POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

FAKULTA BEZPEČNOSTNĚ PRÁVNÍ

Katedra veřejného práva

Evropská unie a regulace internetu

Bakalářská práce

Internet regulation in the European union
Diploma thesis

VEDOUCÍ PRÁCE

Mgr. et Mgr. Bohumil Peterka

AUTOR PRÁCE

Marek Janoušek

PRAHA 2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpala, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 13. 3. 2022 …….

Marek Janoušek

Poděkování

Rád bych touto cestou poděkoval Mgr. et Mgr. Bohumilu Peterkovi, za odborné vedení mé práce, jeho čas a cenné připomínky. V neposlední řadě, patří obrovské poděkování mé rodině, bez které bych tuto práci nemohl dokončit.

ANOTACE

V této bakalářské práci se věnuji regulaci internetu evropské unie, se zaměřením na poslední vývoj regulace této oblasti. Tímto vývojem je přijetí nařízení o digitálních trzích a nařízení o digitálních službách. První část práce popisuje dosavadní vývoj internetové regulace a aktuální rámec této problematiky, za účelem pochopení směru nových změn. Dále, tato část definuje základ pro pochopení internetové problematiky. V druhé části práce je věnována pozornost implementovaným změnám pro kyberprostor novými předpisy z pohledu platforem a uživatelů. Závěr práce pojednává o rozdílech v regulaci internetu světových velmocí USA, Číny a Evropské unie. Záměrem je začlenění internetové regulace do globálního kontextu.

KLÍČOVÁ SLOVA

Nařízení o digitálních trzích, Nařízení o digitálních službách, EU, regulace internetu, online platformy, digitální služby, osobní údaje, USA, Čína

ANNOTIATION

In this thesis, I discuss the regulation of Internet in the European Union, with a focus on recent developments in the regulation of this area. These developments are the adoption of the Digital Markets Act and the Digital Services Act. The first part of the thesis describes the previous developments in internet regulation and the current framework, to understand the direction of the new changes. Furthermore, this part defines the basis for understanding this area. The second part of the thesis focuses on the changes implemented for cyberspace by the new regulations from the perspective of platforms and users. The thesis concludes with a discussion of the differences in Internet regulation between global actors the US, China, and the European Union. The intention is to place internet regulation in a global context.

KEYWORDS

Digital Markets Act, Digital Services Act, EU, internet regulation, online platform, digital services, personal data, USA, China

Obsah

ÚVOD:

Od vzniku ARPANET uplynulo více než 50 let, což se možná zdá být v historickém měřítku krátké období. Opak je pravdou, neboť digitální prostor, jakožto snad nejrychleji se vyvíjející odvětví, zaznamenal nevídané množství změn a pokroků. S nárůstem vlivu digitálních technologií, platforem a služeb na každodenní život se objevila potřeba regulace. Tato regulace se zpočátku rozvíjela jako součást jiných legislativních oblastí, ale postupně se vyvinula do samostatné právní oblasti s širokým spektrem působnosti, především v důsledku struktury a charakteristik internetu.

Rychlý technologický pokrok a rostoucí digitalizace společnosti přinesly nesčetné výzvy a příležitosti. Jednou z významných výzev je regulace online platforem a služeb, která se stává stále složitější vzhledem ke globální povaze internetu a rozmanitosti obsahu dostupného online. V reakci na výzvy navrhla Evropská unie (EU) nařízení o digitálních službách (DSA) jako komplexní rámec pro regulaci online platforem a služeb navazující na nařízení o digitálních trzích (DMA). K pochopení změn v digitálním prostředí, bude úvodí část práce věnována přehledu právní úpravy a základním principům ovládající internet a kyberprostor. Před analýzou předpisů DSA a DMA je předsazen přehled klíčových právních dokumentů tvořících pilíře evropského internetového práva. Nařízení o digitálních službách je předpis účinný od února 2024 a jeho cíl je stanovit jasná pravidla a povinnosti pro online platformy a služby. Zohledňuje nové výzvy, které přináší nově vznikající technologie, jako je umělá inteligence, online reklama a algoritmická rozhodování. Za cíl si klade vytvoření nového regulačního rámce pro online platformy a služby, posílení dosavadních mechanismů. Předpis navazuje na Směrnicí o elektronickém obchodu, která je od svého přijetí v roce 2000 základním kamenem evropské digitální legislativy. Cílem této práce je analyzovat dosavadní kroky EU vedoucí k nejnovější právní úpravě. Finálním přínosem této práce je porovnání evropského modelu regulace internetu s čínským a americkým, jakožto globálními digitálními aktéry.

1. Přehled právní úpravy

Regulace internetu v Evropské unii je složitým a dynamickým procesem, který si klade za cíl harmonizovat národní předpisy a vytvořit jednotný evropský digitální trh. Tento vývoj lze shrnout jako snahu o dosažení konsenzu mezi členskými zeměmi s cílem stanovení evropského standardu, který by mohl sloužit jako vzor pro zbytek světa. Tento proces se vyrovnává s různými regulačními tradicemi jednotlivých členských zemí, které mohou mít různé přístupy k některým oblastem. Příkladem je regulace televize v EU se zaměřovala především na tvorbu kulturní politiky, zatímco regulace internetu, formulovaná ve Směrnici o elektronickém obchodu[1], se soustředila spíše na regulaci trhů služeb a ochranu podnikatelských svobod v online prostředí (Ibrus & Rohn, 2016).

EU se staví do pozice globálního hráče v oblasti kybernetické bezpečnosti a ukazuje své odhodlání řešit technologické výzvy a problémy spojené s kybernetickou bezpečností (Bermanns, 2023, s. 42-50). Přístup EU ke kyberprostoru se zaměřuje na ekonomické a bezpečnostní otázky. Úloha EU v tomto prostoru se přeměnila v intervenční (Renda, 2022, s. 467-490). Vytyčený směr je stát se příkladem pro svět, sjednotit členské státy a chránit uživatele, někdy za cenu tvrdšího přístupu k poskytovatelům.

Přístup Evropské unie k regulaci internetu byl formován velkou škálou faktorů, zahrnující liberalizační iniciativy v oblasti telekomunikací a elektronického obchodu, či samoregulační přístup k otázkám obsahu internetu (Halpin & Simpson, 2002, s. 285-296). Nařízení 95/46/EC[2] o ochraně dat bylo první reakcí na rozšíření internetu a zapojení více uživatelů v devadesátých letech. Průběh těchto let ukazuje na postupné uznávání potřeby právních rámců pro řešení vznikajících problémů a rychlejší aktualizaci toho rychle vyvíjejícího sektoru. Vrcholným ukazatelem, že se Evropská unie významně angažovala v veřejně politických aspektech správy internetu, bylo vytvoření internetové domény nejvyšší úrovně .eu koncem 90. let 20. století (Christou & Simpson, 2006,

[1] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)

[2] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

s. 43). Vytvoření domény .eu bylo významným krokem, protože to umožnilo lepší identifikaci evropských subjektů na internetu a přispělo k budování digitální identity Evropské unie

Regulace internetu v rámci Evropské unie se neomezuje pouze na technické aspekty, ale prolnula se i s širšími politickými úvahami. Ty zahrnují například vyváženost národní bezpečnosti a ochrany osobních údajů, dopady internetu na cestovní ruch a implementaci obecného nařízení o ochraně osobních údajů (GDPR)[3] ve všech členských státech (Dimitrova & Brkan, 2017, s. 751-765). Předmětem zkoumání je též promítnutí režimu ochrany údajů občanů EU do třetích zemí, což odráží zaměření EU na ochranu základního práva na soukromí (Bendiek & Römer, 2019, s.32-43). Třetí země byly vždy v kyberprostoru problémem z několika hledisek, především cloud computing, kterému se budu věnovat později v práci a nejasnost jurisdikce dopadající na firmy se sídlem mimo EU, ale jejichž stránky uživatelé můžou navštěvovat. Tento problém by měla nejnovější úprava nařízení o digitálních trzích[4] eliminovat, více v samostatné kapitole.

Vývoj regulačního prostředí internetu naznačuje přibližování přístupů mezi EU a USA. Tento trend je způsoben sdílenými výzvami, jako jsou kybernetické hrozby, regulace digitálního obsahu, mezinárodní standardy určené mezinárodními dohodami, jako je dohoda o obchodu s digitálním obsahem, a konečně spolupráce na globálním digitálním trhu (Jayasuriya, 2001, 101-120). Lze říct, že historie regulace internetu v právu EU představuje mnohostranný a dynamický proces ovlivněný členskými státy, politickými úvahami a vyvíjející se úlohou EU v oblasti správy internetu. Vývoj právních předpisů EU v oblasti internetu byl poznamenán pomalou reakcí a podpoře konkurence v oblasti sítí a komunikace, příkladem bylo úvodní nastavení cen roamingu v EU (Gual, 2002, s. 42-49). Problémy kyberprostoru vyústily v zaměření na klíčové faktory podporující rozšíření trhu, jako je poskytování obsahu a integrace evropského trhu. Legislativní aktivita

[3] 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)

[4] Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích)

Evropské unie v této oblasti byla rozsáhlá a zahrnovala smlouvy, autorská práva, ochranu údajů, obchodní sdělení, finanční služby, elektronickou hotovost a elektronické podpisy (Dickie, 1999).

Mezi stěžejní dokumenty vývoje internetového práva EU patří směrnice o elektronickém obchodu[5], směrnice o soukromí a elektronických komunikacích[6], GDPR, směrnice NIS 1[7]. Mezi podpůrné dokumenty se řadí směrnice 2005/29/ES[8] o nekalých obchodních praktikách, směrnice 2015/2366 o platebních službách na vnitřním trhu[9] a směrnice 2019/790 o autorském právu na jednotném digitálním trhu.[10] Tyto předpisy sjednotily poskytování digitálního obsahu a online prodej v celé Evropě a zásadně přeformulovaly právní rámec pro digitální obsah. Kromě toho se zabývají širokou škálou otázek, včetně elektronického obchodu, mezinárodní soudní pravomoci, regulace obsahu a projevu, odpovědnosti zprostředkovatelů, duševního vlastnictví, ochrany spotřebitelů, marketingu, ochrany údajů, soukromí, digitální identity, elektronických plateb a kyberkriminality (Savin, 2017, s. 1-15). Všechny uvedené předpisy jsou součástí snahy o harmonizaci a sjednocení právních předpisů s cílem dosáhnout efektivnější interakce nejen v rámci členských států EU, ale také s vnějšími partnery z třetích zemí. Tyto snahy se zvláště zaměřují na oblasti kybernetické bezpečnosti, autorských práv, ochrany osobních údajů a telekomunikačních služeb (Novytsky, 2021, s.370-374).

---

[6] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

[7] 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

[8] Směrnice Evropského parlamentu a Rady 2005/29/ES ze dne 11. května 2005 o nekalých obchodních praktikách vůči spotřebitelům na vnitřním trhu a o změně směrnice Rady 84/450/EHS, směrnic Evropského parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nařízení Evropského parlamentu a Rady (ES) č. 2006/2004 (směrnice o nekalých obchodních praktikách)

[9] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES)

[10] Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES

Zvláště evropská směrnice o elektronickém obchodu vytvořila právní režim pro regulaci evropského elektronického obchodu, který se zaměřuje na oblasti jako je uzavírání smluv online (článek 9 a oddíl 3), odpovědnost poskytovatelů internetových služeb (oddíl 4), ochranu spotřebitelů (článek 3), regulaci země původu a mimosoudní řešení sporů online (článek 17) (Edwards, 2006). Tato směrnice zavedla klíčové principy pro poskytování služeb a upravila odpovědnost zprostředkovatelských služeb za obsah třetích stran na úrovni EU.

Důležitým krokem ke spravedlnosti v kyberprostoru EU bylo nařízení o otevřeném přístupu k internetu (nařízení 2015/2120), které na úrovni EU zavádí ustanovení o neutralitě sítě (Brouwer, 2020). Toto nařízení mělo zásadní dopad na správu internetu ustanovením neutrality sítě, jakož klíčového prvku regulace internetu, který zajišťuje rovné zacházení se všemi daty na internetu, bez diskriminace nebo preference. Vliv EU dopadá i na globální instituce správy internetu jako jsou Internetová korporace pro přidělování jmen a čísel ICANN, Internetová inženýrská skupina IETF, kde EU aktivně působí na rozvoj. EU zaujala pozici vedoucího a vlivného hráče ve vyvíjejícím se procesu globální správy internetu (Christou & Simpson, 2012). EU byla aktivní účastníkem Světového summitu o informační společnosti, účastní setkání IGF a podílí se na diskusi a otázkách týkajících se správy internetu a digitální politiky.

Zapojení EU do regulace internetu se neobešlo bez problémů. Existují obavy, že snahy zaměřené na bezpečnost IT a regulaci internetu na národní úrovni mohou narušit otevřenou a všeobecně přístupnou povahu internetu, což může vést k jeho rozdrobení na národní segmenty (Pohle & Thiel, 2020). Kolem některých aspektů regulace internetu se objevily kontroverze a nejasnosti, jako je slučitelnost různých opatření pro řízení provozu s nařízením o otevřeném internetu 2015/2120 a otázka "nulových tarifů" (Nałęcz, 2021 s. 109-120). Nulové tarify jsou v mezinárodním obchodě součástí trhu uvnitř EU a také s některými přeshraničními zeměmi za cílem snížit nebo odstranit clo. Nařízení o otevřeném internetu by mohlo mít vliv na způsob, jakým jsou nulové tarify uplatňovány nebo interpretovány, zejména pokud jde o dodržování zásad neutrality sítě a zachování rovného přístupu k internetu pro všechny uživatele.

Vyvrcholením je soudní případ Telekom Deutschland GmbH v. Bundesrepublik Deutschland (T-79/12)[11], skončil rozhodnutím Evropského soudního dvora, který podpořil argumenty Telekomu Deutschland. Soudní dvůr Evropské unie (SDEU) rozhodl, že německá vláda porušila evropské právo tím, že zavedla regulaci, která byla diskriminační vůči jiným poskytovatelům telekomunikačních služeb. Toto rozhodnutí mělo důsledky nejen pro Telekom Deutschland, ale i pro celý trh v EU, jelikož ovlivnilo způsob, jakým jsou regulovány telekomunikační služby v souladu s evropskými právními předpisy a zásadami svobodné hospodářské soutěže. Přijetí GDPR v kontextu ekonomiky založené na datech, také vyvolalo významné změny pro podniky (Bendiek & Römer, 2019 s. 32-43). Na tyto změny špatně reagovaly firmy, které musely měnit své obchodní modely, zavést novou infrastrukturu, a to vše pod zvýšenými sankcemi za porušení předpisů. EU zajišťuje transparentnost své obchodní politiky tím, že prostřednictvím nařízení č. 1049/2001[12] poskytuje veřejnosti přístup k dokumentům EU a do dohledu nad transparentností obchodní politiky EU zapojuje evropského ombudsmana (Marx & Loo, 2021, s. 261-271).

Úloha EU v oblasti regulace a správy internetu je mnohostranná a zahrnuje ochranu údajů, neutralitu sítě, aspekty veřejné politiky a globální vliv. Její regulace a politiky měly dopad nejen na členy EU, ale také na mezinárodní společnosti a globální instituce správy internetu. EU se stala důležitým hráčem v mezinárodním kontextu, kdy aktivně formuluje a prosazuje normy a předpisy týkající se internetového prostředí. Tím posiluje svou pozici jako globálního lídra v oblasti digitální regulace a přispívá k utváření budoucnosti internetu a digitální ekonomiky.

[11] Rozsudek Soudního dvora (osmého senátu) ze dne 2. září 2021. Telekom Deutschland GmbH v. Bundesrepublik Deutschland.
[12] Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise

2. Základní pojmy:

2.1. Kyberprostor:

Moderní svět se velmi rychle podrobil vlivu internetu, informačním technologiím a stal se integrální součástí naší společnosti a životů. Rychlost, rozsah a interakce uživatelů jsou jen některé z aspektů, které internet nabízí a které jsou denně využívány.

Pojem kyberprostor označuje elektronické a elektromagnetické spektrum používané k ukládání, úpravě a výměně dat prostřednictvím sítí a fyzických infrastruktur. Jedná se o nekonečný prostor, počítačových interakcí a virtuální objekty. Pojem kyberprostor zahrnuje všechny jevy zprostředkované počítačem a je to nekonečný fenomén bez hranic. Je to prostorové prostředí, které integruje kybernetický a fyzický svět a poskytuje interaktivní prostředí pro každodenní činnosti (Pawar a spol, 2021, s. 210-214). Kyberprostor je proměnný a komplexní, stírá hranice mezi nehmotným a fyzickým prostorem a odráží integraci digitálního a materiálního prostoru. Zpochybňuje koncept prostorového dualismu, který odděluje kyberprostor od fyzického prostoru (Pawar a spol, 2021, s. 210-214). Regulace tohoto prostoru se stává nezbytnou, především s rostoucí kyber kriminalitou, zvyšujícím se objemem dat a potřebou ochrany soukromí a datové bezpečnosti.

Evropská unie a Spojené státy sehrály klíčovou roli v procesu regulace kyberprostoru, přesto se v některých bodech rozcházejí, například v otázkách ochrany dat, soukromí a neutralitě sítě. Evropská unie, konfrontována s rostoucím počtem uživatelů internetu, zaznamenala sílu elektronického obchodu, ale setkala se s vnitřními rozpory ohledně jednotného trhu a ochrany individuálních zájmů. Tato situace představuje výzvu v nalezení regulačního modelu, který by efektivně vyvážil práva uživatelů, legislativní normy, společenské hodnoty a zájmy (Chmiel a spol, 2011).

2.2. Architektura internetu

Internet, nevnikl s cílem vytvoření jeho dnes známé podoby, ale spíše jako organická evoluce reagující na potřeby uživatelů tehdejší sítě ARPANET, která byla původně navržena jako univerzitní síť. Postupné rozšiřování a adaptace na nové požadavky nakonec vedly k transformaci ARPANET v komerčně dostupnou síť, kterou známe dnes jako internet, a to v roce 1990.

Jedinečnost struktury internetu spočívá v jeho vrstvené architektuře, neutralitě a principu end-to-end. Tento princip znamená, že funkce jsou umístěny v koncových zařízeních uživatelů, což umožňuje flexibilitu a decentralizovanou správu. (Savin, 2017, s. 1-8). Nejsou tedy umístěny v prostřednících jako jsou směrovače, modemy a přepínače. Je důležité mít na paměti vlastnosti vrstev internetu při formulaci regulací, neboť přístup by měl být zaměřen na individuální problémy a neřešit je obecně. Internet je nehomogenní a decentralizovaný systém, který nevyžaduje centrální distribuci, což znamená, že každá vrstva má své specifické charakteristiky a potřeby. Regulace by proto měly být navrhovány s ohledem na tuto komplexnost a diverzitu internetového prostředí. (Froomkin, 1997, 129-153)

Problém v architektuře pro regulaci internetu spočívá v tom, že uživatelé mají schopnost vyhýbat se nepříznivým podmínkám přenesením se do prostředí s příznivějším hostováním. Odpovědnost je nejasná jak pro poskytovatele, tak pro hostitele a online platformy, jako jsou sociální sítě. Například šifrování a ochrana dat může bránit v získání dat pro legitimní účely, jako je vyšetřování zločinu. Cloud computing a ukládání dat mimo hranice EU komplikují otázku jurisdikce, správy a ochrany dat. Cloud služby umožňují ukládat a přistupovat k datům odkudkoliv prostřednictvím internetu. Ukládáním dat do třetích zemí může dojít k vystavení riziku neoprávněných přístupů a úniku od jurisdikce EU. Správu dat zhoršují velmi slabým dohledem a transparentností nad používáním dat. Uložená data by teoreticky v jeden moment dodržovaly více právních režimů, což pravděpodobně vyvrcholí v jejich nedodržení. Tato komplexní situace vyžaduje pečlivé zvážení a vyvážení různých zájmů a potřeb v rámci regulace internetu.

Neutralita internetu jako jednoduchý pojem skrývá několik zásadních problémů a politických agend. Tato koncepce zastává názor, že vlády by měly zamezit poskytovatelům internetových služeb v rozlišování mezi různými typy dat. V současné době internet poskytuje stejné standardy služeb bez ohledu na povahu přenášeného obsahu. Problém síťové neutrality vzniká v situaci, kdy poskytovatelé obsahu usilují o rychlejší přístup k infrastruktuře, aby mohli účtovat vyšší poplatky za tzv. prémiový obsah. Tato otázka s politickými důsledky má významný vliv na to, jak bude internet fungovat ve 21. století. Je to jedna z klíčových výzev, kterým čelí regulátoři, když se snaží zajistit rovný přístup a spravedlivé podmínky pro všechny uživatele internetu. (Savin, 2017, s. 1-20) Síťová neutralita podporuje inovace tím, že zajišťuje rovné podmínky pro všechny uživatele internetu a podniky bez ohledu na jejich velikost nebo zdroje. Zabraňuje poskytovatelům internetových služeb upřednostňovat určité webové stránky nebo služby před jinými, což umožňuje začínajícím a malým podnikům konkurovat velkým společnostem za stejných podmínek. Tím, že poskytovatelům internetových služeb zakazuje blokovat nebo omezovat určité typy obsahu, podporuje síťová neutralita rozvoj nových a inovativních online služeb a aplikací. Síťová neutralita rovněž podporuje hospodářskou soutěž a investice do internetové infrastruktury, protože poskytovatelé internetových služeb nemohou využívat své kontroly nad internetovým provozem k potlačování hospodářské soutěže nebo k vymáhání dodatečných poplatků od poskytovatelů obsahu.

Jedinečnost internetu lze tedy spatřovat v jeho decentralizaci, chybějících hranicích, neutralitě, nejasnosti odpovědnosti, šifrování, ochraně dat a vzdáleném přístupu k datům. Tvoří však úskalí a možnost pro nelegální činnost, kterou je třeba čelit.

2.3. Správa internetu

Správa internetu je termín, který se používá k popisu procesů a mechanismů, jimiž je internet řízen a regulován. Zahrnuje vývoj a zavádění politik, standardů a protokolů, které řídí používání a fungování webu. S rozvojem digitálních technologií a propojením globálních sítí nabývá správa internetu na významu. Zahrnuje řadu různých aspektů, včetně technických norem, kybernetické bezpečnosti, ochrany údajů, práv duševního vlastnictví a přístupu k internetu. Spolupráce mezi veřejnými a soukromými subjekty, stejně jako mezinárodní spolupráce, jsou nezbytné pro efektivní správu internetu. Správa hraje zásadní roli při udržování stabilního, bezpečného otevřeného internetu, v podpoře pokroku a hospodářského růstu. Správa internetu v Evropské unii prošla v průběhu času vývojem, ve kterém došlo k posunu směrem k většímu zapojení orgánů veřejné správy a snaze o dosažení digitální suverenity. Evropská unie aktivně podporuje prohlubování svého jednotného digitálního trhu a zavádí reformy zaměřené na řešení problémů v oblasti digitální ekonomik (Heidebrecht, 2024, s. 205-223).

Zavádění moderních digitálních nástrojů a online služeb umožňuje efektivnější řízení veřejných záležitostí a snižuje administrativní zátěž pro občany i podniky. E-government přispívá k transparentnosti, což posiluje odpovědnost institucí a usnadňuje sledování veřejných politik a rozhodovacích procesů. (Linhartová, 2022, s. 267-287). Pro dosažení digitální suverenity v rámci Unie je nezbytné provádět investice, uplatňovat regulace a dokončit výstavbu digitálního vnitřního trhu. (Metakides, 2022, s. 219-225) To zahrnuje zlepšování infrastruktury pro digitální komunikace, podporu inovací v oblasti informačních technologií, vytváření bezpečných prostředí pro online aktivity občanů a podniků a zavádění příslušných právních předpisů pro ochranu osobních údajů, kybernetickou bezpečnost a digitální obchod. Tyto kroky jsou klíčové pro udržení konkurenceschopnosti Evropské unie v digitální éře a zajištění prosperujícího a bezpečného digitálního prostředí pro všechny její občany a podniky.

Strategie Evropské unie zahrnuje využití různých legislativních nástrojů, jako jsou nařízení o digitálních službách[13], digitálním trhu prostředím DMA a ochraně dat skrz GDPR. Pro dosažení úspěchu těchto iniciativ je klíčové správné načasování a koordinace opatření. V posledních desetiletích došlo k významnému rozvoji digitální správy, zvláště s nástupem aktuální generace 5G a připravovanými změnami spojenými s generací 6G. Tento vývoj poskytuje vedoucím představitelům možnost zaměřit se na jiné úkoly než na správu rozhodovacích sítí. Veřejná i soukromá správa, zejména v oblasti informačních technologií, tak představuje robustní obranný mechanismus. Technologický pokrok, zejména v oblasti informačních technologií, výrazně změnil rámcové podmínky pro veřejnou i soukromou správu po celém světě. Digitální technologie řeší stávající socioekonomické problémy, ale současně vyvolávají nové výzvy týkající se bezpečnosti informací, kryptografie a ochrany soukromí.

Rostoucí důležitost digitálních služeb vyústila v prohloubení jednotného digitálního trhu a revizi přístupu k jeho správě. Během snahy o lepší kontrolu nad digitálním prostředím došlo k posunu od tržně liberálního přístupu k více intervenčnímu veřejnému přístupu. Výzvy spojené s digitální ekonomikou, jako je ochrana údajů a regulace digitálních služeb, vyžadovaly širší politické cíle než jen zajištění konkurenceschopnosti. Zúčastněné strany a veřejné orgány nabývaly na významu v procesech řízení, což reflektovalo posun od podnikatelských subjektů (Heidebrecht, 2024, s. 205-223).

2.4. E-komerce

Internet vytvořil nový typ obchodování známý jako elektronický obchod, který umožňuje interakci v online prostředí bez ohledu na státní hranice, především v oblasti nehmotného zboží. Legislativa EU věnuje elektronickému obchodu značnou pozornost a prošla významným vývojem od svého počátku. Evropská unie vytvořila pevný regulační rámec pro elektronický obchod a nedávno došlo k mnoha změnám na úrovni EU v této oblasti. Změny zahrnují strategii pro jednotný digitální trh, průzkumy v odvětví elektronického obchodování a DMA

[13] Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách)

(Dumortier,2022, s. 427-488). Digitální ekonomika poháněná elektronickým obchodem měla významný dopad na právo EU v oblasti hospodářské soutěže, což vedlo ke změnám v posuzování otázek hospodářské soutěže na digitálních trzích (Lodder, 2017, s. 1-14). Zavedeny byly nové metody posuzující charakteristické měřítka a sběr dat. Vlivem ochrany spotřebitelů dochází k transparentnosti cen a potlačení falešných reklam či nekalých praktik. Možná však nejdůležitější je omezení možnosti monopolu a snížení bariéry vstupu pro menší firmy.

Evropský trh elektronického obchodu má zásadní význam pro hospodářství EU a je předmětem pozornosti v oblasti právních předpisů, které jsou navrženy tak, aby zajistily jeho efektivní fungování a ochranu spotřebitelů. (Ekingen, 2022). Oblasti usnadňující obchod jsou kontrola plateb na dálku k zajištění bezpečné transakce, dodržování DPH, ochrana spotřebitele například možností vrácení a ochranou jeho údajů. V tomto směru se výrazně liší od přístupu USA, kde je tendence k upřednostňování minimálních zásahů do obchodních aktivit (Tofan, Bostan, 2022).

Právní prostředí na pomezí práva hospodářské soutěže a elektronického obchodu prochází rychlou aktualizací, což přineslo mnoho změn na úrovni Evropské unie. Strategie pro jednotný digitální trh představena v roce 2015, od té doby byla přetavena do platných právních předpisů. Její cíle jako volný pohyb digitálních služeb, posílení důvěry, podpora podnikání, posílení hospodářské soutěže a zlepšení právního rámce dnes zajišťují předpisy jako DMA, DSA, GDPR a směrnice o autorském právu na jednotném digitálním trhu[14]. Otázky hospodářské soutěže v elektronickém obchodě se soustředí na vertikální dohody mezi podniky na různých úrovních výroby nebo distribuce, označované jako B2P, a také na horizontální dohody mezi konkurenčními podniky na stejné úrovni, známé jako B2B neboli business-to-business (Aamir, 2022, s. 16-19).

[14] Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES

Rozvoj online platforem a nových obchodních modelů v online sektoru představuje výzvu pro právo hospodářské soutěže, zejména v kontextu možného zneužití dominantního postavení na trhu. Jako odpověď na tyto výzvy vznikly regulace jako DMA a DSA, které se zabývají otázkami hospodářské soutěže a regulace digitálního prostředí. Tento trend odráží úsilí EU přizpůsobit právní rámec hospodářské soutěže novým výzvám, které přináší vznik online platforem a nových obchodních modelů, zejména pokud jde o zneužívání dominantního postavení na trhu. Současná legislativa, včetně DMA a DSA, se snaží adresovat tyto problémy a zajistit spravedlivé podmínky pro digitální ekonomiku.

Typy interakce v elektronickém obchodu zásadně ovlivňují tvorbu příslušných regulačních nástrojů. Typ B2B (Business-to-Business) označuje obchodní transakce mezi jedním podnikem a jiným podnikem, kde jeden podnik nabízí své výrobky nebo služby druhému podniku. Právu B2B e-komerce se zaměřuje na obchodní smlouvy mezi firmami, ochranu duševního vlastnictví, správu rizik, odpovědnost, elektronickou autentizaci a záležitosti týkající se elektronického fakturování. B2C (Business-to-Consumer) jsou transakce mezi podniky a spotřebiteli, kde podniky přímo prodávají své výrobky nebo služby jednotlivým spotřebitelům. Právní předpisy týkající se B2C e-komerce upravují ochranu spotřebitelů, příkladem je právo na vrácení zboží, ochranu osobních údajů a spotřebitelské smluvní právo. C2C (Consumer-to-Consumer) transakce, kde spotřebitelé prodávají zboží nebo služby jiným spotřebitelům. Tento typ se často provozuje prostřednictvím online tržišť, kde jednotlivci mohou inzerovat a prodávat své produkty nebo služby ostatním uživatelům. Právní rámec pro C2C e-komerce se zaměřuje na ochranu uživatelů online tržišť a platforem, včetně pravidel pro inzerci, platebních mechanismů, ochranu proti podvodům a podmínky použití. B2G (Business-to-Government) představuje obchodní transakce mezi podniky a vládními subjekty, kde podniky dodávají své produkty nebo služby vládním institucím. G2B (Government-to-Business): E-komerce, kde vládní orgány poskytují služby firmám. To může zahrnovat online portály pro podávání daňových přiznání, žádosti o povolení nebo veřejné zakázky. Právní rámce pro e-komerce mezi vládou a firmami zahrnují právní předpisy týkající se veřejných zakázek,

elektronických služeb veřejné správy, správy údajů a práv spotřebitelů při interakci s veřejnými institucemi online. (Aamir, 2022, s. 16-19).

Různé formy elektronického obchodu mají vliv na hospodářský rozvoj, a vyšší míra inovací v oblasti elektronického obchodování je spojena s vyšším úrovní hospodářského růstu dané země. Kromě toho elektronické obchodování změnilo provoz a obchodní modely v cestovním ruchu a poskytlo užitečný kanál pro šíření informací týkajících se cestování. V rámci B2B elektronického obchodu došlo k usnadnění digitálního marketingu, elektronické výměně dat a podpoře mezinárodního obchodu. (Aamir, 2022, s. 16-19).

V odpovědi na výzvy spojené se zbožím a službami, které se v posledních letech objevily, přijala EU několik iniciativ. Mezi ně patří právní předpisy, které se zabývají ochranou spotřebitelů (směrnicí o právech spotřebitelů[15]), autorskými právy (směrnicí o autorském právu na digitálním trhu[16]), ochranou osobních údajů (skrz GDPR) a elektronickým obchodem. Nejnovější legislativní směry a navrhované reformy se postupem času zpřísňují, jak je patrné v další kapitole. Tímto způsobem se snahy o regulaci internetového obchodu vyvíjejí v souladu s dynamickým charakterem digitálního prostředí a adresují nové výzvy a hrozby, které se objevují v důsledku technologického pokroku a změn ve způsobu, jakým lidé využívají internet.

[15] Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS a směrnice Evropského parlamentu a Rady 97/7/ES

[16] Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES

3. Rámec internetové úpravy

3.1. Směrnice o elektronickém obchodu

Směrnice o elektronickém obchodu 2000/31/ES[17] v Evropské unii slouží k zajištění právní jistoty a harmonizaci pravidel pro online služby. Zavádí mechanismy pro volný pohyb služeb informační společnosti v rámci EU (článek 1) a zajišťuje, aby poskytovatelé služeb nepodléhali v různých členských státech mnoha různým a protichůdným předpisům.

Tato směrnice obsahuje ustanovení týkající se odpovědnosti zprostředkovatelů (oddíl 4), elektronických smluv (článek 9) a poskytování informací poskytovatelů služeb (kapitola 2, oddíl 1). Dále se zaměřuje na odpovědnost zprostředkovatelů v elektronickém obchodě (kapitola 2, oddíl 4) a ustavuje jejich odpovědnost a povinnosti poskytovatelů služeb, jako jsou poskytovatelé internetových služeb a online platforem. Prosazuje princip země původu, což znamená, že poskytovatelé služeb podléhají zákonům a předpisům své domovské země, a nikoli země, kde je služba přijímána (Lodder, 2017, s. 1-14). Směrnice o elektronickém obchodu hraje zásadní roli při usnadňování přeshraničního elektronického obchodu a vytváření rovných podmínek pro online podniky v rámci EU. Tím pomáhá vytvářet rámec pro volný pohyb služeb informační společnosti a zabraňuje vzniku překážek pro poskytovatele služeb v různých členských státech. Tato směrnice sehrála klíčovou roli při zajištění rovného zacházení s papírovými a elektronickými informacemi, čímž zvýšila právní předvídatelnost elektronického obchodu. Dále pomohla vytvořit jasný právní rámec pro elektronické obchodování, což bylo nezbytné zejména pro malé podniky, aby mohly využívat vznikající technologie a získat přístup na nové trhy. Celkově směrnice přispěla k posílení důvěry spotřebitelů v objednávání zboží a služeb online, neboť elektronické transakce byly uznány za právně platné a vymahatelné. (Brownsword, 2018, s. 165-204)

[17] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)

Směrnice zavedla předpisy o obchodních sděleních v elektronickém obchodě (oddíl 2), které se věnují otázkám jako je reklama a marketingové praktiky. Tento oddíl stanovuje pravidla pro elektronický obchod mezi podniky a spotřebiteli, včetně požadavků na označování komerčních sdělení a informací o právech spotřebitelů. Rovněž stanovila pravidla pro uzavírání smluv online (oddíl 3), včetně ustanovení o platnosti a vymahatelnosti elektronických smluv v druhém oddíle (Lodder, 2017, s. 1-14). Směrnice hraje klíčovou roli při usnadňování přeshraničního elektronického obchodu a vytváření rovných podmínek pro online podniky v rámci EU. Jejím účinek podpořil volný pohyb služeb informační společnosti v rámci EU a zabránil podnikům v podléhání různým a protichůdným předpisům v jednotlivých členských státech (Lodder, 2017, s. 1-14).

Hlavním účelem směrnice o elektronickém obchodu je stanovit mezinárodně přijatelná pravidla pro elektronický obchod, odstranit právní překážky a zvýšit právní jistotu v této oblasti. Jednou z hlavních změn, které tato směrnice přinesla, je zavedení rámce podmíněné odpovědnosti pro online zprostředkovatele, který je chrání před odpovědností za nelegální či protiprávní jednání třetích stran na jejich platformách.

3.2. Obecné nařízení o ochraně osobních údajů

GDPR 2016/679 má zásadní význam pro budoucnost globálního digitálního obchodu, zejména pro země, které chtějí získat přístup na trh se 400 miliony spotřebitelů v Evropské unii. Toto nařízení vyžaduje, aby tyto země přijaly podobná opatření k ochraně osobních údajů, což zahrnuje aktualizaci a úpravu svých právních systémů kvůli zpracování rozsáhlých toků dat (Fahey, 2022, s. 30-31). Jakožto komplexní předpis o ochraně osobních údajů v EU stanovuje harmonizovaný rámec pro zpracování a předávání osobních údajů. Tento právní předpis má za cíl chránit soukromí a osobní údaje jednotlivců v digitálním prostředí a zajišťuje dodržování jednotných pravidel v celé EU.

GDPR poskytuje jednotlivcům větší kontrolu nad jejich osobními údaji, včetně práva na přístup, opravu a výmaz údajů (článek 15), a zavazuje organizace, které shromažďují a zpracovávají osobní údaje, k dodržování přísných bezpečnostních opatření (článek 5). Právo být zapomenut poprvé vyřčeno na

půdě soudního dvora ve věci Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos, Mario Costeja González[18]. Rozhodnutí bylo později implementováno v GDPR. Toto pravidlo posílilo práva na ochranu osobních údajů občanů EU a otevřelo cestu k možnosti požadovat od vyhledávačů odstranění určitých informací o sobě.

Předpis rozšiřuje působnost na organizace mimo EU, které zpracovávají údaje obyvatel EU (článek 3). Tato rozšířená působnost zahrnuje jakékoliv organizace, které nabízejí zboží nebo služby občanům EU nebo sledují jejich chování. Subjekty zpracování údajů mají povinnost oznamovat porušení zabezpečení údajů do 72 hodin od zjištění (článek 33). Povinnost zahrnuje oznamování dozorovým orgánům pro ochranu údajů a ve vhodných případech i dotčeným osobám (Chirica, 2017, s.159-176). Tato povinnost má za cíl zajistit rychlou reakci na bezpečnostní incidenty a ochranu údajů dotčených osob. Každý členský stát má svůj dozorový orgán pro ochranu údajů. V České republice zastává tuto pozici Úřad pro ochranu osobních údajů. GDPR posiluje práva fyzických osob v oblasti ochrany osobních údajů a ukládá organizacím přísné povinnosti, včetně pověření pověřence (kapitola 4, oddíl 4) pro ochranu osobních údajů a dodržování technických a organizačních opatření k zajištění ochrany údajů. Dozorovým úřadům poskytuje nařízení větší pravomoci v oblasti prosazování, například formou auditu a možnost ukládat vysoké pokuty za nedodržování předpisů (článek 58). Tyto pokuty se mohou dostat až k výši 4 % celkového ročního obratu (článek 83).

Celkově přináší GDPR důkladnější ochranu osobních údajů a zvyšuje právní jistotu v oblasti digitálního obchodu v rámci EU. Praktické uplatnění GDPR přesáhlo hranice Evropské unie, což znamená, že nařízení je aplikovatelné i na mezinárodní úrovni. Překonává se tak dřívější zásada teritoriality a nahrazuje ji zásada osobnosti, která stanovuje, že GDPR se vztahuje na zpracování osobních údajů fyzických osob bez ohledu na jejich aktuální umístění (Chirica, 2017, s.159-176). Tímto rozšířením praktického působení GDPR se zajišťuje,

[18] Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014.Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González. Věc C-131/12.

že tento právní předpis není omezen pouze na občany EU nebo subjekty působící v rámci EU, ale aplikuje se i na zpracování osobních údajů fyzických osob mimo území EU. Cílem tohoto rozšíření je zajistit ochranu soukromí a osobních údajů fyzických osob v globálním měřítku, přičemž se bere v úvahu rostoucí trend digitalizace a globalizace dat.

3.3. Směrnice o bezpečnosti sítí a informací

Směrnice o bezpečnosti sítí a informací (NIS) [19] je legislativním nástrojem Evropské unie, který má za cíl zavést vyšší standard kybernetické bezpečnosti v klíčových odvětvích a chránit citlivé údaje a základní služby před kybernetickými útoky. Tato směrnice ukládá technické a procedurální požadavky provozovatelům (kapitola 4 a 5) a stanovuje postupy pro reakci v případě hlášení incidentů (Valentino, 2023). V rámci této směrnice jsou stanoveny povinnosti v oblasti kybernetické bezpečnosti a vyžaduje se hlášení bezpečnostních incidentů do orgánů dohledu (články 14 a 16). Směrnice se zaměřuje na přístup založený na rizicích a klade důraz na hlášení vážných incidentů, které mohou způsobit škodu, a informování o kybernetických hrozbách.

Směrnice zavádí síť bezpečnostních týmů typu CSIRT (článek 9 a příloha 1), který sleduje bezpečnostní upozornění od vnitrostátních orgánů. Hlavní funkce těchto týmů je monitorovat a reagovat na incidenty, oznamovat je příslušným stranám a poskytovat analýzy. Mimo jiné se účastní se v mezinárodní síti bezpečnostních týmů, spolupracují se soukromím sektorem. NIS přinesla změny, rozšířením působení na širší spektrum podniků a odvětví, revidovala požadavky na kybernetickou bezpečnost a přidala nové povinnosti a odpovědnosti. Kromě toho vyzývá k vytvoření vnitrostátních reakčních rámců na mimořádné události (Bagnato, 2020, s. 111-122). Směrnice rovněž vyžaduje hlášení významných bezpečnostních incidentů (článek 6) a kybernetických hrozeb orgánům dohledu. Zahrnuje různá odvětví, jako je průmyslová automatizace a robotizace, která podléhají dalším předpisům EU. Implementace směrnice NIS se může lišit v jednotlivých zemích, což povede k rozdílným právním povinnostem

[19] 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

a sankcím pro poskytovatele digitálních služeb. Tyto změny budou ovlivňovat způsob, jakým jsou hlášeny významné incidenty podle stávající směrnice NIS.

Reformou tohoto rámce je směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS 2)[20], která si klade za cíl zlepšit určování významných incidentů hodných hlášení. Navrhuje, aby se s incidenty bez hmotné škody zacházelo stejně jako s těmi, které vedly ke škodě doplněním definice kybernetické hrozby (článek 1), za účelem získat komplexní porozumění kybernetických hrozeb. Aktualizovaná verze rozšiřuje působnost na více podniků a odvětví. (článek 26) K rozšíření dochází také u požadavků a povinností v oblasti kybernetické bezpečnosti (článek 7), zesílení vnitrostátní spolupráce (článek 13) a zejména ke spolupráci členských zemí (kapitola 3). Směrnice NIS 2 přináší odstupňovaný proces hlášení, který rozlišuje mezi subjekty považovanými za základní a důležité (článek 3). Cílem této změny je optimalizovat hlášení a zabránit zahlcení příslušných vnitrostátních orgánů nadměrným počtem oznámení relativně málo nebezpečných hlášení. Klasifikace podniků podle směrnice NIS 2 je určena na základě velikosti podniku, což pomáhá členským státům snížit byrokratickou zátěž spojenou s klasifikací. Provozovatelé, kteří byli dříve vyňati ze směrnice NIS, se nyní mohou setkat s novými povinnostmi týkajícími se dodržování předpisů při svém působení v Evropě. Firmy, které již spadají pod směrnici NIS 1, by měly přehodnotit svůj postoj k dodržování předpisů, aby minimalizovaly svá právní rizika v tomto regionu. Směrnice NIS 2 zavádí minimální technická, provozní a organizační opatření ke kontrole kybernetických hrozeb a povinnost zajistit takovou úroveň bezpečnosti, která odpovídá představovanému riziku. Podniky mohou využít své zkušenosti s NIS 1 k vylepšení své stávající úrovně bezpečnostní vyspělosti a postupů. Směrnice rozšiřuje dosah předchozí směrnice NIS o další podniky a odvětví. (Valentino, 2023).

Směrnice o bezpečnosti sítí a informací je prvním právním předpisem EU v oblasti kybernetické bezpečnosti. Jejím cílem je chránit síťové a informační systémy. Byla zavedena s cílem řešit roztříštěné regulační prostředí a zlepšit

[20] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

úroveň kybernetické bezpečnosti v celé EU. Zavedla rámec pro hlášení kybernetických bezpečnostních incidentů, který vyžaduje, aby byly významné incidenty hlášeny dozorovým orgánům. Tato směrnice přijímá přístup založený na hodnocení rizik a klade důraz na hlášení incidentů, které mohou způsobit škodu, stejně jako na sdílení informací o kybernetických hrozbách s příjemci služeb (Valentino, 2023).

Cílem směrnice NIS 2 je reformovat stávající rámec pro hlášení kybernetických incidentů, který byl nastaven předchozí verzí směrnice NIS. Uznává potřebu proaktivního přístupu k problematice kybernetické bezpečnosti a navrhuje změny v definici významných incidentů, které by měly být hlášeny. Navrhuje, aby se s incidenty, které nepřinesly konkrétní hmotné škody, zacházelo stejně jako s těmi, které škodu způsobily. To by mělo přispět k lepšímu porozumění kybernetickým hrozbám a prostředí, ve kterém působí. NIS 2 rozšiřuje oblast působnosti své předchůdkyně, zahrnuje více společností a odvětví a zavádí nové povinnosti a odpovědnost. Členské státy mají čas do října 2024, aby uvedly své právní předpisy do souladu s novou směrnicí. Harmonizací právních předpisů v oblasti kybernetické bezpečnosti v členských státech EU má směrnice NIS 2 za cíl vytvořit robustnější regionální právní rámec kybernetické bezpečnosti a snížit složitost. Stěžejní body jsou pro ni připravenost, vyšší odolnost a účinnost.

3.4. Nařízení o otevřeném internetu

Nařízení o otevřeném internetu[21] zavádí opatření a zásady, které mají zajistit rovné a neomezené využívání internetu, přičemž brání diskriminaci a předsudkům v přenosu a poskytování internetového provozu. Hlavním cílem je zajištění síťové neutrality v rámci Evropského hospodářského prostoru. To znamená, že všem uživatelům a obsahu na internetu by měla být poskytována stejná úroveň služeb a přístupu bez ohledu na to, jaký obsah prohlížejí nebo odesílají. Nařízení také reguluje otázky datového roamingu (článek 6 a-f) a podporuje svobodný a neomezený přístup k síti (článek 4). Jde o důležitý krok k zajištění otevřeného,

[21] Nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) č. 531/2012 o roamingu ve veřejných mobilních komunikačních sítích v Unii

volného a neomezeného přístupu k internetu pro všechny uživatele v rámci EU. (Dumortier, 2022, s.281-307). Český telekomunikační úřad má za úkol dohlížet na dodržování a vymáhání legislativy v této oblasti a pravidelně vypracovává každoroční zprávy, které jsou dostupné na jejich webových stránkách.

Ochrana otevřeného a neutrálního internetu vyvolává otázky a výzvy v řadě oblastí práva a regulace. Patří mezi ně práva duševního vlastnictví, soukromí a svoboda projevu. Některé aspekty ochrany otevřeného internetu mohou být vnímány jako potenciální hrozba pro práva duševního vlastnictví, zejména v oblasti sdílení obsahu a autorských práv. Obtíže při vymáhání autorských práv a práv duševního vlastnictví mohou vzniknout v důsledku zajištění otevřenosti a neutrality internetu. Otevřený internet vyvolává otázky týkající se ochrany soukromí uživatelů. Je třeba nalézt rovnováhu mezi ochranou soukromí a volným přístupem k informacím, neboť zajištění neutrality a otevřenosti může způsobit, že osobní údaje uživatelů budou přístupnější a snadněji zneužitelné. Regulace otevřeného internetu může mít obzvláště významný dopad na poskytovatele internetových služeb. Pro poskytovatele těchto služeb to znamená, že nemohou upřednostňovat svůj vlastní obsah nebo služby nad obsahem a službami svých konkurentů (Holznagel, Hartman, 2016, s, 488-493). Odpovědí na tyto výzvy je rozšíření evropského regulačního rámce předpisy jako je GDPR, DSA a DMA.

Výsledným přínosem regulace otevřeného internetu je zajištění zásady síťové neutrality, která je považována za klíčový prvek moderního hospodářského rozvoje. Má zásadní význam pro ochranu práv jednotlivců, veřejné morálky, veřejného pořádku a národní bezpečnosti. Regulace internetu v souladu s dohodami světové obchodní organizace (WTO), by měla respektovat zásady volného obchodu, nediskriminace a transparentnosti, aby se minimalizovala rizika obchodních sporů mezi členskými státy, avšak vede se diskuse o tom, zda regulace internetu představuje obchodní překážku (Nanxiang, 2022, 1-30). Některé země a subjekty mohou argumentovat, že určité formy regulace mohou narušovat obchodní prostředí nebo způsobovat nerovnováhu v mezinárodním obchodě.

3.5. Směrnice o soukromí a elektronických komunikacích

E-Privacy nařízení 2002/58/ES[22], které doplňuje a rozšiřuje pozdější předpis GDPR, aplikuje pravidla ochrany údajů na poskytovatele veřejných komunikačních služeb. Toto nařízení upravuje používání souborů cookie, e-mailový marketing (článek 6 a 13) a minimalizaci identifikátorů dle potřeby pro které jsou vyžadovány (článek 12). Obsahuje také ustanovení o bezpečnosti a povinnosti oznamovat porušení zabezpečení osobních údajů (článek 4). Hlavní změny v oblasti směrnice o soukromí a elektronických komunikacích byly provedeny v roce 2009 a zahrnují nařízení č. 611/2013 o oznamování narušení bezpečnosti údajů[23], které sjednocují oznamování narušení bezpečnosti údajů (články 2 a 3) v rámci EU (Chirica, 2017, s.159-176).

Směrnice o soukromí a elektronických komunikacích je navržena tak, aby zahrnovala specifická rizika elektronických komunikací, zejména internetu, pokud jde o ochranu údajů a identifikátorů. Zavedení nových právních předpisů o ochraně osobních údajů přináší pro osoby, které se podílejí na zpracování těchto údajů, několik významných změn. Nejzásadnější je rozdělení údajů na provozní (článek 6) a lokalizační (článek 9), které musí být separovány, pokud nedojde k předešlému souhlasu či jejich anonymizaci. Správci musí přesně informovat o způsobu zpracování, musí respektovat preference uživatele ohledně cookies a sledovacích technologií (článek 5). Směrnice omezuje shromažďování dat jen na nezbytné pro dané účely a vyžaduje ochranu proti nelegálnímu nakládání (článek 6). Uživatelům dává právo na soukromí elektronické komunikace (článek 7), ochranu proti nevyžádané komunikaci jako spam (článek 13) a právo na informovanost (článek4). Aby bylo zajištěno splnění těchto nových práv a povinností v souladu s účinností GDPR, měli by správci přijmout následující opatření. Vypracovat soupis všech operací zpracování, které provádějí. Jasně definovat účel a právní základ každé činnosti zpracování. Uchovávat pouze

[22] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

[23] Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích

údaje, které jsou nezbytně nutné k dosažení cílů zpracování. Posoudit nutnost opětovného získání souhlasu od subjektů údajů nebo aktualizace jim poskytnutých informací. V případě potřeby jmenovat pověřence pro ochranu osobních údajů. (Chirica, 2017, s.159-176)

Směrnice se zabývá riziky spojenými s používáním souborů cookies a podobných technologií a klade důraz na získání informovaného souhlasu uživatelů. Jejím hlavním účelem je ochrana soukromí uživatelů internetu a zajištění spravedlivých postupů při zpracování údajů. Soubory cookie jsou krátké textové řetězce, které webové stránky ukládají do prohlížeče uživatele. Když je webová stránka vyžádá, prohlížeč odesílá všechny uložené soubory cookies jako součást požadavku. Soubory cookie mohou obsahovat další parametry, například dobu platnosti, která určuje, jak dlouho bude soubor cookie odesílán s požadavky na doménu. Současný právní rámec pro udělení souhlasu v právních předpisech o ochraně údajů, který je založen na konceptu osobního oprávnění, často selhává v praxi, protože se často projevuje pouze jako malé upozornění na začátku každé webové stránky, což vede k "znecitlivění souhlasu" a podkopává důvěru v ochranu soukromí (Tomíšek, 2023). Přísnější právní požadavky na získání explicitního souhlasu, jak je navrhováno v obecném nařízení o ochraně osobních údajů, dále oslabují účinnost mechanismu souhlasu, protože pokud budou vyskakovat na každém kroku, uživatelé se je naučí ignorovat. Alternativou je řešení implicitního souhlasu, kdy uživatelé vyjadřují souhlas kliknutím na webové stránky, což se jeví jako uživatelsky přívětivější. Používání souborů cookies a podobných technologií je především regulováno GDP, které definuje upravuje profilování a automatizované zpracování osobních údajů za účelem hodnocení osobních aspektů týkajících se jednotlivce.

Cílem změny směrnice nařízením o oznamování bezpečnostních narušení a zavedením požadavku na rychlé oznamování těchto případů je zvýšit viditelnost procesů, které nakládají s údaji. Transparentnost v tomto kontextu znamená, že organizace musí být schopny jasně a zřetelně komunikovat o bezpečnostních incidentech, které se týkají osobních údajů, a informovat relevantní subjekty, včetně dozorových orgánů a dotčených jednotlivců. Pravidla se soustředí na potřebu organizací přijmout vhodná opatření k prevenci bezpečnostních

narušení a minimalizaci jejich dopadu (Luzak, 2013, s. 221-245). Toto je v souladu se širšími cíli směrnice o soukromí a elektronických komunikacích a se stávající ochranou údajů, jejímž cílem je zvýšit bezpečnost a důvěryhodnost digitálních služeb.

3.6. Regulace obsahu EU

Regulace obsahu na internetu v rámci Evropské unie zahrnuje několik klíčových aspektů a legislativních opatření, která mají za cíl ochranu uživatelů a prevenci šíření nelegálního a škodlivého obsahu. Některé z hlavních prvků regulace obsahu v EU zahrnují směrnici o audiovizuálních mediálních službách (AVMSD)[24], směrnici o boji proti některým formám rasismu[25] a nařízení o potírání šíření teroristického obsahu online.[26] Mimo to EU vyvinula Kodex zásad boje proti dezinformacím z roku 2022 formující strategii pro signatářské platformy.

Směrnice o audiovizuálních službách zavádí nástroje zaměřené na regulaci audiovizuálních mediálních služeb, včetně tradičního televizního vysílání a služeb na vyžádání prostřednictvím internetu. Stanovuje pravidla a normy pro poskytování audiovizuálního obsahu, zajišťuje ochranu uživatelů (články 5,6,7). Zahrnuje ustanovení o platformách pro sdílení videí a jejich obsahu (kapitola 9). Devátá kapitola zahrnuje témata, jako je reklama, ochrana mládeže a propagace evropských děl. Reguluje audiovizuální obsah online a zajišťuje ochranu práv uživatelů ve spojení s nařízením o digitálních službách. Cílem vývoje audiovizuálního prostoru je zlepšit právní jistotu a prosazování regulace online obsahu v EU. Směrnice o audiovizuálním mediálním obsahu se zabývá otázkami, jako je oblast působnosti regulace, ochrana nezletilých osob (článek 6a), pravidla reklamy a propagace evropských děl (článek 11). Cílem směrnice o audiovizuálních mediálních službách je zajistit rovné podmínky pro všechny poskytovatele digitálních služeb, včetně platforem pro sdílení videa, a podporovat

[24] Směrnice Evropského parlamentu a Rady (EU) 2018/1808 ze dne 14. listopadu 2018, kterou se mění směrnice 2010/13/EU o koordinaci některých právních a správních předpisů členských států upravujících poskytování audiovizuálních mediálních služeb (směrnice o audiovizuálních mediálních službách) s ohledem na měnící se situaci na trhu
[25] Rámcové rozhodnutí Rady 2008/913/SVV ze dne 28. listopadu 2008 o boji proti některým formám a projevům rasismu a xenofobie prostřednictvím trestního práva
[26] Nařízení Evropského parlamentu a Rady (EU) 2021/784 ze dne 29. dubna 2021 o potírání šíření teroristického obsahu online

bezpečné a rozmanité online prostředí pro uživatele. Směrnice je součástí pokračujícího úsilí o přizpůsobení regulace vyvíjejícímu se digitálnímu prostředí a o ochranu práv uživatelů v oblasti audiovizuálního obsahu online (Lisičař a spol, 2023, 1478-1483).

Rámcové rozhodnutí o boji proti některým formám a projevům rasismu je nástroj Evropské unie, který má posílit úsilí v boji proti rasistickým a xenofobním jevům. Stanoví minimální trestněprávní požadavky v oblasti rasismu a xenofobie a určuje základní trestné činy (článek 1), které mají být trestány. Rámcové rozhodnutí definuje trestné činy související s rasismem a xenofobií, včetně veřejného podněcování k nenávisti nebo násilí vůči jednotlivcům nebo skupinám osob na základě jejich rasy, barvy pleti, národnostního, etnického nebo rasového původu nebo náboženského přesvědčení. Členské státy musí stanovit přiměřené sankce pro osoby, které se dopustí těchto trestných činů, a zajistit, aby tyto sankce byly účinné, přiměřené a odrazovaly od dalších projevů rasismu a xenofobie (článek 3). Aby bylo zajištěno, že státy mají pravomoc stíhat rasistické a xenofobní trestné činy, a to i v případě, že byly spáchány v zahraničí, stanoví rámcové rozhodnutí pravidla týkající se pravomoci (článek 9). Členské státy jsou povinny zajistit, aby oběti rasismu a xenofobie byly chráněny a měly přístup k právní pomoci a podpoře.

Nařízení o boji proti šíření teroristického obsahu online definuje teroristický obsah a stanoví kritéria pro jeho identifikaci (článek 1 a 2), včetně obsahu podporujícího teroristické skupiny, poskytujícího návody na výrobu zbraní nebo páchání teroristických činů. Provozovatelé internetových služeb, včetně sociálních médií a internetových platforem, budou po příkazu povinni odstranit teroristický obsah ze svých služeb a přijmout opatření, která zabrání jeho šíření (článek 3). Poskytovatelé služeb musí přijmout opatření, která zabrání šíření teroristického obsahu, včetně automatického odhalování a odstraňování (oddíl 3). Nařízení stanoví mechanismy spolupráce mezi poskytovateli online služeb, orgány členských států a orgány EU při odstraňování teroristického obsahu (oddíl 4). Nařízení musí být prováděno při respektování základních práv a svobod, jako je svoboda projevu a ochrana osobních údajů. Nařízení vyžaduje, aby Komise pravidelně monitorovala a vyhodnocovala účinnost opatření přijatých v boji proti

šíření teroristického obsahu online (články 21 a 23). Opatření by měla přispět k ochraně bezpečnosti a svobody občanů v digitálním prostředí tím, že zajistí rychlou a účinnou reakci na teroristický obsah na internetu. Celá tato iniciativa je progresivním krokem vůči kyberprostoru, vymezuje totiž terorismus na internetu jako samostatný problém, který je třeba sjednotit skrz všechny členské státy. Povinnosti jako je odstranění do 1 hodiny od ohlášení (článek 3), kontrolní mechanismy jako je zveřejnění zpráv o transparentnosti (články 7, 8) nástroje k rychlé adaptaci na změny podmínek a nové výzvy v prostředí digitálního obsahu na internetu.

Regulace obsahu v právu EU je předmětem značné pozornosti a kritiky. To platí zejména ve vztahu k online projevům. Svou roli v této regulaci sehrál SDEU, ve věci Glawischnig-Piesczek v. Facebook Ireland[27], kde shledal příkaz k odstranění obsahu Facebooku za hanlivý obsah s globálním účinkem přípustným podle práva EU. Cílem v tomto případě, byla ochrana před škodami způsobenými nezákonnými projevy na internetu. Regulace obsahu je komplexním a dynamickým procesem, který vyžaduje neustálé reakce na nové výzvy a technologické změny. EU udržuje krok s těmito změnami a aktualizuje své právní předpisy a postupy, aby zajistila efektivní ochranu uživatelů online prostředí a současně zachovala svobodu projevu. Koncem lze říci, že ochrana zájmů poškozených nelegálním obsahem je jádrem příspěvku práva EU k regulaci online obsahu.

[27] Rozsudek Soudního dvora (třetího senátu) ze dne 3. října 2019 Eva Glawischnig-Piesczek v. Facebook Ireland Limited C-18/18

4. Úprava jurisdikce EU ve sporech týkajících se internetu.

Jurisdikce ve smyslu uplatnění právní autority na určitém území je v případě internetu předmětem úpravy na úrovní mezinárodního práva, zvláště pokud jsou zapojeny subjekty s různými domicily. Charakter internetového prodeje vede k základnímu konfliktu, kdy prodejci nechtějí být žalováni v zahraničí, zatímco nákupci hledají řešení svých sporů ve své vlastní zemi. Zahrnutí pravidel určujících jurisdikci do elektronických kontraktů internetových stránek je běžnou praxí, která má za cíl definovat, která právní jurisdikce má pravomoc případnými spory. Tento způsob pomáhá v předcházení potenciálních právních sporů a jasně definuje právní rámec pro řešení případných konfliktů. Na toto špatně reagují zejména uživatelé, kteří nejsou dostatečně informováni o důsledcích pro jejich práva a povinnosti. Téma jurisdikce, však není tak snadné jako vyskakující okno na stránkách online platformy.

Internetové transakce umožňují nákupy v různých zemích s širokou nabídkou produktů, ale řešení případných sporů je často složitější než v případě tradičních papírových kupních smluv. V oblasti internetového práva EU je často používán článek 49 a 56 Smlouvy o fungování Evropské unie, poskytující zásadní právní rámec pro volný pohyb osob, zboží, služeb a kapitálu v rámci Evropské unie. Dalším často používaným ustanovením je článek 114, který umožňuje Evropské unii přijímat harmonizační opatření v oblastech, které jsou nezbytné pro dosažení cílů jednotného trhu. Článek 114 však byl v případě Německo v. Evropský parlament a Rada [28] napaden a soud shledal jeho použití nedostatečné, pokud není zaměřen na jednotný trh. Přestože článek 114 tedy poskytuje právní základ pro přijímání legislativy související s jednotným trhem, soudní praxe ukázala, že tento článek není vhodný pro obecnou regulaci internetu, pokud není přímo spojen s cíli jednotného trhu. To znamená, že při používání článku 114 pro regulaci internetu je nutné, aby opatření byla úzce spojena s cíli jednoty a přispívala k odstranění překážek vnitřního trhu. Pokud jde o argument o neproporčnosti regulace internetu prostřednictvím směrnic, je třeba zdůraznit, že směrnice mají

[28] Rozsudek Soudního dvora ze dne 5. října 2000** Jednací jazyk: němčina., Spolková republika Německo v. Evropský parlament a Rada, C-376/98, Recueil 2000

tendenci být flexibilnější než nařízení a mohou umožňovat členským státům určitou míru volnosti při implementaci. Nicméně, pokud je to možné, měla by být upřednostňována právní opatření v podobě nařízení, která mají přímou účinnost, a jsou přímo aplikovatelná ve všech členských státech, což může vést k vyšší právní jistotě a konzistenci v rámci Evropské unie (Lutzi, 2017, s. 687-700). Jurisdikce v oblasti internetového práva prošla významným vývojem a reagovala na změny ve světě a digitálním prostředí. Pravomoc EU zejména silná v oblastech ochrany osobních údajů, ochrany spotřebitelů, duševního vlastnictví, elektronického obchodu a boje s kybernetickými hrozbami. Omezená je naopak například v oblasti vymáhání autorských práv, která zůstává převážně v rukou jednotlivých členských států až na opatření proti nelegálnímu obsahu.

Haagská úmluva o volbě soudu[29] byla snahou odstranit překážky v přeshraničním obchodu a posílit mezinárodní trh, i když nebyla přímo zaměřena na internet. Vytvořila právní prostředí, které je příznivější pro mezinárodní obchod a ovlivnila tak jurisdikci EU v oblasti internetového práva prostřednictvím jednotného a předvídatelného právního rámce. Nařízení Brusel I[30] se zabývalo otázkou soudní příslušnosti v přeshraničních sporech týkajících se internetu a vymáhání práva. Výzvy internetu pro mezinárodní právo soukromé spočívají v rychlosti rozšíření internetu a rychlém zvýšení počtu uživatelů, což zvyšuje počet přeshraničních sporů a komplikuje uplatňování tradičních pravidel o příslušnosti a volbě práva. Zejména to platí u sporů, které se dotýkaly osobnostních práv. SDEU a vnitrostátní soudy upravily tradiční kritéria pro určení příslušnosti, aby lépe odpovídala novým výzvám a specifikům digitálního prostředí. Nařízení Brusel I nahradilo nařízení Brusel I bis o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech.[31] Změny a úpravy v tomto nařízení týkají interpretace a aplikace pravidel o soudní příslušnosti v kontextu digitálních technologií a internetového prostředí. To zahrnuje rozšíření pravidel na nové typy přeshraničních sporů, včetně těch týkajících se internetu, a úpravy

[29] 2014/887/EU: Rozhodnutí Rady ze dne 4. prosince 2014 o schválení Haagské úmluvy ze dne 30. června 2005 o dohodách o volbě soudu jménem Evropské unie
[30] Nařízení Rady (ES) č. 44/2001 ze dne 22. prosince 2000 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech
[31] Nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech

pravidel pro řešení nových výzev, které digitální prostředí přináší. Určuje pravidla posuzování místa škody, místa spáchání deliktu nebo místa, kde došlo k poškození osobnostních práv, ať už na úrovni jednotlivých států nebo v rámci Evropské unie. Tím se snaží zlepšit ochranu občanů a podniků v digitálním prostředí a usnadnit přeshraniční řešení sporů týkajících se internetu. (Wang, 2011, s. 35- 45)

Uplatňování soutěžního práva EU a přijetí konceptu "nadteritoriality" odráží posun v posuzování jurisdikční příslušnosti v případě protisoutěžního jednání na internetu. Tento přístup upřednostňuje roli technologie a vyzývá k přehodnocení způsobu, jakým jsou zásady příslušnosti uplatňovány v online kontextu (Themelis, 2012, s. 325-353). Koherence přístupu k internetovým případům v mezinárodním právu soukromém je nezbytný k zajištění právní jistoty. Je zapotřebí soudržného přístupu, který obecně podřizuje žaloby proti poskytovatelům služeb usazeným v EU spotřebiteli. Tento přístup vyžaduje pouze minimální legislativní změny a více odpovídá charakteru internetové komunikace (Lutzi, 2017, s. 687-700).

Význam globálního dosahu soudních sporů kvůli pravidlům soudní příslušnosti je zjevný, zejména v kontextu ochrany osobních údajů a práv občanů EU. Díky těmto pravidlům je možné podávat žaloby proti subjektům mimo EU za činnosti, které mají dopad na občany EU. Tyto změny odrážejí pokračující snahu EU řešit složitost regulace internetu a přeshraniční dosah jejích právních předpisů. Výzvy spojené s regulací neteritoriálního prostoru, jako je internet, vyžadují jurisdikční pravidla, která jsou flexibilní, ale zároveň předvídatelná, umožňují ochranu práv a zároveň umožňují inovaci v digitálním obchodě a komunikaci.

EU reagovala na výzvy, které přinášejí přeshraniční online spory, a nejednotný přístup k mezinárodnímu právu soukromému tím, že k internetové jurisdikci přistupuje jinak než k tradičním soudním sporům. Judikatura vykládající čl. 7 odst. 2 nařízení Brusel I bis, který určuje soudní příslušnost ve sporech deliktů spáchaných na internetu. Přístup EU k soudní příslušnosti v online sporech byl formován rozhodnutími Soudního dvora EU. Vybrané spory jako eDate

advertising[32], kde soud rozhodl, že pokud dojde k porušení dobré pověsti na internetu, může být žaloba podána na místě, kde došlo k poškození pověsti., Wintersteiger[33] se týkal se otázky jurisdikce v případě online prodeje produktů. Soud rozhodl, že pokud je webová stránka určena k obchodním účelům a jsou na ní uvedeny kontaktní údaje pro zákazníky, může být soudní příslušnost určena na základě tohoto umístění. Případ Petr Hejduk proti EnergieAgentur NRW GmbH (Hejduk)[34] se zabýval otázkou jurisdikce v případě údajně nelegálního obsahu na internetu. Soud rozhodl, že pokud jsou webové stránky určeny k užívání v konkrétním státě a mají vliv na trh v tomto státě, může být soudní příslušnost určena na základě tohoto faktoru. (Feraci, 2019, s. 277-304)

Cílem EU je zabránit výběru nevhodného soudu a dosáhnout rovnováhy mezi svobodou projevu a právem na soukromí. Místo vzniku škody a souvislost sporu s konkrétní zemí jsou jádrem přístupu EU k soudní příslušnosti v online sporech. Závěrem lze říct, že vývoj této oblasti zajistil účinnou ochranu práv a přiměřenou možnost žalovaných předvídat, který soud bude mít pravomoc nad případem, aby strany zapojené do sporu měly jasnou představu o tom, kde bude spor řešen, a aby soudní rozhodnutí byla v souladu s právními normami a zásadami EU.

[32] Stanovisko generálního advokáta - Cruz Villalón - 29 března 2011. eDate Advertising GmbH proti X (C-509/09) a Olivier Martinez a Robert Martinez proti MGN Limited (C-161/10).
[33] Rozsudek Soudního dvora (prvá senát) ze dne 19. dubna 2012. Wintersteiger AG proti Products 4U Sondermaschinenbau GmbH.C-523/10.
[34] Rozsudek Soudního dvora (čtvrtého senátu) ze dne 22. ledna 2015. Pez Hejduk v. EnergieAgentur.NRW GmbH C-441/13

5. Nařízení o jednotném trhu digitálních služeb

Nařízení 2022/2065 ze dne 19. října 2022, nahrazuje staré nařízení o digitálních službách 2000/31/ES a upravuje odpovědnost online zprostředkovatelů. DSA poskytuje rámec pro regulaci online platforem a služeb, včetně velmi rozsáhlých online vyhledávačů a dalších druhů platforem. Evropská komise se prostřednictvím nařízení snaží řešit jak právo na svobodu informací, tak praktická omezení rozsáhlého moderování obsahu s cílem řešit škody způsobené neregulovaným obsahem vytvářeným uživateli.

Základem úpravy je kategorizace digitální služby (článek 3) do několika kategorií. Podle důležitosti jim přisuzují asymetrické povinnosti, zvyšují jejích odpovědnost (kapitola 3, oddíl 1-5). V některých případech mohou být poskytovatelé služeb v důležitých kategoriích podrobeni přísnějším povinnostem a vyšší míře odpovědnosti, zatímco ti v nižších kategoriích mohou mít méně striktní požadavky. Posiluje práva uživatelů online a usiluje o bezpečnější, spravedlivější a transparentnější digitální prostředí. Uživatelská práva zajišťuje ustanoveními jako je právo na informace (článek 32) a sledovatelnost obchodníků (článek 30). DSA má dopad na informační systémy většiny odvětví, protože zavádí povinnosti moderování obsahu, vyřizování stížností a stanovení jasných podmínek (Leiser, 2023). Předpis vešel v účinnost 17. února 2024, toto datum je klíčové k ustavení koordinátorů na národních úrovních, kteří budou dohlížet na plnění povinností. Přesto, že plně účinný je předpis až od února letošního roku, do února minulého roku byly všechny platformy povinny zveřejnit počet aktivních uživatelů. Tento součet byl vytvořen k rozdělení platforem do definovaných kategorií (Nařízení o digitálních službách, 2023).

5.1. Stručný přehled digitální ekonomiky a platforem

Digitální ekonomika zahrnuje ekonomické aktivity založené na digitálních technologiích, včetně výroby, distribuce a spotřeby, umožněné digitálním prostředím. Platformy hrají klíčovou roli v digitální ekonomice. Ty zahrnují online služby a aplikace, které umožňují interakci a transakce mezi uživateli a poskytovateli. Mohou to být internetové obchody, sociální sítě, online tržiště, platební brány. Rozvoj digitálních platforem rovněž vyžaduje vytvoření právního

rámce na ochranu práv uživatelů a řešení antimonopolních problémů. DSA přináší cílené normy, které uživatelům platforem poskytnou dodatečná práva a omezí tržní sílu (Sidorenko a spol, 2022, s. 77-92).

Úkolem právních předpisů v digitální ekonomice je nalézt rovnováhu mezi podporou inovací a hospodářského růstu a zároveň chránit práva a zájmy uživatelů, spotřebitelů a podniků. To zahrnuje řešení otázek, jako je odpovědnost platforem za obsah vytvářený uživateli, dominantní postavení na trhu, ochrana údajů, kybernetická bezpečnost a spravedlivé zacházení s konkurenty (Sidorenko a spol, 2022, s.77-92). Celkově právní předpisy sehrávají zásadní roli při utváření digitální ekonomiky tím, že poskytují právní rámec, který upravuje chování digitálních platforem, podporuje hospodářskou soutěž, inovaci a chrání práva zúčastněných stran v digitálním prostoru. Jsou však vystaveny stálému nátlaku na aktualizaci, aby byly schopny reagovat na měnící se prostředí.

5.1.1. Platformy:

S postupem času se digitální prostředí rozvíjelo a vytvořily se online platformy, které využívají dosah sítě a pozitivních vlastností internetu. Jejich obchodní model je založen na neustálém shromažďování a analýze údajů uživatelů za účelem individuálního profilování.

Zprostředkovatelský model definuje digitální platformy jako zprostředkovatele, kteří propojují uživatele a usnadňují transakce a interakce mezi nimi. DSA tento typ platformy reguluje nejméně, a to jen ve vykazování transparentnosti, úpravě smluvních podmínek tak aby byly přehledné proč a kde omezují obsah. Posledními povinnostmi pro tuto platformu jsou spolupráce s vnitrostátními orgány na příkaz a upravit své kontaktní místo na adresu členské země,

Hostingové služby, které spočívají v ukládání obsahu uživatele nebo v přenosu obsahu uživatele na základě jeho instrukcí. Tento obsah může zahrnovat texty, obrázky, videa nebo jiné formy digitálního obsahu. Podle DSA jsou hostingové služby poskytovány za účelem ukládání obsahu na základě uživatelských instrukcí a zajišťují, aby byl tento obsah dostupný pro uživatele. Hostingové služby mohou zahrnovat poskytování úložiště, správu dat

a infrastrukturu pro ukládání obsahu. Tyto platformy nabývají stejných povinností jako zprostředkovatelský model, ale je jim navíc přidána povinnost oznamování a přijímání opatření (článek 16) a ohlašování trestných činů (článek 6 a oddíl 2).

Online platformy, které jsou zastoupeny sociálními médii, tržišti a obchody. Tento model je definován druhem interakce, který se na ní odehrává, Platforma funguje jako zprostředkovatel a může poskytovat další služby, jako je zpracování plateb nebo řešení sporů (Sidorenko a spol., 2022, s. 77-92). Online platformy tržišť považovány za digitální prostředí, kde se setkávají kupující a prodávající k výměně zboží nebo služeb. Tyto platformy zprostředkovávají transakce mezi uživateli a mohou poskytovat různé služby, jako je zpracování plateb, řešení sporů a marketingová podpora. Online platformy podléhají dosud zmíněným povinnostem (kapitola 4, oddíly 1-2), přidán je jim větší balíček než doposud. Jde o interní systém pro vyřizování stížností, důvěryhodné oznamovatele, opatření proti zneužití, namátkové kontroly tržišť a prověřovat dodavatele i třetích stran, ochrana nezletilých, zákaz cílených reklam profilováním a konečně transparentnost reklamy. (kapitola 4, oddíl 3)

Samostatnou kategorií představují velmi velké platformy: VLOP (Very Large Online Platforms), které mají významný dopad na trh EU a splňují určitá kritéria, jako je vysoký počet uživatelů nebo vysoký obrat. Tyto platformy podléhají přísnějším pravidlům a povinnostem stanoveným v zákoně o digitálních službách. VLOP je zaveden jako kategorie online platforem, které kvůli své velikosti a vlivu na trh EU vyžadují dodatečné povinnosti a odpovědnost. Přesné kritéria pro určení, zda platforma splňuje podmínky VLOP, nejsou v dostupných zdrojích specifikována. Nicméně lze usuzovat, že VLOP jsou ty platformy, které mají významnou přítomnost a vliv v digitálním prostoru EU, což zdůvodňuje zvýšenou pozornost a kontrolu ze strany regulačních orgánů. Je důležité, aby tyto platformy byly podrobeny přísnějšímu dohledu, aby byla zajištěna transparentnost, bezpečnost a ochrana práv uživatelů digitálních služeb (Kaleda, 2023, s. 25-42). Tyto platformy jsou zatíženy nejvíce regulacemi, neboť na ně dopadají všechny zmíněné regulace ostatních platforem (kapitola 4, oddíly 1,2,3) a přidává se kodex chování, spolupráce při krizích, sdílení dat s úřady, možnost zrušit profilování, povinnosti posuzovat rizika a reagovat na krize. (kapitola 4, oddíl 5)

Tyto modely jsou rozděleny dle množství povinností, které jim DSA ukládá. Poskytují různé pohled na jejich úlohy a funkce v digitální ekonomice. Samotné rozdělení umožňuje lepší porozumění jejich provozu v digitálním prostředí. Zásadní rozdíly mezi jednotlivými typy platforem. Různé typy digitálních platforem mají různou právní odpovědnost a povinnosti. Například zprostředkovatelské platformy jsou odpovědné za moderování obsahu a dodržování právních předpisů, zatímco tržní platformy mají povinnost zajistit spravedlivé a transparentní transakce mezi uživateli. Stanovení regulačních přístupů: Klasifikace digitálních platforem do různých kategorií pomáhá regulačním orgánům určit vhodné přístupy. Regulace zprostředkovatelských platforem se může zaměřit na moderaci obsahu a ochranu soukromí, zatímco regulace tržních platforem může řešit hospodářskou soutěž a ochranu spotřebitele. Určení typu platformy je klíčové pro ochranu práv uživatelů. Dopad na práva uživatelů, včetně soukromí, ochrany údajů a svobody projevu, se může lišit v závislosti na typu platformy. Pro každý typ platformy byla regulace přizpůsobena tak, aby řešila konkrétní problémy a rizika. (Sidorenko, 2022. s. 77-92). Celkově je důležité rozlišovat a kategorizovat digitální platformy podle jejich charakteristik, což umožňuje účinnou regulaci internetu prostřednictvím cílených opatření, která berou v úvahu specifika každé platformy.

5.2. Klíčová ustanovení, cíle a oblasti působnosti

DSA ukládá online platformám povinnosti v oblasti řízení obsahu (článek 35), včetně šíření dezinformací a nezákonného obsahu. Obecné monitorovací povinnosti jsou zakázány (článek 8). Klade však důraz na transparentnost v procesu moderování obsahu (kapitola 3). Důležitý kontrolní mechanismus jsou výroční zprávy o moderování článek 15). Online platformy jsou povinny provádět hodnocení rizik (článek 34) a přijímat opatření k minimalizaci rizik (článek 35), aby zajistily důvěryhodnost informačního ekosystému. Důvěryhodní oznamovatelé, kteří jsou partnery platforem, mají oprávnění identifikovat a deaktivovat obsah generovaný uživateli, který byl vyhodnocen jako nezákonný. Očekává se, že online platformy budou poskytovat jasné a přístupné informace o svých postupech moderování obsahu (článek 15), včetně zásad, postupů a kritérií pro odstraňování nebo označování obsahu. Platformy jsou rovněž

povinny zveřejňovat informace o svých hodnoceních rizik a opatřeních k jejich zmírnění, aby zajistily důvěryhodnost informací sdílených na svých platformách (Leiser, 2023).

DSA poskytuje důvěryhodným oznamovatelům (článek 22), kteří spolupracují s platformami, možnost identifikovat a delegitimovat obsah generovaný uživateli, který byl identifikován jako nelegální. Tímto se dále zvyšuje transparentnost úsilí o moderování obsahu. Aby uživatelé lépe pochopili, jak platformy obsah moderují, je důležité, že zásady moderování jsou viditelné (článek 14). To zahrnuje kritéria, která platformy používají k posuzování a hodnocení obsahu, i samotné postupy moderování. Uživatelé mohou lépe porozumět tomu, co mohou při používání konkrétní platformy očekávat, pokud jim budou poskytnuty jasné informace. Silnou stránkou úpravy je povinnost platforem odůvodnit manipulaci s uživatelským obsahem (článek 17). Uživatelům to také umožňuje přizpůsobit své chování pravidlům platformy a lépe porozumět důvodům, proč může být jejich obsah odstraněn nebo označen. Je důležité, aby platformy zajistily, že jejich pravidla moderování obsahu budou uplatňovány konzistentním a viditelným způsobem, aby uživatelé mohli věřit, že jsou vytvořeny rovné podmínky pro všechny. Očekává se, že online platformy budou zveřejňovat informace o svých hodnoceních rizik a opatřeních k jejich zmírnění, čímž prokážou své úsilí o zajištění důvěryhodnosti informací sdílených na svých platformách (Kaleda, 2023, s. 25-42).

DSA ustavuje postavení důvěryhodných oznamovatelů anglicky „flaggers“ (článek 22), kteří spolupracují s platformami při identifikaci a delegitimaci obsahu generovaného uživateli, který byl označen jako nebezpečný či nelegální. Úkol oznamovatelů je zvýšit kvalitu moderování obsahu a rychlost reakce na nebezpečný obsah. Platformy by měly zveřejnit informace o svých partnerstvích s důvěryhodnými oznamovateli a zdůraznit jejich společné úsilí v boji proti dezinformacím. Důvodem těchto požadavků je posílit důvěru v informační ekosystém tím, že uživatelé lépe porozumí tomu, jak platformy moderují obsah a omezit šíření dezinformací. DSA zakazuje obecnou povinnost monitorování platforem, ale platformy jsou přesto povinny přijímat proaktivní opatření k omezení šíření dezinformací (článek 34). Platformy jsou vyzvány, aby spolupracovaly

s důvěryhodnými oznamovači a útvarem zajištění souladu s cílem identifikovat a deaktivovat obsah nelegální či nebezpečný obsah.

DSA zdůrazňuje úlohu hodnocení rizik (článek 34) a opatření ke zmírnění rizik (článek 35) při moderování obsahu, jejichž cílem je zajistit důvěryhodnost informací sdílených na platformách. Cílem těchto politik moderování obsahu je dosáhnout rovnováhy mezi omezením šíření nezákonného obsahu a zachováním transparentnosti a důvěryhodnosti online platforem. (Leiser, 2023, s. 25-42). Od online platforem se očekává, že zavedou opatření k identifikaci obsahu a zmírnění rizik, spojených s šířením nezákonného obsahu. Opatření platforem v boji s nezákonným obsahem mohou zahrnovat vývoj a implementaci technologií pro odhalování potenciálně škodlivého obsahu. Platformy mohou také navázat partnerství s osobami pověřenými zajišťováním souladu (článek 41), aby pomohly identifikovat a zmírnit rizika nezákonného obsahu. Subjekty ověřující fakta získají přístup k datům a nástrojům platformy, aby mohly analyzovat a ověřovat přesnost informací sdílených na platformě. Platformy mohou ověřovatelům faktů poskytnout zdroje a podporu, k efektivnímu ověřování. Osoby pověřené se zajišťováním obsahu mohou úzce spolupracovat s platformami na vytváření a zavádění zásad a postupů pro kontrolu faktů. Platformy mohou zviditelnit obsah ověřený fakty tím, že jej zvýrazní nebo zobrazí varovné nápisy u obsahu označeného za nepravdivý nebo zavádějící. (Leiser, 2023, s. 25-42). Účel je zajistit, aby platformy měly zavedena důkladná opatření ke zmírnění nebezpečí a udržely tak důvěryhodnost informací pro uživatele. Tato opatření mají zvýšit schopnost online platforem řešit problémy, které představují informace a dezinformace, a tím podpořit bezpečnější a spolehlivější online prostředí.

5.3. Regulačních zásady a mechanismy

V kontextu evropského nařízení o digitálních službách dochází k posunu od omezené odpovědnosti a samoregulace k novému režimu proaktivní moderace, včetně ověřování faktů. Předpis zavádí povinnosti pro online platformy, jako je dobrovolné moderování a ověřování faktů, s cílem omezit šíření nezákonného obsahu a zvýšit důvěru v informační systém (článek 7). DSA mění pravidla rizik, protože jim přisuzuje vyšší váhu, zakládající vyšší odpovědnost

platforem. DSA dává pravomoc důvěryhodným oznamovačům a útvaru zajišťující soulad (článek 41), spolupracovat s platformami na zpochybnění nelegálního obsahu. Tato ustanovení v DSA zdůrazňují regulační přístup, který kombinuje proaktivní moderaci, posuzování rizik a partnerství s útvarem zajišťující soulad s cílem řešit problémy falešných zpráv, dezinformací a online manipulace. Důraz na transparentnost a spolupráci má za úkol budovat důvěru v informace sdílené na online platformách (Pehlivan, Ceyhun a Church, 2023, s. 53-59). Motivací za všemi těmito změnami lze vidět snahu zajistit digitální suverenitu a získat kontrolu z rukou velkých společností se sídlem ve třetích zemích, a zároveň vytvářet ideální demokratickou veřejnou online sféru bez škodlivého obsahu.

Soubor změn, doplněný doprovodnými nástroji, vytváří nová pravidla pro regulaci a nahlášení škodlivého obsahu online, včetně obsahu teroristického, materiálů ohrožující vývoj nezletilých (článek 28) a cílené reklamy (článek 26). EU reguluje přísněji velké digitální platformy s cílem omezit jejich tržní moc a chránit základní práva a záruky v technologické a informační společnosti. Přísnější povinnosti velkým online aktérům reflektují přístup založený na riziku, který přiděluje povinnosti platformám s významným dopadem na trh EU. Velmi rozsáhlé online platformy jsou identifikovány jako platformy s významným dopadem na trh EU a splňují specifická kritéria, jako je vysoký počet uživatelů nebo významný obrat. nebo mají významný vliv na šíření informací. (Kaleda, 2023, s. 25-42). Mezi ně patří sociální sítě jako Facebook či Twitter, tržiště jako Amazon, nebo některé platformy společnosti Google jako mapy a vyhledávač.

Předpis si dává za cíl zajistit bezpečnost uživatelů online platforem. Nástroje podporující tuto myšlenku je například povinnost platforem poskytovat jednotné místo pro snadné hlášení nezákonného obsahu (článek 12), aby uživatelé mohli rychle reagovat na škodlivý obsah a přispívat k jeho odstranění (články 16). Pro dohled nad prováděním a prosazováním těchto předpisů byl ustaven nezávislý Evropský sbor pro digitální služby (kapitola 4 oddíl 3). Jejich úkoly jsou popsány v článku 61, jejich úloha je koordinace ve společném vyšetřování, radí Evropské komisi ohledně velmi velkých platforem a vydává stanoviska v souladu s DSA. DSA tvoří rovné podmínky pro všechny

poskytovatele digitálních služeb, včetně subjektů mimo EU. Zavádí povinnosti pro poskytovatele digitálních služeb z třetích zemí, jako je jmenování právního zástupce v EU (článek 13) a dodržování pravidel EU týkajících se nelegálního obsahu (Kaleda, 2023, s. 25-42). Tato revoluční povaha DSA spočívá v tom, že přináší nový přístup k regulaci digitálních služeb, který se neomezuje pouze na subjekty v rámci EU, ale rozšiřuje svou působnost i na subjekty mimo EU, jako jsou poskytovatelé digitálních služeb z třetích zemí. Zavedení rovných podmínek pro všechny poskytovatele digitálních služeb je v tomto ohledu klíčové, neboť dříve byly tyto subjekty mimo dosah regulace EU a mohly operovat s menší mírou odpovědnosti.

DSA má řešit škody způsobené online, zavedením náhrady škody od poskytovatelů, pokud poruší své povinnosti (článek 54). Předpis klade zvláštní důraz na potřebu předcházet šíření nezákonného obsahu, jako je obsah teroristické povahy a materiál týkající se sexuálního zneužívání dětí. Podporuje transparentnost tím, že vyžaduje, aby poskytovatelé digitálních služeb poskytovali jasné informace o svých podmínkách, zásadách moderování obsahu a postupech pro vyřizování stížností. DSA implementuje efektivní a transparentní mechanismy pro hlášení uživatelů a moderování obsahu (Pehlivan, Ceyhun a Church, 2023, s. 53-59). Velmi rozsáhlé online platformy mají další povinnosti, jako je pravidelné hodnocení rizik, poskytování transparentních zpráv a spolupráce s orgány. Předpis také stanovuje požadavek, aby poskytovatelé digitálních služeb jmenovali odpovědnou osobu nebo subjekt v rámci EU, který bude zodpovědný za dodržování DSA (Pehlivan, Ceyhun a Church, 2023, s. 53-59).

5.4. Důsledky pro poskytovatele digitálních služeb, platformy a práva uživatelů.

DSA stanovuje, že platformy s významným dopadem na trh EU budou muset dodržovat více závazků a pravidel. Viditelnost je klíčovým bodem DSA, která vyžaduje, aby platformy poskytovaly uživatelům informace o procesech moderování obsahu a fungování algoritmů. Zároveň se DSA snaží zajistit bezpečnost online prostředí tím, že stanovuje povinnost pro platformy hlásit

nezákonný obsah a aktivně bojovat proti dezinformacím. Nové povinnosti podle DSA neplatí pouze pro poskytovatele digitálních služeb v rámci EU, ale také pro subjekty působící mimo EU. Tyto subjekty musí mít v EU právního zástupce a dodržovat pravidla EU týkající se nelegálního obsahu (Kaleda, 2023, s. 25-42). Což jak jsem zmínil výše je mechanismus, který rozšiřuje pravomoc EU na nové platformy.

Ustanovení DSA změní postupy platforem při moderování obsahu, podpoří spolupráci s externími subjekty a vyvolá otázky týkající se rovnováhy mezi bojem proti dezinformacím a ochranou práv uživatelů. Nastávají obavy z možného omezení svobody projevu v souvislosti se zaváděním povinnosti proaktivního moderování podle DSA. Uživatelé mohou mít obavy z dopadu zvýšeného moderování obsahu na jejich možnost svobodně vyjadřovat své názory a myšlenky online. Zahrnutí důvěryhodných oznamovačů a osobami pověřenými zajištění souladu do moderování obsahu může vyvolat otázky ohledně přesnosti a nestrannosti identifikace a delegitimace obsahu vytvořeného uživateli (Leiser, 2023). Pokud jakákoliv platforma spolupracuje s externími subjekty v boji proti dezinformacím, mohou existovat obavy ohledně možného porušení práv uživatelů na soukromí. Tato potenciální omezení práv uživatelů vycházejí z nutnosti najít rovnováhu mezi bojem proti dezinformacím a ochranou svobody projevu a soukromí. Uživatelé mohou být znepokojeni dopadem zvýšeného moderování obsahu na jejich schopnost svobodně se vyjadřovat a možností neobjektivních nebo nepřesných moderátorských rozhodnutí. Spolupráce mezi platformami a externími subjekty může navíc vyvolat otázky týkající se soukromí uživatelů. (Leiser, 2023). Cílem DSA je najít rovnováhu mezi bojem proti poškozování na internetu a ochranou práv uživatelů na svobodu informací. Ochrana práv uživatelů je zajištěna zřízením právních zástupců nebo kontaktního místa pro efektivní komunikaci (článek 11). Nové povinnosti budou uloženy poskytovatelům digitálních služeb, včetně online platforem, hostingových služeb a hlavních online vyhledávačů. Poskytovatelé digitálních služeb, včetně online platforem, hostingových společností a hlavních online vyhledávačů, budou mít povinnost zabránit šíření nezákonného obsahu, včetně teroristického obsahu a obsahu sexuálního zneužívání dětí (Pehlivan, Ceyhun a Church, 2023, s. 53-59).

Platformy musí zavést účinné a transparentní politiky moderování obsahu, včetně mechanismů pro nahlašování uživatelů a moderování obsahu (článek 16). Poskytovatelé digitálních služeb musí poskytovat jasné informace o svých podmínkách, zásadách moderování obsahu a postupech vyřizování stížností. Velmi rozsáhlé online platformy (kapitola 4, oddíl 5) mají další povinnosti, například provádět pravidelné hodnocení rizik, poskytovat zprávy o transparentnosti a spolupracovat s orgány. Účel je najít rovnováhu mezi řešením škodlivých účinků online a ochranou práv uživatelů na svobodu informací. Poskytovatelé digitálních služeb musí určit odpovědnou osobu nebo subjekt v EU, který zajistí dodržování DSA. Velmi velké online platformy budou mít ve srovnání s ostatními poskytovateli digitálních služeb další povinnosti. Za účelem identifikace a zmírnění rizik spojených s jejich službami budou muset pravidelně provádět hodnocení rizik. (Pehlivan, Ceyhun a Church, 2023, s. 53-59)

Platformy budou muset předkládat alespoň každoroční zprávy o transparentnosti (článek 15), v nichž budou podrobně uvedena opatření přijatá k řešení nezákonného obsahu a účinnost úsilí o jeho moderování. Od velmi velkých online platforem se bude očekávat spolupráce s orgány (kapitola 4, oddíl 5), včetně poskytování informací a pomoci při vyšetřování nezákonného obsahu. To zahrnuje zřízení a udržování účinných kanálů, prostřednictvím kterých mohou uživatelé nahlašovat nezákonný obsah a podávat na něj stížnosti. Od velmi velkých online platforem se bude očekávat, že budou s úřady při auditech (článek 37). Měly by poskytovat informace a pomáhat orgánům při vyšetřování nezákonného obsahu. Spolupráce může zahrnovat výměnu údajů, poskytování přístupu k informacím o uživatelích a pomoc při identifikaci a odstraňování nezákonného obsahu. V zájmu usnadnění spolupráce a výměny informací velmi velké online platformy musí vytvořit účinné komunikační kanály s kontrolními orgány. Tato spolupráce by měla zvýšit účinnost vymáhání práva a zajistit rychlé odstranění nezákonného obsahu z online platforem (Pehlivan, Ceyhun a Church, 2023, s. 53-59).

6. Nařízení o digitálních trzích

Nařízení o digitálních trzích je legislativní iniciativa Evropské komise, která má za cíl regulovat chování digitálních platforem a poskytovatelů služeb na digitálních trzích v rámci Evropské unie. Předpis doplňuje existující nástroje hospodářské soutěže a zajišťuje spravedlivou hospodářskou soutěž v digitálním prostředí. DMA se zaměřuje na problémy spojené s dominantními online platformami a vytvořením mechanismů pro podporu rovných podmínek, jak pro spotřebitele, tak pro podniky. Stanovením pravidel a povinností pro digitální platformy, jako je prevence nekalých praktik (kapitola 3), podpora viditelnosti (článek 6 a 11) a zajištění přístupu k datům a službám (článek 6 a 12), má DMA vytvořit prostor pro konkurenci a inovaci na evropském digitálním trhu. Stanovuje hranice a mechanismy, aby se zabránilo možným nespravedlivým podmínkám ukládaným koncovým uživatelům a podnikům, k zajištění otevřenosti důležitých digitálních služeb (Kaleda, 2023, s. 25-42).

6.1. Oblasti působnosti a hlavní ustanovení

Pravidla představují souhrnný systém, který Evropská unie zavedla za účelem regulovat problém tzv. „gatekeepers“ neboli strážců přístupu, zvýšit spravedlnost a konkurenceschopnost trhů platforem. Tato pravidla určují pravidla chování, která jsou určena pro specifické platformy, jejichž cílem je zabránit fragmentaci vnitrostátních regulací strážců přístupu ze strany členských států EU. Mezi tyto pravidla patří nediskriminující přístup (článek 6), otevřenost reklamy (článek 5), přenositelnost dat (článek 6) a transparentnost algoritmů ovlivňující zobrazení obsahu (článek 21). Kromě toho nová pravidla integrují klíčové koncepty GDPR a zajistí koordinaci mezi Evropskou komisí a orgány pro ochranu údajů v EU. Nicméně v současné době postrádají konkrétní zásady pro posuzování akvizic strážců, což zdůrazňuje potřebu aktualizované a koherentní regulace v rámci digitální ekonomiky. (Witt, 2023)

DMA poskytuje definici strážců přístupu (článek 3) na základě kritérií, jako je velikost, obrat, a vliv na trh. Ti pak podléhají specifickým povinnostem a pravidlům (Nurhayati, 2023, s. 107-174). Zároveň klade otázku, zda tato kritéria přesně vyjadřují tržní sílu a zda je spravedlivé, aby se na základě těchto kritérií určovaly

povinnosti a zákazy pro tyto subjekty (článek 4). DMA se zaměřuje na stanovení seznamu povinností a zákazů pro strážce přístupu (články 5,6,7), které jsou inspirovány antimonopolním šetřením trhu. Důraz klade na to, aby tyto povinnosti byly odůvodněné a dostatečně flexibilní. Kromě toho DMA řeší některé problémy spojené s chováním velkých online platforem, včetně nedostatečného inovačního výkonu a nespravedlivé distribuce odměn. DMA tedy na tyto subjekty klade vyšší nároky a zavádí opatření (článek 6), k podpoře spravedlivého a otevřeného digitálního trhu. Jeho hlavním cílem je zabránit velmi rozsáhlým online platforem v protisoutěžním chování, jako je například využívání své tržní síly k potlačování konkurence, provádění samoobsluhy (článek 5) nebo uplatňování nekalých datových praktik (článek 12).

DSA doplňuje DMA tím, že zavádí pravidla pro online zprostředkovatele a řeší otázky spojené s nezákonným obsahem, transparentností a právy uživatelů. Jedním z hlavních cílů DSA je zajistit, aby uživatelé měli přístup k relevantním informacím a mohli se informovaně rozhodovat. Tímto způsobem právní předpisy dohromady usilují o zvýšení vyšší viditelnost, odpovědnosti a možnosti volby uživatelů v oblasti velmi rozsáhlých online platforem. (Kaleda, 2023, s. 25-42)

DMA vyzývá online platformy, aby aktivně spolupracovaly s příslušnými orgány při řešení nezákonného obsahu (článek 28). Jednou z klíčových priorit DSA je účinný boj proti nezákonnému obsahu, prostřednictvím posílené spolupráce mezi komisí a vnitrostátními orgány ve výročních zprávách (článek 35). Předpis vyzývá platformy, aby implementovaly efektivní systémy pro vyřizování stížností (článek 5) a aktivně tak spolupracovaly s uživateli při řešení jejich nahlášených problémů týkajících se nezákonného obsahu. Podpora komunikace mezi jednotlivými stranami má vytvořit bezpečnější online prostředí a zajištění účinného prosazování předpisů týkajících se strážců přístupu. Taková opatření jsou klíčová pro ochranu uživatelů a posílení důvěry v digitální prostředí (Kaleda, 2023, s. 25-42). Předpis DMA je navržen s cílem regulovat chování strážců přístupu, což jsou online platformy s významným vlivem na digitální trhy. Tato ustanovení obsahují následující body. Strážci přístupu mají zakázáno používat nekalé praktiky, které by mohly poškodit hospodářskou soutěž (kapitola 3). Mezi tyto praktiky se řadí například samo propagace, zneužívání údajů

a vytváření nepřiměřených podmínek pro uživatele. Strážci přístupu musí být transparentní ohledně svých algoritmů řazení, využívání dat a reklamních praktik. Tato opatření mají zajistit spravedlnost a odpovědnost na digitálním trhu (článek 6). DMA stanovuje, že podniky a spotřebitelé musí mít spravedlivý a nediskriminační přístup k datům a službám poskytovaným strážci přístupu (článek 6), přispívající k prohloubení neutrality internetu. Strážci nesmí bránit provozovatelům v přístupu ke klíčovým vstupům a ovlivnit tak uživatele (článek 12).

Evropská komise má v rámci DMA významné pravomoci a povinnosti, aby zajistila řádné fungování digitálního trhu v Evropské unii. Za účelem zjištění potenciálních problémů v oblasti hospodářské soutěže a nekalých praktik strážců přístupu, má Evropská komise pravomoc provádět šetření trhu na digitálních trzích (kapitola 4). Tato šetření mohou zahrnovat analýzu trhu (článek 17), shromažďování údajů (článek 18), posuzování obchodního chování (článek 23) a u uložit nápravná opatření (článek 18), pokud zjistí, že strážci přístupu porušují pravidla DMA. Evropská komise má rovněž pravomoc vymáhat dodržování pravidel DMA ze strany strážců přístupu (článek 33). To zahrnuje možnost ukládat pokuty za porušení povinností podle DMA a případně, přijímat další opatření k zajištění jejich dodržování. Tyto pravomoci umožní Evropské komisi aktivně monitorovat digitální trhy v EU a zasahovat v případech, kdy jsou zjištěny nekalé praktiky nebo porušení pravidel hospodářské soutěže. Pokuty a sankce strážců přístupu, kteří porušují pravidla DMA, mohou být potrestáni vysokými pokutami až do výše 10 % jejich celosvětového obratu a dalšími sankcemi (článek 30). Silným kontrolním mechanismem je spolupráce vnitrostátních orgánů a Evropské komise za účelem zajištění účinného prosazování pravidel a řešení případných problémů na digitálním trhu (článek 37 a 38). (Nurhayati, 2023, s. 107-174). Pro usnadnění koordinace mezi při prosazování ustanovení DMA je zřízena Skupina na vysoké úrovni pro nařízení o digitálních trzích, který bude sloužit jako platforma pro poradenství a doporučení v oblastech spadajících do pravomoci členských států v zájmu jednotného přístupu regulačních nástrojů (článek 40).

Centralizovaný přístup DMA ustavuje harmonizovaný rámec v celé Evropské unii, snižuje roztříštěnost a zajišťuje jednotnost souboru pravidel pro strážce

přístupu. V důsledku zavedení tohoto komplexního právního režimu na úrovni EU, může být nutné aktualizovat stávající vnitrostátní předpisy tak, aby byly v souladu s novým rámcem EU. Celkový dopad DMA na stávající vnitrostátní předpisy spočívá v omezení možnosti jednotlivých členských států přijímat vlastní předpisy zaměřené na strážce přístupu, což podporuje jednotnější a konzistentnější přístup k regulaci na úrovni EU. Výsledkem je snížení fragmentace a nejistoty v digitálním prostředí a posílení právní jistoty pro všechny aktéry na digitálním trhu v rámci EU (Witt, 2023). Smyslem předpisu je bojovat proti dominanci na trhu a podporovat hospodářskou soutěž v digitálním prostředí. Vytyčuje cíl chránit hospodářskou soutěž v rámci jednotlivých platforem, podpořit inovaci a soutěž mezi platformami. DMA dosahuje těchto cílů prostřednictvím revize dosavadních právních předpisů týkajících se hospodářské soutěže a zavedením nových mechanismů, přičemž kriticky posuzuje účinnost dosavadních opatření proti zneužívání dominantního postavení.

6.2. Prosazování regulace

Pravidla DMA nabízejí řadu mechanismů, které umožňují Evropské komisi doladit předpisy tak, aby účinně řešily změny a nadměrné či nedostatečná pravidla. Těmito mechanismy jsou již zmíněné šetření trhu, právo na odchylky a výjimky (článek 10) či přezkum strážce (článek 4) a přerušení povinností (článek 9). Tato flexibilita naznačuje, že pravidla DMA nejsou tak přísná, jak by se mohlo na první pohled zdát. Mohou být přizpůsobena a koordinována podle potřeb trhu a vývoje digitálního prostředí. DMA zajišťuje účinné prosazování prostřednictvím široké škály mechanismů. Podle tohoto právního předpisu jsou platformy povinny přijímat proaktivní kroky k odhalování a odstraňování nezákonného obsahu, což zahrnuje implementaci systémů upozornění a mechanismů pro stahování obsahu, a rychlou reakci na nahlášení uživatelů. Pravidla také posilují pravomoci těchto orgánů tím, že jim umožňují ukládat sankce a pokuty platformám, které nedodržují předpisy. (Kaleda, 2023, s. 25-42).

Evropská komise má pravomoc provádět monitorování a dohlížení trhu s cílem identifikovat strážce přístupu a posoudit, zda dodržují ustanovení DSA. Povoluje sběr dat, provádění průzkumů (články 16 až 19) jako je sledování

dominance určitých subjektů, posuzování vlivu nových technologií nebo analýza chování spotřebitelů. Dále povoluje přijímání stížnosti, podnětů (článek 25) a provádění auditu (článek 15), aby ověřila dodržování předpisů a případného porušování pravidel. Tato šetření jsou důležitá pro identifikaci možných problémů a nedostatků v uplatňování právních předpisů. Pokud se zjistí, že strážce přístupu porušuje DMA, má Evropská komise pravomoc uložit nápravná opatření (článek 18), která mají řešit zjištěné problémy. Tato opatření mohou zahrnovat konkrétní změny v chování nebo ve struktuře subjektů s cílem zajistit spravedlivou hospodářskou soutěž a chránit zájmy spotřebitelů. Pokud není zřízena náprava, lze uložit sankce (článek 32), pokuty (článek 30) a penále (článek 31). Strážcům přístupu, kteří nedodržují DMA, mohou být uloženy vysoké pokuty až do výše 10 % celosvětového obratu, avšak v mimořádných případech až 20 % (článek 30 odstavec 2). Tyto pokuty mají sloužit jako prostředek k zajištění dodržování pravidel a mohou být doplněny dalšími sankcemi v případě opakovaného porušování předpisů. Spolupráce mezi Evropskou komisí a vnitrostátními orgány je klíčem k účinnému prosazování DMA ve všech členských státech Evropské unie. Evropská komise a vnitrostátní orgány společně vytvářejí koordinační mechanismy a postupy pro výměnu informací, spolupráci a konzultace týkající se prosazování DMA. Za účelem lepšího pochopení a provádění předpisu poskytuje Evropská komise podporu a školení vnitrostátním orgánům. S cílem umožnit koordinovaný přístup k vymáhání práva si Evropská komise a vnitrostátní orgány budou společně vyměňovat informace o porušeních a opatřeních přijatých k jejich nápravě. (Nurhayati, 2023, s. 107-174)

7. Srovnání s legislativou USA

Rozdíly v přístupu EU a USA k regulaci internetu jsou výrazné a odrazují různé prioritní oblasti a přístup obou regionů. Zatímco americké orgány se zaměřují na chování, které narušuje hospodářskou soutěž, ve které uplatňují pokročilejší znalosti o trzích a nechtějí škodit tržním mechanismům nadbytečnými pravidly. EU se soustředí na regulaci soukromí a obsahu, což se projevuje v přijetí nařízení dosavadních směrnic a nařízení. V regulaci obsahu EU zaujímá silný postoj zejména k nenávistnému projevu, teroristickým útokům a šíření dezinformací. Platformy jsou zodpovědné za obsah, který hostují. Jsou tak nuceny k odstranění nelegálních a nenávisti podněcujících příspěvků. V USA je omezování svobody projevu proti prvnímu dodatku Ústavy, a proto jsou zákony týkající se regulace obsahu slabé v porovnání s EU. Ve Spojených státech je preferován volný trh pro digitální podnikání, což se odráží v jejich tendenci zachovávat minimální regulaci. Na druhé straně EU uplatňuje přísnější a intervenční přístup k regulaci síťové neutrality a digitálních trhů obecně (Monti, 2022, s. 40-68). Celkově lze říci, že přístupy EU a USA k regulaci internetu reflektují jejich odlišné hodnoty a priority, přičemž USA se více zaměřují na hospodářskou soutěž a EU na ochranu soukromí a regulaci obsahu.

7.1. Přehled právních předpisů USA:

Regulace internetu ve Spojených státech je složitá a nejednotná. Zákony a politiky upravující právo a regulaci elektronických komunikací se často překrývají a někdy si vzájemně odporují. Možnost vlády jednat v oblasti obsahu je omezena prvním dodatkem Ústavy Spojených států.

Síťová neutralita zdůrazňuje rovné zacházení s internetovým provozem, bez ohledu na původ a cíl. Je jednou z charakteristik spravedlivého internetu bez diskriminace a nekalých praktik. V posledních letech však došlo ke změnám v USA. Federální komise pro komunikaci (FCC) vydala v letech 2010 a 2015 Pravidla o síťové neutralitě, která měla zajistit, aby poskytovatelé internetových služeb přistupovali ke všem internetovým přenosům stejně, ale tato pravidla byla později v roce 2017 zrušena. Byl tedy odstraněn rámec zakazující, aby poskytovatelé služeb upřednostňovali určitý obsah oproti jinému.

Jádrem debaty o síťové neutralitě je zásada, že s veškerým internetovým provozem by se mělo zacházet stejně, bez diskriminace. Zrušení pravidel o síťové neutralitě vyvolalo obavy, že poskytovatelé internetových služeb mohou začít upřednostňovat určité služby nebo obsah za poplatek, což by mohlo vést k vzniku dvoustupňového internetu, kde bychom viděli rychlejší a pomalejší přístup k obsahu v závislosti na tom, kolik za něj uživatelé zaplatí. Zahrnuje diskuse o právech uživatelů na přístup k internetu, o právech poskytovatelů internetových služeb na správu svých sítí a o dalších souvisejících otázkách. Ačkoli panuje shoda ohledně důležitosti svobodného a otevřeného internetu, panují neshody ohledně rozsahu a míry neutrality a ohledně odpovědnosti za stanovení a prosazování pravidel. Je nezbytné, aby debata byla založena na vědeckých důkazech, a nikoli na politických či ideologických preferencích. Měla by se zaměřit na veřejný zájem, práva na přístup, sociální blaho a zlepšení internetu. (El-bawab, 2021, s. 6-7)

Téma, na kterém si USA zakládá je svoboda projevu, tato citlivost měla za důsledek zrušení či změny některých zákonů Nejvyšším soudem. Jedním z příkladů je případ FCC v. Fox Television Stations, Inc. v [35]roce 2009, ve kterém Nejvyšší soud rozhodl, že FCC porušila svobodu projevu tím, že pokutovala televizní stanice za obscénní výrazy během živých vysílání. Nejvyšší soud nezrušil přímo zákony týkající se síťové neutrality, ale zohlednil principy svobody projevu při posuzování těchto zákonů. Například v případě National Cable & Telecommunications Association v. Brand X Internet Services[36] v roce 2005 potvrdil rozhodnutí FCC, které klasifikovalo poskytovatele DSL internetu jako informační služby, což omezovalo schopnost státu regulovat je podle federálního práva o telekomunikacích a zachovávalo pravidla síťové neutrality. Další zrušené zákony jsou například zákon o slušnosti komunikací, zákon o ochraně dětí a zákon o ochraně soukromí dětí na internetu kterým se věnuji níže.

Zákon o slušnosti v komunikacích (Communications Decency Act, CDA) z roku 1996 byl prvním významným pokusem Kongresu USA regulovat pornografický materiál online. I když jeho některé části byly Nejvyšším soudem zrušeny jako

[35] FCC v. Fox Television Stations, Inc., 556 U.S. 502 (2009)
[36] National Cable & Telecommunications Association v. Brand X Internet Services, 545 U.S. 967 (2005)

protiústavní, článek 230, který poskytuje online platformám imunitu pro obsah zveřejněný třetími stranami, zůstává klíčovým aspektem regulace internetu. Zákon čelil ústavním námitkám, zejména pokud jde o jeho dopad na svobodu projevu. To nakonec vedlo ke zrušení několika článků. Zákon CDA měl regulovat neslušné projevy na internetu a za jeho šíření měly být ukládány sankce. Kritici však tvrdili, že je příliš široký a nejasný v definici neslušnosti, což by mohlo porušovat práva jednotlivců podle prvního dodatku Ústavy. Přesto, že některé části byly Nejvyšším soudem zrušeny jako protiústavní, článek 230, který poskytuje online platformám imunitu pro obsah zveřejněný třetími stranami, zůstává klíčovým aspektem regulace internetu v USA. Soud zdůraznil význam ochrany svobody projevu, a to i v souvislosti s regulací neslušného obsahu (Slavitt, Knorr, 2002, s. 1-19).

Zákon o ochraně dětí online (COPA) z roku 1998: Účelem zákona COPA bylo chránit děti před nevhodným obsahem na internetu tím, že vyžadoval, aby webové stránky s obsahem pro dospělé zavedly mechanismy ověřování věku uživatelů. Tento zákon byl v roce 2004 zrušen Nejvyšším soudem ve věci Ashcroft v. American Civil Liberties Union[37] s odkazem na obavy z porušování svobody projevu a z toho, že účinně nerozlišuje obsah pro dospělé od obsahu zaměřeného na děti.

Důležitým právním předpisem, který řeší porušování autorských práv na digitálních platformách, je zákon Digital Millennium Copyright Act (DMCA) z roku 1998. Zahrnuje ustanovení o oznamování a stahování, bezpečné přístavy pro poskytovatele online služeb a opatření proti obcházení pravidel (Goodman a spol. 2022).

Zákon o ochraně soukromí dětí na internetu (COPPA) z roku 1998 ukládá požadavky na webové stránky a online služby, které shromažďují osobní údaje dětí mladších 13 let, včetně požadavků na souhlas rodičů a pokynů na ochranu soukromí dětí online. Stránky musí poskytnou rodičům jasné informace a omezuje cílení reklam (Goodman a spol. 2022, s. 165-181).

[37] Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002), followed by 542 U.S. 656 (2004)

Zákon o počítačových podvodech a zneužití počítačů z roku 1986 je federální právní předpis, který řeší neoprávněný přístup k počítačovým systémům a sítím. Ustavuje učité činnosti za trestné činy, jako je hacking, neoprávněný přístup a šíření škodlivého softwaru. Jeho role je především bezpečnostní. (Goodman a spol. 2022, s. 165-181)

Zákon o ochraně dětí na internetu (CIPA), přijatý Kongresem USA v roce 2000, chrání nezletilé před škodlivým obsahem na internetu. CIPA vyžaduje, aby školy a knihovny s federálními finančními prostředky filtrovaly obscénnost, dětskou pornografii a škodlivý obsah. Dále požaduje, aby tyto instituce poskytovaly vzdělávání ohledně bezpečného chování na internetu. Navzdory námětům na ústavnost byla CIPA v roce 2003 Nejvyšším soudem považována za ústavní. Soud zdůraznil, že zákon efektivně chrání děti a zároveň respektuje svobodu projevu. CIPA tedy úspěšně přispívá k bezpečnosti internetu ve školách a knihovnách (Slavitt, Knorr, 2002, s. 1-19).

Kalifornský zákon o ochraně soukromí spotřebitelů (CCPA) z roku 2018, ačkoli není federálním zákonem, je významný jako nejkomplexnější zákon o ochraně osobních údajů na státní úrovni. Zákon CCPA dává spotřebitelům právo vědět, jaké osobní údaje jsou o nich shromažďovány a jak budou tyto údaje použity nebo zveřejněny. Rovněž dává spotřebitelům právo zabránit prodeji jejich osobních údajů a právo na výmaz jejich osobních údajů. CCPA se vztahuje na podniky, které splňují určitá kritéria. Například mohou mít roční hrubé příjmy vyšší než určitá hranice nebo shromažďovat osobní údaje od určitého počtu spotřebitelů. Vyžaduje, aby společnosti poskytovaly spotřebitelům jasná a transparentní oznámení o ochraně osobních údajů a přijaly přiměřená bezpečnostní opatření na ochranu osobních údajů. Vzhledem k pokutám a možným právním krokům v případě nedodržení má zákon CCPA pro podniky významné důsledky. Tento zákon ovlivnil i další státy a země, aby zvážily podobné právní předpisy o ochraně osobních údajů. To vedlo k širšímu celosvětovému zaměření na práva na ochranu soukromí a ochranu údajů.

7.2. Srovnání regulačních rámců v EU a US

Síťová neutralita, je jednou z charakteristik internetové architektury a na jeho počátku o ní nebyly pochyby. Otázka síťové neutrality je však v historii USA sporné téma, které se razantně změnilo v posledních. Pravidla síťové neutrality byla přijata za vlády prezidenta Baracka Obamy, ale v roce 2017 byla Federální komisí pro komunikace zrušena. Tím byla odstraněna povinnost poskytovatelům internetových služeb zachovávat rovné zacházení s veškerým internetovým provozem. Vyvolává to obavy o upřednostňování poskytovateli internetových služeb. Naopak, v Evropské unii byla zavedena pravidla síťové neutrality, která mají za cíl zajistit, že všechen internetový provoz bude zacházen stejně bez diskriminace. Tato pravidla jsou součástí širšího regulačního rámce EU pro telekomunikace a digitální služby a mají za úkol chránit otevřený a spravedlivý internetový prostor pro všechny uživatele. V Evropské unii je síťová neutralita chráněna pokyny Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC). Tyto pokyny stanoví zásady pro zajištění otevřeného a neutrálního internetu (El-bawab, 2021, s. 6-7). Vede to k zamyšlení, proč nereguluje USA neutralitu federálně, ale ponechává jednotlivým státům vlastní iniciativu.

V EU hraje důležitou roli DSA, zaměřen na omezení falešných zpráv, dezinformací a online manipulace. Představuje komplexní právní rámec, který stanovuje proaktivní opatření, požadavky a spolupráci mezi platformami a orgány, aby se těmto problémům účinně předcházelo. Na druhé straně Spojené státy nemají žádný komplexní federální zákon, který by se specificky věnoval těmto problémům. Místo toho se USA spoléhají na stávající zákony, jako je CDA, zejména jeho článek 230, který poskytuje omezenou ochranu odpovědnosti online platforem za obsah vytvářený uživateli. Přesto, že jeho přísnější části byly zrušeny. Zatímco přístup USA je spíše zaměřen na samoregulaci platforem a politiky moderování obsahu vytvářeného uživateli, evropský DSA přináší aktivní opatření a spolupráci, aby zajistil transparentnost, odpovědnost a ochranu spotřebitelů na digitálních trzích (Monti, 2022, s. 40-68). Přístup USA k regulaci internetu se zaměřuje na ochranu svobody projevu a minimalizaci státního zásahu do online prostředí. Zákonodárství jako článek 230 zákona o slušnosti

v komunikacích poskytuje online platformám rozsáhlou imunitu vůči obsahu vytvořenému uživateli. To umožňuje platformám jako sociální sítě a fóra hostit různorodé názory a obsah bez obav z právní odpovědnosti za obsah uživatelů. EU se zaměřuje na ochranu spotřebitelů, práva na soukromí a hospodářskou soutěž v rámci digitálního prostředí. Předpisy jako GDPR klade na společnosti větší požadavky ohledně ochrany osobních údajů, DSA moderování obsahu a DMA zamezení dominantního či monopolního postavení na trhu. Tyto předpisy mají za cíl zajistit transparentnost, bezpečnost a zabezpečení práv uživatelů online služeb v rámci EU.

Ochrana osobních údajů v USA je upravována zejména prostřednictvím různých federálních a státních zákonů, jako je zákon o ochraně soukromí dětí na internetu (COPPA) a kalifornský zákon o ochraně soukromí spotřebitelů (CCPA). COPPA stanoví požadavky na ochranu osobních údajů dětí mladších 13 let, zatímco CCPA poskytuje obyvatelům Kalifornie určitá práva týkající se sběru, používání a sdílení jejich osobních údajů podniky, včetně práva na přístup k těmto údajům a práva na jejich smazání. V přímém kontrastu, EU změnila trh s údaji přísným nařízením GDPR v komparaci s řešeními US má evropské řešení vyšší standard ochrany osobních údajů a dopadajících plošně ne sektorově. GDPR poskytuje občanům EU rozsáhlá práva ohledně jejich osobních údajů a ukládá společnostem přísné povinnosti ohledně jejich zpracování a ochrany. Toto nařízení má účinek za hranice členských států, což znamená, že se vztahuje na jakoukoli společnost, která zpracovává osobní údaje občanů EU, bez ohledu na to, zda má sídlo v EU nebo nikoli.

Regulace obsahu je zvláště rozdílná. První dodatek ústavy, který chrání svobodu projevu, je klíčovým faktorem v regulaci obsahu v USA. To znamená, že zásahy státu do obsahu jsou omezené a primárně se zaměřují na specifické aspekty, jako jsou porušení autorských práv. Zákon DMCA je jedním z hlavních právních nástrojů v oblasti autorských práv na internetu. Zároveň zákon CDA stanovuje určité limity pro nevhodný obsah online, ale platformy mají obvykle velkou volnost v tom, jaký obsah umožňují nebo blokují. EU aktivněji zasahuje do regulace obsahu na internetu s cílem bojovat proti nelegálnímu obsahu a škodlivému chování online. DSA je jedním z klíčových právních předpisů, kterým

se EU zabývá, a má za cíl zajistit transparentnost a odpovědnost při moderování obsahu online platforem. Kromě toho EU přijala opatření zaměřená na odstranění nenávistných projevů a dezinformací z internetu, cíleně se zabývala internetovým terorismem a klade důraz na ochranu uživatelů za udržení bezpečného a respektujícího online prostředí.

Souhrnně lze říct, že zatímco Spojené státy i Evropská unie regulují různé aspekty internetu, EU má tendenci mít komplexnější a aktivnější předpisy týkající se ochrany soukromí, moderování obsahu a hospodářské soutěže. Evropská legislativa, jako například GDPR a nařízení o digitálních službách, poskytuje pevný rámec ochrany dat a pravidel pro digitální prostředí. Naopak Spojené státy často upřednostňují svobodu projevu a tržní přístup k regulaci, což dává online platforem širší pole působnosti a diskrece při formování svých zásad a postupů, včetně boje proti dezinformacím.

8. Srovnání s čínskou legislativou

V oblasti regulaci internetu, Čína a EU zaujaly zcela odlišné přístupy. Čína zvolila měkké právo, které umožňuje rychle reagovat na změny digitálního trhu. EU se naproti tomu rozhodla pro tvrdé právo s využitím přezkumných mechanismů, které mají zmírnit nepružnost a chránit jednotný trh. Obě jurisdikce zavedly opatření k řešení problémů s monopoly a uznaly nadměrnou moc společností digitálních platforem. Právní odpovědnost internetových zprostředkovatelů je mezi digitálními velmocemi upravována odlišně, v USA poskytují široký rozsah občanskoprávní imunity ústavou, zatímco EU a Čína omezují některá práva na pro vyšší bezpečnost. USA se zaměřují na ochranu svobody projevu, zatímco EU klade důraz na vyváženost pravidel a spravedlnost, čínský přístup se zdá být více orientován na kontrolu a regulaci. (Zheng, Snyder, 2023, s. 25-50) Navzdory rozdílům, existuje potenciální shoda mezi EU a Čínou při řešení monopolů v ekonomice digitálních platforem. Další podobnosti lze nalézt v oblasti digitální suverenity, zejména pokud jde o snahu o podchycení důležitosti digitálního prostoru a ochranu citlivých dat.

8.1. Přehled relevantních zákonů a politik v Číně

Regulace internetu v Číně spočívá v kombinaci zákonů, nařízení a vládních politik, které mají za cíl kontrolu obsahu online, zajištění kybernetické bezpečnosti a udržení politické stability. Hlavními předpisy, kterými se internet v Číně řídí, jsou antimonopolní zákon, zákon o kybernetické bezpečnosti a zákon o ochraně osobních údajů.

Účelem antimonopolního zákona je upravit zákaz chování na internetových platformách a chránit práva a zájmy spotřebitelů (Yin a spol, 2023). Zákon o kybernetické bezpečnosti Čínské lidové republiky, přijatý v roce 2016 a účinný od roku 2017, upravuje různé aspekty kybernetické bezpečnosti v zemi. Tento zákon se zabývá ochranou dat, bezpečností sítí a ochranou kritické informační infrastruktury. Přímo chrání osobní údaje a stanoví zásady jejich shromažďování, používání a požadavky na bezpečnost informací. Jedním z hlavních bodů zákona je povinnost provozovatelů sítí zavést opatření na ochranu údajů a zajistit bezpečnost svých sítí. Tento zákon rovněž zakazuje

činnosti, které by mohly ohrozit národní bezpečnost a narušit společenský řád. Definuje tak činy podněcování k rozvrácení národní suverenity a socialistického zřízení, separatismu, podkopávání národní jednoty, propagace terorismu, extremismu, podněcování k etnické nenávisti a diskriminaci, šíření násilných, obscénních nebo sexuálních informací, šíření nepravdivých informací narušujících hospodářský nebo společenský řád nebo poškozující pověst, soukromí, duševní vlastnictví nebo jiná zákonná práva a zájmy jiných osob. (Článek 12). Tímto zákonem Čína usiluje o zvýšení kybernetické bezpečnosti v zemi a ochranu citlivých informací a kritické infrastruktury před kybernetickými hrozbami a útoky. Zákon o ochraně osobních údajů, přijatý v roce 2021, komplexně chrání osobní údaje a stanoví práva fyzických osob na zpracování údajů, povinnosti zpracovatelů údajů a pravidla pro ochranu citlivých osobních údajů. Kromě toho zavedení víceúrovňového systému finančního dohledu nad internetem a zdokonalení zákonů a nařízení o internetových financích pomáhají regulovat internetové finance v Číně. (Xu a spol, 2022, s. 3-8)

Důležitým krokem v regulaci tohoto odvětví v Číně je rozvoj víceúrovňového dohledu nad finančními aktivitami na internetu a zdokonalení právních předpisů týkajících se internetového financování. Tato opatření přispívají k ochraně spotřebitele a prevenci finanční kriminality tím, že umožňují sledování finančních transakcí na internetu a zlepšují dohled nad finančními službami na internetu. Využití soft law umožňuje Číně pružně reagovat na obavy veřejnosti týkající se digitálního trhu. Měkké právo je soubor nástrojů jako jsou doporučení a dohody, které umožňují rychlou reakce na výzvy a trendy v digitálním prostředí. Posílení pravomocí orgánu pro hospodářskou soutěž v Číně je dalším důležitým krokem k překonání nezávazné povahy měkkého práva. To umožní účinněji regulovat a chránit hospodářskou soutěž na digitálním trhu a bojovat proti nekalým praktikám, jako je monopolizace nebo porušování antimonopolních pravidel. (Zheng, Snyder, 2023, s. 25-50).

Čínský přístup ke správě kyberprostoru zdůrazňuje koncept kybernetické suverenity a aktivní zapojení vlády do tvorby internetové politiky. Pravidla a pokyny pro rozvoj a regulaci kyberprostoru v zemi stanovují vládní orgány ve spolupráci s podnikatelským sektorem. Poslední známky zvýšené účasti čínských podniků

naznačují, že soukromý sektor hraje v reformním procesu stále větší roli, což může vést k nové dynamice kyberprostoru. Spolupráce mezi vládou a soukromým sektorem může vést k efektivnějšímu řízení a regulaci kyberprostoru díky kombinaci znalostí a zkušeností obou stran. Podpora rozvoje digitální ekonomiky a posílení úlohy soukromého sektoru může podpořit rozvoj čínské digitální ekonomiky prostřednictvím větší flexibility a inovací v podnikatelském a technologickém sektoru. Čínské kybernetické normy reflektují jejich orientaci na kontrolu, na rozdíl od otevřenějšího přístupu západních zemí. Tento fakt může vést k větší pozornosti Západu vůči čínským kybernetickým normám, zejména v EU. Kybernetická politika v Číně se formuje skrze dialog mezi vládou a podniky, přičemž nedávné reformy ukazují na zvýšené zapojení čínských firem. Při tvorbě a implementaci internetových předpisů a politik v Číně hrají klíčovou roli vládní agentury. Pro posílení spolupráce mezi vládou a soukromým sektorem úzce spolupracují se společnostmi, aby zaručily dodržování předpisů a soulad s cíli vlády. Tato partnerství signalizují úzké propojení mezi veřejným a soukromým sektorem v procesu správy kyberprostoru v Číně. Tyto interakce mezi vládními agenturami a zúčastněnými stranami z odvětví zahrnují spolupráci, koordinaci a konzultace. Vládní agentury poskytují podnikatelské komunitě pokyny a vedení, ale také od ní vyžadují vstupy a zpětnou vazbu.(Gao, 2022).

8.2. Srovnání regulačního přístupu EU a Číny

Čína přijala opatření na ochranu osobních údajů prostřednictvím právních předpisů, jako je zákon o kybernetické bezpečnosti a zákon o ochraně osobních údajů. Tato legislativa chrání osobní údaje fyzických osob a stanovuje jejich práva při zpracování těchto údajů. Komplexní rámec EU zahrnuje tyto oblasti, předpisy jako je GDPR, NIS a dalšími. Osobní údaje prošly četnými změnami a reflektují jejich hodnotu v systému EU. Přesto, že oba systémy upravují oblast bezpečnosti a osobních údajů, existují značné rozdíly v postupech dohledu, vymáhání, definic klíčových pojmů a povahou sankcí za porušení. Pokud jde o omezení obsahu, EU v zájmu dosažení rovnováhy mezi svobodou projevu a ochranou jednotlivců a společnosti zavedla pravidla týkající se nenávistných projevů, teroristického obsahu a nezákonného obsahu. Teroristický obsah byl uznán za natolik zásadní pro kyberprostor, že je regulován samostatně. Jak je vidět, přístup EU směřoval

k omezení šíření škodlivého obsahu a zároveň k ochraně základních práv a svobod jednotlivců. Čína naproti tomu přistupuje k regulaci online obsahu přísněji, zejména pokud jde o politický disent a citlivé otázky. Čínská vláda využívá cenzuru k řízení toku informací a udržování politické stability v souladu se svými prioritami a ideologickými zásadami. To znamená, že obsah na čínském internetu je pečlivě monitorován a filtrován tak, aby odpovídal oficiální vládní linii a k zabránění veřejné diskusi o určitých otázkách. V tomto ohledu Čína upřednostňuje politickou kontrolu a udržování stability. (Nan, 2023, s. 159-172)

Rozdílné přístupy k identifikaci strážců v Číně a EU odrážejí odlišný politický a ekonomický kontext obou regionů. V EU je identifikace strážců přístupu na digitálních trzích založena na jasných identifikačních kritériích a kvantitativních ukazatelích založených na příjmech a uživatelském provozu. K určení toho, kdo by měl být považován za strážce digitálního trhu, se používají transparentní postupy a pravidla. Kritéria zahrnují objektivní ukazatele, jako je podíl na trhu, roční příjmy a počet uživatelů. Naproti tomu čínské internetové platformy mají obvykle vyšší obrat a větší počet uživatelů než jejich protějšky v Evropě. Problematika chování internetových platforem v Číně se týká především situací, kdy dominantní platformy využívají svého silného postavení k potlačení konkurence a zabránění vstupu nových hráčů na trh. Mohou tak bránit inovacím a omezovat schopnost ostatních provozovatelů působit na trhu. Toto chování může vést k vytvoření monopolů, které výrazně ovlivňují digitální ekonomiku a zneužít svého postavení ve svůj prospěch na úkor ostatních účastníků trhu a spotřebitelů. Dosud existují v čínském antimonopolním právu jen omezené nástroje, které by takové chování regulovaly. Existují určité regulace zaměřené na omezení přístupu do odvětví, nejsou však plně účinná při řešení dominantních hráčů na trhu. K problémům monopolního chování a zneužívání moci ze strany platforem je zapotřebí komplexní přístup, který by mohl zahrnovat zavedení zvláštních pravidel pro strážce přístupu. Taková opatření by mohla přispět k regulaci silného postavení dominantních hráčů a k vytvoření spravedlivějšího prostředí pro všechny účastníky digitálního trhu v Číně (Yin a spol, 2023).

Výběr regulačních nástrojů je ovlivněn chováním na digitálním trhu a strukturou hospodářské soutěže. Zatímco EU čelí přeshraničním výzvám a sjednocení

režimu, čínskému digitálnímu trhu dominují domácí technologické společnosti. Čínské orgány pro hospodářskou soutěž mají ve srovnání s Evropskou komisí silnější pravomoci zejména kvůli centralizované povaze čínského politického systému a možnosti provádět rozsáhlé a rychlé zásahy do hospodářských subjektů. EU se od Číny liší svým přístupem ke správě digitálního prostředí. Cílem EU je vytvořit jednotný soubor pravidel pro ochranu vnitřního trhu a poskytnout právní rámec pro digitální ekonomiku. Nařízení posilují jednotný trh a zajišťují jednotná pravidla pro účastníky trhu a jsou přímo závazné pro všechny členské státy. Čína upřednostňuje měkké právo, které jí umožňuje rychle reagovat na obavy veřejnosti a pružně přizpůsobovat své předpisy. Tento přístup umožňuje vládě rychle zasahovat do digitálního prostředí, v souladu s měnícími se potřebami a vývojem trhu, což je podpořeno pravomocemi čínského orgánu pro hospodářskou soutěž. Čína sází na flexibilní regulační přístup, který umožňuje rychlé změny a reakci na aktuální podmínky na trhu, zatímco EU klade důraz na jednotný právní rámec a ochranu jednotného trhu prostřednictvím závazných předpisů. Strategie má své výhody i nevýhody a bude přizpůsobena specifickým potřebám a podmínkám každého trhu. Úloha čínské vlády při utváření digitálních trhů a online obsahu.

Čínská vláda hraje důležitou roli při formování digitálních trhů a online obsahu v Číně. Zavedla přístupy k řízení, které mají regulovat ekonomiku online platforem a zajistit sociálně-politickou stabilitu, hospodářský růst a technologickou soběstačnost. Za účelem kontroly online diskurzu vláda přistupuje k webovým stránkám jako k autoritativním zdrojům informací a uplatňuje logiku masové komunikace. Čínské platformy se staly mocnými světovými aktéry, což vedlo ke změnám ve způsobu, jakým je vláda řídí.

Čína zavedla přísnou regulaci internetového obsahu, aby cenzurovala politicky citlivé informace a podporovala "pozitivní energii". Čínská správa kyberprostoru je pověřena kontrolou internetového obsahu a prováděním cenzurních zákonů, které vyžadují, aby webové stránky a online platformy cenzurovaly obsah považovaný za nezákonný nebo škodlivý, včetně pornografie, násilí a politicky citlivých témat. Čína má propracovaný systém cenzury internetu, který je známý jako "Velký firewall". Omezuje přístup k webovým stránkám a cenzuruje online obsah

pomocí blokování IP adres, filtrování DNS a filtrování klíčových slov. Aby se zabránilo šíření disentu a politicky citlivého obsahu, Velká brána firewall také monitoruje a filtruje domácí internetový provoz. Registrace pod skutečným jménem je politika čínské vlády, která vyžaduje, aby uživatelé internetu při registraci k online službám uváděli svou skutečnou identitu. Je to považováno za způsob, jak zabránit anonymitě na internetu a přimět jednotlivce k odpovědnosti za jejich chování na internetu. Čínská vláda zavedla různá opatření k prosazení registrace skutečných jmen, včetně požadavku, aby poskytovatelé internetových služeb ověřovali totožnost uživatelů, a propojení online účtů se skutečnou totožností jednotlivců (Wang, 2003).

Problémy, jako je používání sítí VPN k obcházení omezení a obtížné ověřování informací o uživateli, brání zavedení registrace pod skutečným jménem v Číně. Čínská vláda se snaží sledovat online aktivity a identifikovat osoby, které se účastní činností považovaných za ohrožující národní bezpečnost nebo sociální stabilitu. K tomu využívá širokou škálu sledovacích a monitorovacích technologií, jako je rozpoznávání obličejů, systémy sledování založené na umělé inteligenci a analýza velkých dat. Tyto technologie umožňují vládě monitorovat uživatele internetu a identifikovat podezřelé chování. Vláda spolupracuje s poskytovateli internetových služeb a technologickými společnostmi při prosazování těchto pravidel a zajišťování jejich dodržování. Tato opatření mají za cíl udržet kontrolu nad internetovým prostředím a potlačit aktivity považované za hrozbu národní bezpečnosti nebo sociální stabilitu (Wang, 2003).

Čínská vláda pod vedením Si Ťin-pchinga hraje významnou roli při formování digitálních trhů a online obsahu v Číně. Vládní politiky v oblasti regulace a řízení kladou důraz na zapojení státu a jeho kontrolu nad regulačními otázkami a rámci souvisejícími s internetem. Cílem čínské regulace a správy internetu je posílit stávající politickou strukturu a podpořit digitální moc Číny v celosvětovém měřítku. Zapojení a kontrola státu do utváření digitálních trhů a online obsahu přispívají k udržení sociální stability, ochraně národní bezpečnosti a prosazování vládního ideologického programu. Čínská vláda je důležitým hráčem, který ovlivňuje čínské digitální trhy a online obsah. Aby kontrolovala online obsah a zajistila jeho soulad s ideologií a hodnotami komunistické strany, zavedla přísná nařízení a cenzurní

opatření. Vláda zavedla komplexní regulační rámec, který vyžaduje, aby internetové společnosti získaly licence a dodržovaly konkrétní pokyny týkající se moderování obsahu a zabezpečení dat. Aby vláda zabránila šíření politicky citlivých informací a zachovala sociální stabilitu, aktivně monitoruje a cenzuruje online platformy, včetně sociálních médií, zpravodajských webových stránek a platforem pro streamování videa. Kromě toho se rozvíjejí domácí digitální platformy a technologie, včetně platforem elektronického obchodu a umělé inteligence, které mají podpořit hospodářský růst a posílit digitální sílu Číny v celosvětovém měřítku. Celkově se čínská vláda snaží udržet politickou kontrolu, prosazovat národní zájmy a rozvíjet digitální vliv Číny na globální scéně prostřednictvím svého zapojení do utváření digitálních trhů a online obsahu (Xu a spol, 2022).

9. Závěr

Regulace internetu, včetně jeho obsahu, digitálních platforem, dat a osobních údajů, je dynamickou oblastí plnou rychlých změn a potřeby časté aktualizace. V nejistých dobách, kdy bezpečnost nabývá na důležitosti, je trend zesilování pravidel patrný i v online prostředí. Celkově se přístup EU k internetové legislativě zaměřuje na ochranu práv jednotlivců, posílení regulace ochrany soukromí, podporu neutrality sítě, harmonizaci digitálních zákonů v členských státech s cílem vytvořit jednotný trh. V reakci na dynamickou povahu digitálního prostředí a nové technologické výzvy je vývoj internetového práva EU nepřetržitým procesem.

Spravedlnost, jednota a ochrana jsou pouze některé z mnoha principů, které současný rámec nabízí. Je třeba si však uvědomit, že cesta k dnešní právní podobě byla poznamenána mnoha překážkami a výzvami. Od přijetí GDPR až po současnost, lze pozorovat posun EU směrem k intervencionistickému přístupu v otázkách souvisejících s ochranou osobních údajů, obsahem na internetu a jednotností digitálního trhu, což se odráží v přijatých předpisech aktualizujících tuto problematiku.

Cílem této práce je analyzovat internetové právní prostředí, jeho vývoj a aktuální stav v porovnání s ostatními zeměmi. Byly představeny právní rámce v oblasti internetu globálních aktérů EU, USA a Číny. Jejich porovnání poukazuje na značné a méně viditelné rozdíly. Pro lepší porozumění digitálního prostoru jako celku byl úvod věnován kritickým pojmům, jako je architektura internetu, kyberprostor a elektronický obchod. Na ty navázaly předpisy, které tvoří základ pro správu vybraných oblastí internetu, a dále bylo nutné zmínit jurisdikci EU v komplexním prostředí internetu, postavenou na několika rozhodnutích Soudního dvora Evropské unie. Kapitoly zaměřené na DSA a DMA nahlížejí na změny, které přináší v kontextu stávajícího právního prostředí EU pro digitální platformy a uživatele. Poslední kapitoly srovnávají postavení dosud projednávaných oblastí s USA a Čínou, aby ukázaly na rozdíly v právních kulturách a individuálních řešeních a lepší pochopení evropských mechanismů.

Téma bakalářské práce je velmi aktuální a bude nezbytné sledovat jeho vývoj v příštích letech, abychom zjistili, jak se změny provedené DSA projeví v prostředí digitálních platforem. Je důležité sledovat, jak se tyto změny promítnou do praxe a jaké budou jejich dopady na chování digitálních platforem, spotřebitelů a digitálního trhu obecně. V budoucnu uvidíme, zda nastavené povinnosti a změny budou v podporovat či kolidovat s dosavadními kroky k zabezpečení otevřeného, spravedlivého a inovativního digitálního prostředí. Je možné, že některé zavedené opatření mohou vyvolat spory mezi digitálními platformami a regulátory, zatímco jiné by mohly posílit důvěru spotřebitelů a podpořit inovace a konkurenci na trhu. Komplexní úprava správy internetu EU, nejen v rámci DSA by mohla sloužit jako vzor pro svět a mohla by být příkladem pro další jurisdikce při regulaci digitálního prostředí. Je proto důležité sledovat, jak bude EU úspěšně implementovat a prosazovat opatření stanovená v rámci DSA a jaké budou jejich dlouhodobé dopady na digitální ekosystém.

Seznam použité literatury

Monografie:

AAMIR, Suhaib. ECommerce Types. Online. In: BUHALIS, Dimitrios (ed.). Encyclopedia of Tourism Management and Marketing. Edward Elgar Publishing, 2022, s. 16-19. ISBN 9781800377486. Dostupné z: https://doi.org/10.4337/9781800377486.ecommerce.types. [cit. 2024-02-04].

BROWNSWORD, Roger. The E-Commerce Directive, Consumer Transactions, and the Digital Single Market – Questions of Regulatory Fitness, Regulatory Disconnection and Rule Redirection. Online. In: GRUNDMANN, Stefan (ed.). European Contract Law in the Digital Age. Intersentia, 2018, s. 165-204. ISBN 9781780686431. Dostupné z: https://doi.org/10.1017/9781780686431.006. [cit. 2024-02-04].

DICKIE, *John. Internet and Electronic Commerce Law in the European Union*. Online. Hart Publishing, 1999. ISBN 978-1-4725-6200-5. Dostupné z: https://doi.org/10.5040/9781472562005. [cit. 2024-002-01].

DUMORTIER, Jos. E-commerce and EU Competition Law. Online. In: *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation)*. Edward Elgar Publishing, 2022, s. 427-488. ISBN 9781800372092. Dostupné z: https://doi.org/10.4337/9781800372092.00021. [cit. 2024-02-03].

DUMORTIER, Jos. Regulation 2015/2120/EU Laying down Measure Concerning Open Internet Access. Online. In: *Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation)*. Edward Elgar Publishing, 2022, s. 281-307. ISBN 9781800372092. Dostupné z: https://doi.org/10.4337/9781800372092.00016. [cit. 2024-02-06].

EDWARDS, Lilian, *The New Legal Framework for E-Commerce in Europe*. Online. Hart Publishing, 2005. ISBN 978-1-8411-3451-2. Dostupné z: https://doi.org/10.5040/9781472563514. [cit. 2024-02-01].

FAHEY, Elaine. The EU as a Global Digital Actor. Online. Hart Publishing, 2022. ISBN 978-1-50995-704-0. Dostupné z: https://doi.org/10.5040/9781509957071. [cit. 2024-02-04].

FERACI, Ornella. Digital Rights and Jurisdiction: The European Approach to Online Defamation and IPRs Infringements. Online. In: CARPANELLI, Elena a LAZZERINI, Nicole (ed.). Use and Misuse of New Technologies. Cham: Springer International Publishing, 2019, s. 277-304. ISBN 978-3-030-05647-6. Dostupné z: https://doi.org/10.1007/978-3-030-05648-3_14. [cit. 2024-03-01].

FROOMKIN, A. Michael. The Internet as a Source of Regulatory Arbitrage. Online. In: KAHIN, Brian a NESSON, Charles (ed.). *Borders in Cyberspace*. The MIT Press, 1997, s. 129-163. ISBN 9780262276603. Dostupné z: https://doi.org/10.7551/mitpress/1648.003.0007. [cit. 2024-02-03].

GOODMAN, Ellen P.; KETTEMANN, Matthias C.; PEUKERT, Alexander a SPIECKER GEN. DÖHMANN, Indra. Law of Digitality. Online. In: The Law of Global Digitality. London: Routledge, 2022, s. 165-181. ISBN 9781003283881. Dostupné z: https://doi.org/10.4324/9781003283881-12. [cit. 2024-02-27].

CHRISTOU, George a SIMPSON, Seamus. The Influence of Global Internet Governance Institutions on the EU. Online. In: COSTA, Oriol a JÃ¸RGENSEN, Knud Erik (ed.). *The Influence of International Institutions on the EU*. Palgrave Macmillan, 2012. ISBN 9780230369894. Dostupné z: https://doi.org/10.1057/9780230369894_6. [cit. 2024-02-02].

INOZEMTSEV, Maxim I.; SIDORENKO, Elina L. a KHISAMOVA, Zarina I. (ed.). The Platform Economy. Online. Singapore: Springer Nature Singapore, 2022. ISBN 978-981-19-3241-0. Dostupné z: https://doi.org/10.1007/978-981-19-3242-7. [cit. 2024-02-21]. 77-92

LODDER, Arno R. a MURRAY, Andrew D. (ed.). *EU Regulation of E-Commerce*. Online. Edward Elgar Publishing, 2017, s. 1-14 ISBN 9781785369346. Dostupné z: https://doi.org/10.4337/9781785369346. [cit. 2024-02-03].

MARSDEN, Christopher T. Internet Co-Regulation. Online. Cambridge University Press, 2011. ISBN 9781107003484. Dostupné z: https://doi.org/10.1017/CBO9780511763410. [cit. 2024-02-27].

METAKIDES, George. A Crucial Decade for European Digital Sovereignty. Online. In: WERTHNER, Hannes; PREM, Erich; LEE, Edward A. a GHEZZI, Carlo (ed.). *Perspectives on Digital Humanism*. Cham: Springer International Publishing, 2022, s. 219-225. ISBN 978-3-030-86143-8. Dostupné z: https://doi.org/10.1007/978-3-030-86144-5_29. [cit. 2024-02-03]

NANXIANG, Sun a LV, Qiusha. *Internet Regulation and the International Trade Regime*. Online. London: Routledge, 2022. ISBN 9781003295884. Dostupné z: https://doi.org/10.4324/b22932. [cit. 2024-02-06].

SAVIN, Andrej. *EU Internet Law*. Online. Edward Elgar Publishing, 2017, ISBN 9781784717971. Dostupné z: https://doi.org/10.4337/9781789908572 [cit. 2024-02-01].

SAVIN, Andrej a TRZASKOWSKI, Jan (ed.). Research Handbook on EU Internet Law. Online. Edward Elgar Publishing, 2014. ISBN 9781782544173. Dostupné z: https://doi.org/10.4337/9781782544173. [cit. 2024-02-08].

SIDORENKO, Elina L. Definition of “Digital Platforms.” Online. In: INOZEMTSEV, Maxim I.; SIDORENKO, Elina L. a KHISAMOVA, Zarina I. (ed.). The Platform Economy. Singapore: Springer Nature Singapore, 2022, s. 77-92. ISBN 978-981-19-3241-0. Dostupné z: https://link.springer.com/chapter/10.1007/978-981-19-3242-7_6. [cit. 2024-02-21].

SYNODINOU, Tatiana-Eleni; JOUGLEUX, Philippe; MARKOU, Christiana a PRASTITOU-MERDI, Thalia, 2021. *EU Internet Law in the Digital Single Market*. Springer. ISBN 978-3030695828.

WANG, Faye Fangfei. Internet Jurisdiction and Choice of Law. Online. Cambridge University Press, 2011. ISBN 9780521199339. Dostupné z: https://doi.org/10.1017/CBO9780511762826. [cit. 2024-02-27].

Časopisecké články:

BAGNATO, Domenica. The network information systems directive (EU) 2016/1148: internet service providers and registraties. Online. *Central and Eastern European eDem and eGov Days*. 2020, roč. 338, s. 111-122. ISSN 2663-9394. Dostupné z: https://doi.org/10.24989/ocg.v.338.9. [cit. 2024-02-05].

BENDIEK, Annegret a RÖMER, Magnus. Externalizing Europe: the global effects of European data protection. Online. *Digital Policy, Regulation and Governance*. 2019, roč. 21, č. 1, s. 32-43. ISSN 2398-5038. Dostupné z: https://doi.org/10.1108/DPRG-07-2018-0038. [cit. 2024-02-01].

BERMANNS, George. Strenthening trust and security in the EU cybersecurity policy. Online. Yearbook of European Union and Comparative Law. 2023, roč. 1, č. 1, s. 42-79. ISSN 2732-9909. Dostupné z: https://doi.org/10.12681/yeucl.33016. [cit. 2024-02-10].

BROUWER, Dennis. A non-discrimination principle for rankings in app stores. Online. *Internet Policy Review*. 2020, roč. 9, č. 4. ISSN 2197-6775. Dostupné z: https://doi.org/10.14763/2020.4.1539. [cit. 2024-02-02].

DIMITROVA, Anna a BRKAN, Maja. Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair. Online. *JCMS: Journal of Common Market Studies*. 2018, roč. 56, č. 4, s. 751-767. ISSN 0021-9886. Dostupné z: https://doi.org/10.1111/jcms.12634. [cit. 2024-02-01].

EKİNGEN, Erman. An Overview of the Concepts of 'Digital Economy' and 'Digital Markets' as Ongoing Trends in EU Competition Law. Online. *Selcuk Universitesi Hukuk Fakultesi Dergisi*. ISSN 1306-8075. Dostupné z: https://doi.org/10.15337/suhfd.1082006. [cit. 2024-02-04].

EL-BAWAB, Tarek S. The Debate about Internet Neutrality. Online. IEEE Communications Magazine. 2021, roč. 59, č. 9, s. 6-7. ISSN 0163-6804. Dostupné z: https://doi.org/10.1109/MCOM.2021.9566564. [cit. 2024-03-01].

GAO, Xinchuchu. An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model. Online. The International Spectator. 2022, roč. 57, č. 3, s. 15-30. ISSN 0393-2729. Dostupné z: https://doi.org/10.1080/03932729.2022.2074710. [cit. 2024-02-21].

GUAL, Jordi. Regulation and the development of electronic communications in Europe. Online. *Info*. 2002, roč. 4, č. 3, s. 42-49. ISSN 1463-6697. Dostupné z: https://doi.org/10.1108/14636690210440004. [cit. 2024-02-01].

HALPIN, Edward F. a SIMPSON, Seamus. Between self-regulation and intervention in the networked economy: the European Union and Internet policy. Online. *Journal of Information Science*. 2002, roč. 28, č. 4, s. 285-296. ISSN 0165-5515. Dostupné z: https://doi.org/10.1177/016555150202800403. [cit. 2024-02-01].

HEIDEBRECHT, Sebastian. From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. Online. *JCMS: Journal of Common Market Studies*. 2024, roč. 62, č. 1, s. 205-223. ISSN 0021-9886. Dostupné z: https://doi.org/10.1111/jcms.13488. [cit. 2024-02-03]

HOLZNAGEL, Bernd a HARTMANN, Sarah. The EU 'open Internet access' regulation and its impact on the digital press. Online. *Convergence: The International Journal of Research into New Media Technologies*. 2016, roč. 22, č. 5, s. 488-493. ISSN 1354-8565. Dostupné z: https://doi.org/10.1177/1354856516660810. [cit. 2024-02-06].

CHMIEL, Anna; SIENKIEWICZ, Julian; THELWALL, Mike; PALTOGLOU, Georgios; BUCKLEY, Kevan et al. Collective Emotions Online and Their Influence on Community Life. Online. *PLoS ONE*. 2011, roč. 6, č. 7. ISSN 1932-6203. Dostupné z: https://doi.org/10.1371/journal.pone.0022207. [cit. 2024-02-03].

CHIRICĂ, Simona, 2017. THE MAIN NOVELTIES AND IMPLICATIONS OF THE NEW GENERAL DATA PROTECTION REGULATION. Online. Perspectives of Business Law Journal. Roč. 2017, č. 6, s. 159-176. ISSN 2286-0649. Dostupné z: https://www.ceeol.com/search/journal-detail?id=1455. [cit. 2024-02-05].

CHRISTOU, GEORGE a SIMPSON, SEAMUS. The Internet and Public–Private Governance in the European Union. Online. *Journal of Public Policy*. 2006, roč. 26, č. 1, s. 43-61. ISSN 0143-814X. Dostupné z: https://doi.org/10.1017/S0143814X06000419. [cit. 2024-02-01].

IBRUS, Indrek a ROHN, Ulrike. Sharing killed the AVMSD star: the impossibility of European audiovisual media regulation in the era of the sharing economy. Online. *Internet Policy Review*. 2016, roč. 5, č. 2. ISSN 2197-6775. Dostupné z: https://doi.org/10.14763/2016.2.419. [cit. 2024-02-01].

JAYASURIYA, Kanishka. Globalization and the changing architecture of the state: the regulatory state and the politics of negative co-ordination. Online. *Journal of European Public Policy*. 2001, roč. 8, č. 1, s. 101-123. ISSN 1350-1763. Dostupné z: https://doi.org/10.1080/1350176001001859. [cit. 2024-02-01].

KALĖDA, Saulius Lukas. New European Union's Regulatory Framework of the Digital Space: the Digital Markets Act and the Digital Services Act. Online. Teisė. 2023, roč. 127, s. 25-42. ISSN 2424-6050. Dostupné z: https://doi.org/10.15388/Teise.2023.127.2. [cit. 2024-02-21].

LEISER, Mark, 2023. Analysing the European Union's Digital Services Act Provisions for the Curtailment of Fake News, Disinformation, & Online Manipulation [online]. Dostupné z: doi: https://doi.org/10.31235/osf.io/rkhx4. [cit. 2024-02-06].

LINHARTOVA, Veronika. The Role of E-Government in the Evaluation of the Quality of Governance in the Countries of the European Union. Online. *Hrvatska i komparativna javna uprava*. 2022, roč. 22, č. 2, s. 267-287. ISSN 18492150. Dostupné z: https://doi.org/10.31297/hkju.22.2.4. [cit. 2024-02-03]

LUTZI, Tobias. INTERNET CASES IN EU PRIVATE INTERNATIONAL LAW—DEVELOPING A COHERENT APPROACH. Online. International and Comparative Law Quarterly. 2017, roč. 66, č. 3, s. 687-721. ISSN 0020-5893. Dostupné z: https://doi.org/10.1017/S0020589317000240. [cit. 2024-02-09].

LUZAK, Joasia. Much Ado about Cookies: The European Debate on the New Provisions of the ePrivacy Directive regarding Cookies. Online. *European Review*

of Private Law. 2013, roč. 21, č. 1, s. 221-245. ISSN 0928-9801. Dostupné z: https://doi.org/10.54648/ERPL2013007. [cit. 2024-02-06].

MARX, Axel a VAN DER LOO, Guillaume. Transparency in EU Trade Policy: A Comprehensive Assessment of Current Achievements. Online. *Politics and Governance*. 2021, roč. 9, č. 1, s. 261-271. ISSN 2183-2463. Dostupné z: https://doi.org/10.17645/pag.v9i1.3771. [cit. 2024-02-02].

MONTI, Giorgio. Taming Digital Monopolies: A Comparative Account of the Evolution of Antitrust and Regulation in the European Union and the United States. Online. The Antitrust Bulletin. 2022, roč. 67, č. 1, s. 40-68. ISSN 0003-603X. Dostupné z: https://doi.org/10.1177/0003603X211066978. [cit. 2024-02-21].

NAŁĘCZ, Andrzej. Comment to the Judgement of EU Court of Justice in Joined Cases C-807/18 and C-39/19 Telenor Magyarország Zrt. v Nemzeti Média- és Hírközlési Hatóság Elnöke. Online. *Polish Review of International and European Law*. 2021, roč. 10, č. 2, s. 109-120. ISSN 2544-7432. Dostupné z: https://doi.org/10.21697/priel.2021.10.2.06. [cit. 2024-02-02].

NAN, Gong. Protection of personal data in China: Legislation in the digital age. Online. Vestnik of Saint Petersburg University. Law. 2023, roč. 14, č. 1, s. 159-172. ISSN 20741243. Dostupné z: https://doi.org/10.21638/spbu14.2023.110. [cit. 2024-02-27].

NURHAYATI, Yati. Regulatory Analysis Digital Markets Act (Dma) European Union In Business Competition. Online. International Journal of Law, Environment, and Natural Resources. 2023, roč. 3, č. 1, s. 107-174. ISSN 2776-4974. Dostupné z: https://doi.org/10.51749/injurlens.v3i1.46. [cit. 2024-02-21].

RENDA, Kadri Kaan. THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER? Online. Ankara Avrupa Calismalari Dergisi. 2022, roč. 21, č. 2, s. 467-495. ISSN 1303-2518. Dostupné z: https://doi.org/10.32450/aacd.1226890. [cit. 2024-02-10].

OSULA, Anna-Maria; AGNES KASPER a ALEKSI KAJANDER. EU Common Position on International Law and Cyberspace. Online. *Masaryk University Journal*

of Law and Technology. 2022, roč. 16, č. 1, s. 89-123. ISSN 1802-5951. Dostupné z: https://doi.org/10.5817/MUJL2022-1-4. [cit. 2024-02-10].

PAWAR, Sunil. C.; MENTE, R. S. a CHENDAGE, Bapu. D. Cyber Crime, Cyber Space and Effects of Cyber Crime. Online. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. S. 210-214. ISSN 2456-3307. Dostupné z: https://doi.org/10.32628/CSEIT217139. [cit. 2024-02-03].

PEHLIVAN, Ceyhun Necati a CHURCH, Peter. The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability. Online. Global Privacy Law Review. 2023, roč. 4, č. 1, s. 53-59. ISSN 26663570. Dostupné z: https://doi.org/10.54648/GPLR2023005. [cit. 2024-02-21].

POHLE, Julia a THIEL, Thorsten. Digital sovereignty. Online. *Internet Policy Review*. 2020, roč. 9, č. 4. ISSN 2197-6775. Dostupné z: https://doi.org/10.14763/2020.4.1532. [cit. 2024-02-02].

SARABDEEN, Jawahitha a MOONESAR, Immanuel Azaad. Privacy protection laws and public perception of data privacy. Online. Benchmarking: An International Journal. 2018, roč. 25, č. 6, s. 1883-1902. ISSN 1463-5771. Dostupné z: https://doi.org/10.1108/BIJ-06-2017-0133. [cit. 2024-02-09].

SLAVITT, Kelly M. a KNORR, Matthew, 2002. CONTENT-BASED REGULATION OF ELECTRONIC MEDIA: INDECENT SPEECH ON THE INTERNET. Online. UIC John Marshall Journal of Information Technology & Privacy Law. Roč. 21, č. 1, s. 1-19. ISSN 1078-4128. Dostupné z: https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1105&context=jitpl. [cit. 2024-02-27].

THEMELIS, Andreas. The Internet, Jurisdiction and EU Competition Law: The Concept of ‘Over-territoriality‘ in Addressing Jurisdictional Implications in the Online World. Online. World Competition. 2012, roč. 35, č. 2, s. 325-353. ISSN 1011-4548. Dostupné z: https://doi.org/10.54648/WOCO2012021. [cit. 2024-02-08].

TOFAN, Mihaela a BOSTAN, Ionel. Some Implications of the Development of E-Commerce on EU Tax Regulations. Online. *Laws*. 2022, roč. 11, č. 1. ISSN 2075-471X. Dostupné z: https://doi.org/10.3390/laws11010013. [cit. 2024-02-04].

TOMÍŠEK, Jan. Jak regulovat cookies v nařízení ePrivacy. Online. *Revue pro právo a technologie*. 2023, roč. 14, č. 27. ISSN 1805-2797. Dostupné z: https://doi.org/10.5817/RPT2023-1-5. [cit. 2024-02-06].

VALENTINO, Lucini. THE EVER-INCREASING CYBERSECURITY COMPLIANCE IN EUROPE: THE NIS 2 AND WHAT ALL BUSINESSES IN THE EU SHOULD BE AWARE OF. Online. *Russian Law Journal*. 2023, roč. 11, č. 6s. ISSN 2313-7851. Dostupné z: https://doi.org/10.52783/rlj.v11i6s.911. [cit. 2024-02-05].

WITT, Anne C. The Digital Markets Act – Regulating the Wild West. Online. SSRN Electronic Journal. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.4395089. [cit. 2024-02-21].

XU, Jian a YU, Haiqing. Regulating and governing China's internet and digital media in the Xi Jinping era. Online. Media International Australia. 2022, roč. 185, č. 1, s. 3-8. ISSN 1329-878X. Dostupné z: https://doi.org/10.1177/1329878X221116402. [cit. 2024-02-21].

YIN, Zhihang; ZHU, S.; CHEN, Y. a LIANG, J. Legal Regulation of Internet Platform Banning Behaviors. Online. SHS Web of Conferences. 2023, roč. 162. ISSN 2261-2424. Dostupné z: https://doi.org/10.1051/shsconf/202316201036. [cit. 2024-02-21].

ZHENG, Kena a SNYDER, Francis. China and EU's wisdom in choosing competition soft law or hard law in the digital era: a perfect match? Online. China-EU Law Journal. 2023, roč. 9, č. 1-4, s. 25-50. ISSN 1868-5153. Dostupné z: https://doi.org/10.1007/s12689-023-00101-8. [cit. 2024-02-21].

Konferenční příspěvky:

LISIČAR, H.; I, T. Katulić a JURIĆ, M. Online Audiovisual Content, Video Sharing Platforms and Regulation under DSA and AVMSD. Online. In: *2023 46th MIPRO ICT and Electronics Convention (MIPRO)*. IEEE, 2023, s. 1478-1483. ISBN 978-

953-233-104-2. Dostupné z: https://doi.org/10.23919/MIPRO57284.2023.10159984. [cit. 2024-03-01].

Seznam legislativy:

Rámcové rozhodnutí Rady 2008/913/SVV ze dne 28. listopadu 2008 o boji proti některým formám a projevům rasismu a xenofobie prostřednictvím trestního práva

Rozhodnutí Rady ze dne 4. prosince 2014, 2014/887/EU: o schválení Haagské úmluvy ze dne 30. června 2005 o dohodách o volbě soudu jménem Evropské unie

Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)

směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů

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

Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

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

Směrnice Evropského parlamentu a Rady (EU) 2018/1808 ze dne 14. listopadu 2018, kterou se mění směrnice 2010/13/EU o koordinaci některých právních a

správních předpisů členských států upravujících poskytování audiovizuálních mediálních služeb (směrnice o audiovizuálních mediálních službách) s ohledem na měnící se situaci na trhu

Směrnice Evropského parlamentu a Rady 2005/29/ES ze dne 11. května 2005 o nekalých obchodních praktikách vůči spotřebitelům na vnitřním trhu a o změně směrnice Rady 84/450/EHS, směrnic Evropského parlamentu a Rady 97/7/ES, 98/27/ES a 2002/65/ES a nařízení Evropského parlamentu a Rady (ES) č. 2006/2004 (směrnice o nekalých obchodních praktikách)

Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES

Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES

SMLOUVA O EVROPSKÉ UNII (KONSOLIDOVANÉ ZNĚNÍ) [online]. Úřední věstník Evropské unie, 2012

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)

Konsolidované znění Smlouvy o fungování Evropské unie Dokument 12012E/TXT

Nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) č. 531/2012 o roamingu ve veřejných mobilních komunikačních sítích v Unii

Nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech

Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách)

Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích)

Seznam judikatury:

Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002), followed by 542 U.S. 656 (2004)

FCC v. Fox Television Stations, Inc., 556 U.S. 502 (2009)

National Cable & Telecommunications Association v. Brand X Internet Services, 545 U.S. 967 (2005)

Rozsudek Soudního dvora (osmého senátu) ze dne 2. září 2021. Telekom Deutschland GmbH v. Bundesrepublik Deutschland.

Rozsudek Soudního dvora (třetího senátu) ze dne 3. října 2019 Eva Glawischnig-Piesczek v. Facebook Ireland Limited C-18/18

Rozsudek Soudního dvora (velkého senátu) ze dne 13. května 2014.Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González. Věc C-131/12.

Rozsudek Soudního dvora ze dne 5. října 2000** Jednací jazyk: němčina., Spolková republika Německo v. Evropský parlament a Rada, C-376/98, Recueil 2000

Rozsudek Soudního dvora (první senát) z 19. dubna 2012. Wintersteiger AG proti Products 4U Sondermaschinenbau GmbH.C-523/10.

Rozsudek Soudního dvora (čtvrtého senátu) ze dne 22. ledna 2015. Pez Hejduk v. EnergieAgentur.NRW GmbH C-441/13

Stanovisko generálního advokáta – Cruz Villalón - 29 března 2011. eDate Advertising GmbH proti X (C-509/09) a Olivier Martinez a Robert Martinez proti MGN Limited (C-161/10).

Webové stránky a elektronické zdroje:

Nařízení o digitálních službách, 2023. Online. Dostupné z: https://www.mpo.cz/cz/podnikani/digitalni-ekonomika/digitalni-sluzby/narizeni-o-digitalnich-sluzbach/. [cit. 2024-02-27].

WANG, Hua, 2003. State control of the Internet in China. Diplomová práce. York University Toronto, Canada: Ryerson University, Communication and Culture.

Seznam zkratek

EU Evropská unie

GDPR 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).

SDEU Soudní dvůr evropské unie

DSA Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES

DMA Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828

NIS 1 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

NIS 2 Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

CDA Zákon o slušnosti v komunikacích (Communications Decency Act)

FCC Federální komise pro komunikaci (Federal Communications Commission)

COPPA Pravidlo o ochraně soukromí dětí na internetu (Children's Online Privacy Protection Rule)

CIPA Zákon o ochraně dětí na internetu (Children's Online Privacy Protection Rule)

CCPA Kalifornský zákon o ochraně soukromí spotřebitelů (California Consumer Privacy Act)

DMCA Zákon o autorských právech v digitálním tisíciletí (The Digital Millennium Copyright Act)

VLOP Very Large Online Platforms and Search Engines neboli velmi velké online platformy