



V Bruselu dne 10.1.2017
COM(2017) 9 final

**SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU
HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ**

"BUDOVÁNÍ EVROPSKÉ EKONOMIKY ZALOŽENÉ NA DATECH"

{SWD(2017) 2 final}

„BUDOVÁNÍ EVROPSKÉ EKONOMIKY ZALOŽENÉ NA DATECH“

1. ÚVOD

Data se stala základním zdrojem ekonomického růstu, tvorby nových pracovních míst a společenského pokroku. Analýza dat usnadňuje optimalizaci procesů a rozhodování, inovace a předvídání budoucích událostí. Tento celosvětový trend skrývá obrovský potenciál v různých oblastech, počínaje zdravotnictvím, životním prostředím, potravinovým zabezpečením, klimatem a účinným využíváním zdrojů, po inteligentní dopravní systémy a inteligentní města.

„Ekonomika založená na datech“¹ je charakterizována ekosystémem různých druhů účastníků trhu – jako jsou výrobci, výzkumníci a poskytovatelé infrastruktury, kteří spolupracují na tom, aby zajistili, že data budou přístupná a použitelná. To účastníkům trhu umožňuje získávat z těchto dat hodnotu, a to pomocí vytváření různých aplikací s obrovským potenciálem pro zlepšení každodenního života (např. řízení provozu, optimalizace sklizní nebo zdravotní péče poskytovaná na dálku).

Hodnota ekonomiky EU založené na datech byla v roce 2014 odhadnuta na 257 miliard EUR neboli na 1,85 % HDP EU.² V roce 2015 se tento odhad zvýšil na 272 miliard EUR, tedy 1,87 % HDP EU (meziroční růst ve výši 5,6 %). Stejný odhad předpovídá, že pokud budou pro ekonomiku založenou na datech včas zavedeny podmínky politického a právního rámce, její hodnota do roku 2020 vzroste na 643 miliard EUR, což by představovalo 3,17 % celkového HDP EU.

Podle obecného nařízení o ochraně osobních údajů (General Data Protection Regulation, GDPR)³ bude od května 2018 existovat jednotný soubor celoevropských pravidel, na rozdíl od současných 28 vnitrostátních zákonů. Nově vytvořený mechanismus jediného kontaktního místa⁴ zajistí, že za dozor nad operacemi zpracování přeshraničních údajů uskutečněnými společnostmi v EU bude zodpovědný jeden orgán pro ochranu údajů. Bude zaručen soulad při výkladu nových pravidel. Konkrétně to bude znamenat, že v přeshraničních případech, kterých se účastní několik vnitrostátních orgánů pro ochranu údajů, bude přijato jediné rozhodnutí, aby se tak zajistilo, že společným problémům se dostane společných řešení. Mimoto nařízení GDPR vytváří rovné podmínky mezi

¹ Ekonomika založená na datech měří celkové dopady trhu s daty – tj. obchodu, v rámci kterého jsou digitální data vyměňována jako výrobky nebo služby odvozené z nezpracovaných dat – na ekonomiku jako celek. To zahrnuje vytváření, shromažďování, ukládání, zpracovávání, šíření, analyzování, rozpracovávání, poskytování a využívání dat umožněné digitálními technologiemi (Studie evropského trhu s daty, SMART 2013/0063, IDC, 2016).

² Studie evropského trhu s daty, SMART 2013/0063, IDC, 2016.

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 95/56/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

⁴ Článek 56 GDPR.

zahraničními společnostmi a společnostmi z EU tím, že pokud společnosti se sídlem mimo EU v EU nabízejí zboží a služby nebo monitorují chování osob, musí uplatňovat stejná pravidla jako evropské společnosti. Z vyšší důvěry spotřebitelů bude mít prospěch jak EU, tak externí obchodní subjekty.

Směrnice o soukromí a elektronických komunikacích se týká důvěrného charakteru služeb elektronických komunikací v EU. Cílem revidované směrnice o soukromí a elektronických komunikacích, navrhované současně s tímto sdělením ve formě nařízení⁵, je zajistit vysokou úroveň ochrany, která bude plně v souladu s nařízením GDPR. Přísná pravidla ochrany údajů nastolí důvěru, která umožní rozvoj ekonomiky založené na datech na celém vnitřním trhu.

Jak zdůraznil předseda Juncker ve svém projevu o stavu Evropské unie 2016 dne 14. září 2016 „[b]ýt Evropanem znamená, že máte právo, aby vaše osobní údaje byly chráněny silnými, evropskými právními předpisy. Protože Evropané nechtějí, aby jim nad hlavami létaly drony, které zaznamenají každý jejich krok, nebo aby firmy ukládaly každé jejich kliknutí myši. Proto se Parlament, Rada a Komise letos v květnu dohodly na společném evropském nařízení o ochraně osobních údajů. Jedná se o silný evropský právní předpis, který se vztahuje na všechny společnosti, kdykoli zpracovávají vaše údaje, bez ohledu na to, kde mají sídlo. Protože v Evropě nám na soukromí záleží. Je to otázka lidské důstojnosti.“

Komise ve svém sdělení „Ochrana soukromí v propojeném světě – Evropský rámec pro ochranu údajů pro 21. století“⁶ z roku 2012 a ve sdělení „Na cestě k prosperující ekonomice založené na datech“⁷ z roku 2014 uznala, že aby se údaje mohly pohybovat volně z jednoho členského státu do druhého, jsou napříč EU zapotřebí moderní, jednotná pravidla, a že evropská digitální ekonomika si ve srovnání s USA osvojuje datovou revoluci jen pomalu a rovněž postrádá srovnatelnou průmyslovou kapacitu. Dospěla k závěru, že skutečnost, že chybí právní prostředí přizpůsobené obchodování s daty v rámci EU, může přispívat k nedostatečnému přístupu k velkým souborům dat, k vytváření možných překážek pro nové subjekty vstupující na trh a k potlačujícím účinkům na inovace.

Bezdůvodná **omezení volného pohybu dat** by pravděpodobně omezila rozvoj ekonomiky EU založené na datech. Tato omezení se týkají požadavků ukládaných veřejnými orgány, pokud jde o lokalizaci dat pro účely jejich ukládání či zpracování. Otázka volného toku dat se týká všech typů dat: podniky a aktéři v rámci ekonomiky založené na datech nakládají s průmyslovými a stroji vygenerovanými údaji, ať už jsou osobní, či nikoli, jakož i s daty vytvořenými lidskou činností. Komise ve strategii pro jednotný digitální trh oznámila, že navrhne iniciativu týkající se volného toku dat, která se bude zabývat omezeními volného pohybu dat z důvodů jiných, než je ochrana osobních údajů v EU, a bezdůvodnými omezeními v oblasti lokalizace dat pro účely jejich ukládání či zpracování. K takovým omezením patří právní akty přijaté členskými státy, správní pravidla a praxe se stejným účinkem. Jak ekonomika založená na datech roste, jejich počet má tendenci se zvyšovat, čímž se vytváří nejistota ohledně toho, kde

⁵ COM(2017) 10.

⁶ COM(2012) 9.

⁷ COM(2014) 442.

mohou být data ukládána či zpracovávána. To může mít dopad na všechna odvětví hospodářství, jakož i na soukromé a veřejné organizace, které mohou mít problémy s přístupem k inovativnějším a/nebo levnějším datovým službám. Bezdůvodná omezení týkající se umístění dat narušují volný pohyb služeb a svobodu usazování stanovené ve Smlouvě a rovněž porušují příslušné sekundární právo. To s sebou nese nebezpečí roztržitého trhu, snížení kvality služeb pro uživatele a snížení konkurenceschopnosti poskytovatelů datových služeb, zejména menších subjektů.

Vzhledem k rostoucímu významu dat a datových služeb v globální ekonomice a případným postojům třetích zemí vůči této otázce je součástí diskuzí mezi EU a jejími obchodními partnery rovněž bezdůvodná lokalizace dat. Pravidla EU týkající se ochrany údajů nemohou být předmětem jednání v rámci dohody o volném obchodu. Jak je vysvětleno ve sdělení o výměně a ochraně osobních údajů v globalizovaném světě⁸, dialogy o ochraně údajů a obchodní jednání s třetími zeměmi musí být vedeny odděleně. Kromě toho bude Komise, jak je uvedeno ve sdělení nazvaném Obchod pro všechny⁹, usilovat o to, aby prostřednictvím obchodních dohod EU stanovila pravidla elektronického obchodování a přeshraničních toků údajů a řešila nové formy digitálního protekcionismu, přičemž mají být plně dodržována pravidla EU pro ochranu údajů a tato pravidla nemají být dotčena.

Dále tím, jak přeměna založená na datech zasahuje i do hospodářství a společnosti, vzniká stále rostoucí množství dat generovaných stroji nebo zpracovávaných na základě vznikajících technologií, jako jsou například internet věcí, továrny budoucnosti a autonomně propojené systémy. Připojení samotné mění způsob, jak získat přístup k datům: k datům, k nimž se obvykle přistupovalo prostřednictvím fyzicky, lze nyní ve stále větší míře přistupovat vzdáleně. Obrovská rozmanitost zdrojů a typů dat a bohaté příležitosti, jak vzhled do těchto dat uplatnit v řadě oblastí, včetně rozvoje veřejné politiky, se teprve začínají objevovat. Aby bylo možné těchto příležitostí využít, musí mít soukromí i veřejní aktéři na trhu s daty přístup k velkým a různorodým souborům dat. Otázky přístupu a přenosu související s daty generovanými těmito stroji nebo procesy jsou proto pro vznik ekonomiky založené na datech zásadní a vyžadují pečlivé posouzení.

Další nově se objevující otázky se týkají uplatňování pravidel týkajících se odpovědnosti za škody vzniklé v důsledku poruchy připojeného zařízení nebo robota a přenositelnosti a interoperability dat. V kontextu nových technologií, jako jsou například internet věcí nebo robotika, existují komplexní a složité vzájemné závislosti, a to jak v rámci produktů (založených na hardwaru a softwaru), tak i mezi vzájemně propojenými zařízeními. Další otázky navíc mohou vyvstat v souvislosti s autonomními stroji, jejichž neočekávané nebo nezamýšlené chování by mohlo poškodit osoby nebo předměty. Tyto jevy mohou vytvořit právní nejistotu ve vztahu k uplatňování stávajícího rámce pro odpovědnost a bezpečnost.

Jak bylo oznámeno ve sdělení týkajícím se jednotného digitálního trhu, cílem Komise je vytvořit jasný politický a právní rámec přizpůsobený pro ekonomiku založenou na datech, a to prostřednictvím odstranění zbývajících překážek bránících pohybu dat a

⁸ COM(2017) 7.

⁹ COM(2015) 497.

řešení právních nejistot vytvořených novými datovými technologiemi. Další cíle, z nichž toto sdělení vychází, jsou zaměřeny na zvýšenou dostupnost a používání dat, podporu nových obchodních modelů založených na datech, jakož i na zlepšování podmínek pro přístup k datům a analýzu dat v EU. Za tímto účelem Komise předkládá konkrétně zaměřené otázky k diskusi s ohledem na „budování evropské ekonomiky založené na datech“.

Z uvedených důvodů toto sdělení zkoumá následující otázky: volný tok dat; přístup a předávání v souvislosti s daty generovanými stroji; odpovědnost a bezpečnost v kontextu vznikajících technologií; a přenositelnost jiných než osobních údajů, interoperabilitu a normy. Toto sdělení rovněž stanoví návrhy týkající se experimentování s běžnými regulačními řešeními ve skutečném prostředí.

Komise o otázkách, které zkoumá toto sdělení, zahajuje rozsáhlý dialog se zúčastněnými stranami. Prvním krokem tohoto dialogu je veřejná konzultace, která byla zahájena souběžně s balíčkem týkajícím se ekonomiky založené na datech¹⁰.

2. VOLNÝ TOK DAT

Dobře fungující a dynamická ekonomika založená na datech vyžaduje, aby byl na vnitřním trhu umožněn a chráněn tok dat. V rychle se vyvíjejícím technologickém kontextu je bezpečný a spolehlivý volný tok dat nezbytný pro ochranu čtyř základních svobod jednotného trhu EU obsažených ve smlouvách (zboží, pracovníků, služeb a kapitálu). Datové služby rostou rychle v EU i celosvětově. Efektivní a přístupný jednotný trh v tomto odvětví by vytvořil významné příležitosti pro další růst a pracovní místa.

Tento růst a inovace v oblasti ekonomiky založené na datech, jakož i zavádění přeshraničních veřejných služeb, mohou být ohroženy překážkami bránícími volnému pohybu dat v EU, jako jsou například bezdůvodné požadavky, jež ukládají veřejné orgány, týkající se lokalizace dat. Opatření týkající se lokalizace dat fakticky znovu zavádějí digitální „hraniční kontroly“¹¹. Sahají od požadavků orgánů dozoru, aby poskytovatelé finančních služeb svá data ukládali lokálně, přes uplatňování pravidel o profesním tajemství, která obnášejí lokální ukládání nebo zpracovávání dat, až po rozsáhlá nařízení, která vyžadují lokální ukládání archivovaných informací vytvořených veřejným sektorem, bez ohledu na jejich citlivost.

Obavy o ochranu soukromí jsou legitimní, veřejné orgány by je ale neměly bezdůvodně používat jako důvod pro omezení volného toku dat. Jak je uvedeno výše, nařízení GDPR stanoví jednotný soubor pravidel s vysokou úrovní ochrany osobních údajů pro celou EU. Posiluje důvěru spotřebitelů v on-line služby a prostřednictvím posílených vnitrostátních orgánů pro ochranu údajů zajišťuje jednotné uplatňování pravidel ve všech členských státech. Nařízení GDPR posiluje důvěru nezbytnou pro zpracovávání dat a slouží jako základ pro volný tok osobních údajů v EU. Nařízení GDPR zakazuje omezení volného pohybu osobních údajů v Unii v případech, kdy jsou tato omezení založena na

¹⁰ <https://ec.europa.eu/digital-single-market/news-redirect/52039>.

¹¹ OECD: „Emerging Policy Issues: Localisation Barriers to Trade“ („Aktuální politické otázky: Lokalizační překážky obchodu“), 2015 a práce na dokumentu stále probíhá.

důvodech souvisejících s ochranou osobních údajů¹². Nařízení GDPR nicméně nepokrývá omezení založená na jiných důvodech, než je ochrana osobních údajů, např. na daňových nebo účetních zákonech. Mimo působnost nařízení GDPR dále zůstávají i jiné než osobní údaje, tj. údaje, které se nevztahují k identifikované nebo identifikovatelné fyzické osobě¹³, a které se mohou týkat například jiných než osobních údajů generovaných stroji.

Omezení týkající se umístění dat mohou vzniknout v důsledku právních předpisů nebo správních pokynů či praxe, které vyžadují, aby bylo ukládání nebo zpracovávání dat¹⁴ v elektronickém formátu¹⁵ omezeno na konkrétní zeměpisnou oblast nebo jurisdikci. Někdy jsou omezení uvalena členskými státy v přesvědčení, že orgány dozoru mohou snadněji kontrolovat data uložená lokálně. Lokalizace se rovněž používá jako zástupná varianta za záruky, pokud jde o soukromí, audit a vymáhání práva, jakož i o bezpečnost dat. V praxi však tato opatření k cílům, jichž mají dosáhnout, přispívají jen zřídka.

Bezpečnost informací závisí na řadě jiných faktorů, než kde jsou fyzicky uloženy, jako například na zachování jejich důvěrnosti a integrity v době, kdy jsou dostupná mimo zařízení, kde jsou uložena. V této souvislosti bude bezpečné ukládání a zpracovávání dat spíše než omezení týkajícími se umístění dat umožněno nejmodernějšími osvědčenými postupy v oblasti správy IKT v měřítku mnohem větším než jednotlivé systémy. Například aby byla data chráněna před lokálními přírodními katastrofami nebo kybernetickými útoky, mohou zařízení pro ukládání dat umístěná v různých členských státech navzájem sloužit jako záložní zařízení a lze přitom využít technická a organizační opatření stanovená ve směrnici o bezpečnosti sítí a informačních systémů¹⁶ (směrnice NIS). Dostupnost dat pro účely regulace a dohledu, která není jakkoli zpochybněna, by navíc byla lépe zaručena zlepšením spolupráce mezi vnitrostátními orgány nebo mezi těmito orgány a soukromým sektorem spíše než prostřednictvím omezení týkajících se lokalizace. V oblasti charakterizované úzkou spoluprací mezi orgány dozoru, jako například finanční služby, by požadavky týkající se lokalizace dat naopak mohly být kontraproduktivní.¹⁷

Požadavky týkající se lokalizace dat nicméně mohou být v konkrétních souvislostech nebo ve vztahu k určitým údajům opodstatněné a přiměřené, zejména do doby, než budou

¹² Čl. 1 odst. 3. Např. dynamická IP adresa, kterou poskytovatel online mediálních služeb uchovává v souvislosti s přístupem osoby na internetovou stránku, kterou tento poskytovatel zpřístupnil veřejnosti, pro uvedeného poskytovatele představuje osobní údaj, pokud má k dispozici právní prostředky, které mu umožňují nechat identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu. Viz rozsudek ve věci C-582/14, Breyer, ECLI:EU:C:2016:779, bod 49.

¹³ Jak je definováno v čl. 4 odst. 1 nařízení GDPR.

¹⁴ Data uchovávaná jak soukromě, tak veřejně.

¹⁵ Včetně kopií souborů dat.

¹⁶ 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, Úř. věst. L 194, 19.7.2016, s. 1.

¹⁷ Řada ustanovení EU týkajících se finančních služeb a Evropského systému dohledu nad finančním trhem vyžaduje, aby orgány dohledu měly přístup k údajům o finančních institucích a transakcích kdekoli na území EU. Požadavky, které vyžadují, aby byla data ukládána na dotyčném území státu, nebo které podmiňují přístup orgánů dohledu ke správním postupům, by mohly omezit přístup orgánů dohledu k údajům, které jsou pro provádění jejich mandátů zásadní.

zavedena účinná ujednání o přeshraniční spolupráci, například zajištění bezpečného zacházení s určitými údaji týkajícími se kritické energetické infrastruktury nebo dostupnost elektronických důkazů (např. lokalizovaných kopií souborů dat) pro orgány činné v trestním řízení či lokální ukládání údajů obsažených v určitých veřejných rejstřících.

Jak celosvětově, tak i v Evropě bohužel převažuje trend směrem k další lokalizaci dat, což je přístup, který často vychází z nesprávného pojetí, že lokalizované služby jsou automaticky bezpečnější než přeshraniční služby. Trh s datovými službami je navíc podstatně ovlivněn nedostatkem transparentních pravidel a silným vnímáním potřeby data lokalizovat. To může omezit přístup organizací podnikatelského a veřejného sektoru k levnějším nebo inovativnějším datovým službám nebo přinutit podniky působící přeshraničně, aby zajišťovaly nadměrné kapacity pro ukládání a zpracovávání dat. Podnikům založeným na využívání dat, zejména začínajícím podnikům a malým a středním podnikům, by to rovněž mohlo bránit v rozšiřování jejich činností, ve vstupu na nové trhy (např. tím, že budou muset investovat do datových center ve 28 členských státech) nebo v centralizování dat a analytických kapacit, aby mohly vyvíjet nové produkty a služby.

Evropa v současné době zajišťuje 84 % své konečné poptávky v oblasti služeb „souvisejících s IKT“ (poradenství, hosting, vývoj) vnitřně v rámci EU. Pokud by tyto služby mohly prostřednictvím odstranění omezení týkajících se lokalizace dat snadněji fungovat rovněž přes hranice v rámci EU, mohlo by to vést k ziskům v oblasti HDP ve výši až 8 miliard EUR ročně v podobě úspor nákladů a vyšší efektivity¹⁸.

Lokalizace dat rovněž brání širšímu přijetí cloudového ukládání a cloudového computingu. To může mít rovněž širší společenské účinky. Účinnější využití IT zdrojů by mohlo přispět ke snížení spotřeby energie a emisí uhlíků o čistých 30 % nebo více. Malý podnik, který by se přesunul na cloud, by tím, že by své provozní aplikace používal na cloudu místo toho, aby ty stejné aplikace používal na své vlastní infrastruktuře, mohl snížit svou spotřebu energie a emisi uhlíků o více než 90 %. Očekává se, že globální trh s energeticky účinnými datovými centry do konce roku 2020 vzroste na téměř 90 miliard EUR. Roztříštěný trh s datovými službami by plnému rozvoji těchto energeticky účinnějších služeb v EU bránil a rovněž by ohrozil ochotu investovat.

V zájmu řešení výše uvedených problémů a omezení a realizace plného potenciálu evropského ekonomiky založené na datech by měla být jakákoli činnost členského státu ovlivňující ukládání nebo zpracovávání dat vedena „**zásadou volného pohybu dat v rámci EU**“, jakožto závazku odvozeného od jejich závazků vyplývajících z ustanovení Smlouvy týkajících se volného pohybu služeb a svobody usazování a z příslušných sekundárních právních předpisů. Jakákoli stávající nebo nová omezení týkající se umístění dat by musela být pečlivě odůvodněna na základě Smlouvy a příslušného sekundárního práva jakožto nezbytná a přiměřená pro dosažení hlavního cíle obecného zájmu, jako například veřejné bezpečnosti¹⁹.

¹⁸ „Uvolnění vnitřních toků dat v EU: Ekonomické posouzení opatření týkajících se lokalizace dat v členských státech EU“, ECIPE, 2016, výpočet založen na zvýšeném konkurenčním tlaku v rámci cenově plně transparentního „průmyslového“ jednotného digitálního trhu.

¹⁹ S ohledem na to, že výjimky ze Smlouvy musí být vykládány restriktivně. Příslušné sekundární právo zahrnuje nařízení GDPR, směrnici 2000/31/ES (směrnice o elektronickém obchodu), směrnici 2006/123/ES (směrnice o

Zásada volného pohybu osobních údajů²⁰ zakotvená v primárním a sekundárním právu by se měla použít rovněž v případech, kdy nařízení GDPR členským státům umožňuje, aby si zvláštní záležitosti upravovaly samy. Členské státy by měly být podporovány v tom, aby nevyužívaly deregulační doložky v nařízení GDPR k dalšímu omezování volného toku dat.

Ve svých závěrech ze dne 15. prosince 2016 Evropská rada vyzvala k odstranění zbývajících překážek uvnitř jednotného trhu včetně těch, které brání volnému toku dat²¹.

Za účelem provádění zásady volného pohybu dat Komise učiní následující dva kroky:

- Po zveřejnění tohoto sdělení Komise zahájí strukturované dialogy s členskými státy a dalšími zúčastněnými stranami o opodstatněných a přiměřenosti opatření týkajících se umístění dat, přičemž jako výchozí bod poslouží omezení, která Komise dosud zaznamenala.
- V návaznosti na výsledky dialogů a další shromažďování důkazů o rozsahu a povaze omezení týkajících se umístění dat a jejich dopadů, zejména na malé a střední podniky a začínající podniky, mimo jiné prostřednictvím doprovodné veřejné konzultace, zahájí Komise v případě potřeby řízení o nesplnění povinnosti, aby vyřešila neopodstatněná nebo nepřiměřená opatření týkající se umístění dat, a, bude-li to nutné, může Komise rovněž přijmout další iniciativy týkající se volného toku dat. Jakákoli další opatření v této souvislosti budou prováděna v souladu se zásadami lepší právní úpravy.

3. PŘÍSTUP K DATŮM A PŘEDÁVÁNÍ

Stále rostoucí množství dat je generováno stroji nebo zpracováváno na základě vznikajících technologií, jako je například internet věcí. Tato data jsou stále více využívána jako klíčový prvek nových inovativních služeb s cílem zlepšit produkty nebo výrobní procesy a podpořit rozhodování.

Rozmanitost dat generovaných těmito stroji či procesy představuje pro aktéry na trhu s daty bohaté příležitosti, jak inovovat a uplatnit vzhled do těchto dat. Například data zachycená čidly používanými v moderních zemědělských podnicích mohou být použita k vytvoření aplikace pro optimalizování sklizní, nebo data shromážděná čidly v semaforech mohou být použita k vytvoření aplikace pro řízení provozu nebo k optimalizaci tras.

Aby mohli účastníci trhu z tohoto typu dat získat maximální hodnotu, potřebují mít přístup k velkým a různorodým souborům dat. Toho se však obtížněji dosahuje, pokud si je tvůrci dat nechávají pro sebe a tato data jsou pak v důsledku toho analyzována

službách) a pokud se jedná o návrhy technických předpisů a návrhy předpisů pro služby informační společnosti, směrnici 2015/1535 (směrnice o transparentnosti).

²⁰ Volný pohyb osobních údajů je obsažen v článku 16 Smlouvy o fungování Evropské unie a pravidla pro volný pohyb osobních údajů jsou stanovena ve stávajících a budoucích právních předpisech EU týkajících se ochrany údajů. Čl. 1 odst. 3 obecného nařízení o ochraně údajů stanoví: „Volný pohyb osobních údajů v Unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán“.

²¹ <http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/>

odděleně v uzavřených prostorech. Otázky přístupu a předávání související s nezpracovanými daty (tj. s daty, která od svého zaznamenání nebyla zpracována nebo změněna) generovanými těmito stroji nebo procesy jsou proto pro vznik ekonomiky založené na datech zásadní a vyžadují pečlivé posouzení.

Otázka přístupu k datům generovaným stroji je projednávána v několika odvětvích, jako například doprava, trhy s energií, chytrá prostředí pro život a zdravotnictví a pečovatelské služby.

Před prozkoumáním stávající situace týkající se přístupu k datům v EU je důležité vyjasnit, jaký typ dat je v tomto kontextu projednáván.

3.1. Typ uvažovaných dat

Obecně platí, že údaje mohou být osobní, nebo jiné než osobní. Například údaje generované domácími čidly teploty mohou být ze své povahy osobní, pokud je lze dát do souvislosti s žijící osobou, zatímco údaje týkající se vlhkosti půdy osobní nejsou. Osobní údaje mohou být přeměněny na neosobní prostřednictvím procesu anonymizace. Pokud jsou údaje považovány za osobní²², použije se rámec pro ochranu údajů, zejména nařízení GDPR.

Data generovaná stroji jsou vytvářena bez přímého zásahu člověka počítačovými procesy, aplikacemi či službami nebo čidly zpracovávajícími informace obdržené od zařízení, softwaru či strojního zařízení, ať už virtuálního či skutečného.

Data generovaná stroji mohou být ze své povahy osobní, nebo jiná než osobní. Pokud data generovaná stroji umožňují identifikaci fyzické osoby, považují se za osobní údaje s tím důsledkem, že dokud tato data nebudou plně anonymizována, platí všechna pravidla týkající se osobních údajů (např. lokalizační údaje mobilních aplikací).

Jedním ze společných témat spojujících volný tok dat s nově vznikajícími otázkami přístupu a předávání dat je skutečnost, že podniky a aktéři v rámci ekonomiky založené na datech budou pracovat jak s osobními, tak i s neosobními údaji, a že toky dat a soubory dat budou pravidelně obsahovat oba typy. Veškerá politická opatření musí tuto ekonomickou realitu a rámec pro ochranu osobních údajů brát v úvahu a současně respektovat základní práva jednotlivců.

3.2. Omezený přístup k datům

Za účelem posouzení této nově vznikající otázky je nejprve nutná analýza toho, jak mohou společnosti a další účastníci trhu přistupovat k velkým a různorodým souborům dat potřebným v ekonomice založené na datech.

Dostupné důkazy²³ ukazují, že společnosti disponující velkými množstvími dat se obecně přiklánějí k používání převážně vlastních kapacit pro analýzu dat. Ve většině případů

²² Jak je definováno v čl. 4 odst. 1 nařízení GDPR.

²³ Mezinárodní datové centrum (IDC), Studie evropského trhu s daty, první průběžná zpráva, 2016; Podpůrná studie posouzení dopadů o nově vznikajících otázkách vlastnictví dat, interoperabilitě, (opětovně) použitelnosti a

jsou data generována a analyzována stejnou společností, a i tehdy, pokud je analýza zadána subdodávkou, nemusí k dalšímu opětovnému použití dat dojít. Kromě toho si výrobci, společnosti nabízející služby nebo jiní účastníci trhu disponující daty v některých případech data vygenerovaná svými stroji nebo prostřednictvím svých produktů a služeb nechávají pro sebe, čímž potenciálně omezují opětovné použití na navazujících trzích. Řada společností nevyužívá nebo neumožňuje využívat uživatelsky vstřícná aplikační programovací rozhraní (API)²⁴ (která stanoví, jak by spolu různé aplikace měly vzájemně interagovat), která mohou sloužit jako bezpečné vstupní porty pro nová a inovativní použití dat, kterými tyto společnosti disponují.

Proto celková výměna dat v současné době zůstává omezená. Trhy s daty pomalu vznikají, ale nejsou široce využívány. Společnosti nemusí být vybaveny správnými nástroji a dovednostmi pro kvantifikaci ekonomické hodnoty svých dat a mohou se obávat ztráty nebo ohrožení své konkurenční výhody, kdyby byla data dostupná konkurentům.

3.3. Nezpracovaná data generovaná stroji: právní situace na úrovni EU a na vnitrostátní úrovni

Nezpracovaná data generovaná stroji nejsou chráněna stávajícími právy duševního vlastnictví, jelikož nejsou považována za výsledek duševního úsilí a/nebo nemají žádnou úroveň původnosti. Právo *sui generis* směrnice o databázích (96/9/ES) – která dává tvůrcům databází právo zabránit neoprávněnému vytěžování a/nebo zužitkování celého obsahu databáze nebo jeho podstatné části – může poskytnout ochranu pouze za podmínky, že vytvoření takové databáze zahrnuje podstatný vklad do pořízení, ověření nebo předvedení jejího obsahu. Nedávno přijatá směrnice o ochraně obchodního tajemství (2016/943/EU), která by měla být provedena do vnitrostátního práva do června 2018, bude obchodním tajemstvím poskytovat ochranu před jejich neoprávněným získáním, využitím a zpřístupněním. Aby byla data považována za „obchodní tajemství“, je nutné přijmout opatření na ochranu důvěrného charakteru informací, které představují „duševní kapitál společnosti“.

Podle právních předpisů různých členských států se právní nároky na data uplatňují, pouze pokud tato data splňují zvláštní podmínky pro to, aby byla považována například za práva duševního vlastnictví, právo o databázích nebo obchodní tajemství. Na úrovni EU by však nezpracovaná data generovaná stroji jako taková příslušné podmínky obecně nesplnila.

Na vnitrostátní úrovni ani na úrovni EU tak v souvislosti s nezpracovanými daty generovanými stroji, která nejsou považována za osobní údaje, nebo v souvislosti s podmínkami jejich hospodářského využití a obchodovatelnosti v současné době neexistují komplexní politické rámce. Tato otázka je tak do velké míry ponechána na smluvních řešeních. Dostatečnou reakcí by mohlo být použití stávajících nástrojů obecného smluvního práva a práva hospodářské soutěže dostupných v Unii. Mimoto

přístupu k datům a odpovědnosti, první průběžná zpráva, 2016; Konference na vysoké úrovni GR Connect, 17. října 2016.

²⁴ Například: <https://developer.lufthansa.com/>, <https://data.sncf.com/api>, <https://api.tfl.gov.uk/>, <https://dev.blablacar.com/>

mohou být připraveny dobrovolné nebo zastřešující dohody pokrývající určitá odvětví. Pokud je však vyjednávací síla různých účastníků trhu nerovná, řešení založená pouze na tržním přístupu nemusí být k zajištění spravedlivých a pro inovace příznivých výsledků, k usnadnění snadného přístupu pro nové subjekty vstupující na trh a k vyvarování se patovým situacím dostačující.

3.4. Situace v praxi

Výrobci nebo poskytovatelé služeb se v některých případech mohou stát *de facto* „vlastníky“ dat, které jejich stroje nebo procesy vygenerovaly, a to i tehdy, pokud jsou tyto stroje vlastněny uživateli. *De facto* kontrola těchto dat může být pro výrobce zdrojem diference a konkurenční výhody. To však může být problematické, protože výrobce uživateli často brání, aby povolil využívání dat jinou stranou.

Různí účastníci trhu kontrolující data tak mohou v závislosti na zvláštnostech trhů využít mezer v právním rámci nebo právních nejistot popsaných výše, a to tak, že na uživatele uvalí nepřiměřené standardní smluvní podmínky, nebo prostřednictvím technických prostředků jako jsou formáty s existujícím vlastníkem nebo šifrování. Několik členských států rozšířilo oblast působnosti směrnice na ochranu spotřebitelů o nepřiměřených smluvních podmínkách rovněž na transakce mezi podniky (Business to Business, B2B), ale nečinily tak všechny. To by mohlo vést například k tomu, že uživatelé a podniky budou donuceni k ujednáním o výlučném využívání dat. Může se objevit dobrovolné sdílení dat, ale vyjednávání takových smluv by pro slabší strany mohlo znamenat značné transakční náklady, ať už kvůli nerovné vyjednávací pozici nebo kvůli značným nákladům na najmutí právních odborníků.

3.5. Budoucí rámec EU pro přístup k datům

Některé členské státy v současné době prozkoumávají zajištění přístupu k datům generovaným stroji a mohou se rozhodnout, že tuto otázku budou regulovat samy. U nekoordinovaného postupu hrozí, že povede k roztržitosti, což by mělo neblahý vliv na rozvoj ekonomiky EU založené na datech a na fungování přeshraničních datových služeb a technologií v rámci vnitřního trhu.

Komise má proto v úmyslu vést s členskými státy a dalšími zúčastněnými stranami dialog, aby prozkoumala možný budoucí rámec EU pro přístup k datům. Podle názoru Komise by se měl tento dialog týkat nejúčinnějších nástrojů, jak dosáhnout těchto cílů:

- **Zlepšení přístupu k anonymním datům generovaným stroji:** Data generovaná stroji se prostřednictvím sdílení, opětovného použití a shromažďování stanou zdrojem vytváření hodnot, inovací a rozmanitosti obchodních modelů²⁵.
- **Usnadnění a vytváření pobídek ke sdílení těchto dat:** Všechna budoucí řešení by měla podporovat účinný přístup k datům a zohledňovat například možné rozdíly ve vyjednávací síle účastníků trhu.

²⁵ Pokud se jedná o osobní údaje, použije se nařízení GDPR.

- **Ochrana investic a majetku:** Všechna budoucí řešení by rovněž měla zohledňovat oprávněné zájmy účastníků trhu, kteří investují do vývoje produktu, zajistit přiměřenou návratnost jejich investic a přispět tak k inovaci. Všechna budoucí řešení by zároveň měla zajistit vyvážené sdílení přínosů mezi držiteli dat²⁶, zpracovateli a poskytovateli aplikace v rámci hodnotových řetězců.
- **Zabránit tomu, aby došlo k vyzrazení důvěrných dat:** Všechna budoucí řešení by měla zmírňovat rizika vyzrazení důvěrných dat, zejména stávajícím nebo potenciálním konkurentům. V tomto ohledu by před tím, než bude posouzeno, zda určitá data mohou být sdílena, či nikoliv, mělo být rovněž umožněno provést řádnou klasifikaci dat.
- **Minimalizovat patové účinky:** Měla by být zohledněna nerovná vyjednávací síla společností a soukromých osob. Mělo by se zabránit patovým situacím, zejména u malých a středních podniků, začínajících podniků a soukromých osob.

V rámci dialogů se zúčastněnými stranami má Komise v úmyslu projednat tyto možnosti řešení otázky přístupu k datům generovaným stroji, které se liší v míře jejich stupně zásahu:

- **Pokyny pro vytváření pobídek k tomu, aby podniky sdílely data:** Komise by mohla za účelem zmírnění účinků rozdílných vnitrostátních právních předpisů a poskytnutí větší právní jistoty pro společnosti vydat pokyny, jak by měla být ve smlouvách řešena práva na kontrolu jiných než osobních údajů. Tyto pokyny by byly založeny na stávajících právních předpisech, zejména na požadavcích na transparentnost a spravedlnost stanovených právními předpisy EU v oblasti uvádění na trh a spotřebitelského práva, na směrnici o obchodním tajemství a na autorském právu, zejména na směrnici o databázích. Komise má v úmyslu v roce 2017 zahájit posouzení směrnice o databázích.
- **Podpora vývoje technických řešení pro spolehlivou identifikaci a výměnu dat:** Sledovatelnost a jasná identifikace zdrojů dat jsou předpokladem pro skutečnou kontrolu dat na trhu. Pro vytvoření důvěry v systém může být nezbytné definovat spolehlivé a případně standardizované protokoly pro perzistentní identifikaci zdrojů dat. Vytvoření ekosystémů vývojářů aplikací a algoritmů, kteří by měli zájem o data, kterými disponují společnosti, mohou rovněž podporovat aplikační programovací rozhraní (API). API mohou podnikům a veřejným orgánům pomoci identifikovat různé druhy opětovného použití dat, kterými disponují, a pomoci jim mít z nich prospěch. Na tomto základě by mohlo být zvažováno širší využití otevřených, standardizovaných a dobře zdokumentovaných API, a to prostřednictvím technických pokynů včetně identifikace a šíření osvědčených postupů pro společnosti a subjekty veřejného sektoru. To by mohlo zahrnovat zpřístupňování dat ve strojově čitelných formátech a poskytování souvisejících metadat.
- **Základní smluvní pravidla:** Standardní pravidla by mohla popisovat měřítko vyváženého řešení smluv týkajících se dat a řádně zohledňovat rovněž probíhající kontrolu účelnosti celkového fungování směrnice o nepřiměřených smluvních

²⁶ Subjekt, který data generovaná stroji v praxi spravuje a ponechává si je.

podmínkách. Pravidla by mohla být doplněna zavedením kontroly nepřiměřenosti ve smluvních vztazích mezi podniky (B2B)²⁷, což by vedlo k zneplatnění smluvních doložek, které se výrazně odchyľují od standardních pravidel. Rovněž by mohly být doplněny souborem doporučených standardních smluvních podmínek navržených zúčastněnými stranami. Tento přístup by mohl omezit právní překážky pro malé podniky a snížit nerovnováhu ve vyjednávacích pozicích a přitom by stále umožňoval vysoký stupeň smluvní volnosti.

- **Přístup pro vědecké účely a pro účely veřejného zájmu:** Veřejným orgánům by mohl být udělen přístup k datům v případech, kdy by to bylo ve „veřejném zájmu“ a zásadně by to zlepšilo fungování veřejného sektoru, například přístup statistických úřadů k obchodním údajům nebo optimalizace systémů řízení provozu na základě údajů v reálném čase od soukromých vozidel. Přístup statistických úřadů k obchodním údajům by obvykle přispěl ke zmírnění zátěže ohledně hlášení statistických údajů spočívající na hospodářských subjektech. Přístup k datům z různých zdrojů a schopnost kombinovat je obdobně zásadní také pro vědecký výzkum v oblastech jako jsou lékařství, životní prostředí a společenské vědy.
- **Právo producenta dat:** Producentovi dat, tj. vlastníkovi nebo dlouhodobému uživateli (tj. nájemci) zařízení, by mohlo být uděleno právo používat a povolit používání neosobních údajů. Cílem tohoto přístupu by bylo vyjasnit právní situaci a dát producentovi dat větší výběr, a to otevřením možnosti, aby uživatelé využívali svá data a přispěli tím k uvolnění dat generovaných stroji. Příslušné výjimky by však musely být jasně stanoveny, zejména poskytování nevýhradního přístupu k datům výrobcům nebo veřejným orgánům, například z důvodu řízení provozu nebo z důvodu ochrany životního prostředí. Pokud se jedná o osobní údaje, jednotlivec si zachovává právo svůj souhlas kdykoli po povolení používání odvolat. Před tím, než druhá strana povolí osobní údaje dále používat, musí s nimi být nakládáno anonymně tak, že jednotlivec není nebo nadále nebude identifikovatelný. Nařízení GDPR nadále zůstává použitelné pro veškeré osobní údaje (ať už generovaná stroji, či jinak), dokud tyto údaje nebudou anonymizovány.
- **Přístup za úhradu:** Pro subjekty disponující daty, jako jsou například výrobci, poskytovatelé služeb nebo jiné strany, by mohl být vyvinut rámec případně založený na určitých hlavních zásadách, jako jsou spravedlivé, přiměřené a nediskriminační podmínky (fair, reasonable and non-discriminatory, FRAND), na jehož základě by se poskytoval přístup k datům, kterými disponují, a to po anonymizaci a za úhradu. Bylo by třeba zohlednit příslušné oprávněné zájmy, jakož i potřebu chránit obchodní tajemství. Za účelem zohlednění zvláštností každého odvětví by rovněž mohly být zváženy různé režimy přístupu pro různá odvětví a/nebo obchodní modely. Například v některých případech by pro podniky i pro společnost mohl být upřednostňovanou možností otevřený přístup k datům (úplný nebo částečný).

²⁷ Měřítka pro úroveň nepřiměřenosti pro B2B by se samozřejmě muselo lišit od smluv B2B, aby tak odráželo vyšší stupeň smluvní volnosti ve vztazích mezi podniky (B2B).

S cílem shromáždit více důkazů o fungování trhů s daty dle sektorů a prozkoumat možná řešení bude Komise ohledně výše uvedených otázek konzultovat zúčastněné strany. Pro diskuzi o možných řešeních a pro zabránění neplánovaným vedlejším účinkům, které by potlačily inovace nebo bránily konkurenci, je v tomto kontextu zásadní široká diskuze na makroúrovni. Mimoto se budou konat diskuze s příslušnými zúčastněnými stranami v datovém hodnotovém řetězci pro konkrétní odvětví.

4. ODPOVĚDNOST

Další vznikající otázka se týká uplatňování stávajících pravidel týkajících se odpovědnosti v ekonomice založené na datech ve vztahu k produktům a službám založeným na vznikajících technologiích, jako jsou například internet věcí, továrny budoucnosti a autonomně propojené systémy. Internet věcí je rychle rostoucí síť předmětů každodenního života, jako jsou hodinky, vozidla a termostaty, které jsou připojené k internetu. Autonomně propojené systémy, jako jsou například samořízená vozidla, jednají nezávisle na lidech a jsou schopny chápat a interpretovat svá okolí. Tyto vznikající technologie používají čidla, aby jim poskytla mnoho typů dat, která jsou často vyžadována pro to, aby produkt nebo služba fungovaly.

Všechny tyto inovace pravděpodobně přispějí k bezpečnějšímu a kvalitnějšímu životu, ale nevyhnutelně zde u každého zařízení zůstává možnost chybného návrhu, poruchy nebo manipulace. Mohlo by k tomu dojít v důsledku toho, že čidlo přenese nesprávná data, například kvůli závadám softwaru, problémům s připojením nebo nesprávnému fungování stroje. Povaha těchto systémů znamená, že může být obtížné určit přesný zdroj problému, který vedl k poškození, což s sebou nese otázku, jak zajistit, aby tyto systémy byly pro uživatele bezpečné, aby se minimalizoval vznik škody, a kdo by měl nést odpovědnost za škodu, pokud k ní dojde.

Otázka, jak uživatelům i výrobcům takovýchto zařízení poskytnout jistotu v souvislosti s jejich případnou odpovědností, je proto pro vznik ekonomiky založené na datech velmi důležitá.

4.1. Pravidla EU týkající se odpovědnosti

Občanské právo obecně rozlišuje dva druhy právní odpovědnosti: smluvní, kde odpovědnost za škodu vyplývá ze smluvního vztahu mezi stranami, a mimosmluvní²⁸, kde je odpovědnost stanovena mimo smlouvu. Důležitým typem mimosmluvní odpovědnosti je odpovědnost za vadné výrobky. Na úrovni EU směrnice o odpovědnosti za vadné výrobky (85/374/EHS) („směrnice o odpovědnosti za výrobky“) stanoví zásadu „objektivní odpovědnosti“, tj. odpovědnosti bez zavinění: v případě, že vadný výrobek způsobí spotřebiteli škodu, výrobci mohou být odpovědní, aniž by na jejich straně došlo k nedbalosti nebo zavinění. V kontextu internetu věcí a autonomně propojených systémů (např. robotika) však může být obtížné nebo nejasné, jak ustanovení této směrnice²⁹

²⁸ Pravidla EU týkající se odpovědnosti se vztahují pouze k mimosmluvní odpovědnosti.

²⁹ Odkazy na objektivní odpovědnost výrobců v případě vadných výrobků se nachází v jiných právních předpisech týkajících se bezpečnosti výrobků, například ve směrnici o rádiových zařízeních (2014/53/EU), v nařízeních o zdravotnických prostředcích, ve směrnici o strojních zařízeních (2006/42/ES) a ve směrnici o obecné bezpečnosti výrobků (2001/95/ES).

použít, a to z těchto důvodů: charakteristika těchto systémů, například komplikovaný hodnotový řetězec výrobku nebo služby, spolu s vzájemnou závislostí mezi dodavateli, výrobcí a třetími stranami, nejistota ve vztahu k právní povaze zařízení patřících do internetu věcí, tj. zda se jedná o výrobky, o služby nebo o výrobky k nimž patří prodej služby, a autonomní povaha těchto technologií.

Komise zahájila komplexní posouzení směrnice o odpovědnosti za výrobky, aby posoudila její celkové fungování a to, zda pravidla vytvořená pro velmi různá prostředí zůstávají vhodná pro vznikající technologie, jako je internet věcí nebo autonomně propojené systémy.

4.2. Další možný postup:

Cílem Komise je zvýšit právní jistotu, pokud jde o odpovědnost v kontextu vznikajících technologií, a tím vytvořit příznivé podmínky pro inovace. Kromě zachování *status quo*³⁰ je možné prozkoumat různé přístupy, mezi něž patří:

- **Přístupy týkající se vytváření rizik nebo řízení rizik:** Podle těchto přístupů by odpovědnost mohli nést účastníci trhu vytvářející významná rizika pro ostatní, nebo účastníci trhu, kteří mají nejlepší možnosti, jak tato rizika minimalizovat, nebo jim zabránit.
- **Dobrovolné nebo povinné systémy pojištění:** Tyto systémy by se mohly doplňovat s výše uvedenými přístupy týkajícími se odpovědnosti. Odškodnily by strany, které utrpěly škodu (např. spotřebitel). Tento systém by musel poskytovat právní ochranu investic uskutečněných podnikem a zároveň ujistit oběti ohledně spravedlivé náhrady nebo řádného pojištění v případě škody.

Všechny přístupy by musely zohledňovat činnost jedince používajícího technologii a přesněji určit, jaká by měla být úloha uživatelů dané technologie.

Komise bude konzultovat zúčastněné strany ohledně přiměřenosti stávajících pravidel EU týkajících se odpovědnosti v kontextu internetu věcí a autonomně propojených systémů, jakož i ohledně možných přístupů k překonání stávajících obtíží při přidělování odpovědnosti. Rovněž je prováděna souběžná veřejná konzultace o celkovém posouzení uplatňování směrnice o odpovědnosti za výrobky. Komise zhodnotí výsledky a zváží možnosti budoucích opatření.

5. PŘENOSITELNOST, INTEROPERABILITA A NORMY

Dalšími nově vznikajícími otázkami v ekonomice založené na datech jsou přenositelnost neosobních údajů, interoperabilita služeb za účelem umožnění výměny dat a vhodné technické normy pro provádění smysluplné přenositelnosti.

³⁰ Komise by mohla vydat pokyny, jak pravidla EU týkající se odpovědnosti uplatňovat na internet věcí a robotiku.

5.1. Přenositelnost jiných než osobních údajů

Přenositelnost dat znamená, že spotřebitelé a podniky mohou snadno přenést data z jednoho systému do druhého. V ekonomice založené na datech je obecně spojována s nízkými náklady na změnu a tudíž i s malými překážkami vstupu. Nařízení GDPR dá jednotlivcům právo získat osobní údaje, jež poskytl poskytovateli služeb, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému poskytovateli³¹.

Nicméně co se týče neosobních údajů, tak v současné době neexistují žádné povinnosti, které by zaručily alespoň minimální úroveň přenositelnosti údajů, a to dokonce ani pro široce používané on-line služby, jako jsou poskytovatelé cloud hostingu. To je částečně způsobeno tím, že požadavky na provádění přenositelnosti údajů mohou být technicky náročné a nákladné, jelikož různí poskytovatelé stejných služeb mohou svá data ukládat různě.

Smysluplná přenositelnost neosobních údajů by rovněž musela zohlednit širší aspekty správy údajů zahrnující transparentnost pro uživatele, řízený přístup a interoperabilitu, aby různé platformy spojily dohromady způsoby, které by podněcovaly inovace.

5.2. Interoperabilita

Úvahy ohledně přenositelnosti údajů často úzce souvisí s otázkou interoperability dat, která různým digitálním službám umožňuje hladkou výměnu dat usnadněnou vhodnými technickými specifikacemi. Směrnice o použití informací veřejného sektoru a související pokyny (včetně evropského rámce interoperability) zdůrazňují význam bohatých, standardizovaných metadat, které odpovídají zavedené slovní zásobě, pro usnadnění vyhledávání a interoperability. Na prostorové informace veřejného sektoru se v současné době uplatňuje směrnice o infrastruktuře pro prostorové informace v Evropském společenství (INSPIRE) a její nařízení o interoperabilitě a pokyny pro služby prostorových dat a data, včetně dat získaných z čidel³².

V případě on-line platform tato interoperabilita dat usnadňuje nejen přepínání, ale také souběžné používání několika platform (tzv. „multi-homing“), jakož i rozsáhlou výměnu dat napříč platformami, což má potenciál posílit inovace v digitální ekonomice.

5.3. Normy

Aby bylo možné provádět smysluplnou přenositelnost technologicky neutrálním způsobem, musí být účinné politiky přenositelnosti podpořeny vhodnými technickými normami. Komise se zavázala³³, že podpoří vhodné normy pro zlepšení interoperability, přenositelnosti a bezpečnosti cloudových služeb, a to lepším začleněním práce společenství otevřených zdrojů do procesu vytváření norem na evropské úrovni. Příklady

³¹ Článek 20.

³² Data generovaná stroji jsou „prostorová data“, jelikož čidla spolu s měřením obvykle předávají jejich přesnou nebo nepřesnou pozici (lokaci).

³³ COM(2016) 176 final: Priority pro normalizaci IKT pro jednotný digitální trh

tohoto přístupu jsou specifikace TOSCA pro cloudové aplikace, jejichž cílem je zvýšit přenositelnost a provozní řízení cloudových aplikací a služeb³⁴, a technické specifikace a pokyny pro prováděcí nařízení INSPIRE³⁵.

5.4. Další možný postup

Další možnosti, jak řešit výše uvedené otázky, zahrnují:

- **Vývoj doporučených smluvních podmínek, které by usnadnily změnu poskytovatelů služeb:** Vzhledem k tomu, že přenositelnost a změna poskytovatelů datových služeb jsou na sobě vzájemně závislé, mohl by být prozkoumán vývoj standardních smluvních podmínek, které by požadovaly, aby poskytovatel služeb prováděl přenositelnost dat zákazníků.
- **Vývoj dalších práv na přenositelnost dat:** Na základě práva na přenositelnost dat stanoveného nařízením GDPR a na navrhovaných pravidlech týkajících se smlouvy na dodání digitálního obsahu by mohla být zavedena další práva na přenositelnost neosobních údajů, která by pokrývala především kontexty B2B a zároveň řádně zohledňovala výsledky probíhající kontroly účelnosti klíčových částí právních předpisů EU v oblasti uvádění na trh a spotřebitelského práva³⁶.
- **Experimenty s normami pro konkrétní odvětví:** Mohly by být zahájeny experimentální přístupy pro konkrétní odvětví, jejichž cílem by byl vývoj přísnějšího přístupu k pravidlům týkajícím se přenositelnosti zakódovaný prostřednictvím norem. To by zpravidla zahrnovalo spolupráci více zúčastněných stran včetně tvůrců norem, průmyslu, technické komunity a veřejných orgánů.

Komise bude ohledně těchto otázek konzultovat zúčastněné strany a na základě toho určí, zda jsou nutná další opatření a zda mohou mít podobu výše uvedených opatření, ať už samostatně, nebo v kombinaci.

6. EXPERIMENTOVÁNÍ A TESTOVÁNÍ

Experimentování tvoří důležitou část zkoumání nově vznikajících otázek v digitální ekonomice. Bude prozkoumáno, zda by bylo možné k podpoře těchto druhů pokusů a experimentů využít financování z programu Horizont 2020.

Před tím, než bude dosaženo závěrů týkajících se vhodnosti možných řešení pro přístup k datům a odpovědnosti, by měl být ve spolupráci se zúčastněnými stranami zorganizována specializovaná zkouška pro otestování těchto otázek ve skutečném prostředí. Je třeba evropské řešení, které bude vycházet ze spolupráce a experimentování mezi členskými státy.

³⁴ <https://www.oasis-open.org/committees/tosca>

³⁵ Právní předpisy INSPIRE: <http://inspire.ec.europa.eu/inspire-legislation/26>

³⁶ http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

Vzhledem k přeshraničnímu rozměru tohoto sektoru by pro tento pokus mohla být použita kooperativní, propojená a automatizovaná mobilita³⁷.

V několika členských státech již byly započaty projekty, jejichž cílem je vyvinout kooperativní systémy a vyšší úroveň automatizace³⁸. Tyto projekty umožňují vozidlům, aby se propojila mezi sebou i se silniční infrastrukturou, jako jsou semaforey nebo dopravní značení. Mimoto má Komise v úmyslu spolupracovat se skupinou zainteresovaných členských států na vytvoření zákonného testovacího rámce pro provádění experimentů na základě harmonizovaných pravidel týkajících se přístupu k datům a odpovědnosti. Aby byl umožněn přístup k dostatečně velkému objemu dat, měly by být pokusy založeny na plánu 5G a hladce fungovat spolu s technologiemi, které jsou již používány a podle zásady doplňkovosti³⁹.

Další zajímavý experiment bude pocházet z geoprostorového odvětví, a to se vznikem nového datového ekosystému založeného na programu Copernicus – Evropského programu pozorování Země a třetího největšího poskytovatele dat na světě. Komise vyvíjí inovativní řešení, aby podpořila vývoj aplikací založených na programu Copernicus a na dalších prostorových datech, přičemž se snaží řešit především otázky přístupu k datům, interoperability a předvídatelnosti.

7. ZÁVĚR

K vybudování ekonomiky založené na datech potřebuje EU politický rámec, který by umožnil používání dat pro vědecké, společenské a průmyslové účely napříč hodnotovým řetězcem. Komise za tímto účelem zahajuje rozsáhlý dialog zúčastněných stran o otázkách zkoumaných v tomto sdělení. Prvním krokem tohoto dialogu bude veřejná konzultace. Otázky přístupu k datům a odpovědnosti budou rovněž testovány ve skutečném prostředí, a to v oblasti kooperativní, propojené a automatizované mobility.

Pokud se jedná o volný tok dat, Komise bude na tomto problému nadále pracovat v souladu s výše nastíněným přístupem, aby byla plně uplatněna zásada volného toku dat v rámci EU, a bude-li to nutné případně i prostřednictvím přednostních donucovacích opatření. Komise bude rovněž nadále sledovat a shromažďovat důkazy a v případě potřeby zváží přijetí dalších iniciativ v oblasti volného toku dat.

Na základě výsledků dialogu se zúčastněnými stranami Komise rovněž rozhodne, zda je nutné přijmout další opatření v oblasti nově vznikajících otázek a případně navrhně řešení. Úlohu v tomto kontextu může hrát experimentování ve skutečných podmínkách.

³⁷ Viz COM(2016) 766 ze dne 30.11.2016.

³⁸ Viz COM(2016) 766: Evropská strategie pro kooperativní, inteligentní dopravní systémy.

³⁹ Viz COM(2016) 588: 5G pro Evropu: Akční plán.