb, alebo
 - ohrozuje **bezpečnostné záujmy** Slovenskej republiky.



GENERAL TECHNOLOGY

The HUAWEI ban explained: A complete timeline and everything you need to know

What has happened to HUAWEI since May 2019? Here's a full summary of the HUAWEI ban.

By C. Scott Brown • December 12, 2022



Právo na dobrou správu vecí veřejných



Charta v článku 41 obsahuje **právo na dobrú správu vecí verejných**:

- „1. Každý má právo, aby inštitúcie, orgány, úrady a agentúry Únie vybavovali jeho záležitosti nestranne, spravodlivo a v primeranej lehote.*
- 2. Toto právo zahŕňa najmä:*
 - a) právo každého na vypočutie pred prijatím akéhokoľvek individuálneho opatrenia, ktoré by sa ho mohlo nepriaznivo dotýkať;*
 - b) právo každého na prístup k spisu, ktorý sa ho týka, za predpokladu rešpektovania oprávnených záujmov dôvernosti a služobného a obchodného tajomstva;*
 - c) povinnosť administratívy odôvodniť svoje rozhodnutia.*
- 3. Každý má právo na náhradu škody spôsobenej inštitúciami alebo zamestnancami Únie pri výkone ich funkcií v súlade so všeobecnými zásadami spoločnými pre právne poriadky členských štátov.*
- 4. Každý sa môže obrátiť na inštitúcie Únie v jednom z jazykov zmlúv a musí dostať odpoveď v rovnakom jazyku.“*

+ Európsky kódex dobrej správnej praxe

Právo na súkromie



Právo na súkromie je predmetom ochrany v článku 7 Charty:

„Každý má právo na rešpektovanie svojho súkromného a rodinného života, obydlia a komunikácie.“

- SDEÚ *Digital Rights Ireland*

"možno vyvodiť presné závery týkajúce sa súkromného života osôb, ktorých údaje boli uchovávané, ako ich každodenné zvyklosti, miesta ich trvalého alebo prechodného pobytu, denné alebo iné presuny, vykonávané činnosti, spoločenské vzťahy týchto osôb a spoločenské kruhy, v ktorých sa pohybujú."

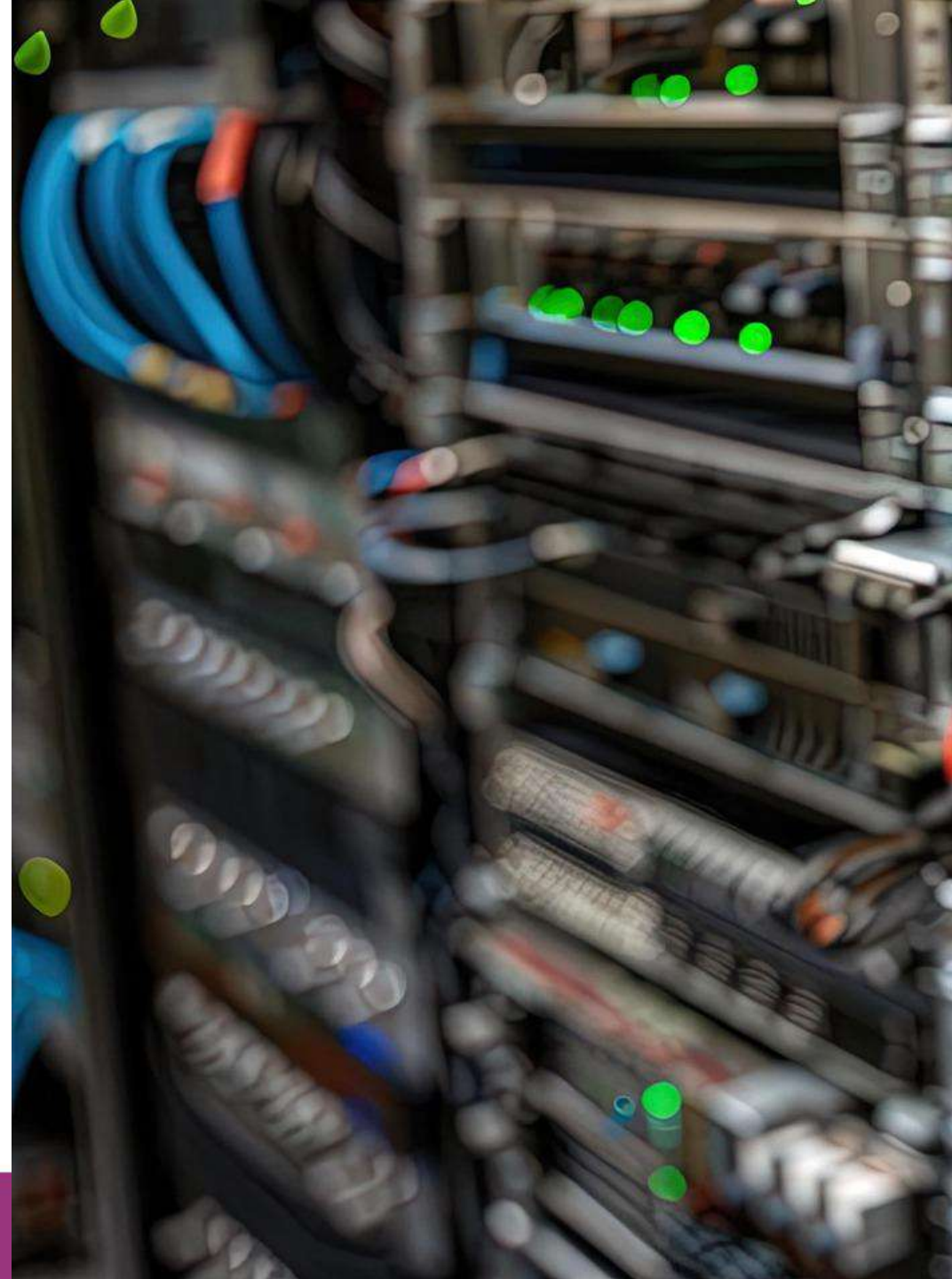
- Zásada ochrany a bezpečnosti údajov

- Uznesenie Ústavného súdu SR, sp. zn. PL. ÚS 13/2020

„Tieto povinnosti sú realizáciou ústavnej povinnosti štátu aktívne chrániť dôvernosc a integritu informačných systémov, ktoré obsahujú osobné údaje jednotlivca. Právo na ochranu dôvernosti a integrity informačných systémov predstavuje súčasť ochrany podľa čl. 19 ods. 3 a čl. 22 ústavy (podobne BVerfG, 1 BvR 370/07, 1 BvR 595/07, BVerfG 120). Zároveň sú tieto opatrenia predpokladom akceptovateľného závažného zásahu do práva na ochranu osobných údajov (SDEÚ, Digital Rights Ireland, C-293/12 and C-594/12, ods. 66 – 67)

- Nález Ústavného súdu SR - PL. ÚS 25/2019-117 (eKasa)
- pri orgánoch verejnej moci je požiadavka vysokej úrovne bezpečnosti pri spracúvaní údajov jednou z esenciálnych záruk proti zneužitiu

Právo na ochranu osobných údajov



Právo na ochranu osobných údajov je zakotvené v článku 8 Charty, na základe ktorého:

- „1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú*
 - 2. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu.*
 - 3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.“*
- Cezhraničné prenosy (parametre na bezpečnosť údajov)

Právo na informácie

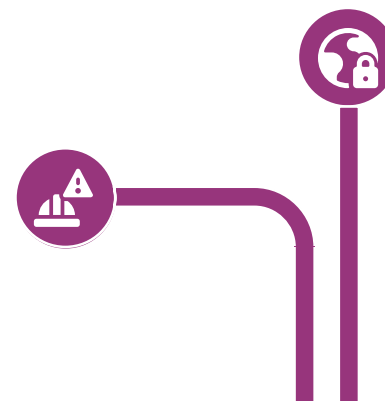


Charta základných práv EÚ dané upravuje právo na informácie v článku 11:

- „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.“

Informácie o
bezpečnostných
incidentoch/hrozbách/zraniteľnostiach/
udalostiach

Všeobecné informácie
o kybernetickej
bezpečnosti



Právo na (kybernetickú) bezpečnosť?



Článok 6 Charty základných práv EÚ

- *Každý má právo na slobodu a osobnú bezpečnosť*

Právo na slobodu a bezpečnosť

- Medzinárodná bezpečnosť
- Negatívny záväzok štátu
- Bezpečnosť ako dôvod obmedzenia práv
- Pozitívny záväzok štátu



Volume 13, Issue 1
March 2013

[Next >](#)

JOURNAL ARTICLE

Four Concepts of Security—A Human Rights Perspective

[Get access >](#)

[Piet Hein van Kempen](#) 

Human Rights Law Review, Volume 13, Issue 1, March 2013, Pages 1–23,

<https://doi.org/10.1093/hrlr/ngs037>

Published: 04 February 2013

 Cite  Permissions  Share ▼

Abstract

Email

Twitter

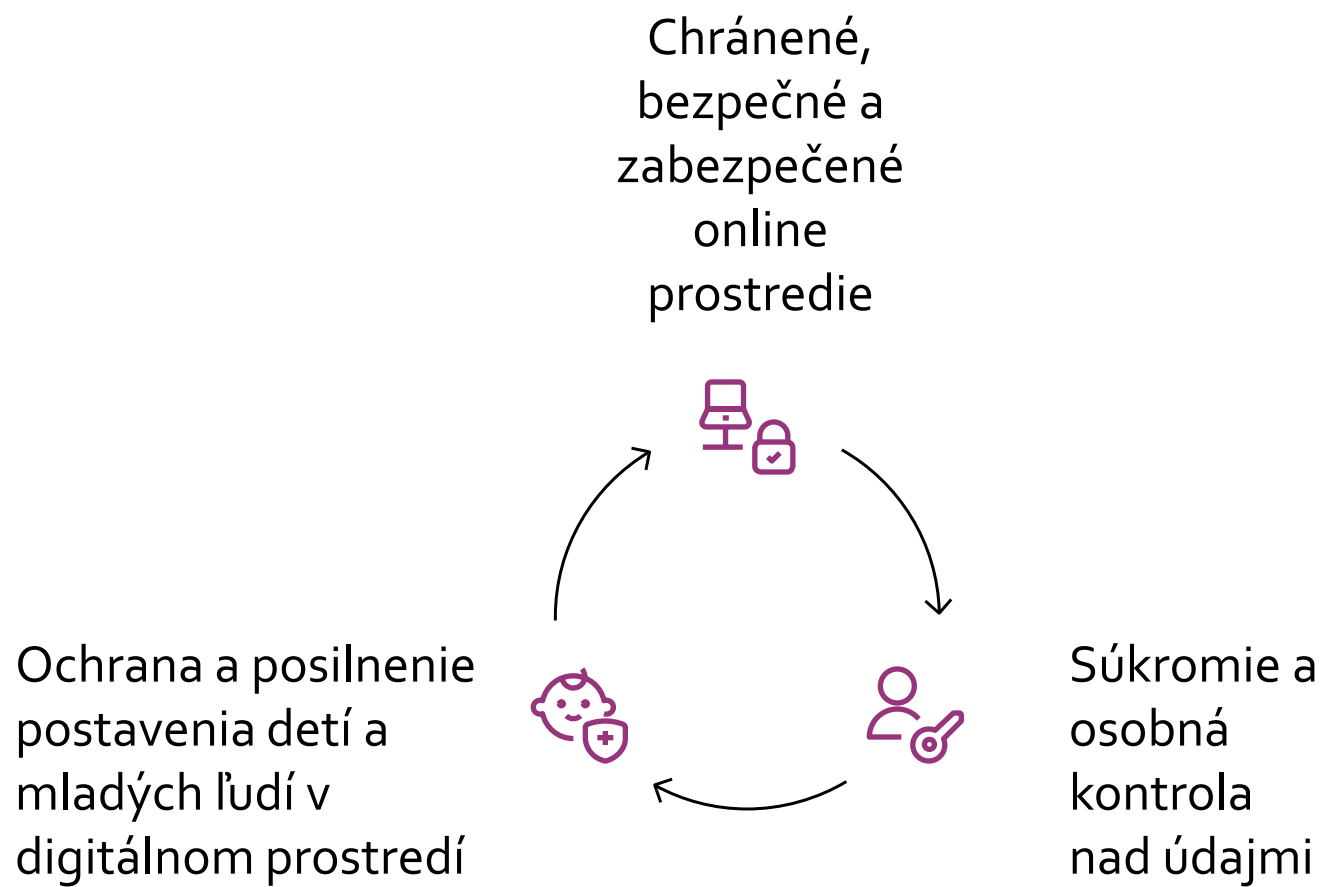
Európske vyhlásenie o digitálnych právach a zásadách v digitálnom desaťročí

KAPITOLA V

Bezpečnosť, ochrana a posilnenie
postavenia



#DigitalEU



KAPITOLA V

Bezpečnosť, ochrana a posilnenie postavenia

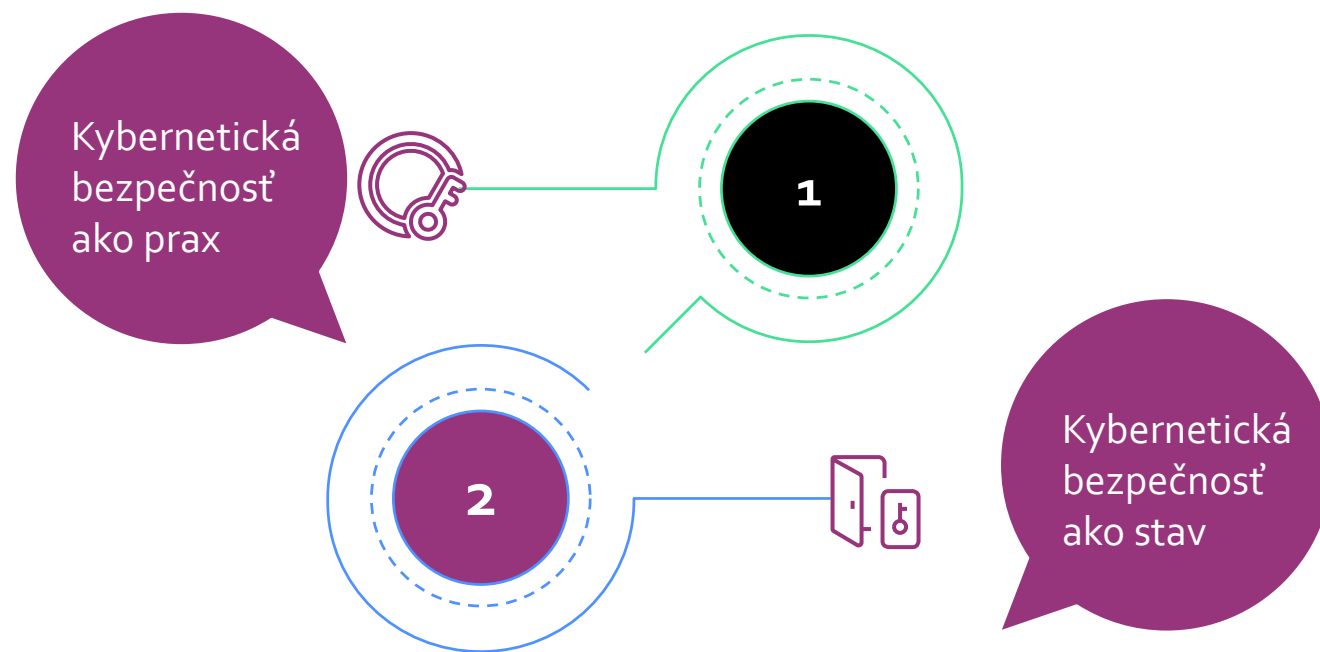
Chránené, bezpečné a zabezpečené online prostredie

16. Každý by mal mať prístup k digitálnym technológiám, produktom a službám, ktoré sú navrhnuté tak, aby boli bezpečné a chránené a aby chránili súkromie, čo vedie k vysokej úrovni dôvery, integrity, dostupnosti a pravosti spracúvaných informácií.

Zaväzujeme sa:

- a) prijímať ďalšie opatrenia na podporu výsledovateľnosti produktov a zabezpečenie toho, aby sa na digitálnom jednotnom trhu ponúkali len produkty, ktoré sú bezpečné a sú v súlade s právnymi predpismi EÚ;
- b) chrániť záujmy ľudí, podnikov a verejných inštitúcií pred kybernetickobezpečnostnými rizikami a kybernetickou kriminalitou vrátane porušenia ochrany údajov a krádeže totožnosti alebo manipulácie s ňou. To zahŕňa požiadavky na kybernetickú bezpečnosť pripojených produktov uvádzaných na jednotný trh;
- c) bojovať proti tým, ktorí sa v rámci EÚ snažia oslabiť bezpečnosť online a integritu digitálneho prostredia alebo propagujú násilie a nenávisť digitálnymi prostriedkami, a vyvodzovať voči nim zodpovednosť.

Právo na (kybernetickú) bezpečnosť



Právo na (kybernetickú) bezpečnosť

- činnosti a opatrenia na dosiahnutie kybernetickej bezpečnosti
- konkrétne akcie jednotlivcov, organizácií a štátov
- príklady: implementácia technických opatrení, monitorovanie hrozieb, reakcia na incidenty...

Kybernetická
bezpečnosť
ako prax

Právo na (kybernetickú) bezpečnosť

Kybernetická
bezpečnosť
ako prax

- **adresáti**
 - organizácie – T/O BO
 - jednotlivci – kybernetická hygiena
 - tí, ktorí musia konať (napr. poskytovatelia kritickej infraštruktúry, digitálni poskytovatelia služieb)
- **príjemcovia:** tí, ktorí majú prospech z BO (napr. občania, podniky)
- **predmet a pôsobnosť** (čo chráni KB?)
 - siete a IS?
 - údaje?
 - osoby?

Právo na (kybernetickú) bezpečnosť

- stav dosiahnutý po úspešnej realizácii praxe
- jednotlivci a organizácie existujú v chránenom kybernetickom priestore
- kľúčové prvky: ochrana pred kybernetickými hrozbami, očakávanie trvalej bezpečnosti



Kybernetická
bezpečnosť
ako stav

Právo na (kybernetickú) bezpečnosť

Kybernetická
bezpečnosť
ako prax

- **činnosti potrebné na ochranu** (sietí a informačných systémov, užívateľov takýchto systémov a iných osôb) dotknutých **kybernetickými hrozbami**.
- **všetky osoby**, bez ohľadu na to či sú používatelia SIS **majú právo na ochranu pred každou potenciálnou okolnosťou, udalosťou alebo činnosťou**, ktorá by ich mohla poškodiť, narušiť alebo inak negatívne ovplyvniť.

Kybernetická
bezpečnosť
ako stav

Právo na kybernetickú bezpečnosť



Právo na KB

- formálne zaviesť právo na kybernetickú bezpečnosť do práva EÚ ako prostriedok na posilnenie postavenia jednotlivcov v digitálnej oblasti
- jednotlivci musia byť schopní **chrániť sa pred digitálnymi hrozbami**
 - konkrétnymi právnymi nástrojmi
- ukladalo by **povinnosti ostatným rešpektovať a zabezpečovať kybernetickú bezpečnosť**
- paralely s právami ako súkromie a ochrana údajov

Etika kybernetickej bezpečnosti





Právo

Morálka (etika)

Trh

Architektúra - kód



Čo je to etika?



Etika

- filozofická disciplína, ktorá sa zaoberá otázkami ako by sme mali žiť, myšlienkami dobra a pracuje s pojmami ako „správne“ a „nesprávne.“
- „...pojomom „etika“ sa označuje teória morálky, veda o mravnosti, čiže filozofická disciplína, ktorá sa venuje skúmaniu morálky, jej pôvodu, podstaty a obsahu morálnych kategórií.“
- skúma racionálnu a praktickú reflexiu toho, čo je dobré a zlé; a zároveň skúma na inej úrovni čo je správne a nesprávne

Deskriptívna etika

Skúma tradície, princípy a zvyky rôznych ľudí a kultúr.

Etická teória

(normatívna etika)

Formuluje princípy správneho správania (usmernenia).

Aplikovaná etika

Skúma konkrétne etické problémy v praxi.

Etické
dilemy

Konflikty
hodnôt

Vzt'ah práva a etiky



Právo a etika

- modality, ktoré sú schopné regulovať správanie jednotlivcov
 1. právo a etika reflektujú úplnú jednotu - univerzálny morálny rámec
 2. právo a etika úplne odlišné fenomény, ktoré pochádzajú z odlišného zdroja
 3. pohľad prieniku a vzájomného ovplyvňovania medzi právom a etikou
- prienik P/E – základné ľudské práva a slobody
- etifikácia práva – odvolávanie sa na etiku, etické hodnoty, princípy (napr. Etické usmernenia pre dôveryhodnú AI)

Etické hodnoty kybernetickéj bezpečnosti



Etické hodnoty KB



Skupina hodnôt	Špecifikácia
BEZPEČNOSŤ	- Bezpečnosť jednotlivca - Národná bezpečnosť - Informačná bezpečnosť - Dôvernosť, integrita, dostupnosť
SÚKROMIE	- Autonómia - Dôstojnosť - Identita - Osobnosť - Anonymita - Dôvernosť
SPRAVODLIVOSŤ	- Spravodlivosť - Nediskriminácia - Rovnosť - Demokracia
ZODPOVEDNOSŤ	- Accountability - Liability - Transparentnosť - Vysvetliteľnosť

Konflikty hodnôt v kybernetickej bezpečnosti





Súkromie



Bezpečnosť



Súkromie



Spravodlivosť



Súkromie



Zodpovednosť



Zodpovednosť



Bezpečnosť



Spravodlivosť



Bezpečnosť

Ďakujem za pozornosť!