



CONSUMERPRO

BOOSTING PROFESSIONALS
IN CONSUMER PROTECTION

Digitální práva

Teoretický podkladový dokument

2022- 2023

Digital Rights - Czech Republic
November 2022 - version 1



OBSAH

Obsah	2
Úvod k teoretickému podkladovému dokumentu.....	4
1. Ochrana údajů	5
1.1. Úvod a historie politiky ochrany údajů pro spotřebitele	5
1.2. Proč je ochrana údajů pro spotřebitele důležitá	5
1.3. Hlavní výzvy týkající se ochrany údajů spotřebitelské politiky	5
1.4. Klíčová práva a povinnosti spotřebitelů v kostce.....	6
1.5. Zákony a nařízení na úrovni EU a na národní úrovni	7
1.6. Judikatura.....	7
1.7. Co mohou spotřebitelé dělat, pokud mají problém?.....	7
1.8. Další zdroje - informační přehledy, publikace, odkazy	9
2. Platformy.....	10
2.1. Úvod a historie spotřebitelské politiky platformem	10
2.2. Proč jsou platformy pro spotřebitele důležité	11
2.3. Hlavní výzvy týkající se platformem	11
2.4. Klíčová práva a povinnosti spotřebitelů v kostce.....	14
2.5. Akt o digitálních službách.....	16
2.6. Judikatura.....	18
2.7. Co mohou spotřebitelé dělat, pokud mají problém?.....	18
2.8. Další zdroje - informační přehledy, publikace, odkazy	18
3. Internet věcí (IOT)	20
3.1. Úvod a historie	20
3.2. Proč je IOT pro spotřebitele důležitá	20
3.3. Hlavní výzvy v rámci IOT.....	20
3.4. Klíčová práva a povinnosti spotřebitelů v kostce.....	21
3.5. Zákony a předpisy na úrovni EU I.....	23
3.6. Judikatura.....	24
3.7. Co mohou spotřebitelé dělat, pokud mají problém?.....	24
3.8. Další zdroje – informační přehledy, publikace, odkazy.....	25

Tento materiál vznikl v rámci projektu [Consumer PRO](#), který je iniciativou Evropské komise v rámci Evropského spotřebitelského programu. Podpora ze strany Evropské komise neznamena schválení jeho obsahu, který odráží pouze názory autorů. Komise nese odpovědnost za jakékoli použití informací v něm obsažených.



ÚVOD K TEORETICKÉMU PODKLADOVÉMU DOKUMENTU



Vážený čtenáři,

Tento teoretický podkladový dokument je součástí školicích materiálů vytvořených pro iniciativu EU Consumer Pro, jejímž cílem je, aby spotřebitelské organizace a další aktéři spotřebitelské politiky byli lépe vybaveni za účelem ochrany spotřebitelů ve své zemi.

Cílem tohoto dokumentu je poskytnout vám a vašim týmům užitečné a relevantní informace o digitálních právech. Jeho obsah připravili odborníci BEUC na politiku v oblasti digitálních práv z pohledu evropské legislativy, aby vám pomohl:

- rychle vyškolit vaše týmy odborníků,
- jednoduše vyhledat relevantní informace,
- umožnit vašim zaměstnancům lépe informovat spotřebitele o jejich právech a
- zvýšit povědomí o digitálních právech a jejich vymáhání ministerstvy a úřady.

Tento teoretický podkladový dokument je součástí řady školicích materiálů, které jsou přizpůsobeny národním specifikům, pokud členské státy EU taková specifika uplatňují. Na vyžádání nebo [online](#) jsou k dispozici doplňující teoretické podkladové dokumenty k tématům digitálních práv a kolektivních nároků, a to v angličtině a v mnoha dalších evropských jazycích.

O společnosti Consumer PRO

Consumer PRO je iniciativa Evropské komise v rámci Evropského spotřebitelského programu, kterou realizuje BEUC – Evropská organizace spotřebitelů. Jejím cílem je posilovat postavení evropských spotřebitelských organizací a dalších aktérů spotřebitelské politiky prostřednictvím neformálního vzdělávání. Projekt zahrnuje členské státy EU, Island a Norsko.

Další informace získáte na adrese: Info@consumer-pro.eu.



1. OCHRANA ÚDAJŮ

1.1. Úvod a historie politiky ochrany údajů pro spotřebitele

Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je v Evropské unii základním právem. Podle čl. 8 odst. 1 [Listiny základních práv Evropské unie](#) a čl. 16 odst. 1 [Smlouvy o fungování Evropské unie \(SFEU\)](#) má každý právo na ochranu osobních údajů, které se ho týkají. Kromě toho článek 7 Listiny základních práv stanoví, že každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.

Obecné nařízení o ochraně osobních údajů (GDPR) je předpisem, který upravuje zpracování osobních údajů v EU. Vyžaduje, aby organizace, a to jak veřejné orgány, tak společnosti, používaly osobní údaje spotřebitelů transparentním a spravedlivým způsobem. Posiluje vaše práva a vztahuje se na všechny organizace, které zpracovávají osobní údaje osob, jež se nacházejí v EU, bez ohledu na to, kde tyto organizace sídlí.

Pravidla ohledně soukromí a elektronických komunikací (v současnosti [směrnice o soukromí a elektronických komunikacích](#), která je předmětem přezkumu) chrání důvěrnost elektronických komunikací a obsahují také zvláštní ochranu spotřebitelů před nevyžádanými obchodními sděleními zasílanými prostřednictvím služeb elektronických komunikací.

1.2. Proč je ochrana údajů pro spotřebitele důležitá

Ačkoli jsou digitální informační technologie a vznik **nových online služeb pro spotřebitele** přínosné, představují **také velkou výzvu pro základní práva vztahující se k soukromí a ochraně osobních údajů**. Obchodní modely, které v současnosti dominují digitálnímu světu, jsou založeny na sledování a analýze každého kroku spotřebitelů. Společnosti využívají shromážděné informace k vytváření uživatelských profilů, s nimiž se obchoduje online a které se používají k poskytování behaviorálně cílené reklamy. Tyto profily mohou být rovněž využívány k diskriminaci spotřebitelů a ovlivňování jejich chování. Je tedy důležité zajistit, aby spotřebitelé měli i nadále kontrolu nad svými osobními údaji a mohli využívat inovativní digitální produkty a služby, aniž by se museli vzdát svého soukromí.



1.3. Hlavní výzvy týkající se ochrany údajů spotřebitelské politiky

Pro spotřebitele je velmi obtížné kontrolovat, co se s jejich údaji v praxi děje. Jejich práva nejsou často respektována a nezřídka jsou nuceni vzdát se svého soukromí, pokud chtějí využívat digitální produkty a služby.

Spotřebitelé jsou pod neustálým drobnohledem komerčních subjektů a z jejich osobních údajů těží nesčetné množství společností, z nichž o mnohých tyto spotřebitelé ani neslyšeli.

Zásady ochrany osobních údajů jsou vágní, dlouhé, složité a velmi těžko srozumitelné a spotřebitelům, pokud chtějí užívat danou službu, nezbývá než s nimi souhlasit. Spotřebitelé často získávají iluzi kontroly a z udílení souhlasu se systematicky stává bezmyšlenkovitě "zaškrtování políček".

GDPR mělo mnoho z těchto problémů řešit. Téměř čtyři roky poté, co vstoupilo v platnost, však nedošlo k žádným významným změnám v obchodních postupech. Úroveň dodržování předpisů je v některých oblastech nízká a jejich prosazování prozatím není zcela účinné. Orgány pro ochranu údajů mají potíže vypořádat se se všemi stížnostmi, které jsou jim adresovány, a nová struktura orgánů založená za účelem lepší vymahatelnosti práva na mechanismu spolupráce a konzistentním výkladu a uplatňování práva v rámci celé EU, čelí významným výzvám.

Dalším problémem je, že reforma pravidel ohledně soukromí a elektronických komunikací (ePrivacy), která má doplnit GDPR a dále chránit důvěrnost komunikace, se projednává již více než pět let a finální dohoda je stále v nedohlednu. (Více informací o nařízení o soukromí a elektronických komunikacích naleznete v [informačním dokumentu BEUC \(dostupný v AJ\)](#)).

1.4. Klíčová práva a povinnosti spotřebitelů v kostce

GDPR vyžaduje, aby organizace, a to jak veřejné orgány, tak společnosti, používaly osobní údaje spotřebitelů transparentním a spravedlivým způsobem. Obsahuje řadu [zásad, kterými se řídí](#) používání osobních údajů:

Spotřebitelům také poskytuje [řadu práv](#), které jim zajišťují, aby měli kontrolu nad svými údaji. Spotřebitelé mají mimo jiné právo:

- být jasně a srozumitelně informováni o tom, jak jsou jejich osobní údaje využívány, přičemž musí být uvedeno, které údaje jsou používány, kým a pro jaké účely.
- získat přístup k údajům, které o nich organizace uchovávají, a získat jejich kopii.
- opravit své údaje, pokud jsou nepřesné.
- přimět organizace, aby vymazaly jejich údaje.
- požádat organizace, aby dočasně nebo trvale přestaly používat jejich údaje.
- obdržet své údaje v běžně používaném formátu, aby je mohli převzít a použít jinde.
- napadnout automatizovaná rozhodnutí založená na jejich osobních údajích, která se jich významným způsobem dotýkají (např. zamítnutí žádosti o půjčku).
- být informováni, pokud dojde ke ztrátě nebo krádeži jejich údajů.
- podat stížnost k vnitrostátnímu úřadu pro ochranu osobních údajů nebo podat žalobu k soudu.

1.5. Zákony a nařízení na úrovni EU a na národní úrovni

- [Listina základních práv EU](#)
- [Nařízení \(EU\) 2016/679 \(konsolidované znění\)](#) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR).
- [Směrnice 2002/58/ES \(konsolidované znění\)](#) o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)
- [Pokyny, doporučení a osvědčené postupy Evropského sboru pro ochranu osobních údajů \(v ČR na stránkách ÚOOÚ\)](#)
- [Kodexy chování – metodická příručka ÚOOÚ](#)
- [Stanoviska evropského inspektora ochrany údajů \(k dispozici v AJ, NJ a FJ\)](#)
- [Příklad kodexu chování: Federace přímého marketingu \(pouze v AJ\)](#)

Na národní úrovni

Ústředním správním úřadem pro oblast ochrany osobních údajů je v ČR Úřad pro ochranu osobních údajů (ÚOOÚ).

Právní předpisy v oblasti ochrany osobních údajů platné v ČR naleznete [zde](#).

Poradnu ÚOOÚ naleznete [zde](#).

Názory a rozhodnutí ÚOOÚ, naleznete [zde](#).

1.6. Judikatura

Sbírku rozhodnutí Úřadu pro ochranu osobních údajů a Soudního dvora a články o GDPR najdete na adrese: <http://www.gdprhub.eu> (pouze v AJ).

Na oficiálním právním portálu EU: Soubor [Eurlex](#) o GDPR. Jedná se o seznam případů a předběžných otázek Evropského soudního dvora, které se týkají GDPR: seznam judikatury najdete v části "*informace o dokumentech*".

1.7. Co mohou spotřebitelé dělat, pokud mají problém?

Pokud se spotřebitel domnívá, že byla porušena jeho práva podle GDPR, má dvě možnosti:

- Podání stížnosti u vnitrostátního úřadu pro ochranu osobních údajů. Tím je v České republice [Úřad pro ochranu osobních údajů](#).
- podat žalobu proti společnosti/organizaci přímo u soudu. To však nebrání spotřebiteli, aby podal stížnost rovněž u vnitrostátních orgánů pro ochranu údajů (ÚOOÚ), pokud si to přeje.

Pokud se spotřebitel domnívá, že ÚOOÚ nevyřídil jeho stížnost správně nebo pokud není spokojen s jeho odpovědí či pokud ho neinformuje o průběhu nebo výsledku do tří měsíců

ode dne podání stížnosti, může spotřebitel soudu podat žalobu přímo proti Úřadu pro ochranu osobních údajů.

Orgány veřejné správy

Na národní úrovni:

Ministerstvem odpovědným za agendu ochrany osobních údajů, které rovněž stanovuje vnitrostátní politiku v této oblasti a zajišťuje provádění GDPR na vnitrostátní úrovni je ministerstvo vnitra.

Kromě vnitrostátních úřadů pro ochranu osobních údajů stojí za pozornost i další veřejnoprávní orgány:

Na evropské úrovni:

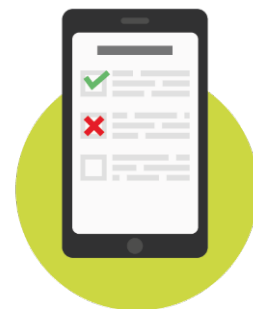
- Evropská komise, která má na starosti zajištění správného provádění GDPR členskými státy a má také pravomoc "aktivovat" některá ustanovení GDPR prostřednictvím aktů v přenesené pravomoci (např. pro vytvoření standardizovaných "ikon ochrany osobních údajů" – článek 12 odst. 8 GDPR).
- [Evropský sbor pro ochranu osobních údajů \(EDPB\)](#), který sdružuje všechny vnitrostátní orgány pro ochranu osobních údajů. Jeho hlavním úkolem je zajistit jednotnost při uplatňování a výkladu GDPR.
- [Evropský inspektor ochrany údajů – EDPS \(stránky dostupné pouze v AJ,NJ, FJ\)](#), který dohlíží na to, aby instituce EU dodržovaly osobní údaje osob, a radí institucím v otázkách ochrany údajů.

Alternativní řešení sporů (ADR)

Mimosoudní řízení a jiné postupy řešení sporů mezi správci a subjekty údajů v souvislosti se zpracováním osobních údajů mohou být zavedeny prostřednictvím kodexů chování přijatých odvětvovými orgány (článek 40 GDPR), aniž je dotčeno právo subjektů údajů podávat stížnosti u svého úřadu pro ochranu osobních údajů a domáhat se soudní ochrany u soudu.

1.8. Další zdroje – informační přehledy, publikace, odkazy

- [Webové stránky Evropské komise s informacemi o GDPR](#)
- [Knihovna Evropské komise o GDPR - infografiky, informační přehledy a další materiály určené občanům a podnikům](#)
- [Informační list BEUC - Co pro vás znamená právo EU v oblasti ochrany údajů? \(dostupné v AJ\)](#)
- [Zpráva BEUC - Dlouhá a klikatá cesta: Příklad přeshraničního vymáhání ochrany údajů z pohledu spotřebitele \(dostupné v AJ\)](#)
- [AccessNow - Uživatelská příručka k ochraně údajů v EU: Vaše práva a jejich uplatňování \(dostupné AJ\)](#)
- [Agentura pro základní práva - Evropská příručka ochrany údajů](#)
- [Základní příručka k ochraně osobních údajů zveřejněná ÚOOÚ](#)
- [Informační listy](#) zveřejněné evropským inspektorem ochrany údajů (EDPS) – dostupné pouze v AJ, NJ a FJ
- [Historie GDPR](#) a [slovníček pojmů](#) (EIOÚ) – dostupné v AJ, obdobně k historii GDPR [článek na webu euroskop.cz](#) a [slovníček nejdůležitějších pojmů](#) na webu ÚOOÚ



2. PLATFORMY

2.1. Úvod a historie spotřebitelské politiky platformem

Spotřebitelé nakupují stále více služeb a produktů online, zejména prostřednictvím tzv. platformem.

V prvních letech elektronického obchodování se takové nákupy uskutečňovaly především na internetových stránkách společností, které měly i kamenné obchody na hlavních ulicích. Dnes se nákupní chování spotřebitelů radikálně mění: stále více lidí si objednáva služby a výrobky prostřednictvím internetových tržišť, přičemž tyto výrobky a služby jsou evropským spotřebitelům zasílány přímo ze zemí mimo EU.

Nákupy se uskutečňují nejen prostřednictvím platformem elektronického obchodu, jako je Amazon Marketplace, AliExpress, wish.com nebo eBay, ale také prostřednictvím platformem sociálních sítí, jako je Instagram.

Například v roce 2017 bylo z Číny do Německa odesláno přibližně 100 milionů objednávek. To je o 40 milionů více než v roce 2016. Obrovský nárůst byl zaznamenán i v dalších evropských zemích.

Kromě toho se množí podvody, kdy prodejci, kteří se vydávají za evropské společnosti, ale ve skutečnosti objednávají zboží prostřednictvím platformem z Číny, zakládají v EU internetové obchody a prodávají toto zboží spotřebitelům za vyšší cenu, než za jakou je nabízeno například na wish.com. To bylo mj. zaznamenáno v Dánsku a ve Francii¹.

Existují také velmi vážné obavy, že mnohé z těchto výrobků nespĺňují evropské právní předpisy a technické normy, které byly přijaty za účelem ochrany práv spotřebitelů, bezpečnosti, zdraví a životního prostředí². Zatímco výrobci a distributoři se sídlem v EU jsou odpovědni za bezpečnost výrobků a jejich soulad s právními předpisy, v případě výrobců, kteří nesídlí v EU, tomu tak často není, protože zprostředkovatelé, tj. platformy elektronického obchodu, odpovědnost za soulad s předpisy odmítají.

V současné době se projednávají důležité legislativní návrhy, které mají některé z těchto problémů řešit, zejména [akt o digitálních službách](#), který již dokonce 16. listopadu 2022 vstoupil v platnost a [návrh obecného nařízení o bezpečnosti výrobků](#).



¹ k tématu článek na [webu Le Parisien](#) (dostupné ve FJ), obdobně o tématu na [webu dTest](#)

² <https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html> (dostupné v AJ)

2.2. Proč jsou platformy pro spotřebitele důležité

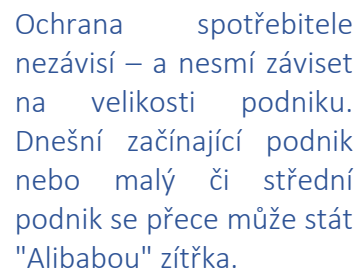
Nakupování, komunikace s přáteli a rodinou, sdílení zážitků, sledování filmů, poslech hudby, čtení knih, rezervace výletů, vaření podle nového receptu, plánování programu na večer, pohyb po městě, žádost o pomoc sousedů a hledání informací na webu – to jsou jen některé základní příklady činností, které denně provádějí miliony spotřebitelů. Pro každou z těchto činností existuje jedna nebo více online platform, které k těmto činnostem nabízejí odpovídající službu. Spotřebitelé využívají prudkého rozvoje platform, který představuje řadu výhod, ale rovněž výzev z hlediska ochrany spotřebitelů.

2.3. Hlavní výzvy týkající se platform

V době přijetí [směrnice o elektronickém obchodu](#) (v roce 2000) byly platformy jako Google, Amazon nebo Booking.com ještě v plenkách. Mnoho dalších dnes známých zprostředkovatelů ještě vůbec neexistovalo. Například Facebook a Shopify byly spuštěny v roce 2004. Etsy byl založen v roce 2005, Airbnb v roce 2008 a platformy Instagram, Wish a AliExpress spatřily světlo světa v roce 2010.

Během posledních 20 let se obchodní modely některých z těchto a dalších společností změnilo. Změnila se také dynamika tržní síly v tomto odvětví.

Na evropském digitálním trhu došlo k tzv. "[datafikaci](#)" (převod informací na data, která jsou základem digitálních obchodních modelů), k nárůstu počtu platform, k růstu kolaborativní ekonomiky³ a k diverzifikaci poskytovatelů služeb z hlediska funkcí, vertikální integrace a velikosti. Přesto musí každá společnost hrát podle pravidel. Ochrana spotřebitele nezávisí – a nesmí záviset – na velikosti společnosti. Koneckonců, dnešní start-up nebo malý či střední podnik se může stát Alibabou zítřka.



Ochrana spotřebitele nezávisí – a nesmí záviset na velikosti podniku. Dnešní začínající podnik nebo malý či střední podnik se přece může stát "Alibabou" zítřka.

Mnoho platform se od základu přetransformovalo. Některé se již neomezují na svou původní roli informačních nebo důvěryhodných zprostředkovatelů (např. srovnávací nebo hodnotící platformy jako Yelp), ale nově je prostřednictvím nich možné uzavírat různé transakce. Jedná se o obchodní modely, díky nimž platforma spadá do kategorie "*online tržiště*"⁴, na něž organizace zabývající se ochranou spotřebitelů v současnosti zaměřují svou pozornost. Tento typ platformy je definován modernizační směrnicí (směrnice Omnibus)⁵ jako "*služba využívající software, včetně internetových stránek, části internetových stránek nebo aplikace, provozovaná obchodníkem nebo jeho jménem, která umožňuje spotřebitelům uzavírat*

³ [Dokument BEUC ke kolaborativní ekonomice, dostupný zde \(pouze v AJ\)](#)

⁴ Studie k tématu zpracovaná Německým spolkovým spotřebitelským centrem (VZBV) na str. 17, dostupná [zde](#) (pouze v NJ)

⁵ Čl. 2 odst. 1 písm. n) [směrnice o nekalých obchodních praktikách](#), ve znění směrnice (EU) 2019/2161

smlouvy na dálku s jinými obchodníky nebo spotřebiteli". Vzhledem k tomu se úloha platformy často neomezuje pouze na samotné umožnění uzavření smlouvy mezi prodávajícími a kupujícími, ale zahrnuje i další služby, jako jsou platební služby, služby související s dodáním (např. distribuční centra), vyřizování vrácení zboží a vyřizování reklamací⁶.



Jiné platformy se rozrostly o další funkce. Existují např. "hybridní platformy", které mohou kombinovat různé zprostředkovatelské funkce nebo vertikálně integrované platformy. Ty druhé jmenované nefungují pouze jako zprostředkovatelé, ale také konkurují obchodníkům, a to buď přímo, nebo prostřednictvím přidružených společností. Například Amazon je prodejcem, online tržištěm, společností poskytující cloudové služby, platformou pro sdílení videí, vydavatelem, reklamní společností, výrobcem propojených zařízení a společností zabývajících se umělou inteligencí.

Spotřebitelské organizace se zasazují o úpravy legislativního rámce, které by reagovaly na tuto novou tržní realitu. Akt o digitálních službách (Digital Service Act – nařízení DSA) je z tohoto hlediska velmi důležitou iniciativou. Komise předložila návrh DSA v prosinci 2020, v platnost vstoupil 16. listopadu 2022 a členské země EU musí zmocnit národní koordinátory digitálních služeb do 17. února 2024, což je datum, odkdy bude akt o digitálních službách plně použitelný pro všechny subjekty v oblasti jeho působnosti, více o [zde](#).

Specifické výzvy

Výzva č. 1. Šíření široké škály nelegálního obsahu.

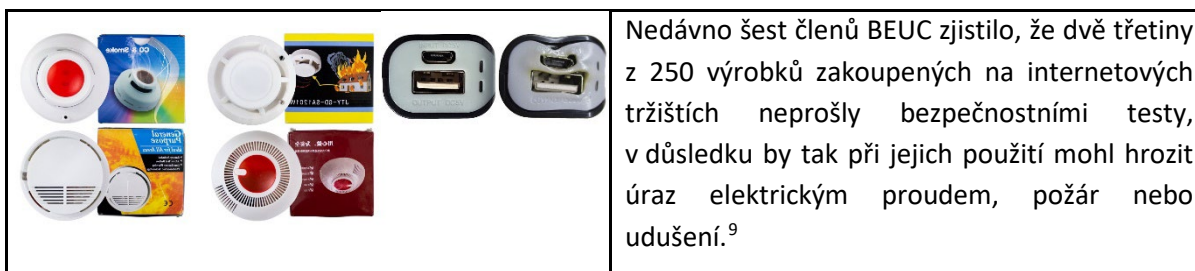
Digitální služby se do jisté míry staly prostředkem pro rozsáhlé porušování spotřebitelského práva; zdrojem příjmů pro prodej reklamy nebo propagaci nebezpečných, závadných a nezákonných výrobků na internetu, například⁷:

	Britský člen BEUC, společnost Which?, zjistil, že na internetu se prodávají vánoční světýlka, která mohou vzplanout nebo způsobit úraz elektrickým proudem ⁸ .
	Dánská spotřebitelská rada odhalila, že kosmetika na wish.com není v souladu s právními předpisy EU.

⁶ K tématu studie Německého spolkového spotřebitelského centra (VZBV) na str. 18, dostupná [zde](#) (pouze v NJ)

⁷ Viz příklady publikované BEUC, [zde](#) (dostupné pouze v AJ)

⁸ Článek k závadným vánočním světýlkům zpracovaný britskou organizací Which? (člen BEUC), dostupný [zde](#) (pouze v AJ)



Výzva č. 2. Nedostatečné odlišení činnosti online tržiště od ostatních funkcionalit platformy.

Debata o reformě [směrnice o elektronickém obchodu](#) se do jisté míry zaměřuje na otázky, jako jsou nenávistné projevy, obsah související s teroristickými hrozbami, obsah chráněný autorskými právy, svoboda projevu nebo úvahy o jednotném trhu. I když se jedná o důležité otázky, EU by neměla ztrácet ze zřetele ani konkrétní problémy ochrany spotřebitele. Je proto třeba zajistit, aby spotřebitelé, kteří nakupují výrobky nebo služby prostřednictvím internetových tržišť¹⁰, byli dostatečně chráněni.

Je nutné rozlišovat mezi prodejem nelegálních výrobků a činnostmi jako je např. zveřejňování komentářů na sociálních sítích. Zatímco v druhém případě je předmětem zájmu svoboda projevu, v prvním případě jde především o bezpečnost výrobků a ochranu spotřebitele.

Výzva č. 3. [Směrnice o elektronickém obchodu](#) se "nevztahuje na poskytovatele služeb usazené ve třetí zemi"¹¹.

Někteří poskytovatelé usazení ve třetích zemích využívají omezení teritoriality podle směrnice a vytvářejí tak nespravedlivé a nerovné podmínky na trhu.

Výzva č. 4. Způsob, jakým [směrnice o elektronickém obchodu](#) reguluje poskytovatele hostingů, využívají některé platformy, včetně (ale nejen) online tržišť, k tomu, aby se vyvarovaly jakékoli odpovědnosti, nebo tak, že z obav z odpovědnosti nepodnikají v dané oblasti žádné smysluplné kroky.

Výzva č. 5. Současná legislativa má mezery v regulaci online tržišť. Malá pozornost je věnována ziskům online tržišť z nelegálního obsahu.

Výzva č. 6. Nová pravidla mohou členským státům bránit ve správném řešení cílů veřejného zájmu.

Například ve věci C-390/18¹² Soudní dvůr EU rozhodl, že Airbnb je třeba považovat za službu informační společnosti (ve smyslu čl. 2 písm. a) [směrnice o elektronickém obchodu](#)).

⁹ Více v tiskové zprávě BEUC ze dne 24. února 2020, dostupné [zde](#) (pouze v AJ).

¹⁰ [Směrnici o nekalých obchodních praktikách ve znění modernizační směrnice](#) (článek 2, písm. n)) je online tržiště definováno jako "služba využívající software, včetně internetových stránek, části internetových stránek nebo aplikace, provozovaná obchodníkem nebo jeho jménem, která umožňuje spotřebitelům uzavírat smlouvy na dálku s jinými obchodníky nebo spotřebiteli".

¹¹ 58. bod odůvodnění směrnice o elektronickém obchodu.

¹² [Rozsudek soudního dvora ze dne 19. prosince 2019, dostupný zde.](#)

Vzhledem k tomu, že Francie neoznámila Komisi zákon, který vyžaduje profesní licenci realitního makléře pro společnosti jako je Airbnb, nemůže proto tuto povinnost Airbnb uložit, protože by tím porušila čl. 3 odst. 4 písm. b) [směrnice o elektronickém obchodu](#). Tento případ ukázal, že směrnice o elektronickém obchodu tím, že na první místo klade hledisko vnitřního trhu, způsobuje členským státům problémy při přijímání právních předpisů a opatření na ochranu spotřebitelů. Je však důležité poznamenat, že toto rozhodnutí neznamená, že by vlády nemohly taková opatření vůči společnostem jako je Airbnb uplatnit. Evropský soudní dvůr (SDEU) jasně uvedl, že oznamovací povinnost ve směrnici o elektronickém obchodu *"nemá zabránit členskému státu v přijímání opatření, která spadají do jeho vlastní oblasti působnosti a která by mohla ovlivnit volný pohyb služeb, ale má zabránit členskému státu, aby zásadně zasahoval do pravomoci členského státu, v němž je usazen poskytovatel dotčené služby informační společnosti"*.

Výzva č. 7. Nedostatečný dohled a vymáhání právních norem.

Digitální trh se překotně vyvíjí a zdá se, že příslušné orgány na toto tempo nejsou schopny adekvátním způsobem reagovat, nemají dostatečné odborné zázemí ani zdroje potřebné k monitorování a řešení problémů, k nimž na trhu dochází.

2.4. Klíčová práva a povinnosti spotřebitelů v kostce

[Směrnice o elektronickém obchodu](#) je již dlouhou dobu jedním ze základních kamenů regulace internetu. Směrnice o elektronickém obchodu mimo jiné zavedla zásadu země původu s některými důležitými výjimkami (např. u spotřebitelských smluv), dále klíčové informační povinnosti vůči příjemcům služeb (např. spotřebitelům) či výjimky a omezení odpovědnosti pro poskytovatele online zprostředkovatelských služeb. Obsah směrnice:

- **Článek 1 – 3: Obecná ustanovení**
- **Článek 4 – 15: Zásady**

Oddíl 1: Požadavky na usazování a informování

Oddíl 2: Obchodní sdělení

Oddíl 3: Uzavírání smluv elektronickou cestou

Oddíl 4: Odpovědnost poskytovatelů zprostředkovatelských služeb

- **Články 16 – 20: Provádění**
- **Články 21 – 24: Závěrečná ustanovení**

[Kde najdete nejdůležitější ustanovení směrnice o elektronickém obchodu?](#)

- **Hlavní cíl:** fungování vnitřního trhu, tím, že zajistí volný pohyb služeb informační společnosti mezi členskými státy (článek 1).



- Mezi **další cíle** patří "*právní jistota a důvěra spotřebitelů*" (7. bod odůvodnění), zajištění vysoké úrovně ochrany spotřebitele a ochrany nezletilých osob (10. bod odůvodnění).
- **Oblast působnosti:** doplňuje právo Společenství platné pro služby informační společnosti, aniž je dotčena úroveň ochrany spotřebitelů (článek 1)
- **Definice** (článek 2)
- **Základní informace pro spotřebitele a další příjemce** (články 5, 6, 10)
- **Práva při zadávání objednávek online** (článek 11)
- **Zásady odpovědnosti zprostředkovatele** (články 12-15). Nejdůležitějšími zásadami jsou:
 - Poskytovatelé hostingových služeb nenesou odpovědnost za obsah třetích stran, pokud po zjištění této skutečnosti urychleně odstraní nebo znemožní přístup k nezákonnému obsahu (článek 14).
 - Členské státy mají zakázáno ukládat poskytovatelům obecnou povinnost monitorování (článek 15).
- **Kodexy chování** (článek 16)
- **Alternativní řešení sporů** (článek 17)
- **Soudní prostředky** – členské státy mají povinnost zajistit rychlé přijetí opatření včetně předběžných opatření "*s cílem ukončit zjištěné porušování práva a předejít dalšímu poškození dotčených zájmů.*" (článek 18).
- **Spolupráce členských států** (článek 19)
- **Sankce** (článek 20)

Od přijetí směrnice o elektronickém obchodu v roce 2000 se digitální služby dále vyvíjejí a přinášejí stále nové výzvy. Například zásada "bezpečného přístavu" dává některým platformám možnost vyvarovat se za určitých okolností odpovědnosti. Někteří poskytovatelé digitálních služeb nepřebírají odpovídající odpovědnost a neposkytují spotřebitelům adekvátní odškodnění v případě poruchy/vadného plnění. Stejně tak některé dobrovolné iniciativy oddálily tolik potřebná regulační opatření. Některé z těchto problémů jsou však řešeny v rámci aktu o digitálních službách.

Sdružení Consumer PRO vypracovalo také dva další dokumenty na téma Obecné spotřebitelské právo a Kolektivní nároky, které mohou tuto kapitolu vhodně doplnit.

2.5. Akt o digitálních službách

Akt o digitálních službách (dále také jako „nařízení DSA“) upravuje povinnosti vztahující se k digitálním službám, které zajišťují propojení spotřebitelů se zbožím, službami a obsahem.

Cílem aktu o digitálních službách je lépe chránit spotřebitele a základní práva v online prostředí, zavést účinný rámec transparentnosti a odpovědnosti pro online platformy, a tím podpořit spravedlivější a otevřenější digitální trhy.

Na rozdíl od směrnice o elektronickém obchodu je akt o digitálních službách nařízením, takže harmonizuje pravidla v celé EU a bude přímo použitelný. Nová pravidla by tedy měla zajistit stejnou úroveň ochrany všech občanů v EU.

Akt o digitálních službách mimo jiné obsahuje:

- Opatření proti nelegálnímu obsahu (včetně zboží a služeb) zveřejněnému online jako je mechanismus, který uživatelům umožní takový obsah oznámit a spolupráce platform s "důvěryhodnými oznamovateli" - mj. čl. 16 a čl. 22 nařízení DSA;
- nová pravidla o sledovatelnosti podnikatelských uživatelů na internetových tržištích (známá také jako "povinnost znát svého zákazníka"), jejichž cílem je lépe identifikovat prodejce nelegálního zboží – článek 30 nařízení DSA;
- záruky pro uživatele, včetně možnosti napadnout rozhodnutí platform o moderování obsahu – odstavec 26 odůvodnění a článek 14 a 15 nařízení DSA;
- Další opatření pro transparentnost online platform, včetně algoritmů používaných pro doporučení a cílenou reklamu – článek 27 nařízení DSA;
- Povinnost velmi velkých online platform předcházet zneužívání svých systémů, zejména řešením systémových rizik a zahrnutím dohledu prostřednictvím nezávislých auditů zaměřených na přijatá opatření – kapitola 3, oddíl 5 nařízení DSA, posouzení rizik – článek 34, povinnost podrobit se auditu – článek 37;
- Nová struktura dohledu, která odráží složitost online prostoru, v níž hlavní roli hrají členské státy, zejména prostřednictvím národních koordinátorů digitálních služeb, kteří budou podpořeni ze strany nově vzniklého orgánu – Evropského sboru pro digitální služby (platforma pro společné jednání zástupců členských států a komise v dané oblasti). V případě velmi velkých online platform má Komise posílenou úlohu v oblasti dohledu a prosazování - Kapitola 4 nařízení DSA.

Ačkoli akt o digitálních službách přinese velmi potřebná zlepšení, pokud jde o ochranu spotřebitelů v oblasti digitálních služeb, jedním z bodů, kde nedochází k zásadním změnám,



je režim odpovědnosti pro online tržiště. Akt o digitálních službách zachovává zásady vynětí z odpovědnosti zprostředkovatele původně stanovené směrnicí o elektronickém obchodu, i když s některými vyjasněními a drobnými zlepšeními. Zákony a nařízení na úrovni EU (shrnutí):

NAŘÍZENÍ / SMĚRNICE	DATUM PODÁNÍ ŽÁDOSTI	PŘEZKOUMÁNÍ / HODNOCENÍ: TYP OPATŘENÍ	DATUM SPLNĚNÍ	KOMENTÁŘ
Směrnice o elektronickém obchodu	17/01/2002 (transpozice)	Zpráva EK o přezkoumání (článek 21)	Před 17. 7. 2003 a poté každé dva roky	Od roku 2012 nám není známo žádné formální hodnocení. Z hlediska hospodářské soutěže může být zajímavá Závěrečná zpráva o šetření v odvětví elektronického obchodování z roku 2017
		Akt o digitálních službách (DSA)	Návrh zveřejněn v prosinci 2020. Nařízení vstoupilo v platnost 16. listopadu 2022.	Návrh DSA předložený v prosinci 2020 spolu s aktem o digitálních trzích (DMA), který obsahuje konkrétní pravidla zaměřená na platformy typu gatekeeper – strážci na vnitřním trhu. Klíčová témata DSA z pohledu spotřebitele: odpovědnost zprostředkovatelů, zejména online tržišť; povinnosti "znát svého zákazníka" - KYC, postupy pro oznámení a přijímání opatření, požadavky na transparentnost, vymáhání a koordinace mezi členskými státy, povinnosti v souvislosti s cílenou reklamou a používáním doporučujících systémů.
Nařízení 2019/1150 - P2B (Platform to business) (Nařízení o podpoře spravedlnosti a transparentnosti pro podnikatelské uživatele online zprostředkovatelských služeb)	12/07/2020	Pokyny EK k požadavkům na transparentnost pořadí relativní důležitosti (článek 5)	Zveřejněno 7. prosince 2020	
		EK podporuje kodexy chování (článek 17).	Bez data	Součástí přezkumu bude analýza jejich fungování.
		Přezkumná zpráva EK (článek 18)	13/01/2022 a každé tři roky	
Modernizační směrnice (směrnice Omnibus)	28. listopadu 2021 (transpozice)	Článek 7 - Transpozice	Článek 6 - Podávání zpráv Komisí a přezkum. Zpráva, kterou má EK zveřejnit	

	28. května 2022 (aplikace)		do 28. května 2024, opatření týkající se prodeje potravin a podomního prodeje.	
--	----------------------------	--	--	--

2.6. Judikatura

- **Re: Modernizační směrnice (Omnibus):** zatím neexistuje relevantní judikatura, jelikož je aplikovatelná od 28. května 2022. Podívejte se na teoretický podkladový dokument BEUC k obecnému spotřebitelskému právu, kde najdete informace o judikatuře k dalším nástrojům spotřebitelského práva.
- **Re: Směrnice o elektronickém obchodu:** viz seznam [zde \(v sekci "Ovlivněno rozsudkem"\)](#).

2.7. Co mohou spotřebitelé dělat, pokud mají problém?

- Obráťte se přímo na prodejce/platformu (tento krok není povinný).
- Možnost alternativního řešení sporů – ADR (tento krok není povinný).
- Příslušné orgány členských států: liší se v závislosti na zemi a tématu.

Na národní úrovni

Subjekty ADR v České republice (příslušné podle toho, jaké spotřebitelské oblasti se spor týká):

Česká obchodní inspekce (ČOI), Štěpánská 15, 120 00 Praha 2, Česká republika

Tel.: +420 296 366 155, e-mail: esc@coi.cz, web: <https://www.coi.cz>

Dále Český telekomunikační úřad, Energetický regulační úřad, Finanční arbitr a rovněž subjekty, které o to požádaly, splnily zákonné povinnosti a jsou pověřeny Ministerstvem průmyslu a obchodu (Česká advokátní komora, Sdružení českých spotřebitelů, z.ú. a Kancelář ombudsmana České asociace pojišťoven, z.ú.)

2.8. Další zdroje – informační přehledy, publikace, odkazy

- Rejstřík expertních skupin Komise a dalších podobných subjektů (viz [zde](#)).
- Stanovisko BEUC Zajištění ochrany spotřebitele v ekonomice platform: ([zde - pouze v AJ](#))
- Poziční dokument BEUC Collaborative economy ([zde - pouze v AJ](#))
- BEUC: Přijmout akt o digitálních službách tak, aby fungoval ve prospěch spotřebitele ([zde - pouze v AJ](#))
- Stanovisko BEUC k návrhu aktu o digitálních službách ([zde - pouze v AJ](#))
- Tisková zpráva: nařízení DSA vstupuje v platnost, dostupný [zde](#)
- Briefing Evropského parlamentu k návrhu aktu o digitálních službách ([zde - pouze v AJ](#))

- Informační přehled v otázkách a odpovědích – Akt o digitálních službách: zajištění bezpečného online prostředí odpovědného vůči uživatelům, dostupný [zde](#).



3. INTERNET VĚCÍ (IOT)

3.1. Úvod a historie

Během posledních několika let se propojená zařízení stala všudypřítomnými v životě mnoha spotřebitelů. Zatímco dříve jsme běžně seděli u počítače, abychom se připojili k internetu, nyní nosíme chytré telefony připojené k internetu všude s sebou. Současně je stále více každodenních zařízení kolem nás vybaveno senzory a připojeno k internetu. Vzestup propojených zařízení, od chytrých kávovarů a bezpečnostních kamer až po automobily a lékařské přístroje, je obecně znám jako "internet věcí" neboli IoT.

3.2. Proč je IOT pro spotřebitele důležitá

V posledních letech se propojená zařízení stala všudypřítomnými v životě mnoha spotřebitelů a vzestup propojených zařízení mění způsob našeho života. Přestože digitalizace zařízení přináší spotřebitelům mnoho výhod, rizika a výzvy, které s sebou nese, jsou stejně důležité, ne-li ještě důležitější. Co se například stane, když se poskytovatel služeb vašeho systému inteligentní domácnosti rozhodne vypnout své servery? A kdo je zodpovědný za to, když je váš chytrý televizor ohrožen nebo se stane nepoužitelným kvůli nedostatku aktualizací softwaru? A co dopad na naše soukromí?



Mimo jiné z těchto důvodů je důležité v rámci EU vypracovat srozumitelná opatření se zřetelem na budoucí vývoj a právní rámec, které zajistí zachování práv spotřebitelů v této propojené společnosti.

3.3. Hlavní výzvy v rámci IOT

Připojení velkého množství zařízení k internetu přináší spotřebitelům příležitosti i rizika. Propojený svět slibuje větší pohodlí, bezproblémové zážitky a potenciálně významné zlepšení kvality života. Souhrnné informace z těchto zařízení by také mohly vést k novým poznatkům v oblastech, jako je lékařství, umělá inteligence či urbanismus.

Například chytrá domácnost plná propojených zařízení a senzorů se může naučit návyky a preference svého majitele a podle toho přizpůsobit své funkce. Současně spolu mohou jednotlivá zařízení komunikovat, takže například nízký srdeční rytmus zjištěný chytrými hodinkami vygeneruje zprávu a urgentně ji zašle do nejbližší nemocnice. Kromě toho funkce umožňující vzdálené sledování zařízení prostřednictvím internetu mohou pomoci zachovat určitou nezávislost osobám, jež se jinak neobejdou bez pomoci či asistence druhých osob, například odemknutím dveří na dálku, aniž by tyto osoby musely ke dveřím dojít. V odvětvích, jako je průmysl či zdravotnictví, bude mít internet věcí potenciálně transformační účinky z pohledu efektivity a shromažďování informací.

Výzvy, které s sebou propojená zařízení přináší, však nejsou z pohledu spotřebitele pouze pozitivní. Dotýkají se celé řady oblastí a otázek: ochrany soukromí a dat, kybernetické bezpečnosti, zastarávání výrobků, udržitelnosti, spotřeby energie, hospodářské soutěže, bezpečnosti, práv spotřebitelů atd.

Propojená zařízení například obvykle shromažďují obrovské množství dat o svých uživateli a svém okolí. Tento rozsáhlý sběr dat vyvolává řadu naléhavých obav souvisejících s ochranou údajů a soukromí. S tím, jak se čím dál širší síť senzorů a zařízení proplétá do více aspektů našeho života, rostou také potenciální rizika a rozsah narušení bezpečnosti dat a kybernetických útoků. Každé nové zařízení, které připojíme k internetu, potenciálně přidává další prostor pro útok a řetězec zařízení je často tak silný, jak silný je jeho nejslabší článek. Rozvoj a implementace umělé inteligence v technologiích internetu věcí také přináší výzvy související se spravedlností, odpovědností a dalšími aspekty.

Mezi další problémy, které internet věcí přináší nebo prohlubuje, patří umělé omezování životních cyklů výrobků, [proprietární uzamčení \(lock-in efekt\)](#) a některé aspekty odpovědnosti za vady výrobku.

Síťová zařízení mají také zvýšenou spotřebu energie kvůli potřebným síťovým komponentům. K velké části této spotřeby energie dochází v důsledku nepřetržité odezvy zařízení prostřednictvím sítě (režim nečinnosti – standby). Odborníci předpokládají, že celosvětové energetické ztráty v důsledku spotřeby zařízení nacházejících se v pohotovostním režimu vzrostou ze 7,5 TWh v roce 2015 na 47 TWh v roce 2025, a to na základě spotřeby síťových zařízení, která jsou trvale připojena k elektrické síti ¹³

3.4. Klíčová práva a povinnosti spotřebitelů v kostce

Pokud jde o propojená zařízení, vztahují se na ně i práva spotřebitelů platná pro nepropojená zařízení. Na spotřebitelské produkty internetu věcí se například vztahují pravidla o zákonné záruce (ve smyslu směrnice o digitálním obsahu a směrnice o prodeji zboží). Platí také pravidla o informování spotřebitelů v místě prodeje (dle směrnice o právech spotřebitelů). V určitém rozsahu se na zařízení internetu věcí vztahují také pravidla právních předpisů o bezpečnosti výrobků.¹⁴

Více informací o směrnici o prodeji zboží a směrnici o právech spotřebitelů naleznete v doplňujícím teoretickém podkladovém dokumentu k obecnému spotřebitelskému právu.

Vzhledem k propojení těchto zařízení však platí zvláštní povinnosti:

- 1) Za prvé musí být zajištěno, že zařízení, která shromažďují osobní údaje spotřebitelů, tyto údaje zpracovávají v souladu s pravidly stanovenými v GDPR. Tato pravidla

¹³ [Energy Efficiency of the Internet of Things, Technology and Energy Assessment Report](#)

¹⁴ Podle těchto pravidel musí být všechna zařízení bezpečná. Neexistuje dohoda o tom, zda pojem "bezpečnost" zahrnuje také "zabezpečení". Přijímané stanovisko je, že právní předpisy o bezpečnosti výrobků se vztahují na propojená zařízení, pokud bezpečnostní zranitelnost zařízení vede k ohrožení bezpečnosti (např. hacker zneužije zranitelnost v požárním hlásiči k jeho vypnutí – pokud by vypukl požár, obyvatelé domácnosti by byli fyzicky ohroženi).

zahrnují mimo jiné zásady minimalizace údajů, omezení účelu a ochrany údajů již od návrhu a povinnost získat souhlas uživatele v závislosti na účelu zpracování údajů.¹⁵

- 2) Za druhé, podle [směrnice o rádiových zařízeních](#) budou muset výrobci propojených zařízení od roku 2024 zajistit, aby jejich zařízení vykazovala určitou úroveň zabezpečení. Tato opatření musí zajistit, aby zařízení (i) neměla nepříznivý vliv na síť či její provoz a nezpůsobovala tak nepřijatelné zhoršení kvality služeb; (ii) obsahovala bezpečnostní zařízení, které zajistí ochranu osobních údajů a soukromí uživatele a účastníka, a (iii) podporovala určité funkční charakteristiky zajišťující ochranu před podvody, jako je [ransomware](#).
- 3) Podle [směrnice o digitálním obsahu](#) musí být propojeným zařízením dodávány aktualizace, včetně bezpečnostních, po dobu, kterou mohou spotřebitelé rozumně očekávat. Tato povinnost je spojena se zákonnou záruční lhůtou, ale může ji i přesáhnout.

Na národní úrovni

Transpozicí modernizační směrnice bude prodávající v ČR s účinností od 1. ledna 2023 povinen zabezpečit, že kupujícímu budou mj. poskytovány aktualizace, které jsou nezbytné, aby si věc po převzetí uchovala vlastnosti podle § 2161 (jakost při převzetí) zákona č. 89/2012 Sb, občanský zákoník, a že bude na jejich dostupnost upozorněn, a to a) po dobu dvou let, mají-li být podle smlouvy digitální obsah nebo služba digitálního obsahu poskytovány soustavně po určitou dobu, a je-li ujednáno poskytování po dobu delší dvou let, po celou tuto dobu,

b) po dobu, po kterou to kupující může rozumně očekávat, mají-li být podle smlouvy digitální obsah nebo služba digitálního obsahu poskytnuty jednorázově; to se posoudí podle druhu a účelu věci, povahy digitálního obsahu nebo služby digitálního obsahu a s přihlédnutím k okolnostem při uzavření smlouvy a povaze závazku.¹⁶

- 4) Za čtvrté, podle aktu EU o kybernetické bezpečnosti, pokud existují certifikační systémy a vztahují se na dané propojené zařízení, musí výrobce tohoto zařízení informovat spotřebitele o období, během něhož bude koncovým uživatelům nabízena bezpečnostní podpora, zejména pokud jde o dostupnost aktualizací souvisejících s kybernetickou bezpečností.
- 5) Spotřebitelé mohou důvodně očekávat, že přístup k internetovým službám je poskytován neutrálním a nediskriminačním způsobem v souladu s nařízením o otevřeném internetu. Poskytovatelé internetových služeb musí k veškerému internetovému provozu přistupovat stejně, bez diskriminace, omezení nebo rušení

¹⁵ Další informace o ochraně údajů a obecném nařízení o ochraně osobních údajů (GDPR) naleznete v kapitole 1.

¹⁶ Upraveno v ustanovení §2161b občanského zákoníku ve znění účinném od 1. ledna 2023

("síťová neutralita"). Zachování otevřeného a neutrálního přístupu k internetu je nezbytné, pokud chceme uplatňovat své základní svobody a demokratická práva na účast v dnešní online propojené společnosti. Je to také předpokladem pro to, abychom mohli využívat výhod internetu věcí. Spotřebitelé potřebují neomezený a neutrální internet, aby mohli využívat svá propojená zařízení k přístupu ke zpravodajství a kulturnímu obsahu nebo k nakupování bez omezení.

- 6) Pokud jde o pravidla týkající se odpovědnosti za vady výrobku, příslušná směrnice – směrnice o odpovědnosti za vadné výrobky, byla vypracována již v roce 1985, tedy dávno předtím, než bylo možné uvažovat o používání propojených zařízení, natož předvídat s tím související budoucí výzvy. Dnes již není přizpůsobena tomu, aby se vypořádala s výzvami, které přináší internet věcí, a aby zajistila odškodnění spotřebitelů v případě, že nastane porucha – služba nebo výrobek má vady. Aktuálně proto probíhá proces revize této směrnice. V dubnu 2020 vydala organizace BEUC několik doporučení, která mají zajistit, aby pravidla EU o odpovědnosti za škodu způsobenou vadou výrobku byla uzpůsobena internetu věcí a potřebám spotřebitelů v digitálním věku.¹⁷

3.5. Zákony a předpisy na úrovni EU I

- [Směrnice 2014/53/eu Evropského parlamentu a Rady ze dne 16. dubna 2014 o harmonizaci právních předpisů členských států týkajících se dodávání rádiových zařízení na trh a zrušení směrnice 1999/5/es \(konsolidované znění\)](#)
- Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („[akt o kybernetické bezpečnosti](#)“)
- [Směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků \(konsolidované znění\)](#)
- [Směrnice Evropského parlamentu a Rady \(EU\) 2019/770 ze dne 20. května 2019 o některých aspektech týkajících se smluv o poskytování digitálního obsahu a digitálních služeb.](#)
- [Nařízení Evropského parlamentu a Rady \(EU\) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu \(konsolidované znění\)](#)
- Zpráva Evropské komise o [šetření v oblasti spotřebitelského internetu věcí](#)

* Další příslušné zákony, které jsou uvedeny v jiných modulech, jako je GDPR a *acquis* o právech spotřebitelů, zde nejsou uvedeny, ale jak je vysvětleno výše, jsou použitelné i v kontextu internetu věcí jako u jakéhokoli jiného produktu nebo služby, např. pokud propojené zařízení zpracovává osobní údaje, bude muset dodržovat GDPR.

¹⁷ BEUC, *Product liability 2.0 - How to make EU rules fit for consumers in the digital age*, duben 2020, dostupný [zde \(pouze v AJ\)](#)

3.6. Judikatura

Pokud jde o "síťovou neutralitu" (viz bod 5 kapitoly 3.4), Soudní dvůr EU nedávno ve věcech C-854/19, C-5/20 a C-34/20 rozhodl, že nabídky, které při čerpání mobilních dat konkrétními aplikacemi uplatňují "nulový tarif"¹⁸ a u nichž zároveň dochází k tomu, že jsou s nabídkou spojeny různé druhy omezení (šířka pásma, tethering nebo omezení roamingu), jsou v rozporu s čl. 3 odst. 3 nařízení o otevřeném internetu, a tudíž jsou podle práva EU nezákonné. Poskytovatelé služeb by proto měli v souladu s tímto výkladem přezkoumat své obchodní praktiky, aby zajistili, že budou plně respektovat pravidla EU týkající se neutrality sítě. Podobnou argumentaci by mohl Soudní dvůr použít rovněž u poskytovatelů služeb, kteří nabízejí "nulový tarif" pro aplikace spojené s propojenými zařízeními (např. poskytovatel internetových služeb v rámci marketingové kampaně nabízí výhodnou, tj. nulovou sazbu pro aplikaci používanou k ovládání chytré kamery).

3.7. Co mohou spotřebitelé dělat, pokud mají nějaký problém?

Na propojená zařízení se vztahuje několik právních předpisů. V závislosti na relevantním předpise mají spotřebitelé různé možnosti.

- Pokud se jedná o problém související s jejich osobními údaji (viz bod 1) v kapitole 3.4), použije se GDPR.
- Podle směrnice o rádiových zařízeních budou moci spotřebitelé v případě problémů s bezpečností svých zařízení (viz bod 2 v kapitole 3.4) od roku 2024 informovat své vnitrostátní orgány dozoru nad trhem (v ČR - Český telekomunikační úřad), které následně zahájí šetření daného zařízení. Rozhodnutí orgánu dozoru nad trhem může vést až k nařízení stažení daného výrobku z trhu.
- Pokud zařízení nebylo dodáno v souladu s očekáváním spotřebitelů, pokud jde o poskytování bezpečnostních aktualizací (viz bod 3 v kapitole 3.4), mají spotřebitelé právo odstoupit od smlouvy, obdržet přiměřené snížení ceny nebo požadovat, aby bylo zařízení uvedeno do souladu se smlouvou (viz směrnice o digitálním obsahu).
- Podle zákona o kybernetické bezpečnosti platí, že pokud je poskytování bezpečnostních aktualizací kratší, než oznámil výrobce (viz bod 4 v kapitole 3.4), spotřebitelé mají možnost podat stížnost k vnitrostátnímu orgánu. Pokud spotřebitelé s rozhodnutím vnitrostátního orgánu nesouhlasí, mají právo se proti němu bránit u soudu.
- Pokud není síťová neutralita dodržována (viz bod 5 v kapitole 3.4), mohou si spotřebitelé stěžovat u regulačního orgánu pro telekomunikace, který bude muset na jejich základě jednat.

¹⁸ „nulový tarif“ je obchodní praktika, kdy poskytovatel internetového připojení uplatňuje „nulový tarif“ nebo výhodnější tarif na veškerý datový provoz nebo jeho část spojenou s určitou aplikací nebo kategorií specifických aplikací nabízených partnery tohoto poskytovatele. Tato data se proto neodečítají od objemu dat zakoupených v rámci základního paušálního tarifu. Taková varianta, nabízená v rámci omezených balíčků, umožňuje poskytovatelům internetového připojení zvýšit atraktivitu jejich nabídky. Viz např. ROZSUDEK SOUDNÍHO DVORA (osmého senátu) ze dne 2. září 2021 ve věci C-854/19, dostupný [zde](#).

3.8. Další zdroje – informační přehledy, publikace, odkazy

Pracovní dokument útvarů Evropské komise - [Pokrok v oblasti internetu věcí v Evropě \(dostupný pouze v AJ\)](#)

Zpráva Evropské komise o [šetření v oblasti spotřebitelského internetu věcí \(IoT\)](#)

Poziční dokument BEUC: [Ochrana evropských spotřebitelů ve světě připojených zařízení \(pouze v AJ\)](#)

Informační přehled BEUC: [Zajištění kybernetické bezpečnosti spotřebitelských výrobků \(pouze v AJ\)](#)

AK EUROPA - [Očekávání spotřebitelů k internetu věcí \(pouze v AJ\)](#)





Tento dokument byl vypracován na základě smlouvy o poskytování služeb uzavřené s Evropskou komisí. Jeho obsah vyjadřuje pouze názory autora a je na jeho výhradní odpovědnost. Evropská komise nepřebírá žádnou odpovědnost za případné využití informací v něm obsažených.