

OCHRANA OSOBNÍCH ÚDAJŮ A HOSPODÁŘSKÁ SOUTĚŽ:

POHLED ÚOHS A ÚOOÚ
NA DIGITÁLNÍ TRHY

Obsah

Obsah	2
Úvodní slovo předsedy ÚOHS	3
Úvodní slovo předsedy ÚOOÚ	4
Ochrana osobních údajů a hospodářská soutěž v digitální éře: vývoj, výzvy a legislativa EU	5
Nařízení o digitálních trzích – spravedlivé trhy a data	6
Nařízení o digitálních službách – bezpečnější online prostor a data	7
Nařízení o datech – sdílení dat pro inovace vs. soukromí	8
Akt o umělé inteligenci – důvěra v AI a tržní rovnováha	8
Průnik mezi hospodářskou soutěží a ochranou osobních údajů	9
Hospodářská soutěž z pohledu ochrany dat	9
Ochrana osobních dat z pohledu hospodářské soutěže	10
Vývoj doktríny v akademické literatuře	11
Synergické aspekty spolupráce správních orgánů	12
Společné posouzení cílů ochrany dat, soukromí a hospodářské soutěže	12
Konfliktní situace – střety mezi soutěží a soukromím	14
(A) Přístup k osobním datům vs. jejich ochrana	14
(B) Dominance založená na datech vs. ochrana soukromí	15
(C) Inovace ve prospěch ochrany soukromí vs. soutěžní omezení	15
Případové studie a rozhodnutí	17
Závěr	19

Úřad pro ochranu hospodářské soutěže

tř. Kpt. Jaroše 7, 602 00 Brno

Redakční rada: Milena Marešová, Martin Švanda

Texty: Sekce hospodářské soutěže ÚOHS, Úřad pro ochranu osobních údajů

Foto: archiv ÚOHS

Telefon: 542 167 111

E-mail: posta@uohs.gov.cz

<https://uohs.gov.cz/>

Uzávěrka textu: 31. 10. 2025

Grafická úprava: Metoda, spol. s r. o.

Úvodní slovo předsedy ÚOHS

Digitální éra přináší společnosti velké množství příležitostí, ale také nové výzvy jak pro fungování trhů, tak pro ochranu základních práv jednotlivců zejména v oblasti nakládání s jejich osobními daty. Právo na ochranu osobních údajů a hospodářská soutěž byly dlouhou dobu vnímány jako oddělené oblasti, každá s vlastními cíli, nástroji a metodami prosazování. Dynamický rozvoj technologií, od online platforem, přes umělou inteligenci až po rozsáhlé datové ekosystémy, nám však dennodenně ukazuje, že obě odvětví je nezbytné vnímat jako spojené nádoby. Právě jejich vzájemná souhra se totiž stává klíčem k udržení inovativního tržního prostředí i ochrany spotřebitelů.

Nacházíme se v době, kdy digitální technologie a data prostupují všemi oblastmi hospodářského i společenského života. Ačkoliv s nimi související inovace představují významný zdroj pokroku a růstu, nevyhnutelně s sebou přinášejí i řadu zásadních a zcela nových právních, etických a institucionálních otázek. Data se stala jedním z nejcennějších aktiv digitální ekonomiky a způsob jejich využívání může výrazně ovlivnit hospodářskou soutěž i důvěru občanů v zajišťování ochrany jejich soukromí, resp. osobních dat ze strany podnikatelských subjektů.

I proto jsme se společně s Úřadem pro ochranu osobních údajů rozhodli vypracovat informační list Ochrana osobních údajů a hospodářská soutěž: pohled ÚOHS a ÚOOÚ na digitální trhy, jenž se této strategicky významné problematice vztahu ochrany osobních údajů a hospodářské soutěže v digitální ekonomice věnuje. Informační list nabízí separátní i společný pohled obou institucí, zmiňuje vývoj evropské regulace, zejména přijetí zásadních digitálních aktů, a přináší souhrn vybraných příkladů z rozhodovací praxe Evropské komise, Soudního dvora Evropské unie i národních soutěžních a dozorových orgánů dokládajících změnu přístupu k nastíněné problematice a postupné sbližování obou zmíněných oblastí.

Takto nastavený trend rovněž přirozeně vyvolává rozsáhlé diskuse o spolupráci mezi soutěžními úřady a úřady pro ochranu osobních údajů. Rozhodovací praxe některých zahraničních úřadů potvrzuje, že jedi- ně koordinovaný a odborně propojený přístup dokáže zajistit, aby digitální trhy zůstaly otevřené, férové a zároveň respektovaly základní práva ochrany soukromí jednotlivců. Cílem Úřadu pro ochranu hospodářské soutěže a Úřadu pro ochranu osobních údajů je nabídnout v tomto infolistu ucelený rámec pro pochopení, jak lze podporovat hospodářskou soutěž v digitálním prostředí a současně zajišťovat ochranu soukromí každého jednotlivce.

Věřím, že výsledný materiál bude přínosný nejen pro veřejnost, ale stane se i cenným podkladem pro odbornou diskusi a inspirací k dalším krokům vedoucím k vyváženému a efektivnímu prosazování práva v digitální ekonomice ve prospěch občanů, podniků i celé společnosti. Jsem přesvědčen, že Úřad pro ochranu hospodářské soutěže i Úřad pro ochranu osobních údajů mohou svými správnými kroky přispět k průběhu digitální transformace způsobem podporujícím inovace, posilujícím důvěru občanů a chránícím zdravé konkurenční prostředí.



doc. JUDr. PhDr. Petr Mlsna, Ph.D.
předseda Úřadu pro ochranu
hospodářské soutěže

Úvodní slovo předsedy ÚOOÚ

Úvodem mi dovoluji poděkovat Úřadu pro ochranu hospodářské soutěže a jmenovitě jeho předsedovi, panu doc. JUDr. PhDr. Petru Mlsnovi, Ph.D., že Úřad pro ochranu osobních údajů může přispět do jeho informačního listu věnovanému vztahu hospodářské soutěže a ochrany osobních údajů. Na první pohled by se mohlo zdát, že se jedná o dvě samostatné oblasti evropského práva – hospodářská soutěž je pevně zakotvena ve Smlouvě o založení Evropského společenství pro uhlí a ocel (ESUO) z roku 1951, tedy již od samotných počátků evropské integrace, zatímco ochrana osobních údajů se rozvíjela později, především v návaznosti na prudký rozvoj technologií a digitalizace a jejich ingerenci do našeho soukromí.

Obě oblasti však dnes spojuje jeden zásadní prvek, kterým jsou data. Data – nahlíženo naší optikou – v podobě údajů osobních i neosobních, anonymizovaných, pseudonymizovaných či syntetických. Tato data se stala palivem digitální ekonomiky a základním zdrojem celé řady obchodních modelů, až se někdy zapomíná, že jejich ochrana je základní lidské právo. Právě proto již nelze ochranu osobních údajů a hospodářskou soutěž vnímat odděleně.

Vývoj evropského práva tuto skutečnost dobře dokládá. V oblasti ochrany dat byl nejprve přijat rámec směrnice 95/46/ES, později pak obecné nařízení o ochraně osobních údajů, které od roku 2018 zajišťuje jednotnou a moderní úpravu. V oblasti hospodářské soutěže je základem kontrola spojování podniků a zákaz zneužívání dominantního postavení. Tyto instituty dnes ovšem často zahrnují i otázky spojené se zpracováním osobních údajů – například při vymezování relevantního trhu, při hodnocení dominance či při spojování podniků založených na využívání velkých dat.

Tento trend potvrzuje i judikatura. Přelomový rozsudek Soudního dvora Evropské unie ve věci Meta Platforms a německého Bundeskartellamt ukázal, že soutěžní orgány mohou zohledňovat i otázky související s ochranou osobních údajů. To otevírá cestu k širší spolupráci mezi orgány ochrany dat a hospodářské soutěže a k hledání rovnováhy mezi podporou inovací a ochranou základních práv jednotlivců.

Evropská unie současně přijímá novou digitální legislativu – akt o digitálních službách, akt o digitálních trzích, akt o správě dat, akt o umělé inteligenci či nařízení o transparentnosti politické reklamy. Tyto předpisy vytvářejí právní rámec pro férové, transparentní a bezpečné digitální prostředí. Zároveň však kladou nové požadavky na dozorové orgány a vyžadují jejich těsnou spolupráci, založenou na zásadě loajální spolupráce, která je pevně zakotvena ve Smlouvách.

Dovolte mi zdůraznit, že tato spolupráce není jen fakultativní možností, ale v mnoha ohledech nezbytností. Jen propojením odborných poznatků ochrany osobních údajů a hospodářské soutěže můžeme dosáhnout synergického efektu a čelit výzvám, které přináší digitální ekonomika. To platí i v případech, ve kterých se právem chráněné zájmy dostávají do kolize – ať už jde o přístup k osobním údajům versus jejich ochranu, dominanci založenou na datech versus právo na soukromí či inovace založené na datech versus ochranu soutěžního prostředí.

Jsem přesvědčen, že naše společné úsilí povede k lepší ochraně práv jednotlivců, k férovému a otevřenému trhu a k odpovědnému využívání technologií. Úkolem nás všech je podporovat digitální inovace, ale současně chránit základní hodnoty, na nichž stojí Evropská unie – svobodu, soukromí a důstojnost člověka.



Mgr. Jiří Kaucký
předseda Úřadu pro ochranu
osobních údajů

Ochrana osobních údajů a hospodářská soutěž v digitální éře: vývoj, výzvy a legislativa EU

Ochrana osobních údajů i hospodářská soutěž jsou zakotveny jako hodnoty v právu EU, prvotně ve **Smlouvě o fungování EU (SFEU)**¹ tvořící základ pro sekundární a další navazující právní úpravu či podzákonné předpisy. Z pohledu svého významu představují tradiční odvětví evropského práva, která vznikla v odlišnou dobu, z různých důvodů a v současnosti se dále rozvíjí. Obě oblasti se liší předmětem ochrany, cíli, systematickou, zásadami a metodami prosazování zakotvenými v příslušných právních rámcích.²

Zatímco vznik hospodářské soutěže je časově spojen již s počátečním obdobím po vzniku Evropského hospodářského společenství (EHS), kdy bylo nutné odstraňovat překážky obchodních vztahů v rámci společného trhu,³ právní ochrana soukromí a osobních údajů vznikala později. Nejprve jako právní úprava některých členských států tehdejšího Evropského společenství (ES) s cílem chránit jednotlivce, a to i s ohledem na vývoj technologií, jejichž prostřednictvím lze zpracovávat a zveřejňovat enormní množství dat včetně osobních údajů. Dále se stalo soukromí, případně osobní údaje, předmětem ochrany v dokumentech mezinárodních organizací, především v OECD⁴ a Radě Evropy,⁵ poté následovala první evropská směrnice na ochranu soukromí a osobních údajů přijatá v roce 1995.⁶

Další vývoj ochrany soukromí a osobních údajů představovalo přijetí **obecného nařízení o ochraně osobních údajů** (účinné od 25. května 2018⁷) připravované jako reakce na očekávaný rozvoj technologií. Důvodem přijetí úpravy ve formě nařízení byla potřeba zajistit jednotnou ochranu osobních údajů v EU, neboť směrnice se v tomto ohledu nejevila jako dostatečně účinná. Nové nařízení v mnoha ohledech přejala předchozí systematiku a způsob ochrany osobních údajů upravené ve směrnici prostřednictvím aplikace obecných zásad a rovněž přijalo nové instituty. Doplnění zásad pro ochranu osobních údajů, zavedení institutu pověřence pro ochranu osobních údajů, posouzení ochrany osobních údajů či principu *privacy by design*⁸ významně zpřesnilo a prohloubilo právní úpravu osobních údajů.

Nové organizační uspořádání v podobě spolupráce **Evropského sboru na ochranu osobních údajů (Sbor)** a dozorových orgánů na ochranu osobních údajů v členských zemích EU umožňuje účinně chránit základní právo na ochranu osobních údajů. Toto právo nicméně není absolutní, v konkrétních případech musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality být v rovnováze s dalšími základními právy. Interpretace nařízení prostřednictvím pokynů Sboru, na jejichž přípravě se podílí pracovníci dozorových úřadů členských zemí, přispívá k jednotnému uplatňování obecného nařízení a k výkladu obtížných otázek vyplývajících z praxe.

1 V případě hospodářské soutěže se jedná především o čl. 101 a 102 SFEU, v případě osobních údajů o čl. 16 SFEU.

2 Zejména nařízení Rady (ES) č. 1/2003 ze dne 16. prosince 2002 o provádění pravidel hospodářské soutěže stanovených v čl. 81 a 82 Smlouvy a nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

3 Nařízení Rady EHS č. 17/62.

4 Dokument Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data dostupný na: <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf>.

5 Úmluva Rady Evropy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních údajů.

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

7 Obecné nařízení o ochraně osobních údajů ze dne 27. dubna 2016 (GDPR).

8 Princip *privacy in design* znamená, že ochrana osobních údajů je již na počátku integrována do návrhů produktů, služeb a systémů.

Z ústavního hlediska ochranu osobních údajů na úrovni EU významně posílila od roku 2016 i **Listina základních práv EU (Listina)**, která v čl. 8 výslovně zakotvila právo na ochranu osobních údajů včetně jeho základního obsahu a instituce určené k jeho ochraně.⁹ Hospodářská soutěž na druhou stranu nepředstavuje individuální základní právo, avšak patří mezi ústavní hodnoty fungování ekonomiky chráněné právním řádem.¹⁰ Význam soutěže jako veřejného statku obecně spočívá v podpoře konkurenčního prostředí, které přináší spotřebitelům lepší ceny, kvalitu a volbu, podporuje inovace a celkovou prosperitu. Konečným cílem hospodářské soutěže je tedy kromě ochrany trhu i ochrana spotřebitele, jejíž vysokou úroveň Listina garantuje.¹¹ V digitální době navíc hospodářská soutěž může nepřímým způsobem ovlivňovat i oblast soukromí, pokud například firma s monopolním postavením diktuje uživatelům podmínky ohledně sběru dat.

Obě uvedené oblasti evropského práva se v současné době připravují na to, aby byly schopny reagovat na neobyčejně dynamický a rychlý rozvoj technologií včetně umělé inteligence. Situace může vyžadovat doplnění právní úpravy, ale rovněž změnu aplikace a interpretace stávajícího práva. Soutěžní úřady a úřady pro ochranu osobních údajů nadto budou nuceny hledat rovnováhu mezi dvěma pilíři moderní digitální společnosti a zabývat se otázkou, jak chránit soukromí jednotlivců a zároveň efektivně podporovat otevřenou soutěž.

Pokrok v oblasti technologií včetně rozvoje umělé inteligence a digitalizace má obecně potenciál přinést pro společnost řadu možností, zlepšení, inovací a úspor, ale je spojen s riziky, mj. v oblasti základních práv včetně práva na ochranu osobních údajů. I proto EU přistoupila k přípravě digitálních aktů, které se novými otázkami souvisejícími s technologickým vývojem zabývají. Digitální akty představují souhrnný pracovní pojem regulující některé otázky či právní vztahy v souladu s cíli stanovenými v konkrétních oblastech. Jde např. o zavedení kategorie strážce přístupu u digitálních služeb nebo ochranu některých konkrétních právních vztahů nebo hodnot (ochrana dětí, ochrana spotřebitelů, přístup k datům pro třetí subjekty, transparentnost reklamy).

Digitálními akty lze rozumět zejména následující nařízení:

- **nařízení o digitálních trzích (Digital Markets Act, DMA), od 2. 5. 2023,¹²**
- **nařízení o digitálních službách (Digital Services Act, DSA), od 17. 2. 2024,¹³**
- **nařízení o datech (Data Act), od 12. 9. 2025,¹⁴**
- **akt o umělé inteligenci (AI Act), od 2. 8. 2026.¹⁵**

Nové digitální akty budou rovněž vyžadovat kontinuální zvyšování odbornosti pracovníků příslušných úřadů a rozsáhlou institucionální spolupráci mezi státními orgány a dalšími institucemi. Do této oblasti patří i spolupráce dozorových orgánů zabývajících se ochranou osobních údajů a hospodářské soutěže na evropské i vnitrostátní úrovni.

Nařízení o digitálních trzích – *spravedlivé trhy a data*

Akt o digitálních trzích cílí na velké online platformy označované jako „strážce přístupu“ a zavádí pro ně soubor ex ante povinností. Jeho účelem je zajistit spravedlivé otevřené digitální trhy a rovné podmínky, aby žádná dominantní platforma nezneužila své postavení. DMA navíc výslovně zahrnuje i pravidla týkající se nakládání s uživatelskými daty, čímž propojuje soutěžní a datovou problematiku. Platformy,

⁹ Čl. 8 Listiny, úřední věstník C 202, 7.6.2016.

¹⁰ V ČR zejména zákonem č. 143/2001 Sb., o ochraně hospodářské soutěže a o změně některých zákonů (zákon o ochraně hospodářské soutěže, ZOHS), v EU čl. 101 a 102 SFEU.

¹¹ Čl. 38 Listiny; v politikách EU je obecně zajištěna vysoká úroveň ochrany spotřebitele.

¹² Nařízení EP a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích).

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

¹⁴ Nařízení EP a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (nařízení o datech).

¹⁵ Nařízení EP a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

tzv. gatekeeperi, například **nesmí kombinovat osobní údaje o uživatelích z různých svých služeb nebo od třetích stran, pokud k tomu nezískají souhlas uživatele**.¹⁶ Zákaz má zabránit dominantním firmám propojovat data z více zdrojů (např. ze své sociální sítě, messengeru a dalších aplikací) a získávat tak konkurenční výhodu na úkor soukromí uživatelů. DMA doplňuje požadavky GDPR, když u gatekeeperů de facto zpřísňuje podmínky pro zpracování dat, díky čemuž přenechává jejich reálnou kontrolu uživatelům.¹⁷

DMA dále gatekeeperům ukládá povinnosti podporující **interoperabilitu a datovou otevřenost**.¹⁸ Gatekeeperi musí umožnit propojení svých služeb s nabídkami konkurence (např. interoperabilita komunikačních služeb), aby uživatelé nebyli nuceni využívat pouze jednu platformu. Také musí zajistit **přenositelnost dat** (data portability)¹⁹ spočívající v umožnění uživateli snadno přenést svá data k jiné službě. K tomu patří i povinnost poskytnout reálný přístup k uživatelským datům třetím stranám (např. obchodním uživatelům platformy), a to průběžně a v reálném čase. Tato opatření mají **omezit uzamykání uživatelů u dominantních platform** tím, že usnadňují přechod ke konkurenci a podporují soutěž při současném zachování kontroly uživatele nad osobními údaji. DMA tedy reprezentuje nový model regulace digitálních monopolů, spojuje antimonopolní cíle (férová soutěž) s prvky ochrany soukromí (např. souhlas se zpracováním dat, transparentnost profilování). Nenahrazuje klasické soutěžní právo, ale doplňuje jej a stanovuje pro gatekeepery jasná pravidla ex ante.²⁰

Vedle evropského DMA vznikají v některých členských státech paralelní národní nástroje zaměřené na regulaci digitálních platform. Nejvýznamnějším příkladem je **ustanovení § 19a německého soutěžního zákona (GWB)**, platné již od roku 2021, které se stalo inspirací i pro unijní regulaci DMA. Ustanovení § 19a GWB umožňuje Spolkovému kartelovému úřadu (Bundeskartellamt) označit podnik jako subjekt s „významným postavením napříč trhy“. Nejedná se o koncept srovnatelný s dominantním postavením, ale o zvláštní kategorii silné digitální firmy, která má prostřednictvím svých služeb zásadní dopad na hospodářskou soutěž i mimo konkrétní trh, na němž operuje. Pokud je firma tímto způsobem označena (§ 19a odst. 1 GWB), může jí úřad zakázat konkrétní praktiky, které považuje za škodlivé pro soutěž (§ 19a odst. 2 GWB), např. sebeupřednostňování vlastních služeb, vázání služeb (bundling), zneužívání datové dominance (např. odepření přístupu k datům třetím stranám), omezování interoperability nebo přenositelnosti dat, vynucování souhlasu se zpracováním údajů bez reálné alternativy. Po zavedení daného ustanovení se německý úřad nejdříve zaměřil na firmy jako Google, Amazon, Meta, Apple a Microsoft a formálně je vymezil jako subjekty podléhající § 19a GWB. Tento přístup umožňuje rychlejší a flexibilnější zásah než klasické ex post nástroje podle čl. 102 SFEU. Rozhodnutí podle § 19a GWB podléhají soudnímu přezkumu, což vede k cenné praxi pro celý prostor EU.

Nařízení o digitálních službách – bezpečnější online prostor a data

Akt o digitálních službách se zaměřuje na regulaci obsahu a uživatelského prostředí při poskytování digitálních služeb na online platformách. Jeho hlavním cílem je zvýšit bezpečnost online prostředí, transparentnost algoritmů a odpovědnost platform za obsah (boj proti nelegálnímu obsahu, dezinformacím apod.). DSA obsahuje i prvky týkající se ochrany dat a soukromí, které nepřímo ovlivňují tržní prostředí, například **zakazuje cílenou reklamu mířenou na děti** (nezletilé uživatele) nebo využívání citlivých osobních údajů (o etnicitě, politických názorech, zdravotním stavu apod.) pro účely profilování reklam. Velké platformy také musí umožnit uživatelům **vypnout personalizované algoritmické doporučování obsahu**. Uživatel má tedy právo zvolit si neuspořádaný feed bez profilování.²¹

16 Čl. 5 DMA.

17 Více na: <https://usercentrics.com/knowledge-hub/digital-markets-act-dma-impacts-user-privacy-and-consent-management/#:~:text=For%20these%20companies%2C%20the%20DMA,that%20align%20with%20DMA%20regulations.>

18 Čl. 7 DMA.

19 Čl. 6 DMA a také čl. 20 GDPR.

20 Již v prvním roce účinnosti došlo k jejich vymáhání. Komise např. v dubnu 2025 uložila společnosti Meta (Facebook) pokutu za neumožnění svým uživatelům vybrat si službu s menším rozsahem zpracování osobních dat, čímž porušila DMA.

21 K dopadu DSA na digitální platformy více na: <https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms#:~:text=The%20DSA%20bans%20targeted%20advertisement,old%20to%20private%20by%20default.>

Taková opatření posilují informační autonomii uživatelů a ochranu jejich soukromí. Nepřímo mohou mít dopad i na soutěž, neboť zpřísnění pravidel pro cílenou reklamu se promítá i do fungování hráčů, kteří staví svůj obchodní model na masivním sledování uživatelů. DSA tak doplňuje DMA v tom smyslu, že klade důraz na uživatelská práva v digitálním prostředí, včetně aspektu ochrany osobních údajů a důvěry uživatelů v online služby. Kombinace DMA a DSA představuje komplexní přístup, kdy DMA kontroluje tržní sílu velkých platform a DSA cílí na jejich společenskou odpovědnost a uživatelská práva.

Nařízení o datech – sdílení dat pro inovace vs. soukromí

Nařízení o datech představuje novou regulaci zaměřenou na otevření přístupu k datům v ekonomice. Cílem je podpořit inovace a soutěž tím, že data nebudou koncentrována u jednoho poskytovatele služby. Nařízení o datech **poskytuje uživatelům právo získat data, která generují, a sdílet je s třetí stranou podle své volby**. To má např. **zamezit lock-in efektu**, kdy uživatel nemůže přejít ke konkurenci, protože jeho data zůstávají u původního dodavatele.

Z pohledu soutěže se jedná o prolomení datového uzavření a snížení bariér vstupu pro nové hráče. Zároveň však nařízení o datech respektuje ochranu osobních údajů. Výslovně stanoví, že právo na sdílení dat nesmí být na újmu práv subjektů údajů podle GDPR.²² Jinými slovy, pokud sdílená data obsahují osobní údaje, správce musí zajistit jejich zpracování v souladu s GDPR. V praxi to znamená, že firmy musí při sdílení dat zajistit anonymizaci nebo mít právní důvod podle GDPR (souhlas, smlouvu apod.).

Nařízení o datech představuje kompromis mezi snahou odemknout hodnotu dat pro ekonomiku a potřebou chránit soukromí jednotlivců. V ideálním případě by měl přinést více datové mobility, což by se pozitivně promítlo do kvality soutěže (uživatel či firma budou moci snadněji měnit poskytovatele), a současně by měl ponechat pevné záruky pro ochranu osobních údajů.

Akt o umělé inteligenci – důvěra v AI a tržní rovnováha

Akt o umělé inteligenci, přijatý v roce 2024, představuje první **komplexní právní rámec pro AI systémy**.²³ Primárně se zabývá regulací rizikových aplikací, aby AI systémy byly bezpečné, důvěryhodné a respektovaly základní práva a hodnoty (včetně ochrany soukromí, zákazu diskriminace apod.). AI Act zavádí kategorii vysoce rizikových AI systémů, pro které stanoví přísné požadavky (posouzení rizik, dokumentace, dohled, transparentnost). Například AI systémy používané k vyhodnocování osob (v zaměstnání, ve finančních službách atd.) musí splňovat kritéria minimalizace zaujatosti a ochrany dat. Ochrana osobních údajů je zde zahrnuta pod podmínkou, že AI musí být vyvíjena a nasazována v souladu s GDPR (např. tréninkové datasey nesmí být získány v rozporu s právem na ochranu osobních údajů a soukromí).

V kontextu hospodářské soutěže AI Act nepůsobí přímo jako antimonopolní nástroj, ale nepřímo ovlivňuje soutěž **nastavováním rovné povinnosti pro všechny vývojáře a uživatele AI technologií**. Velcí hráči disponující obrovskými datovými zdroji a výpočetním výkonem budou těmito pravidly vázáni stejně jako menší subjekty. Navíc požadavek na transparentnost určitých AI systémů (např. povinnost označit obsah generovaný AI nebo poskytnout vysvětlení u rozhodování AI) zvyšuje důvěru uživatelů. Tím AI Act podporuje férové prostředí, kde soutěž probíhá v mantinelech respektujících práva občanů.

22 Čl. 1 bod 5 Nařízení a datech.

23 Více na: https://www.edps.europa.eu/artificial-intelligence/artificial-intelligence-act_en#:~:text=The%20Artificial%20Intelligence%20Act%20entered,risks%20of%20powerful%20AI%20models.

Průnik mezi hospodářskou soutěží a ochranou osobních údajů

Ochranu osobních údajů a hospodářskou soutěž již nelze vnímat odděleně. Obě oblasti jsou nezbytné pro fungování férové, inovativní a důvěryhodné digitální společnosti. Evropská unie proto upřednostňuje integrovaný přístup, kdy nové právní rámce pro digitální trhy spojují soutěžní regulaci s ochranou dat, aby se navzájem podporovaly. Soutěžní politika chrání trh před monopolním zneužíváním (například datovou nadvládou), zatímco právo na ochranu údajů poskytuje ochranu jednotlivcům před ztrátou soukromí a zvyšuje důvěru v digitální služby. Podle Evropského inspektora ochrany údajů je spolupráce mezi jednotlivými institucemi v oblasti ochrany dat, hospodářské soutěže a práv spotřebitelů klíčová pro zajištění funkčního vnitřního trhu i blaha spotřebitelů.

Hospodářská soutěž z pohledu ochrany dat

Pohled ochrany osobních údajů na hospodářskou soutěž vychází z jejího uznání jako nástroje regulace trhu, jehož produkty či služby jsou často založeny na zpracování dat. Společnou **oblast zájmu zjevně představují data**, která se v digitální ekonomice stala základem mnoha obchodních modelů. Data mohou představovat obecně osobní i neosobní údaje, ale i data anonymizovaná, pseudonymizovaná či syntetická. Vztah ochrany osobních údajů a hospodářské soutěže dosud nebyl dostatečně zkoumán, není tedy přesně vymezen. Lze předpokládat, že v digitální ekonomice založené na datech je tento vztah složitý, má více různých podob a rozměrů. Jak obecně, tak v konkrétních případech by mělo být vzájemné působení nadále zkoumáno či analyzováno.

Pokud jde o **společný prvek obou oblastí**, z pohledu ochrany osobních údajů lze vyjít ze zaměření právního rámce ochrany osobních údajů na ochranu jednotlivce v digitálním světě. Tento cíl se zdá být zásadně odlišný od cíle, který sleduje právní rámec hospodářské soutěže, což je primárně systémová ochrana soutěže na trhu, obvykle prostřednictvím kontroly spojování podniků, zákazu zneužití dominantního postavení a protisoutěžních dohod. Nicméně hospodářská soutěž v konečném důsledku sleduje rovněž ochranu zájmu jednotlivce v postavení spotřebitele, a to z pohledu podpory jeho blahobytu, především v podobě nižší ceny a možnosti volby produktu či služby na trhu. I osobní údaje se stávají faktorem odrážejícím kvalitu hospodářské soutěže, a je proto třeba brát v úvahu instituty ochrany osobních údajů i v kontextu jejího fungování.

V rámci hospodářské soutěže se primárně zkoumají parametry jako relevantní trh či postavení soutěžitelů na trhu (jejich tržní síla), do této kategorie lze však nyní zařadit i zpracování osobních údajů. Například relevantní trh, jako výchozí základ pro stanovení dominance a jejího možného zneužití, může být určen pro produkty, systémy či služby založené na zpracování dat, které mohou mít podobu osobních či neosobních údajů. K osobním údajům mohou soutěžitelé rovněž přistupovat různě, což vytváří prostor pro hodnocení stavu hospodářské soutěže. Dále, pokud je soutěžitel v dominantním postavení, spotřebiteli může být odepřena možnost alternativní volby v souladu s ochranou osobních údajů. Rovněž spojování podniků uskutečňující se mezi subjekty, jejichž podnikatelská činnost je založena na zpracování velkého objemu dat včetně osobních údajů, zahrnuje otázky osobních údajů.

Mezi hospodářskou soutěží a osobními údaji může existovat řada společných prvků, např. povinnost strážce přístupu dle DMA zajistit přenositelnost dat, usnadnění změny poskytovatele či poskytnutí bezplatného přístupu k datům. Také nařízení o spravedlivých trzích uvádí některé příklady datových propojení, k nimž je potřebné přistoupit z pohledu ochrany osobních údajů. Vhodným opatřením může být podle nařízení anonymizace dat, ochrana osobních údajů konečných uživatelů proti re-identifikaci, zveřejňování a uplatňování všeobecných podmínek přístupu či nestranný a nezávislý mechanismus řešení sporů zavedený v EU. Při nabídce konkurenčních služeb v daném oboru podnikání může být pro spotřebitele

podstatné, zda jsou data zpracovávána v souladu s pravidly ochrany osobních údajů, či nikoliv. V tomto ohledu například uživatele v poslední době zajímá, zda je v souladu s pravidly ochrany osobních údajů použití modelu *consent or pay*.

Praxe **consent or pay** vyvolává aktuální otázky ochrany osobních údajů řešené ve více členských státech EU. Jedná se o to, že v evropském online prostoru se lze často u služeb či webových stránek setkat se zaváděním binárního modelu souhlasu se zpracováním dat *consent or pay*. Model spočívá v tom, že uživatel nemůže použít službu, pokud nezvolí jednu z variant „zaplatit nebo poskytni souhlas“. Ve skutečnosti má subjekt údajů pouze možnost zaplatit poplatek za službu bez shromažďování osobních údajů nebo získat přístup zdarma včetně souhlasu s behaviorální reklamou, kdy poskytuje osobní údaje.

Sbor k této otázce vydal stanovisko,²⁴ v němž uvedl, že ve velké většině případů nebude možné, aby velké online platformy splňovaly požadavky na platný souhlas, pokud uživatelům umožňují výběr pouze mezi výše zmíněnými dvěma variantami. Zdůvodnil, že osobní údaje nelze považovat za obchodovatelnou komoditu. Velké online platformy by proto měly mít na paměti, že je třeba zabránit, aby se základní právo na ochranu osobních údajů přeměnilo na prvek, který musí uživatel zaplatit. Naopak se doporučuje, aby velké online firmy zvážily alternativu služby bez behaviorální reklamy, která by představovala skutečnou variantu pro uživatele.

Ochrana osobních dat z pohledu hospodářské soutěže

Digitální ekonomika posledního desetiletí ukazuje zásadní propojení mezi osobními údaji a hospodářskou soutěží. Osobní data se stala cenným aktivem, které firmám umožňuje inovovat služby, cílit reklamu a budovat tržní sílu. Právo hospodářské soutěže a právo na ochranu osobních údajů přitom tradičně sledují odlišné cíle. První zajišťuje konkurenční prostředí, druhé chrání soukromí jednotlivců. Do jaké míry se však tyto oblasti prolínají? Pomáhají si (synergie), nebo se spíše nacházejí v konfliktním postavení?

Úroveň ochrany soukromí se postupně stává součástí **parametrů kvality**.²⁵ Vedle ceny, inovací či rozsahu služeb mohou podniky přitahovat spotřebitele i lepší ochranou jejich dat. **Komise v posledních letech uznala, že parametr soukromí může hrát roli v soutěžním hodnocení, pokud jej spotřebitelé považují za podstatný.** Komise například ve svém rozhodnutí Microsoft/LinkedIn (2016) konstatovala, že soukromí představuje významný faktor kvality na trhu profesních sociálních sítí.²⁶ Obdobně již dříve Federální obchodní komise (FTC) v USA připustila, že spojení firem může ovlivnit *necenové soutěžní parametry, jako je soukromí spotřebitelů*. Změna úhlu pohledu uvedených institucí signalizuje, že ochrana dat není vnímána jen jako regulační povinnost, ale i jako prvek konkurenčního boje. Firmy soupeří o důvěru uživatelů a jejich údaje, přičemž silnější ochrana může představovat konkurenční výhodu.

Přístup Komise k otázce vztahu hospodářské soutěže a soukromí se neustále vyvíjí, což ilustrují i dvě významné akvizice **Facebook/WhatsApp**²⁷ a **Microsoft/LinkedIn**²⁸. Námitky v případě Facebook/WhatsApp z roku 2014 se zakládaly zejména na argumentaci, že koncentrace dat v rukou Facebooku vede k nižší ochraně soukromých dat uživatelů. Komise však v té době hodnotila parametr soukromí odděleně a dospěla k závěru, že obavy z koncentrace dat týkající se ochrany soukromí spadají pod právo na ochranu osobních údajů, nikoliv soutěžní právo.²⁹ Soukromí tedy považovala za „vnější“ faktor nespádající do rámce soutěžního posouzení. Obecně se domnívala, že si uživatelé komunikační aplikace vybírají hlavně podle ceny,

24 Stanovisko 08/2024 k platnému souhlasu v souvislosti s modely „souhlas nebo platba“ zavedenými velkými online platformami dostupné na: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_cs.

25 Více na: <https://www.twobirds.com/en/insights/2019/global/the-interplay-of-data-protection-and-competition-law-issues-beyond-the-facebook-case>.

26 Více na: <https://www.jdsupra.com/legalnews/big-data-an-ongoing-concern-for-eu-57817/>.

27 Rozhodnutí Komise ze dne 3. 10. 2014 COMP/M.7217 Facebook/WhatsApp.

28 Rozhodnutí Komise ze dne 6. 12. 2016 M.8124 Microsoft/LinkedIn.

29 Rozhodnutí Komise ze dne 3. 10. 2014 COMP/M.7217 Facebook/WhatsApp, bod 164: „Pro účely tohoto rozhodnutí Komise analyzovala potenciální koncentraci dat pouze v rozsahu, v jakém pravděpodobně posílí postavení Facebooku na trhu online reklamy nebo v jeho dílčích segmentech. Veškeré obavy týkající se ochrany soukromí, které vyplývají ze zvýšené koncentrace dat pod kontrolou Facebooku v důsledku transakce, nespádají do působnosti pravidel EU o hospodářské soutěži, ale do působnosti pravidel EU o ochraně osobních údajů.“

funkcí a sítě přátel, nikoliv primárně podle zásad soukromí. O dva roky později ve věci Microsoft/LinkedIn však uznala, že uživatelé profesních sítí, jako např. LinkedIn, kladou na ochranu dat důraz, a shledala, že by se posuzovaná fúze mohla negativně promítnout do kvality služby z hlediska soukromí.³⁰ Komise konkrétně uvedla, že úroveň ochrany osobních údajů je důležitým konkurenčním parametrem mezi LinkedIn a konkurenčními sítěmi a mohla by být koncentrací dotčena. **Změna přístupu umožnila zohlednit i parametr soukromí při posuzování spojení soutěžitelů, díky čemuž bylo spojení soutěžitelů schváleno s podmínkami včetně ochrany dat uživatelů.**

Vývoj doktríny v akademické literatuře

Obdobný vývoj lze pozorovat i v akademické sféře. Řada autorů (Costa-Cabral, Lynskey aj.)³¹ v letech 2014–2016 kritizovala striktní oddělení obou problematik a považovala za nezbytné vnímat soutěž i v oblasti ochrany dat. Před rokem 2015 bylo nahlíženo na soutěžní právo a právo na ochranu soukromí jako na dvě zcela odlišné oblasti s napjatým vztahem, rozdílnými cíli i nástroji, a nejevilo se žádoucí je jakkoliv propojovat (**tzv. privacy-antitrust paradox**).

S rozvojem digitálních platforem se však rozšířil koncept spotřebitelského blahobytu o kvalitativní faktory. Dnes již četné publikace zdůrazňují komplementaritu soutěžní a datové regulace, obě mají chránit spotřebitele před vykořisťováním (soutěžní právo před ekonomickým, koncept soukromí před právním zneužitím informací). Např. OECD v roce 2020/2021 pořádala kulatý stůl k průsečíku hospodářské soutěže a soukromí a konstatovala, že předmětné oblasti se mohou vzájemně posilovat, ale je potřeba hledat koherentní přístup. Evropská literatura³² se zaměřuje i na synergii a limity integrace. Jedním z častých závěrů je, že právo na ochranu osobních údajů může posílit hospodářskou soutěž tím, že poskytuje uživatelům kontrolu (např. právo na přenositelnost dat z GDPR usnadňuje přechod ke konkurenci), zatímco soutěžní právo chrání prostředí, kde si firmy konkurují i kvalitou zacházení s daty.

Na druhou stranu, nebudou-li role mezi institucemi jasně rozděleny, hrozí duplicitní nebo chaotické vymáhání. Soutěžní úřady by problematiku soukromí měly brát v úvahu tam, kde ovlivňuje parametry hospodářské soutěže nebo je prostředkem možného zneužití dominantního postavení,³³ a v případě složitějších otázek GDPR by měly spolupracovat s úřady na ochranu osobních údajů. Soutěžní úřady tedy nesmí ignorovat kontext GDPR, zároveň však musí respektovat kompetence a rozhodnutí úřadů pro ochranu osobních údajů. Tím se vytváří rámec, v němž obě složky práva spolupracují pro dosažení celkového cíle, férových trhů s respektem k právům spotřebitelů a ochraně osobních údajů.

30 Rozhodnutí Komise ze dne 6. 12. 2016 M.8124 Microsoft/LinkedIn, bod 253.

31 Cate, Fred H.; Kuner, Christopher; Millard, Christopher; Svantesson, Dan Jerker B. a Lynskey, Orla, „When Two Worlds Collide: The Interface Between Competition Law and Data Protection“ (2014). Articles by Maurer Faculty. 2623; Costa-Cabral, Francisco a Lynskey, Orla, „The Internal and External Constraints of Data Protection on Competition Law in the EU“ (2015). LSE Law, Society & Economy Working Paper 25/2015.

32 Např. Costa-Cabral, Francisco a Lynskey, Orla, „Family ties: the intersection between data protection and competition in EU law“ (2017). Common Market Law Review; Kellerbauer, Manuel; Klamert, Marcus a Tomkin, Jonathan, „The EU Treaties and the Charter of Fundamental Rights: A Commentary (2019; recenze/odkazy z roku 2021; aktuálně 2. vyd. 2024).

33 Obdobný postup nastínil generální advokát Rantos a potvrdil jej i Soudní dvůr Evropské unie (SDEU) v případě Facebook. Dostupné na: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:62021CC0252>.

Synergické aspekty spolupráce správních orgánů

V návaznosti na velmi rychlý rozvoj technologií založených na datech, které přímo či nepřímo ovlivňují hospodářskou soutěž, získal vztah ochrany hospodářské soutěže a ochrany osobních údajů nový potenciál a stal se předmětem diskuse. Důvodem je nezbytnost komplexního posouzení provázanosti předmětných oblastí, kterou právní rámec ochrany hospodářské soutěže a osobních údajů samostatně neposkytují.

Za „bod zvratu“ od původně tradičně odděleného vnímání obou oblastí lze považovat rozsudek SDEU ve věci C-252/21 **Meta Platforms vs. Bundeskartellamt**,³⁴ kterému nicméně v EU předcházela diskuse o vzájemném vztahu hospodářské soutěže a ochrany osobních údajů. Ve věci byl veden spor mezi společností Meta Platforms a německým Bundeskartellamtem, zda je možné, aby Bundeskartellamt samostatně posoudil otázku ochrany osobních údajů.

Bundeskartellamt v únoru 2019 rozhodl, že Facebook zneužil dominantního postavení podmiňováním užívání své sociální sítě téměř neomezeným sběrem osobních dat uživatelů ze svých platform (Facebook, WhatsApp, Instagram) a jejich kombinováním z webů třetích stran.³⁵ Pokud chtěl uživatel používat Facebook, musel akceptovat takto nastavené podmínky. Bundeskartellamt považoval takové obchodní podmínky za porušující evropské zásady ochrany osobních údajů, zejména z důvodu nedostatku svobodného souhlasu dle GDPR, a dospěl k závěru, že představují zneužití dominance ve formě vykořisťujících podmínek.

Předmětné rozhodnutí nakonec vedlo k propojení hospodářské soutěže a ochrany osobních údajů. Porušení pravidel GDPR se stalo elementem při posuzování protisoutěžního jednání. Bundeskartellamt umožnil společnosti Facebook slučovat data z různých zdrojů pouze na základě dobrovolného souhlasu uživatelů. Tento inovativní přístup byl zpočátku diskutabilní, případem Facebook se proto zabývaly soudy v Německu i SDEU.

Předkladatel předběžné otázky Oberlandesgericht Düsseldorf se dotázal SDEU, zda orgán posuzující hospodářskou soutěž může v rámci posuzování, jestli došlo ke zneužití dominantního postavení ze strany podniku, konstatovat, že všeobecné podmínky provozování služby nejsou v souladu s právním rámcem GDPR. SDEU na otázku odpověděl kladně, tj. že Bundeskartellamt byl oprávněn otázku posoudit, čímž nabídl možnost širšího posuzování vzájemného vztahu hospodářské soutěže a ochrany osobních údajů.

Rovněž digitální akty, reagující na rozvoj digitálních produktů a služeb, předpokládají využití širší institucionální spolupráce dotčených orgánů. Digitální akty by tedy neměly být vnímány izolovaně, ale naopak poskytovat prostor pro vzájemnou spolupráci orgánů, která nemusí být předem přesně vymezena a vyplývat z praxe. Důvodem je potřeba chápat vztahy a jevy v digitální společnosti z různých pohledů. Základním východiskem pro tento přístup je komplexnost technologií a hledání rovnováhy mezi možnostmi a podporou jejich širokého využívání a eliminací možných rizik. Tento přístup je již rozvíjen v pokynech Sboru zaměřujících se na souhru relevantních aktů a ochrany osobních údajů. Prozatím byla zvažována koordinace mezi ochranou osobních údajů a aktem o digitálních službách, případně souhra osobních údajů s umělou inteligencí.

Společné posouzení cílů ochrany dat, soukromí a hospodářské soutěže

Spolupráce mezi úřady na ochranu osobních údajů a pro hospodářskou soutěž je v rozsudku Bundeskartellamtu popsána v podobě **tzv. loajální spolupráce** zakotvené v čl. 4 odst. 3 Smlouvy o EU. Podle této zásady a podle ustálené judikatury se v oblastech spadajících do unijního práva musí členské státy, včetně jejich správních orgánů, vzájemně respektovat a pomáhat si při plnění úkolů vyplývajících ze Smluv, přijímat veškerá vhodná opatření k plnění závazků, vyplývajících zejména z aktů orgánů EU, a zdržet se všech opatření, jež by mohla ohrozit dosažení cílů.³⁶

34 Rozsudek SDEU (velkého senátu) C-252/21 ve věci Meta Platforms vs Bundeskartellamt ze dne 4. července 2023.

35 Více na: <https://www.hausfeld.com/en-us/what-we-think/competition-bulletin/data-exploiting-as-an-abuse-of-dominance-the-german-facebook-decision/>.

36 Podle zásady loajální spolupráce se EU a členské státy navzájem respektují a pomáhají si při plnění úkolů vyplývajících ze Smluv.

Právě tento druh spolupráce může za předpokladu spojení odborných poznatků přinést synergický efekt. Nenastane však automaticky, ale jeho předpokladem je věcně správné propojení dotčených oblastí. Spolupráce obou úřadů tedy předpokládá činnost odborníků schopných rozvíjet, spojovat a aktualizovat poznatky příslušných oblastí. Za určitých okolností se přitom nemá jednat o fakultativní spolupráci, nýbrž o obligatorní. Z rozsudku SDEU ve věci C-252/21 vyplývá, že se může jednat například o situace, kdy soutěžní orgán potřebuje posoudit soulad zpracování s GDPR a musí své kroky sladit s příslušným dozorovým orgánem (příp. vedoucím dozorovým úřadem), aby byla zajištěna konzistence aplikace a výkladu GDPR.³⁷

Společné posouzení ochrany dat a hospodářské soutěže však nelze chápat jako určitý druh procesně společného řízení. Oba úřady vykonávají odlišné funkce, sledují rozdílné cíle a budou nadále plnit úkoly, k nimž byly zřízeny. Rovněž může nastat situace, kdy posuzující orgán bude mít dostatek informací k provedení samostatného posouzení, jak tomu bylo ve věci Bundeskartellamt. Soutěžní orgán například v praxi povede řízení, v jehož rámci narazí na otázku spadající do oblasti ochrany soukromí, tj. jiné oblasti, než ve které vykonává pravomoc. Obrátí se proto na příslušný orgán, úřad na ochranu osobních údajů, který by ji měl analyzovat, posoudit a své stanovisko poskytnout soutěžnímu orgánu. Variant spolupráce však může být více, jak vyplývá i z rozsudku C-252/21. V úvahu dále připadá například pokračování soutěžního orgánu ve vlastním šetření, neodpoví-li dozorový úřad v přiměřené lhůtě na vyžádání stanoviska, nebo pouhé oznámení jeho zamýšlených kroků s možností podat námitky ze strany úřadu pro ochranu osobních údajů apod.

V praxi takovou spolupráci vidíme například ve Velké Británii, kde **britský soutěžní úřad (CMA) a Úřad pro ochranu údajů (ICO)** posuzovaly plán společnosti Google týkající se **omezení cookies v prohlížeči Chrome** (projekt „Privacy Sandbox“). CMA řešil obavu, aby Google nezneužil změny k posílení své tržní síly v online reklamě, zatímco ICO dohlížel na zachování přínosu pro soukromí uživatelů. Výsledkem byly dobrovolné závazky Googlu upravující design nové technologie, aby respektovala soutěž i ochranu soukromí. Google se zavázal k transparentnímu vývoji za dohledu CMA a konzultacím s ICO, který tento postup uvítal s tím, že spotřebitelé mají prospěch ze společného posuzování cílů v oblasti ochrany dat, soukromí a hospodářské soutěže.³⁸

Dalším příkladem může být zavádění funkce **App Tracking Transparency (ATT) v iOS** (opatření společnosti Apple ve prospěch ochrany soukromí), kdy si **francouzský soutěžní úřad** (Autorité de la concurrence, ADLC) **vyžádal stanovisko Úřadu pro ochranu osobních údajů** (CNIL). Stěžovatelé (zejména firmy z reklamního odvětví) argumentovali znevýhodňováním konkurence ze strany společnosti Apple, ADLC však dospěl k závěru, že dané opatření má legitimní cíl v ochraně soukromí uživatelů a zásah soutěžního orgánu není namístě.³⁹ Francouzský případ ukazuje, že pro posouzení údajného omezování soutěže je relevantní i pro-soukromá motivace. Soutěžní právo tedy nemá bránit opatřením přispívajícím k ochraně dat uživatelů, pokud jsou v souladu se soutěžními pravidly.

Jak ukazují uvedené případy, řada soutěžních orgánů zohledňuje v rámci vymáhání soutěžního práva v nějaké podobě aspekt týkající se ochrany osobních údajů, a to například tím, že si vyžádá stanoviska od úřadu na ochranu osobních údajů a v odůvodnění rozhodnutí na něj následně odkáže. SDEU v této souvislosti rovněž zdůraznil⁴⁰, že soutěžní úřad není přímo příslušný sankcionovat porušení GDPR (to náleží primárně úřadům na ochranu údajů), ale může soulad jednání s GDPR považovat za vodítko při posuzování protisoutěžního jednání.

Rozhodnutí SDEU tedy potvrdilo, že soutěžní orgány mohou chránit spotřebitele i proti excesům v oblasti nakládání s daty, zejména u soutěžitelů s dominantním postavením na digitálním trhu, avšak musejí přitom postupovat v souladu s právem na ochranu údajů a spolupracovat s příslušnými institucemi.

37 Rozsudek SDEU (velkého senátu) C-252/21 ve věci Meta Platforms vs Bundeskartellamt ze dne 4. července 2023, bod 54-55.

38 Více na: <https://techcrunch.com/2022/02/11/uks-cma-accepts-googles-post-cookie-pledges-will-closely-monitor-privacy-sandbox-plan/>.

39 Více na: <https://techcrunch.com/2022/09/20/facebook-superprofiling-cjeu-ag-opinion/>.

40 Rozsudek SDEU (velkého senátu) C-252/21 ve věci Meta Platforms vs Bundeskartellamt ze dne 4. července 2023.

Konfliktní situace – střety mezi soutěží a soukromím

Potenciálně může existovat řada střetů mezi hospodářskou soutěží a soukromím. Některé z nich lze pojmenovat, některé si však patrně dosud neumíme ani představit. Ze zkušeností v oblasti ochrany osobních údajů vyplývá, že varianty konkrétních možných situací budou mnohem širší a vždy je bude nutné posuzovat případ od případu. Níže jsou rozebrány hlavní scénáře konfliktu a zmíněny vybrané případy jejich řešení:

(A)

Přístup k osobním datům vs. jejich ochrana

Soutěžitelé požadují sdílení dat s cílem vyrovnat podmínky na trhu. Pokud dominantní firma disponuje unikátní databází uživatelských údajů, mohou konkurenti či nové firmy požadovat přístup k těmto datům jako k tzv. **essential facility**, tj. nezbytné infrastruktuře nutné pro působení na trhu i pro samotný vstup na něj. Soutěžní právo v určitých situacích skutečně ukládá dominantům povinnost zpřístupnit klíčové zdroje konkurentům za účelem předejití narušení hospodářské soutěže, avšak v případě osobních údajů naráží takový přístup na limity práva na soukromí. GDPR a další předpisy obecně zakazují sdílení osobních dat s třetími stranami bez právního důvodu, tj. bez souhlasu subjektu údajů nebo jiného zákonného titulu.

i Případ GDF Suez – Francie 2014: Francouzský soutěžní úřad (ADLC) se zabýval případem, kdy **dominantní dodavatel plynu GDF Suez odmítal poskytnout konkurentům přístup k databázi svých zákazníků** (jména, adresy, tel. čísla, údaje o spotřebě), jelikož se jednalo o informace chráněné zákonem o ochraně osobních údajů. **ADLC však uznal, že bez těchto dat nemohou alternativní dodavatelé efektivně oslovit zákazníky a soutěžit. Nařídil proto dodavateli GDF Suez sdílet uvedené údaje zákazníků s konkurenty za jasných podmínek chránících jejich soukromí.** Konkrétně musel GDF Suez své zákazníky předem informovat, že ostatní společnosti mohou žádat přístup k jejich údajům a umožnit jim vznést námitku (opt-out). Cílem daného řešení bylo zajistit fungování soutěže na trhu a zároveň respektovat právo zákazníků na kontrolu nad svými daty. ADCL spolupracoval při šetření případu GDF Suez s francouzským regulátorem pro ochranu dat. Oba úřady dospěly k závěru, že interoperabilita dat může být nařízena, pokud je dodržena podmínka informovanosti a vůle subjektů údajů.⁴¹

V obecné rovině tedy platí, že dominant nemůže zneužít GDPR jako univerzální obranu proti povinnosti sdílet data, je-li sdílení nezbytné pro efektivní hospodářskou soutěž. Úřady se musí snažit nalézat způsoby, jak obě povinnosti sladit, typicky prostřednictvím požadavku souhlasu, opt-outu, anonymizací aj. Za problematické lze považovat situace, kdy se sdílení dat s konkurencí provádí hromadně a individuální souhlasy představují časově náročnou aktivitu. Situaci lze demonstrovat na příkladu „chytrých“ (propojených) automobilů, u nichž se generuje velké množství technických i provozních dat o uživateli vozidla (styl jízdy, poloha, telemetrie apod.). Taková data mohou být dále využita celou řadou subjektů (servisy, pojišťovny, navigační aplikace), kdy samotné získání souhlasu majitele vozu pro každé jednotlivé sdílení dat se jeví nereálné. Komise se proto snaží nalézat vhodná legislativní řešení například v rámci iniciativy „Přístup k údajům, funkcím a zdrojům vozidla“⁴². V úvahu přichází používání buď anonymizovaných, či pseudonymizovaných dat, na která se GDPR nevztahuje, nebo méně přísně, případně zavedení zvláštní zákonné povinnosti ke zpřístupnění určitých dat odvětvově. Připravovaná regulace přístupu k datům z automobilů by měla stanovit, jakým způsobem mají výrobci zpřístupnit údaje třetím stranám.

41 Více na: <https://www.twobirds.com/en/insights/2019/global/the-interplay-of-data-protection-and-competition-law-issues-beyond-the-facebook-case>.

42 Více na: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Přístup-k-udajum-funkcim-a-zdrojum-vozidla/public-consultation_cs.

(B)**Dominance založená na datech vs. ochrana soukromí**

Osobní údaje mohou být zdrojem tržní síly, neboť firmy s přístupem k velkému množství uživatelských dat (tzv. big data) mohou lépe zacílit své služby, zdokonalovat AI algoritmy i zvyšovat míru lock-in efektu uživatelů ve svém ekosystému. Soutěžní úřady se proto zabývají i otázkou, zda samotné disponování datovými soubory nepředstavuje bariéry vstupu na trh či jej nelze zařadit mezi faktory určující dominantní postavení soutěžitelů. Při následných úvahách o případném omezení tohoto typu dominance v podobě např. zpřístupnění dat menším hráčům však nelze opomínat právo na soukromí a ochranu osobních údajů uživatelů.

i Příklad fúze – Google/Fitbit: V roce 2020 oznámila společnost Google akvizici výrobce chytrých fitness náramků Fitbit. **Při posuzování fúze se objevily obavy, že Google získá citlivá zdravotní a lokalizační data milionů uživatelů, což posílí jeho postavení v online reklamě i v dalších oblastech. Google se proto zavázal, že zdravotní data z Fitbit nevyužije pro cílenou reklamu a datové soubory bude uchovávat odděleně.**

Případ poukázal na potenciální konflikt mezi oblastí soutěžního práva a ochrany osobních údajů. Ačkoliv fúze nemusela z čistě soutěžního hlediska vzbuzovat významné pochybnosti, z hlediska koncentrace osobních dat se jevila problematická. Do budoucna lze očekávat, že u tzv. spojení založených na datech (data-driven mergers) budou soutěžní úřady svůj postup více koordinovat s orgány pro ochranu údajů a dopady spojení na spotřebitele tak budou hodnoceny komplexněji. Evropský inspektor ochrany údajů (EDPS) v návaznosti na potřebu spolupráce mezi uvedenými subjekty doporučil, aby přezkum datových spojení zahrnoval i analýzu jejich dopadů na oblast soukromí, a to jako součást posuzování vlivu na prospěch či zájmy spotřebitelů.⁴³

(C)**Inovace ve prospěch ochrany soukromí vs. soutěžní omezení**

Problematické mohou být i situace, kdy opatření na podporu soukromí konkrétního soutěžitele (např. změna pravidel nakládání s daty uživatelů) omezuje dosavadní obchodní modely a je konkurenty vnímáno jako zneužití dominance.

i Příklad omezení cookies (Privacy Sandbox): Společnost Google před několika lety slíbila, že v rámci svého prohlížeče Google Chrome ukončí podporu cookies třetích stran a nahradí je vlastním nástrojem, tzv. Privacy Sandbox, za účelem lepší ochrany soukromí uživatelů. Zvažovaný krok společnosti by měl dopad na celý online reklamní ekosystém. Zatímco uživatelské soukromí by podléhalo větší ochraně, menší ad-tech firmy varovaly, že Google tím posílí svou roli a získá konkurenční výhodu, neboť na rozdíl od menších firem disponuje vlastním prohlížečem Chrome s velkým tržním podílem a obrovskými finančními a technickými zdroji.

CMA situaci řešil preventivně a přijal **závazky** společnosti Google za účelem odstranění obav z narušení hospodářské soutěže vyplývajících z jeho šetření. **Společnost Google poté v dubnu 2025 oznámila, že nezavede nové samostatné upozornění pro soubory cookies třetích stran, a potvrdila svůj záměr nezrušit tyto soubory třetích stran.**

Iniciativy na ochranu soukromí ze strany soutěžitelů v dominantním postavení tedy mohou vzbuzovat rovněž otázky ohledně možného narušení hospodářské soutěže. Soutěžní úřady však proti nim zakročí pouze tehdy, pokud budou schopny narušit (i potenciálně) hospodářskou soutěž (např. eliminace konkurence apod.). Obecně platí, že pro-soutěžní interpretace GDPR je preferována. Každý soutěžitel, i ten dominantní, má plné právo zvyšovat úroveň ochrany dat nad rámec minima, neboť hospodářská soutěž probíhá i o důvěru spotřebitelů.

⁴³ Stanovisko EDPS zaměřené na problematiku ochrany osobních údajů, hospodářské soutěže a ochranu spotřebitele dostupné na: <https://www.insideprivacy.com/international/european-union/the-new-edps-opinion-privacy-and-competitiveness-in-the-age-of-big-data/>.

Naopak dohody firem o nesoutěžení v oblasti zásad ochrany soukromí nebo jakékoliv zneužívající praktiky dominantních soutěžitelů v podobě např. excesivního sběru dat či skrytých datových praktik by byly považovány za protisoutěžní a nezákonné. V digitálních ekosystémech se soukromí stává necenovým parametrem kvality. Zhoršení ochrany soukromí v důsledku omezení práv uživatelů v praxi zpravidla povede k posílení bariér vstupu. I výše popsany německý případ Meta/Facebook a následné předběžné rozhodnutí SDEU ve věci C-252/21 potvrzuje, že otázka zpracování osobních údajů je dnes vnímána jako významný parametr soutěže.

Případové studie a rozhodnutí

Pro ilustraci je níže uveden přehled klíčových kauz za uplynulé desetiletí, kde se protнула agenda ochrany dat a soutěžního práva:

Facebook/WhatsApp (EU, 2014) – fúze sociální sítě a komunikační aplikace: Komise ji schválila bez podmínek. Námitky ohledně koncentrace osobních dat odmítla s tím, že spadají do rámce ochrany soukromí, nikoliv hospodářské soutěže. Konstatovala, že i po spojení zůstane na trhu dost alternativ a WhatsApp v daném období nesbíral data k reklamním účelům.⁴⁴

Microsoft/LinkedIn (EU, 2016) – fúze profesní sítě s technologickým gigantom: Byla schválena s podmínkami. Komise zde výslovně uznala, že ochrana dat je významným parametrem kvality na trhu profesních sítí a že by mohla být ohrožena. Obávala se zejména, aby Microsoft nesloučil databáze a nezneužil údaje z LinkedIn pro posílení Windows/Office ekosystému. Podmínky zahrnovaly mimo jiné závazky k zachování API pro konkurenční sociální sítě a možnost uživatelů lépe kontrolovat data. Rozhodnutí Komise potvrdilo, že parametr soukromí může hrát roli v soutěžním hodnocení fúzí.

Německý případ Facebook (Bundeskartellamt, 2019) – zneužití dominance exploatací dat: Bundeskartellamt shledal, že Facebook zneužil monopol na trhu sociálních sítí vynucováním podmínek porušujících GDPR. Jednalo se o první soutěžní rozhodnutí, které definovalo porušení soukromí jako formu soutěžního deliktu (vykořisťující zneužití). Příkaz omezil Facebooku sběr dat bez souhlasu. Příklad vyvolal celoevropskou debatu, která vedla **k řízení o předběžné otázce u SDEU**. Unijní soud pak v roce 2023 potvrdil pravomoc soutěžních orgánů zohlednit aspekty soukromí a stanovil procedurální pravidla spolupráce s dozorovými orgány podle GDPR. Tento precedens představuje milník v integraci soutěžního a datového práva.

Google – případy „big data“ (EU, USA, 2007, 2020–2022): Google jako digitální gigant figuruje v řadě soutěžních kauz týkajících se dat. Již starší případ Google/DoubleClick (USA 2007) vztahující se ke spojení online reklamní firmy s Googlem vyvolal diskuse o dopadech na soukromí. Americký soutěžní úřad (Federal Trade Commission) sice fúzi schválil, ale ve svém rozhodnutí zmínil, že zkoumal i necenové dopady jako ochranu soukromí a neshledal v tomto případě soutěžní problém v oblasti kvality/privacy. Uvedl také, že nemá pravomoc ukládat podmínky nesouvisející přímo se soutěží a že obecné obavy o soukromí je vhodnější řešit sektorovou úpravou. V EU pak Google čelil třem velkým antitrustovým řízením (Shopping, Android, AdSense), která se týkala zneužití dominance jinými způsoby (upřednostňování služby, vázání aplikací, omezování konkurence v reklamě), otázka osobních dat v nich však nehrála přímou roli.

⁴⁴ O několik let později Facebook data s WhatsApp propojil, za což byl pokutován Komisí pro klamavé údaje v oznámení fúze, ale nešlo o přehodnocení soutěžního posouzení z roku 2014.

Apple ATT (Francie, 2021): ADLC odmítl vydat předběžné opatření proti pro-soukromé funkci ATT, čímž naznačil, že soutěžní zásah do prospěšného opatření na ochranu dat by musel být velmi opodstatněný. Případ rovněž potvrdil roli synergie mezi soutěžním právem a ochranou dat.

WhatsApp – změna podmínek (2021): Začátkem roku 2021 WhatsApp oznámil úpravu podmínek soukromí umožňující větší sdílení údajů s Facebookem. Indická komise pro hospodářskou soutěž (CCI) se v návaznosti na tento krok zabývala otázkou, zda WhatsApp nezneužívá svou tržní sílu a nedochází k výrazné kvalitativní degradaci služby (méně soukromí) vůči uživatelům bez reálné alternativy. Případ ukazuje ochotu postihovat exploataci uživatelů skrze zásahy do jejich soukromí i mimo Evropu. Podobně v Turecku soutěžní úřad v roce 2021 zakročil (byť dočasně) proti vynucování nových podmínek WhatsApp s odkazem na ochranu spotřebitelů. WhatsApp následně informoval turecký úřad pro hospodářskou soutěž, že nové podmínky pro sdílení uživatelských údajů se v Turecku nebudou uplatňovat.

Amazon a data o obchodnících (USA, 2022): Komise vedla se společností Amazon v letech 2020–2022 řízení o zneužití dominance. Amazon využíval neveřejná data od nezávislých prodejců na tržišti k prosperitě svých vlastních produktů. Jakkoli nejde o osobní údaje, je to paralelní problém, neboť data jako taková (obchodní informace) posloužila k narušení soutěže. Amazon se v závěru roku 2022 zavázal předmětnou praktiku omezit; postup byl schválen tzv. závazkovým rozhodnutím. Daný případ ilustruje, že „data power“ je pod drobnohledem soutěžních autorit. Na poli osobních údajů se Amazon dostal do sporu např. při akvizici iRobot (2022).

Závěr

V posledním desetiletí se vztah mezi ochranou osobních údajů a soutěžním právem posunul od téměř úplné separace k čím dál užšímu prolínání. **Synergické tendence lze zaznamenat v uznání parametru soukromí jako konkurenční výhody, kdy zhoršení ochrany dat může signalizovat snižování kvality pro spotřebitele.** Soutěžní orgány v EU proto začaly aktivně zohledňovat dopady na soukromí v rámci svých analýz (zejména u digitálních platforem), a to jak v případě kontroly spojování podniků, tak při posuzování zneužití dominance. Přibýlo také společných iniciativ mezi soutěžními regulátory a úřady na ochranu osobních údajů, což napomáhá k vytváření jednotného přístupu (případ Google/CMA/ICO, Apple/CNIL). Zároveň se vyvinuly nové legislativní nástroje (DMA, DSA a národní úpravy jako německé ustanovení § 19a GWB), které řeší datovou moc *ex ante* a snaží se nastavit pravidla, aby velcí hráči nemohli kombinovat či zneužívat data na úkor soutěže.

Stále však platí, že právo na soukromí může klást limit jinak žádoucímu sdílení informací pro konkurenci. Nadále je nezbytné nalézat legální cesty k vyvážení cílů v soutěžní oblasti a oblasti ochrany soukromí (jako např. souhlasy, anonymizace, regulatorní sandboxy). Rovněž soutěžní úřady musejí být schopny rozlišit jednání založená na snaze zlepšit podmínky ochrany soukromí pro uživatele ze strany dominantních soutěžitelů od jednání, u nichž argument soukromí slouží pouze k potlačení konkurence.

Dodržování GDPR se jednoznačně stává součástí **soutěžní compliance**. Ignorování pravidel ochrany dat může vést nejen k pokutám od orgánů ochrany osobních údajů, ale i k postihům ze strany soutěžních orgánů, pokud tím soutěžitel naruší hospodářskou soutěž a sníží tak úroveň spotřebitelského blahobytu. Naproti tomu kvalitní ochrana dat může sloužit i jako konkurenční výhoda vedoucí k odlišení se od konkurence a přilákání zákazníků.

Soutěžní a datová regulace jsou stále více vnímány jako součást širšího rámce ochrany spotřebitele a fungování trhů. Jak uvedl britský úřad pro ochranu osobních údajů, integrace těchto cílů vede k lepším výsledkům pro uživatele. Lze očekávat, že v budoucnu budou velké digitální platformy pod dvojitým dohledem, jakmile selže samoregulace, nastoupí koordinované vymáhání ze strany soutěžních i datových úřadů. Případy jako Facebook či Google nastavily precedens v tom smyslu, že digitální dominance a tok osobních dat představují spojené nádoby, které je třeba vnímat společně.

Synergie převládají tam, kde vedou k prospěchu spotřebitele (kvalitnější služby, větší kontrola nad daty, otevřenější trhy). Konflikty je třeba řešit případ od případu za použití principu proporcionality a vzájemné komunikace příslušných institucí. Vývoj v EU jasně směřuje ke komplexní regulaci digitálních platforem, která integruje soutěžní, datové i spotřebitelské požadavky, aby digitální ekonomika byla inovativní, férová a zároveň respektovala základní práva na soukromí.

Závěrem je třeba doporučit, aby společnosti, zejména velcí soutěžitelé disponující rozsáhlými daty o svých uživateli, vnímaly nejen potřebu ochrany osobních údajů, ale také principy hospodářské soutěže a měly v tomto ohledu kvalitně nastavený compliance program. To jim umožní předcházet porušení příslušných předpisů a vyhnout se tak hrozcím vysokým pokutám.

INFORMAČNÍ LIST 2/2025