STATI

Chytře protiprávní „chytré“ smlouvy Mezi efektivností smluvní agendy a zakódovanou protiprávností zejména v ochraně soutěže

Josef Bejček*

Abstrakt: Tzv. chytré smlouvy založené na softwarové technologii blockchainů se začínají prosazovat nejen ke zvýšení efektivnosti smluvní agendy, zejména ke zrychlení realizace práva a jako nespecifický nástroj právního zajištění, ale svými charakteristickými rysy svádějí i ke svému patologickému protiprávnímu použití. Mohou sloužit k pseudonymizaci (a v důsledku anonymizaci) právních vztahů, k nezákonným finančním operacím v rámci skupiny zúčastněných, ale mimo dohled veřejné moci, k zastřeným a zvnějšku obtížně kontrolovatelným a odhalitelným protiprávním jednáním. Jednu z akutních protiprávních aplikací chytrých smluv představuje jejich využití ke skryté kartelizaci, jež může podstatně snížit spotřebitelský blahobyt. Namístě je obezřetný právně-politický přístup čelící tomuto nebezpečí, který by však nezhatil kladný potenciál této nové technologie.

Klíčová slova: blockchain, chytré smlouvy, koluze, cenové algoritmy, hospodářská soutěž

Úvodem

V příspěvku rozebírám a komentuji vybrané aktuální souvislosti blockchainové technologie použité v tzv. chytrých smlouvách. Po popisu technické podstaty těchto jevů se věnuji otevřeným otázkám možného zneužití těchto technologií k tajným ujednáním ohrožujícím hospodářskou soutěž a zejména k automatizaci algoritmizované koluze.

Komentuji současné možnosti použití českého práva, s nimiž si musí vystačit při zvládání těchto výzev, a uvádím i některé zahraniční a evropské praktické i doktrinální přístupy. Je nadále zřejmé, že se v právu nevyhneme nutné reakci na tyto nové výzvy a že tzv. více ekonomický přístup v soutěžním právu se bude stále více obohacovat a doplňovat o přístup více technologický.

Paušalizace pohodlného normativního přístupu, na niž jsme si jako právníci uvykli v době industriální a postindustriální, bude v éře informatické zřejmě stále více ustupovat svědomitému zkoumání technické podstaty a jejího dopadu na právní vztahy, na hospodářskou soutěž a na blahobyt spotřebitelů v každém jednotlivém případě.[1]

* Prof. JUDr. Josef Bejček, CSc., katedra obchodního práva, Právnická fakulta Masarykovy univerzity v Brně. Podstatně rozšířená verze příspěvku předneseného na sympóziu Právo – Obchod – Ekonomika, Štrbské Pleso, 25. 10. 2019 a uveřejněného ve stejnojmenném sborníku [SUCHOŽA, J. – HUSÁR, J. – HUČKOVÁ, R. (ed.), UPJŠ v Košiciach, 2019] na s. 361–381.

1 PODSZUN, R. Kartellrecht in der Internet-Wirtschaft: Zeit für den more technological approach. *Wirtschaft und Wettbewerb*. 2014, Nr. 3, s. 1.

1. Podstata blockchainů a jejich vztah k tzv. chytrým smlouvám

1.1 Co je blockchain

Pro porozumění automatizaci a digitalizaci smluv je nutno znát pojem blockchainu, jenž se vyskytuje v posledních několika letech v odborných diskusích i mezi právníky, ač jejich podstatná část tápe v tom, co vlastně znamená. Jde o termín převzatý z oblasti IT, který se rozšířil a zdomácněl po celém světě tak rychle, že se v zájmu jednotnosti a srozumitelnosti ani nepřekládá.[2]

Blockchainy – přes svoji zdánlivou složitost a častou averzi netechnicky vzdělaných lidí při úvodním přiblížení se obsahu pojmu – umožňují zjednodušit každodenní právní agendu zejména rutinního a opakovaného charakteru, závislou na splnění jasně stanovených podmínek. Některými svými rysy však zpochybňují základní zásady smluvního práva, pokud je přímo nestaví na hlavu.[3] Prohlašují se za nejzlomovější technologii za posledních několik desetiletí.[4]

Někdy se blockchainy označují za symbol jakési čtvrté průmyslové revoluce, který může spolu s chytrými smlouvami vytvořit nové formy organizace a nové typy digitálního podnikání, které ovšem budou vyžadovat kvalitativně nové technické a právně regulatorní zásahy. Předvídá se dokonce vznik nového *lex numerica*, respektive *lex cryptographica*.[5] Protože blockchain není samozřejmě nic jiného nežli technologie k ochraně jistých práv, a nikoliv nějaký právní systém či podsystém, může být takové označování zavádějící. Nicméně zabývat se především obsahovými otázkami je nejen snad módní, ale bude to asi brzy dokonce prakticky nutné.[6]

Blockchain je vlastně rozptýlená nehierarchická (distribuovaná a sdílená) datová struktura (účetní kniha), jež umožňuje transparentní a bezpečné internetové uchování a přenos informace bez nutnosti spoléhat se na nějakou třetí osobu stojící mimo něj.

Každá operace na blockchaimu se zaznamená do bloku, jehož obsah je potom algoritmizovaně zakódován do hodnoty zvané *hash*. Ten je nezměnitelný a je komukoliv v blockchainu přístupný.[7] Pro kontraktaci představuje blockchain velký přínos, neboť ji značně urychluje a zvyšuje její kredibilitu. To, co se dříve odehrávalo během mnoha dnů a desítek výměn dopisů, mailů, telefonátů a prezenčních jednání, se dá v určitých případech vyřídit velmi rychle řadou autentizovaných a zřetězených elektronických záznamů (bloků), které nevývratně dokládají smluvní úkony či jiné skutečnosti – mohou se například

---

2 To je efektivní a pohodlné a nelze to přičítat jen anglojazykovému „imperialismu" či „kolonialismu". Blockchain se totiž „zrodil" právě pod tímto jménem a jakýkoliv překlad, pokud by navíc nebyl současně toporný, by ztěžoval komunikaci a mezinárodní dorozumění odborných komunit. Řada dalších anglických slov měla a bude mít podobný osud. Proto termín používám jako přejatý včetně skloňování a nezvýrazňuji jej v textu kurzívou, jako kdyby byl cizojazyčný. Je věcí vývoje, zda slovo setrvá v původní podobě (podobně jako třeba *leasing, interview, software*...), nebo se počeští na (dnes ještě) oči trhající „blokčejn" (ve stylu jiných na milost již vzatých slov, jako kovboj, franšíza, víkend, šoubyznys, lídr...).

3 KRAUS, D. – OBRIST, T. – HARI, O. *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*. Cheltenham, England: Edward Elgar Publishing, 2019, s. XI.

4 GUILLAUME, F. Aspects of private international law related to blockchain transaction. In: KRAUS, D. – OBRIST, T. – HARI, O. *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, s. 49 an., s. 93.

5 MIGNON, V. Blockchains – perspectives and chalenges. In: KRAUS, D. – OBRIST, T. – HARI, O. *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, s. 8–17.

6 Podle Světového ekonomického fóra bude do roku 2027 10 % globálního HDP uloženo na blockchainu. SCHREPEL, T. Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox. *Georgetown Law Technology Review*. 2019, 281.

7 CARRON, B. – BOTTERON, V. How smart can a contract be? In: KRAUS, D. – OBRIST, T. – HARI, O. *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, s. 104 an.

vytvářet „moduly“ chytrých smluv, zařaditelné automaticky do smluv, aby monitorovaly a informovaly o důvěryhodných zdrojích a spojovaly je s jistými účinky.[8]

Blockchain není totéž, co pouhý externí počítačový výkon (*cloude computing*), neboť se nespoléhá na poskytovatele dat, která mají být uchována nebo zpracována – každý uživatel používá vlastní zdroje na základě *peer-to-peer*. Každý uživatel disponuje vlastní kopií distribuované „účetní knihy“ na svém vlastním počítači,[9] takže může současně kontrolovat data, jež vkládá do blockchainu, a též je zpracovávat, protože má na ve svém počítači kompletní kopii blockchainu.[10] Žádný účastník blockchainu nemá kontrolu nad databází, jež je decentralizovaná a zpětně nezměnitelná v rámci sítě *peer-to-peer*. Je-li nově vložená informace v souladu s dříve uloženými a verifikovanými daty v blockchainu, stane se součástí jeho databáze a přiřadí se dřívějším blokům; je-li v nesouladu, automaticky se odmítne. Tak se udržuje sekvence spolehlivých a nezměnitelných záznamů.

Komplexní zakódování a transparentní seřazení trvalých údajů dat v časové řadě může v některých případech ohrozit osobní data.[11]

Za nevýznamnější rysy blockchainového protokolu se pokládají:[12]

- decentralizace (důvěra se sdílí mezi účastníky bez nutnosti spoléhat se na vnější autoritu a riskovat její případnou chybu);[13]
- nezměnitelnost (každý blok v oné „účetní knize“ navazuje kryptograficky – tedy zašifrovaně, zakódovaně – na blok předchozí a je trvalý po celou dobu fungování sítě);
- transparentnost (účastníci sítě mají přístup k procesu utváření konsenzu v řetězci, stejně jako k celému záznamu na blockchainu, což posiluje důvěru a zajišťuje spolehlivou stopu pro audit i důvěryhodnost spolupráce);
- bezpečnost a odolnost (bezpečný je blockchain z hlediska individuálních transakcí, neboť zajišťuje, že jen oprávněná osoba může disponovat svým majetkem. Je ale bezpečný i jako celek, protože chrání vlastnictví účastníků před manipulací, podvrhy, paděláním, zbytečnými výdaji a nepovoleným přístupem. Umožňuje stranám, které si nezbytně nemusí důvěřovat, kontrahovat bez třetí strany nebo prostředníka a zajistit splnění obsahu smlouvy).

---

8 PARSON, R. From supply chain to blockchain: Where can digitalization make a difference in international trade. *LIDC Lexology*. May 10, 2018. Dostupné z: <www.clydeco.com/insight/article/from-supply-chain-to-blockchain-where-can-digitization-make-a-difference-in>, s. 1; MITTON, A. et al. Smart contracts – tomorrow's technology today. *LIDC Lexology*. May 9, 2018. Dostupné z: <https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/smart-contracts-tomorrows-technology-today>, s. 1. Přístup 27. 8. 2019.

9 Ten se v blockchainovém žargonu označuje jako *node* („uzel“).

10 LISA, G. et al. A guide to blockchain and data protection. *LIDC Lexology*. November 19, 2018. Dostupné z: <https://www.lexology.com/library/detail.aspx?g=47dd4aa0-6f97-48b1-8160-f263bd345863>, s. 1.

11 To má mj. dopady i na povinnosti ve vztahu k ochraně dat podle GDPR, jimiž se tu vědomě nezabývám. Jen poznamenávám, že požadavky na ochranu osobních dat mohou fungování veřejných i soukromých blockchainů zkomplikovat; těch veřejných přirozeně více. Pseudonymizace účastníků blockchainu totiž dovoluje jejich identifikaci prostřednictvím funkce „User ID“ (SCHÄFER, Y. Blockchain vs. GDPR. *LIDC Lexology*. December 10, 2018. Dostupné z: <https://www.skwschwarz.de/en/news/articles/detail-of-article/news/blockchain-vs-gdpr/4/detail/News/>, s. 1. Přístup 27. 8. 2019).

12 Podle WITZIG, P. – SALOMON, V. Cutting out the middleman: a case study of blockchain technology induced reconfigurations in the Swiss financial services industry. In: KRAUS, D. – OBRIST, T. – HARI, O. *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, s. 24.

13 I přes běžnou pseudonymizaci není nemožné zjistit identitu účastníka – proto nejsou chytré smlouvy z hlediska účastníka vhodné tam, kde je zásadní důvěrnost (citlivé finanční operace, kde by měla být vyloučena možnost odhalení – srov. DE FILIPPI, P. – WRIGHT, A. *Blockchain and the Law*. Harvard University Press, 2018, s. 83). Z hlediska možnosti případné veřejné kontroly finančních operací (praní špinavých peněz) je to ovšem naopak velmi výhodné…

Z hlediska přístupu k blockchainu se rozlišují typy otevřené a uzavřené. Otevřené mohou být veřejné bez nutnosti povolení,[14] a veřejné s nutností povolení.[15] V rámci oněch uzavřených systémů se rozlišují konsorcia[16] na jedné straně, a soukromé sítě s povolením – „podniky").[17] Tyto typy se liší nejen evidentními podmínkami vzniku, ale i možností číst záznam, činit záznamy a možností zavazovat se prostřednictvím blockchainu.[18]

Jednou z nejzajímavějších aplikací blockchainu jsou tzv. chytré smlouvy. Jde vlastně o počítačové kódy spojené s prohlášeními, jež počítačový software provede, naplní-li se podmínky předem definované v kódu. Příkladem může být pravidelná platba za určených podmínek k určitému datu. Jakmile byl kód zadán, nemůže být změněn, takže realizaci dohody stran zaručuje systém, který to činí s teoreticky 100% spolehlivostí. Díky záznamu v blockchainu se tak digitálními prostředky zaručuje odolnost proti padělání a datovaný a bezpečný záznam o dohodě stran a jeho bezpečné uchování.[19] Smluvní aktivita stran se může rozvíjet bez jakékoliv vazby na oficiální orgány veřejné moci. Problém však může nastat v případě sporu z chytré smlouvy, který nebude řešitelný automaticky (*self-executing*). Autonomie blockchainu zpochybňuje nejen transparentnost transakcí, ale v důsledku oslabuje či znemožňuje vymáhání práva.[20] Proto se někdy blockchainy dokonce emfaticky označují jako „a-legální" nebo jako „přírodní síly", na něž lze stěží aplikovat vládu práva.[21] Transparentnost přitom není nějaký samoúčel, ale mezitímní krok na cestě k porozumění.[22] V některých oblastech, které z politických důvodů transparentnost vyžadují,[23] nelze širší uplatnění blockchainů očekávat.

Blockchain zajišťuje i dokonalou evidenci pohybu zboží nebo materiálu v průběhu výroby a distribuce a spouští automaticky kroky k provedení plateb, jakmile obdrží potvrzení o dodání zboží. Může tedy sloužit i jako svého druhu nespecifický způsob zajištění dluhu, který je přitom rychlejší a podstatně levnější než např. platba prostřednictvím akreditivu nebo dokumentárního akreditivu. Pak se prvotní a atraktivní výhody block-

---

14 Např. Bitcoin, Ethereum. Kontroverzní je ovšem problém konformity virtuální měny a právního státu (ŠTIKA, M. Má naprosto svobodná virtuální měna bitcoin místo v právním státě? *Bulletin advokacie*. 2018, č. 5, s. 29 an.; JOCHMAN, D. Skutečně nemá „naprosto svobodná virtuální měna bitcoin" místo v právním státě? *Bulletin advokacie*. 2018, č. 12, s. 44).

15 Např. systém *Sevrin*.

16 Např. více bank sdílí společnou účetní knihu.

17 Např. vnitřní bankovní účetní kniha sdílená mezi mateřskou společností a pobočkou.

18 WITZIG, P. – SALOMON, V. *Cutting out the middleman: a case study of blockchain technology induced reconfigurations in the Swiss financial services industry*, s. 25; HILEMAN, G. – RAUCHS, M. 2017 Global Blockchain Benchmarking Study. Dostupné z: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224>, s. 20. Přístup 29. 8. 2019.

19 Stejné výhody jako záznam smluveného ujednání má jakýkoliv záznam v blockchainu, včetně např. záznamu osobních dat. Dají se tak uchovávat zdravotní karty pacientů, kteří mohou po provedení medicínského úkonu automaticky zaplatit (sami, nebo za určitých podmínek prostřednictvím zdravotní pojišťovny). Technologie se dá využít i pro potřeby různých certifikací a autentizací, protože splňuje požadavky veřejných registrů (knihy narození, sňatků, úmrtí, katastr nemovitostí, obchodní rejstřík – ten se zkouší např. v Ženevě. V Estonsku funguje již několik let blockchain pro potřeby veřejné správy; podobně KRAUS, D. – OBRIST, T. – HARI, O. *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law*, s. 55–57.

20 Tak např. automatizovaně uzavíraná chytrá smlouva prostřednictvím blockchainu, jejímž předmětem je dodávka ilegálního zboží, nebo jež zveřejní informace porušující práva na soukromí, nemůže být zablokována. *„Už mluvíme o programování mravnosti do myslících strojů a dokážeme si v nich představit i jiné lidské sklony, ale určitě to bude špatně. Ať se jakkoliv pokoušíme tomu vyhnout, budeme mít stroje, jež porušují právo."* Srov. SCHNEIER, B. When Thinking Machines Break the Law. Dostupné z: <https://www.schneier.com/blog/archives/2015/01/when_thinking_m.html>. Přístup 20. 8. 2019.

21 Srov. WOOD, G. CoinScrum and Proof of Work:Tools for the Future. Dostupné z: <https://www.youtube.com/watch?v=WdgQI6CA4-E>. Přístup 15. 8. 2019.

22 PASQUALE, F. *The Black Box Society*. Cambridge, Massachusetts: Harvard University Press 2015, s. 8.

23 Typicky ve vztazích zvaných *Business to Government* (B2G), zasahujících mj. zadávání veřejných zakázek, uveřejňování smluv v registru smluv podle zákona o registru smluv; podobně ve vztazích podléhajících sektorové regulaci a dozoru nad smlouvami, jako např. v oblasti bankovnictví, pojišťovnictví apod.

chainu (zejména jeho pseudonymita a případná uzavřenost navenek u uzavřených systémů) mohou stát překážkou pro uplatnění práva. Přirozenou reakcí je snaha státu, aby jeho funkce nebyly nahrazeny nebo dokonce vyloučeny nějakou technologií.[24]

1.2 Chytré smlouvy

Blockchainová technologie zpochybňuje samotnou podstatu smlouvy, respektive vyvolává potřebu smlouvy redefinovat. Pojem „chytré smlouvy“[25] není vlastně vůbec výstižný, neboť navozuje dojem jakési bezsubjektové virtuální chytrosti. Přitom je jasné, že veškerou „chytrost“ (včetně eventuálních samoučicích schopností) vložil do blockchainové sítě programátor. Nejde přitom vůbec o smlouvy *stricto sensu*, ale o pouhou technologii samovykonávající (*self-executing*) smluvní agendu.

To, co „chytré smlouvy“ v právních vztazích provádějí, je povýtce kauzální deterministická automatizovaná reakce na splnění předem zadaných podmínek – jde tedy spíše o *automated contracts* nežli o *smart contracts*. Tzv. chytrá smlouva nemusí tedy být ani chytrá a ani to nemusí být smlouva, ale jen soubor příkazů. Směsice žargonu z pomezí práva informačních technologií a práva se však jako obvykle díky záplavě recyklací prosadila; proto můžeme i my oportunisticky a bez újmy na komunikativnosti tento (striktně vzato nepřesný) termín používat, a to i bez uvozovek a adjektiva „tzv.“, aniž by tento pojem byl definován v našem právu.[26] Chytrá smlouva je však striktně vzato stále jen jakýsi nepřesný a i zavádějící název pro software fungující v rámci blockchainové technologie, využívaný především k racionalizaci, urychlení a zajištění smluvní agendy.

Lze vysledovat pokusy o typizaci běžně se vyskytujících situací, v nichž se chytré smlouvy používají.[27] Chytré smlouvy mohou především

A) posílat a přijímat

a) faktická data bez skutečného právního významu;[28]
b) s právem chráněným obsahem;[29]
c) představující virtuální vlastnictví;[30]

---

24 Blockchainy se přitom využívají nejen v soukromém, ale i veřejném právu, takže žádná panika kvůli erozi právního státu v důsledku jejich zavádění nepanuje. Přístup jednotlivých států k nim se různí. Tak např. Velká Británie a Estonsko je již zavádějí, ve Francii se zkoumají potenciální možnosti využití, Čína a Brazílie jsou skeptické. Srov. ADAIR, M. Comparing Public Sector Blockchain Use Across Europe. Dostupné z: <https://www.mhc.ie/latest/blog/comparing-public-sector-blockchain-use-across-europe>. Přístup 21. 10. 2019.

25 Poprvé jej použil SZABÓ, N. Smart Contracts, Formalizing and Securing Relationships on Public Networks. *First Monday*. 1997, č. 9. Dostupné z: <https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First>, s. 2. Přístup 10. 8. 2019.

26 To není ostatně tak neobvyklé. Běžně se např. operuje s termínem *soft law*, i když toto „právo“ některé zásadní definiční znaky práva postrádá (mocenská legitimita tvůrce; kvalifikovaná publicita; závaznost; vynutitelnost státní mocí); přitom to nebrání v plnění významné regulatorní funkce takového kvazipráva. Je zajímavé, že některé státy měly potřebu právně definovat pojmy, které jsou jinak doménou doktríny či praxe i bez tohoto zakotvení. Tak např. v Itálii definovali letos zákonem (č. 12 z 11. 2. 2019) DLT (*distributed ledger technologies*), ale i chytré smlouvy jakožto počítačové programy působící na DLT, jejichž provedení automaticky zavazuje dvě nebo více stran na základě účinků tím předurčených (GREENBAUM, J. et al. Italy recognizes the legal value of DLT and smart contracts. *LIDC Lexology*. February 15, 2019. Dostupné z: <https://www.hlengage.com/italy-recognises-the-legal-value-of-dlts-and-smart-contracts>, s. 1. Přístup 15. 3. 2019). Definice je evidentně bezcenná a (kromě významu symbolického uznání i tak existující fakticity) asi zbytečná.

27 Jak uvádějí CARRON, B. – BOTTERON, V. *How smart can a contract be?*, s. 106 an.

28 Typu, že se něco událo, např. že cestující byl odbaven na letišti.

29 Např. práva k duševnímu vlastnictví (autorská práva, ochranné známky), zdravotní záznamy, klasifikované informace pro vládní činitele…

30 Určité množství kryptoměny.

B) vydávat data představující práva (např. kupóny, poukázky a jiné doklady opravňující hlasovat nebo k přístupu do určitých funkcí);

C) vydávat data představující aktiva;[31]

D) mít obsah podobný vynutitelné klasické smlouvě.[32]

Smyslem chytrých smluv bývá především jejich uzavření samotné, nebo chytré smlouvy následují již dříve dosažený smluvní konsenzus a mají sloužit k zajištění sjednaného způsobu plnění.

Chytré smlouvy mohou (ale nemusí) být jen virtuálním digitálním odrazem (digitálním duplikátem) smlouvy základní (skutečné), jíž by měly být nadřazeny a již by měly jen vykonávat. Pokud je smlouva uzavřena tradičně, není povinné její pokračování a správa prostřednictvím blockchainu. Autonomie vůle a smluvní svoboda mají přednost. Je-li blockchain „pokračováním" tradičně uzavřené smlouvy, budou strany čelit potížím s přenosem právních klauzulí (z nichž některé jsou neurčité a vyžadují interpretaci[33]) do počítačového kódu, ale mohou naopak nastat potíže i při dekódování obsahu.

Blockchainové smlouvy by proto neměly obsahovat neurčité právní pojmy, respektive „subjektivní klauzule".[34] To fakticky omezuje použitelnost blockchainů zejména na masové spotřebitelské či distributorské smlouvy s jednoznačně určenými a kvantifikovanými povinnostmi bez možnosti uvážení. Deterministická logika používaná v blockchainech na druhé straně snižuje možnost dezinterpretace v oněch jasně vymezených oblastech.

Cenou za algoritmizaci bude tedy zjednodušení a „binarizace" vztahů, omezení variability obsahu a adaptibility na konkrétní situace. Na druhé straně se sníží náklady na monitoring smluv a zmenší se prostor pro oportunní chování.

Změny ve vnějším regulatorním prostředí a jejich aktualizace se kvůli nezměnitelnosti blockchainu také nemusí dostatečně projevit – to může vést k „zautomatizovanému" a nevědomému porušování práva soukromého i veřejného včetně sankčních důsledků. Smluvní strany mohou však svoji smluvní agendu konsenzuálně umístit výlučně do počítačového blockchainového prostředí, tedy bez „opory" v „reálném" světě, a mohou tak kvazikontrahovat ještě před „klasickou" kontraktací podle práva, nebo úplně mimo ni. To se může stát i spontánně a implicitně reakcí na předsmluvní či smluvní projevy v počítačovém prostředí. Sporné budou především problémy projevu úmyslu kontrahentů (nabídky a akceptace) v prostředí blockchainu (včetně charakteru projevu učiněného

31 Držitel aktiva má potom nárok vůči výstavci.

32 Počítačové podpůrné nástroje byly často vyvíjeny právě s tímto cílem.

33 K tomu srov. CARRON, B. – BOTTERON, V. *How smart can a contract be?*, s. 115 an.

34 Jak uvádí BONELLO, L. How smart can a contract be? *LIDC Lexology*. July 24, 2018. Dostupné z: <https://www.lexology.com/library/detail.aspx?g=af0a1ffd-cb9d-4665-baa2-50690685a780>, s. 1. To však může být „hraběcí rada", protože v mnoha případech může právě neurčitost zvyšovat efektivnost smlouvy (DE FILIPPI, P. – WRIGHT, A. *Blockchain and the Law*, s. 77). Závislost na předem daných definovaných podmínkách může být vedle jejich praktické nezměnitelnosti paradoxně nevýhodou (a tedy nejen deklarovaným výdobytkem) chytrých smluv. Nejasnost a „vrozená" rozmlženost přirozeného jazyka umožňující jeho kontextové vnímání a interpretaci, nemusí být nedostatkem, ale záměrem. V řadě situací by zákonodárce bez neurčitých pojmů nemohl vůbec regulovat vztahy regulaci vyžadující, ale neurčité pojmy mu to umožňují s příslušným výkladovým prostorem při aplikaci práva. *Proponents who argue for a complete replacement of semantic contracts underestimate the power of fluid human behavior and judgment in the contracting process. The flexibility of semantic contracts is a feature, not a bug* (SKLAROFF, J. M. *Smart Contracts and the Cost of Inflexibility*. University of Pennsylvania Law School Penn Law: Legal Scholarship Repository. 2018. Dostupné z: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1009&=&context=prize_papers>, s. 303. Přístup 15. 8. 2019).

vůči více subjektům – půjde o právně závazné nabídky, nebo jen o oznámení, popřípadě o *invitatio ad offerendum*?). Nejisté budou i projev skutečného úmyslu prostřednictvím počítačového kódu a důsledky porušení smlouvy.[35] Chytré smlouvy pracují jakožto počítačové programy nezávisle a vykonají smluvní závazek i přes jeho nesoulad s právní úpravou, takže nezákonné plnění nebo podmínky způsobující neplatnost či zdánlivost právního jednání mohou představovat problém.[36] Nejasné mohou být i důsledky neporozumění stran programovacímu kódu zobrazujícímu smlouvu.[37]

Motivací chytrých smluv z podstatné části určitě bylo právě vyhnout se pravidlům státu (srov. kryptoměny). Anonymní charakter blockchainu, který příjemně vzrušuje (krypto)anarchisty a delikventy svojí lehkostí uzavřít nezákonnou a z vnějšku špatně detekovatelnou smlouvu (např. kartelovou), může naopak odrazovat jiné, kteří se rozporu se zákonem obávají. Ti v rámci různě nastavených standardů péče (potřebné, obvyklé, běžné, odborné, řádného hospodáře apod.) minimalizují rizika a chytrým smlouvám se raději chytře vyhýbají. Chytré smlouvy jsou totiž jen technologicky podmíněným nástrojem či modelem rozhodovací delegace. Nedá se ovšem evidentně předem a obecně odpovědět na otázku, zda naplní např. požadavek péče řádného hospodáře takové alibistické jednání (vyhýbání se chytrým smlouvám) spojené jen s rizikem, že by se společnost mohla dostat do rozporu se zákonem, nebo zda naopak není porušením této péče rezignace na prokazatelné úspory transakčních nákladů, na zvýšenou rychlost transakcí (ale i jejich menší jistotu) ve srovnání se situací, kdy by se chytré smlouvy použily a žádná protiprávnost by se přitom nestala.

Přitom právě anonymita (pseudonymita[38]) blockchainu znamená u otevřených blockchainů (na rozdíl od uzavřených a tzv. schvalovaných) velké riziko. Blockchain svojí anonymitou může svádět k použití právě proto, aby se ztížil přístup vnější právní kontroly a aby se usnadnilo protiprávní jednání s vírou v *lex cryptographica*. Blockchain sice snižuje náklady na ověřování digitální informace, ale nesnižuje náklady na ověřování informace vnější (*offline*).[39] Zanedbání nebo vynechání takové kontroly může dobrověrného účastníka chytré smlouvy dostat do rozporu třeba i s veřejnoprávním zákazem určitého jednání (přestupek, trestný čin, kartelová dohoda apod.).

Neplatnost smlouvy umístěné na blockchainu pro rozpor se zákonem nebo dobrými mravy (ale i se zákonným požadavkem na formu smlouvy) nemůže být samozřejmě brána v úvahu jako nějaká polehčující okolnost. Problémy mohou vzniknout i při nesouladu vůle a jejího projevu (omyl). Automatizovaně „chytrý“ kontrakt se zásadně bude uskutečňovat navzdory poznání kontrahenta, že jeho skutečná vůle byla jiná, a to do doby, než se omyl napraví dohodou, nebo než se postižená strana domůže nápravy u soudu či rozhodce.

---

35 CARRON, B. – BOTTERON, V. *How smart can a contract be?*, s. 122 an.

36 KRUPIČKOVÁ, P. Smart contracts – revoluce v smluvním právu 21. století? *Revue pro právo a technologie*. 2017, roč. 8. č. 15, s. 29.

37 FRADERA, F. Conference Report on „Digital Revolution: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies, Challenges for Law in Practice“. *European Review of Private Law*. 2018, No. 5, s. 709.

38 Každý uzel (*node*) má unikátní alfanumerickou adresu (veřejný klíč) sestavenou z 30 znaků, která jej charakterizuje. Tento veřejný klíč je odvozen od soukromého klíče, který si každý uživatel ukládá mimo síť.

39 CATALINI, CH. – TUCKER, C. Antitrust and Costless Verification: An Optimistic and Pesimistic View of the Implication of Blockchain Technology. *MIT Sloan Research Paper*. 2018, No. 5523–18. Dostupné z: <https://www.competitionpolicyinternational.com/antitrust-and-costless-verification-an-optimistic-and-a-pessimistic-view-of-the-implications-of-blockchain-technology/>, s. 1. Přístup 15. 8. 2019.

Zatímco u tradičních smluv je stupeň důvěry založen na úrovni poznání druhé smluvní strany a na zkušenosti s ní, u chytrých smluv je důvěra vkládána do počítačového algoritmu stojícího za dohodou.[40] Blockchainové smlouvy nebudou praktické u dlouhodobých vztahů naplněných důvěrou a vzájemnou znalostí partnerů (*relational contracts*), připodobňovaných manželstvím, na rozdíl od riskantních „vztahů na jednu noc".[41] V posléze uvedeném případě lze očekávat nízkonákladové a vysoce standardizované smlouvy a jen omezené nebo žádné možnosti individualizace (*customization*). Tento přesun od individualizace a nahodilosti kontraktace (v agrární společnosti) k deindividualizaci a standardizaci (industriální společnost, informatická společnost) je ale obecně a dlouhodobě pozorovatelný[42] a nesouvisí nutně s blockchainy a s chytrými smlouvami.

Ani smlouvy uzavírané výlučně v zakódovaném prostředí blockchainů se nevymykají právní úpravě smluvního práva (přísliby se vesměs učiní předem a teprve pak se převádějí do počítačových kódů). Komunikace v tomto prostředí na druhé straně přirozeně negarantuje právní relevanci tam učiněného jednání. Posouzení vyžaduje důkladnou analýzu a individualizaci v každém jednotlivém případě.

Kvůli těmto a podobným potížím se použití chytrých smluv, jež jsou jen počítačovým kódem nesrozumitelným většině stran, pokládá za velmi riskantní. Doporučuje se analogické používání pravidel o obchodních podmínkách (včetně inkorporačních pravidel, pravidel o překvapivých ujednáních, pravidel o intepretaci vůle apod.).[43] Patrně by u nás platila i zákonná ochrana slabší strany podle § 433 o. z.

Použitelnost těchto smluv bude zatím asi dost omezená zejména na technologické specialisty (kteří typicky nemají kognitivní deficit), pokud jejich předmětem bude jasně vymezené a snadno popsatelné plnění za jasně stanovených podmínek a pokud provozovatelé těchto sítí vyvinou maximální možné úsilí a vysvětlí všem stranám účinky a rizika používání těchto smluv. Nejčastější využití chytrých smluv jakožto „následovníků" dřívějších klasických (právních) smluv je vlastně jen racionalizační automatizací dalšího „provozu" smluv, která by velké problémy nemusela vyvolávat. Nebezpečný může být převod tradičního obsahu již uzavřených smluv do počítačových kódů a obráceně; riziko hrozí při pokusech vyplnit mezery smluvních ujednání tradičními nástroji (dispozitivní normy, zákonná interpretační pravidla). Výhodou tohoto použití chytrých smluv může být odstranění rizika mezi partnery, již si nedůvěřují, a proto by jinak (a za cenu zvýšení transakčních nákladů) bývali použili služeb třetí strany.[44]

---

40 Označuje se to někdy jako *trustless trust* (SAVELYEV, A. Contract Law 2.0: „Smart" contracts as the Beginning of the End of Classic Contract Law. Moscow, National Research University, Higher School of Education. *WP BRP 71/Law*. 2016, s. 11). V případě dohod kartelových, které jsou právně nevynutitelné, je budování důvěry mezi účastníky klíčové. To je v klasických poměrech sotva možné bez osobního kontaktu. Robotické algoritmizované nástroje pracují bez potřeby emocionální důvěry vytvářené na osobních tajných setkáních; kredibilita se dosahuje spíše vzájemným očekáváním bleskové odvety za porušení dohody (MEHRA, S. K. Antitrust and the Robo-Seller: Competition in the Time of Algorithms. *Minnesota Law Review*. 2016, 100, s. 1357).

41 DE FILIPPI, P. – WRIGHT, A. *Blockchain and the Law*, s. 84.

42 SAVELYEV, A. *Contract Law 2.0: „Smart" contracts as the Beginning of the End of Classic Contract Law*, s. 9.

43 CARRON, B. – BOTTERON, V. *How smart can a contract be?*, s. 140 an.

44 Přistihl jsem se v této souvislosti, že jsem se už v minulém století dopustil návrhu na *smart contracts*, aniž mě na rozdíl od pozdějších proponentů tohoto termínu napadlo to takto nabubřele označit (neboť nešlo o nic chytřejšího než pouhou algoritmizovanou a predikovatelnou deterministickou sekvenci jednoznačných aplikačních příkazů). Jednalo se mj. o návrh dílčí automatizované aplikace práva ve formě automatizovaného účtování a vymáhání majetkových sankcí i o další možnosti omezené ovšem v té době nejen technologicky a ekonomicky, ale i společensko-politicky (BEJČEK, J. K možnostem automatizace právního jednání a rozhodování socialistických hospodářských organizací. *Právník*. 1982, č. 5, s. 392–404; BEJČEK, J. O právních otázkách řízení hospodářství s pomocí výpočetní techniky. *Právník*. 1983, č. 9, s. 823–840.) Jeden můj diplomant tuto situaci

Chytré smlouvy bez předchozí klasické kontraktace se zdají spíše teoretickou možností. Uvažovat se dá i o kombinaci rámcové klasické smlouvy a realizačních chytrých smluv, které ji podle dohodnutých pravidel naplňují. Rigidní povaha chytrých smluv předpokládá jejich „samorealizaci“ (*self-execution*) až po dosažení přesně specifikovaného souboru příkazů což je v měnícím se ekonomickém a obchodním prostředí mnohdy nežádoucí omezení[45] oproti tradičním písemným nebo ústním smlouvám, které umožňují svoje změny, často velmi pružné. Doporučuje se proto raději kombinovat chytré smlouvy se smlouvami tradičními (písemnými), dokud se nepodaří zajistit zakódování větší flexibility do blockchainu.[46]

Sdílím skepsi k tomu, že by počítačové kódy mohly (mimo úzce vymezené repetitivní, rutinní a jednoznačné situace binárního charakteru) oslabit či vyřadit zákonná pravidla, pokud by se připustilo oddělení počítačové logiky od „lidského pocitu spravedlnosti“;[47] jsem ovšem srovnatelně skeptický k této podobě patosu založeného na neuchopitelných a mnohavýznamových „vznešených“ slovech.

1.3 Chytré smlouvy v českém právu

Naše právo je ve vztahu k chytrým smlouvám a blockchainu zatím zdrženlivé, ať už je to z jakýchkoliv důvodů (patrně to nebudou především důvody koncepční). Neexistence zvláštní úpravy těchto novinek není na zásadní překážku jejich zavádění a využívání. To je ostatně obecnější závěr platný i v mezinárodním srovnání. Přestože se základní aspekty chytrých smluv (nezměnitelnost, samovykonatelnost, časová neomezenost) chápou v různých právních řádech odlišně, lze předpokládat, že softwarové algoritmy v budoucnu změní obraz smluv. Možná prý budou někdy smlouvy uskutečnitelné bez práva a budou se odehrávat v globálním prostoru bez národních hranic; zatím však smlouvy probíhají „klasicky“ v národních právních úpravách vyjádřených v normální řeči, a nikoliv v počítačových kódech; díky tomu lze vymezit rysy smluvního vztahu a odpovídající práva.[48]

---

komentoval s jemnou ironií: „*S myšlenkou chytrých smluv přišel na konci minulého století americký vědec Nick Szábo, či dokonce před ním v československém prostředí cimrmanovským počinem Josef Bejček*.“ Sluší se tu však připomenout především průkopnický přínos prací V. Knappa z 80. let 20. století z oblasti právní kybernetiky a informatiky pro oblast tzv. dodavatelsko-odběratelských vztahů. Tento velikán právní teorie byl (ovšem všeobecně) velmi střídmý a skeptický k zavádění „nové“ (spíše módní) terminologie.

45 Strany si mohou v konkrétní situaci např. přát splnění smlouvy i v případě, že nejsou splněny všechny předpokládané podmínky, mohou mít zájem podmínky změnit nebo zrušit v zájmu dosažení kýženého výstupu.

46 O'NEIL, A. R. Beyond Bitcoin – Will Blockchain and Smart Contracts Self-Execute Their Way into the Utility Industry? *Legal Reporting Service*. 2018, Vol. 54, No. 12, s. 4. Ona flexibilita však může být zase jen typová (klasifikovaná, omezená, předprogramovaná), tedy nikoliv úplná.

47 Už se nicméně vyskytly před pár lety pokusy o vytvoření „vypočitatelných“ (*computable*) smluvních podmínek (CARRON, B. – BOTTERON, V. *How smart can a contract be*?, s. 74).

48 Srov. SCHURR, F. A. Anbahnung, Abschluss und Durchführung von Smart Contracts im Rechtsvergleich. *Zeitschrift für Vergleichende Rechtswissenschaft*. 2019, 118, s. 257–284. Konstatuje se zde (s. 284), že *smart contracts* nejsou smlouvami v právním smyslu, ale spíše formou automatizovaného uzavírání a/nebo provádění smluv, pro něž stávající soukromoprávní pravidla plně dostačují. Na tom nic nemění příležitostná snaha některých zemí definičně se „vypořádat“ s novým pojmem kvůli vyšší právní jistotě. V této subkapitolce se s poděkováním i omluvou inspiruji i myšlenkami a postřehy neznámého studenta, jehož práci (*Blockchain a tzv. smart contracts pohledem českého práva*) jsem jako anonymní hodnotitel posuzoval na brněnské právnické fakultě v rámci studentské soutěže pořádané v zimě 2019 jednou advokátní kanceláří, která mi zpětnou vazbu neposkytla, takže jeho identitu neznám. Při korekturách mohu již doplnit: Roman Šafář, dnešní doktorand.

Námitky, že u chytrých smluv chybí volní prvek na straně dlužníka,[49] nemají v našem právním prostředí velkou váhu, protože podle § 1724 o. z. se ustanovení o smlouvách použijí přiměřeně i na projev vůle, kterým se jedna osoba (*sic!*) obrací na osoby jiné, ledaže to vylučuje povaha projevu nebo vůle. Formální vyjádření vůle v počítačovém kódu není samo o sobě rovněž na závadu, protože každý má podle § 559 o. z. právo zvolit si pro právní jednání libovolnou formu, není-li ve volbě formy omezen ujednáním nebo zákonem.

Smlouvy vyžadující písemnou formu *stricto sensu* nemusejí být z možnosti být „chytrými" vyloučeny, neboť podle § 562 o. z. je písemná forma zachována i při právním jednání učiněném elektronickými nebo jinými technickými prostředky umožňujícími zachycení jeho obsahu (to blockchain umožňuje) a určení jednající osoby (což blockchain i při pseudonymizaci zpětně rovněž umožňuje, protože historie transakcí na něm proběhnuvších je transparentní a dekódovatelná). Nemělo by stačit určení konkrétního účtu,[50] ale jeho majitele, respektive oprávněné osoby.

Pokud ovšem konkrétní blockchainová síť neposkytuje možnost identifikovat skutečného účastníka, podmínka určitelnosti jednající osoby nebude naplněna s důsledky neplatnosti jednání, a to nejen takového, které vyžaduje písemnou formu (§ 562 o. z.). Přednost by měla dostat neplatnost pouze relativní (§ 574 o. z.), což by ovšem neplatilo, pokud by ujednání stran bylo v rozporu s veřejným pořádkem nebo se základními zásadami právního řádu nebo by bylo hrubě nemravné (§ 580 o. z.).

Chytré smlouvy samozřejmě nemohou v důsledku vyloučit např. obecnou ochranu slabší strany podle § 433 o. z. nebo ochranu spotřebitele podle § 1810 a násl. nebo podle veřejnoprávního zákona o ochraně spotřebitele. Tyto rozpory by mohlo nedohledatelné označení strany smlouvy maskovat, a proto by mělo být nepřípustné.

V anonymitě (respektive pseudonymitě) smluvních stran může spočívat problém určitosti smlouvy kvůli označení smluvních stran. Pokud je označení strany neurčité nebo nesrozumitelné, dovozovalo se, že smlouva je absolutně neplatná.[51] Skutečného kontrahenta chytré smlouvy druhá strana typicky nezná, ale není to důvod k vyslovení neplatnosti, protože pomocí technických prostředků lze tuto osobu identifikovat. Navíc podle § 574 o. z. platí zásadní přednost platnosti právního jednání před jeho neplatností.[52]

Náležitost podpisu právního jednání chytré smlouvy umožňují naplnit, pokud se podepisuje identifikovatelná osoba (viz výše).[53]

---

49 SAVELYEV, A. *Contract Law 2.0: „Smart" contracts as the Beginning of the End of Classic Contract Law*, s. 18.

50 Tak KRUPIČKOVÁ, P. *Smart contracts – revoluce v smluvním právu 21. století?*, s. 26.

51 Rozhodnutí NS sp. zn. 2 Cdon 824/97 ze dne 27. 10. 1999. Dostupné z: <https://www.codexisuno.cz/5sw#!17>. Tento striktní přístup by se dnes (ale ani dříve – tedy i před vydáním nového o. z.) neuplatnil mj. proto, že o absolutně neplatné smlouvě by bylo možné hovořit, jen bylo-li by označení účastníka natolik neurčité či nesrozumitelné, že pochybnosti o tom, kdo jím je, nebylo možno odstranit ani výkladem právního úkonu (§ 37 obč. z. 1964). V blockchainu se označení účastníka nevykládá, ale on se jen zpětně identifikuje.

52 Shodně KUČERA, Z. Smart contracts pohledem právníka. *Právní prostor*. 13. 12. 2017. Dostupné z: <https://www.pravniprostor.cz/clanky/pravo-it/smart-contracts-pohledem-pravnika>, s. 2. Přístup 20. 8. 2019.

53 Zákon č. 297/2016 sb., o službách vytvářejících důvěru pro elektronické transakce stanoví podle požadavku nařízení eIDAS (Nařízení EP a REU č. 910/2014 z 23. 7. 2014 o elektronické identifikaci a službách vytvářejících důvěru službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a zrušení směrnice 1999/93/ES) tři typy elektronických podpisů relevantních pro chytré smlouvy: zaručený, uznávaný, a tzv. jiný typ. Zaručený elektronický podpis musí naplnit čtyři znaky, a to 1) jednoznačné spojení s podepisující osobou, 2) možnost identifikace podepisujícího, 3) konstrukce z dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou, 4) připojení k podepisovaným datům způsobem umožňujícím zjistit jakoukoliv následnou změnu dat.

2. Koluzivní „chytré“ smlouvy

Blockchainy se mohou stát technickým prostředníkem koluze[54] nebo mohou být i jejich kvazisubjektem. Svou technickou povahou mohou zvyšovat důvěru mezi účastníky spiknutí (protože podmínky dohody jsou na blockchainu nezměnitelné) a navíc mohou velmi ztěžovat možnost odhalení regulátorem soutěže, takže účastnící kartelu nejenže mají pocit větší nezranitelnosti, ale nezranitelnější opravdu jsou.[55]

Tato „přidaná hodnota“ blockchainových kartelů může velmi oslabit motivaci účastníků požádat o program shovívavosti (*leniency*), založený na nabídce podstatného upuštění od sankce nebo úplné kartelové imunity v případě odhalení kartelu, a to v závislosti na zásluze účastníka na odhalení kartelu a na jeho součinnosti s antimonopolním úřadem.[56] Je zatím předčasné dohadovat se o tom, zda rozšíření blockchainů povede ke snížení žádostí o *leniency*; je to určitě pravděpodobné, i při zvážení jiných nespecifických faktorů.[57] Zejména bude hrát roli riziko a pravděpodobnost detekce zakázané protisoutěžní dohody ze strany veřejné moci, nebo i poškozených soutěžitelů a spotřebitelů v rámci snahy o soukromé vymáhání náhrady škody. Čím vyšší riziko odhalení (a tedy čím nižší důvěra v utajení dohody[58]) bude, tím pravděpodobněji se účastníci dohody budou rozhodovat pro žádost o program *leniency*.

Z hlediska teorie her a efektivního porušení smlouvy je blockchain příspěvkem ke zvýšení důvěry a jistoty účastníků o chování zbytku kartelu, a navíc snižuje pravděpodobnost odhalení, takže se kartel může stát ještě atraktivnější tržní strategií. Blockchainová technologie přinejmenším vzbuzuje obavy ze své svůdnosti k „efektivnější“ kartelizaci většího rozsahu a delšího trvání.

Dají se rozlišovat dva typy využití blockchainu při kartelizaci.[59] Jeden z nich využívá přímo podmínek vstupu, používání a výstupu z kartelu za pomoci blockchainu, a druhý využívá kartelových dohod vytvořených mimo prostředí blockchainu a díky němu je zefektivňuje.

Využívání privátního a veřejného klíče splňuje všechny podmínky 1, 3 a 4. Bude-li tedy identifikovatelná smluvní strana, naplní se všechny podmínky potřebné pro uznání písemného právního jednání v rámci chytré smlouvy učiněného elektronickými prostředky. Tuto speciální problematiku rozebírají u nás mnohem podrobněji jiní autoři, např. R. Polčák či F. Korbel, na jejichž práce odkazuji.

54 Pod tímto pojmem se vesměs rozumí tajná dohoda mezi konkurenty, jež vede v důsledku k uplatňování nadsoutěžních cen. Je to však nepřesné, neboť tacitní koluze či vědomý paralelismus dohodou v „pravém smyslu“ (jakožto souborem vědomých závazků a porozumění) není; chybí u nich i přímá komunikace konkurentů. Za „náhradní důkaz“ skryté komunikace se přijímá tzv. nepřirozený paralelismus“, jenž by nemohl být nastat pouhou náhodou a bez předchozího srozumění stran. Srov. HARRINGTON, J. E. Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agents* (Aug. 22, 2017). Dostupné z: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3037818>, s. 24. Přístup 20. 8. 2019. Koluzí není ani tzv. cenové následování (*conscious parallelism*). To sice může mít podobný či stejný výsledek jako koluze, ale na rozdíl od ní není výsledkem koordinace, ale jeho podstatou je nápodoba jednání jiného soutěžitele na trhu. Srov. Rozsudek krajského soudu v Brně z 8. ledna 2009, sp. zn. 62 Ca 15/2007 (kartel stavebních spořitelen).

55 SCHREPEL, T. Collusion by Blockchain and Smart Contracts. *Harvard Journal of Law and Technology*. 2019, Vol. 33, No. 1, s. 124. Dostupné též z: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3315182>, s. 9. Přístup 20. 8. 2019.

56 Srov. § 22ba českého z. o. h. s. (zák. č. 143/2001 Sb. v platném znění). Též rozhodnutí Komise COMP 39188 z 15. října 2008 (C 5955) ve věci T-587/08 (*Fresh Del Monte Produce, Inc. vs. Internationale Fruchtimport Gesellschaft Weichert GmbH & Co. KG*).

57 V Evropě údajně poklesl počet žádostí o *leniency* z 64 v roce 2014 na 32 v roce 2015 a na 24 v roce 2016 (údaj podle YSEWYN, J. – KAHMANN, S. The decline and fall of the leniency programme in Europe. *Concurrences*. 2018, No. 1. Dostupné z: <https://www.concurrences.com/en/review/issues/no-1-018/articles/the-decline-and-fall-of-the-leniency-programme-in-europe-86060-en>. Přístup 20. 8. 2019.

58 Říká se někdy, že důvěra začíná tam, kde končí předpověď.

59 Viz SCHREPEL, T. *Collusion by Blockchain and Smart Contracts*, s. 128 an.

2.1 Koluzní ujednání na blockchainu

Otázka je, zda blockchain může sám o sobě představovat zakázanou dohodu. Vzhledem k tomu, že jde o sdílení informací, které mohou být obchodně citlivé (nejde tedy o veřejné informace) a mohou podstatně snižovat nejistotu účastníků informační výměny o budoucím chování jiných subjektů[60] (růst koordinačního potenciálu), je to možné. Důkazní břemeno o takovém dopadu informační výměny spočívá na antitrustovém orgánu. V zásadě nebude při vytváření *veřejných* blockchainů a účasti v nich dovoditelný jejich antitrustový charakter, ledaže by byly vytvořeny s jediným cílem: sdílet budoucí informace proto, aby mohli soutěžitelé koludovat.

Protisoutěžní mohou být i podmínky přístupu k blockchainu (typicky ve formě bojkotu nebo diskriminace; může jít navíc o zneužití dominance v podobě odmítnutí spolupráce či kolektivního bojkotu). Blockchain se dá využít ke kontrole některých z jeho dominantních účastníků nad jinými.

2.2 Koluzní ujednání využívající blockchain

Koluzní ujednání se nemusejí týkat podmínek přístupu na blockchain, ale mohou jej využít k usnadnění koluzivních dohod o tržní strategii (o cenách, rozsahu a omezení výroby, o inovační strategii apod.).[61] Tak se mohou např. bez použití chytrých smluv i na veřejném blockchainu prostě jen sdílet viditelné a dohledatelné informace o tom, zda se nějaká tajná dohoda dodržuje. Ty jsou přístupné na veřejném blockchainu všem, z nichž někteří však nemusejí mít o významu uveřejňovaných informací tušení. Soukromý blockchain zvyšuje díky výlučnosti přístupu soudržnost účastníků tajné dohody. Informace vkládané do něj mohou navíc podléhat ověřování.

Dohody omezující soutěž lze uskutečňovat prostřednictvím chytrých smluv na blockchainu např. tak, že se na něm propojují jen takové nabídky a objednávky, které odpovídají dojednanému omezení soutěže (např. teritorialitě nebo jiné výlučnosti). V budoucnosti nelze vyloučit ani zapojení tzv. umělé inteligence, která by mohla podle zakódovaných pravidel optimalizovat protisoutěžní dopady (např. u *bid-riggingu*).

2.3 Provozování koluze na blockchainu

Účastníci koluzního ujednání na blockchainu se mohou těšit výhodám pohodlného života nejméně ze dvou důvodů – jednak blockchain vylučuje riziko, že ostatní účastníci kartelu budou podvádět a nebudou jej dodržovat, a jednak minimalizuje riziko odhalení kartelu. Hovoří se o dvojakém současně působícím účinku – o viditelnosti (mezi účastníky navzájem) a o neprůhlednosti (navenek).

Prvý dopad zvyšuje soudržnost členů kartelů a upevňuje důvěru mezi nimi; jde o ekonomické hledisko stability kartelu, jež se dá ještě zvýšit, pokud blockchain umožňuje automatizovanou korekci kartelově nekonformního jednání ukládáním cílených sankcí porušitelům. Možnost automatizovaně se mezi kartelisty pozorovat a postihovat za neloa-

60 Srov. Sdělení komise č. 5282 z 14. ledna 2011 (C 11/1).

61 SCHREPEL, T. *Collusion by Blockchain and Smart Contracts*, s. 139 an.

jálnost vede k tomu, že se účastníci obávají kartel nedodržovat. Automatizace některých aspektů kartelových dohod odstraňuje (či přinejmenším do velké hloubky algoritmů „zanořuje“) některé důležité důkazy o realizaci těchto dohod. To je kvalita v podobné úrovni nedostupná v kartelech provozovaných mimo blockchain. Na druhé straně mohou chytré smlouvy napomoci k tomu, aby koludující účastník z dohody vystoupil.

Vlastnost transparentnosti a viditelnosti kartelové dohody v soukromém blockchainu (mezi kartelisty) je doprovázena souběžnou neprůhledností navenek, protože veřejné blockchainy jsou přístupné všem a jejich výhoda, že se zakázané ujednání skryje, je menší než u blockchainů soukromých. Antitrustové právo a příslušné orgány usilují o rozbití důvěry mezi kartelisty (mj. programem shovívavosti, který motivuje ke „zradě“); technologie blockchainu představuje velmi účinnou protiváhu tohoto úsilí, která je ve spojení s vysokou latencí kartelů a v průměru velmi nízkou pravděpodobností jejich odhalení velmi nebezpečná z hlediska veřejného zájmu na zachování soutěžního prostředí. Může totiž zvyšovat rozsah zasažení trhů kartelizací, jakož i agresivitu takových dohod. Blockchainy tedy jistě zkomplikují práci antitrustovým úřadům, protože kódují obsah smluv i jejich účastníky; kromě právníků a ekonomů budou tedy potřebovat stále více i specialisty na programování a informační technologie.[62]

Empirie i prostý selský rozum opravňují k domněnce, že účinné sankce za porušení kázně uvnitř kartelu napomáhají jeho trvalosti a soudržnosti. Blockchainy mohou mít v tomto směru docela negativní dopad – díky své transparentnosti dovnitř a nezměnitelnosti záznamů, zejména ve spojení s chytrou smlouvou v podobě automatizovaného uložení sankce za porušení kartelové disciplíny. Asi nelze ani vyloučit, že na blockchainech se bude skrývat jen závadná dohoda omezující soutěž nebo její část, zatímco ty kartelově nezávadné „nevinné“ části budou vedeny v tradiční podobě lehce přístupné zvenku (zejména antitrustovým orgánům), aby nevyvolávaly prvoplánově podezření.

Dovozuje se,[63] že program shovívavosti pomáhá u takových dohod, jež jsou nevýnosné a špatně koncipované a které by se rozpadly tak jako tak. Blockchainy kombinované s chytrými smlouvami jsou způsobilé dosáhnout stejného cíle, ale rychleji. Zatímco tedy *leniency* zvyšuje nejistotu mezi účastníky kartelu tím, že snižuje vzájemnou důvěryhodnost a ztěžuje uzavření zakázané dohody (demotivuje), chytré smlouvy úroveň jistoty zvyšují tím, že spolehlivě trestají každé porušení dohody. Výsledek tedy může být i přes protichůdný mechanismus podobný. Aktuální výzva pro antitrustové orgány je naučit se identifikovat koluzi dosahovanou prostřednictvím blockchainů a chytrých smluv, a nikoliv se držet klasických osvědčených nástrojů, které se bez analýz programování a sofwaru mohou míjet účinkem. Bude třeba adekvátně reagovat na decentralizační tendence projevené blockchainy a chytrými smlouvami. Některá navrhovaná centralizovaná řešení[64] jsou dosud sporná z hlediska efektivnosti a snad až zničující z pohledu samotné funkčnosti oněch technologií.

---

62 Problém může vzniknout i u mateřských společností, jež nebudou muset vědět o koluzi mezi svými dceřinými společnostmi, docílené díky blockchainu. Přitom by jim důsledky takové koluze měly být zásadně přičítány (jak upozorňuje SCHREPEL, T. *Collusion by Blockchain and Smart Contracts*, s. 150).

63 Ibidem, s. 159.

64 Jako např. systém řízení identity, umožňující odhalení skutečné totožnosti účastníků; nebo přidání regulatorního „špionážního“ uzlu (*node*) do blockchainu; nebo pokutování klíčového autora či účastníka blockchainu použitého k nezákonným aktivitám (Ibidem, s. 161 a prameny tam uvedené).

3. Algoritmizovaná koluze

Algoritmy se používají stále častěji a začínají zasahovat i do právních vztahů. Řada rozhodovacích procesů se algoritmizuje nebo semialgoritmizuje. Tento proces se většinou pokládá za nezvratný a spojuje se s nezbytností adaptovat se na něj. Objevují se však i varování, že nejen politici, ale i šéfové koncernů, generálové nebo lékaři se díky stále se zdokonalujícím algoritmům stanou namísto samostatných aktérů rozhodování jakýmsi rozhraním (*interface*) pro algoritmy, které budou rozhodovat a jednat za ně.[65] Jednou z oblastí, kde se to začíná projevovat, je ochrana hospodářské soutěže.

Algoritmizace v digitalizované ekonomice je dvousečný proces, který může nejen zvýšit konkurenceschopnost a snížit marginální náklady, ale může též svádět i k protisoutěžním těžko odhalitelným spiknutím.[66] Algoritmy se dnes již v řadě odvětví pokládají za klíč k úspěchu,[67] přestože mohou posílit tacitní koluzi, omezovat spotřebitelské možnosti výběru a ohrožovat pluralitu.[68]

3.1 Algortimy jako nástroj srozumění?

Použití algoritmů může narušit funkci trhu především tím, že velmi usnadňuje koluzi. Algoritmy mohou nahradit explicitní koluzi mlčenlivou koordinací.[69] To je kvůli transparentnosti trhu a homogenitě produktů zvláště nebezpečné na oligopolizovaných trzích, které ve světě začínají v jistých tržních segmentech převládat. Samotná komunikace (třeba právě prostřednictvím počítačových algoritmů) ještě však neznamená koluzi a ani dohodu. Jen usnadňuje vzájemné srozumění mezi svými účastníky, ale není pro ně nezbytná[70] (srov. vědomý paralelismus, který žádnou komunikaci nevyžaduje). Algoritmy spolu mohou komunikovat, ale vlastní (nenaprogramované) srozumění nejsou s to mít a projevit.

---

65 Srov. HENKEL, Ch. H. Facebook is phantastisch für die Demokratie. *Neue Zürcher Zeitung*. 21. 11. 2019.

66 JANKA, F. S. – UHSLER, S. B. Antitrust 4.0 – The Rise of Artificial Intelligence and emerging challenges to antitrust law. *European Competition Law Review*. 2018, Iss. 3, s. 113.

67 V elektronickém obchodování je používání algoritmů již zvyklost. Algoritmizace synergicky spojuje a umocňuje možnosti matematiky, počítačů a internetu a umožňuje obchodníkům použít zcela nových nástrojů na rozdíl od dřívějšího vědomého spoléhání se na nedokonalé predikce a intuici (MEHRA, S. K. *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, s. 1331); týká se to i oblastí, v níž dříve tyto iracionální „testy" kralovaly (onlineové seznamky). Algoritmy jsou schopny pracovat spolehlivě, s bleskovou rychlostí, neúnavně a bez přestávek po celá léta. Jejich efektivnost zejména ve fázi sběru dat je technicky nesouměřitelná s klasickými možnostmi sledování pramenů člověkem – ten by se měl věnovat analýze dokonale sebraných aktuálních dat a zpětné vazbě na výstupy algoritmů (srov. některé excesy algoritmické cenotvorby citované v poznámkách níže).
V sektorovém průzkumu provedeném Evropskou komisí (*Comission Staff Working Document, Preliminary Report on the E-Commerce Sector Inquiry*. Brussels, 15 September 2016, SWD, 2016, 312 final, s. 281, bod 902) se uvádí, že 53 % respondentů z řad maloobchodníků sleduje online ceny konkurentů, 67 % z nich tak činí prostřednictvím softwaru a 78 % maloobchodníků přizpůsobuje své ceny podle výsledků sledování. Není však zřejmé, zda ono přizpůsobování je klasické nebo algoritmické. Vedoucí manažeři Uberu naopak prohlašují, že ne Uber, ale algoritmy stanovují cenu a že algoritmy jim vlastně určují, jaký je trh (MEHRA, S. K. *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, s. 1324).

68 PICHT, P. G. Competition (law) in the era of algorithms. *European Competition Law Review*. 2018, Iss. 9, s. 403.

69 OECD, 2017. *Algorithms and Collusion, Competition Policy in the Digital Age*. Dostupné z: <http://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf>, s. 24. Přístup 20. 8. 2019.

70 Výjimečně se dokonce judikovalo, že mlčenlivé porozumění vytvářené a probíhající po dlouhou dobu postačuje k dosažení dohody, a to dokonce i bez osobní komunikace (srov. případ *United states v. Consol. Packaging Corp. 575 F2d 117, 126, 7th Cir. 1978*, cit. podle HARRINGTON, J. E., Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agents*, s. 40). Za komunikaci se také dá pokládat zveřejnění jednostranného zvýšení cen předem, prokáže-li se svědecky, že se tak stalo s nadějí (!), že konkurenti provedou totéž (ibidem, s. 46). Tak extenzívní a expanzívní pojetí by v našem právu asi neprošlo.

Z hlediska ekonomického je přitom zakázaná explicitní koluze stejně škodlivá a nežádoucí jako tolerovaná koluze tacitní (mlčky učiněná, neboli paralelní chování) – snižuje výstup, vede k nadsoutěžním cenám a snižuje spotřebitelský blahobyt. Při mlčky učiněném srozumění se sice účastníci výslovně nedomlouvají na výsledku, nekomunikují spolu o ceně či jiném předmětu protisoutěžní dohody a svoje volby činí nezávisle, ale jsou si vědomi výrobních funkcí konkurentů a patřičným způsobem kalkulují jejich ekonomickou odpověď.[71] Převládá dlouhodobě názor, že vědomý paralelismus by měl zůstat legální, i když vede ke škodám. I když soutěžitel spoléhá na to, že jeho chování konkurence napodobí, nepůjde o zakázanou dohodu, a to nikoliv proto, že by takové chování bylo žádoucí (neboť je naopak nežádoucí), ale zcela pragmaticky proto, že je právně téměř nemožné na takovou provázanou cenotvorbu reagovat a vymyslet nějaký korektivní právní nástroj. Znamenalo by to nařizovat, aby se ceny stanovily bez ohledu na předpokládanou reakci soutěžitelů.[72] To je v tržní ekonomice absurdní a nemožné.

Soutěžní právo (přinejmenším v EU a v USA) tedy zakazuje jen explicitní koluzi, zatímco koluzi tacitní toleruje. Jinak by se totiž bránilo inteligentní adaptaci konkurentů na chování soupeřů; navíc by se těžko postihovalo (a vůbec prokazovalo) protisoutěžní srozumění, jež ani není protisoutěžní dohodou, na jejíž postih bylo antitrustové právo vymyšleno. Přes řadu teoretických výhrad k tomuto konceptu striktní oddělenosti dohody a mlčenlivého srozumění jde o cestu prakticky (materiálně-právně i procesně a důkazně) schůdnou, jíž se ve světě i u nás tradičně přidržují i soudy. Opačný přístup (pokládat za zakázanou dohodu i tacitní koluzi[73]) by byl jednak *de lege lata* nezákonný (nejde o dohodu), a jednak by svojí extenzitou kriminalizoval úplně standardní a racionální chování obchodníků a ochromil by je v konkurenčním boji. Zakázat tacitní koluzi nelze nejen z teoretických, ale především z praktických důvodů. Ze stejných důvodů není možno zakázat veškeré praktiky (včetně cenových algoritmů) jen proto, že usnadňují koluzi. Jiná by byla ovšem konkrétní možná situace, pokud by se zjistilo, že algoritmus nemá jinou funkci, než usnadnit koluzi nebo jí přímo dosáhnout, aniž tedy má jakýkoliv přínos k efektivnosti nebo ve prospěch zákazníků či soutěže. V takovém případě by mohlo jít o nepřímý indikátor pravděpodobné protisoutěžní dohody prostřednictvím algoritmu, ale o nic víc. Existence zakázané dohody by se musela dokázat věrohodnějšími prostředky. Nemyslím, že samotná existence usnadňujících praktik by obstála jako nepřímý důkaz dohody.[74]

Nasazení algoritmů může usnadnit koluzi nejméně čtyřmi cestami.[75] Především obrovská kapacita sběru a analýzy velkého množství dat o konkurentech umožňuje odhalit jejich výrobní funkce a obchodní strategie. Zadruhé, algoritmy brání nedobrovolné destabilizaci koluzivní rovnováhy, kterou by jinak mohl způsobit omyl při reakci na chování protistrany. Algoritmy dále nepodléhají lidským slabostem, jako např. laxnosti zástupce či oportunismu při upřednostňování krátkodobých a osobních výhod před dlouhodobou

71 PICHT, P. G. *Competition (law) in the era of algorithms*, s. 404.

72 Srov. HARRINGTON, J. E., Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agent*ss odkazem na judikaturu, s. 64.

73 Názor, že by se měla i tacitní koluze zakázat (srov. KAPLOW, L. On the meaning of Horizontal Agreements in Competiotion Law. *California Law Review*. 2011, Vol. 99, No. 3, June, s. 683) je podle mého soudu extrémní a nerealistický, protože znamená kriminalizaci zcela racionální a nezbytné cenové reakce na jednání konkurenta na trhu.

74 Jak tvrdí GAL, M. S. Algorithms as Illegal Agreements. *Berkeley Technology Law Journal*. 2019, Vol. 34, No. 67, s. 104.

75 PICHT, P. G. *Competition (law) in the era of algorithms*, s. 405.

prosperitou díky dodržování mlčky učiněné koluze. A konečně algoritmy zvyšují četnost a snižují latenci (zvyšují transparentnost) reakcí mezi účastníky trhu.

Koordinace lidských vůlí může být nahrazena automatizovanými přeceňovacími mechanismy i na principu *hub and spoke*.[76] Algoritmy monitorující ceny konkurentů mohou snadno přerůst do koordinační fáze spojené dokonce s trestáním odchylek[77] od dohodnutých cen či jiných podmínek; právě ceny jsou ovšem nejsnáze kontrolovatelné a také jsou nejatraktivnějším objektem koluze.

Na nejnižší úrovni se můžeme setkat s tzv. expertními algoritmy,[78] které fungují podle předem zadaných parametrů a není u nich problém s přičitatelností důsledků jejich činnosti.[79] Snadno mohou naplnit definici zakázané dohody. Složitější to může být u reaktivních algoritmů, jež berou v úvahu rozhodnutí jiných hráčů. Některé vyspělejší algoritmy pracují nejen na základě statických programových pokynů, ale mohou mít i samoučicí schopnosti, vytvářejí si „vlastní" (programem ovšem vymezený) rozhodovací prostor a postup na základě analýzy dat na vstupu. Jsou přitom schopny řádově snížit čas jinak potřebný k adaptivním reakcím lidské inteligence na chování konkurenta a snížit počet opakovaných „her" nutných k dosažení zkoordinované rovnováhy.[80] Představují jakýsi druh umělého zástupce lidí i při jejich případné protiprávní aktivitě.[81] To může zatemnit přičitatelnost takto rafinovaně „outsourcovaného" jednání konkrétní osobě.

3.2 Přičitatelnost algoritmizovaného jednání

Některé algoritmy nemusí být prvoplánově navrženy k porušování práva (ale třeba jen k maximalizaci zisku[82]), ale přesto „se" ho autonomně „dopustí". Protože algoritmy ze své povahy nedisponují myslí a nemohou mít ani záměr nebo úmysl uzavřít dohodu, mohla by být právně technickým řešením přičitatelnost výsledku tomu, kdo takový algoritmus s koluzivním potenciálem má pod kontrolou, respektive jej používá, aniž jej nutně musí sám vyvinout. Regres vůči profesionálnímu programátorovi za porušení zadání není samozřejmě vyloučen. Tradiční ilegální cenotvorba (v kartelech *offline*) nepřestane být nezákonná jen proto, že proběhne *online*. Fakt, že algoritmus osoba jej používající sama nevyvinula, nemůže být sám o sobě relevantní.

Očekávatelný bude patrně nejčastěji eventuální úmysl. Nasazení samoučících algoritmů s možností sjednocovat ceny patrně dovolí konstatovat existenci eventuálního úmyslu dopustit se zakázané dohody. Ani onen eventuální úmysl ovšem není u koluzních skutkových podstat potřebný; forma zavinění není důležitá z hlediska spáchání deliktu,

---

76 Metafora označující centrální roli náboje kola (*hub*), jehož vliv se projevuje prostřednictvím loukotí či špic (*spokes*).

77 To zvyšuje účinnost kartelu, protože důvěra v to, že se ostatní od dohody neodchýlí a nesníží tak profit ostatním účastníkům, je nahrazena spolehlivějším automatismem postihu odchylek.

78 OECD, 2017. *Algorithms and Collusion, Competition Policy in the Digital Age*, s. 11–12.

79 Mohou např. bleskurychle detekovat změny cen u konkurentů (např. u čerpacích stanic) a okamžitě se jim přizpůsobit i bez výměny cenových informací s konkurentem. Srov. s těžkopádným objížděním konkurenčních stanic kurýrem zjišťujícím dávkově a přetržitě cenové pohyby toho dne.

80 GAL, M. S. *Algorithms as Illegal Agreements*, s. 82.

81 Již v roce 2015 uplatňovala třetina prodejců Amazonu automatizované (algoritmizované) ceny (CALVANO, E. – CALZOLARI, G. – DENICOLO, V. – PASTORELLO, S. Artificial intelligence, algorithmic pricing, and collusion, *VOX CEPR Policy portal*. Dostupné z: <https://voxeu.org/article/artificial-intelligence-algorithmic-pricing-and-collusion>, s. 1. Přístup 12. 8. 2019). Již i ti nejmenší obchodníci si tuto vymoženost mohou dovolit.

82 GAL, M. S. *Algorithms as Illegal Agreements*, s. 106.

na rozdíl od dopadu na výši sankce. Pouhé paralelní chování nelze postihnout samo o sobě, protože může být výsledkem nezávislého racionálního jednání.

Pokud se paralelismus spojí s využíváním monitorovacího algoritmu, jenž takové nezávislé racionální jednání usnadňuje a poskytuje mu spolehlivější informační základnu, nelze ani to přičíst automaticky k tíži uživatele algoritmu, pokud se neprokáže existence naprogramované adaptace – ta by se již dala chápat jako druh koluze. Bezpečným přístavem by mohlo naopak být průkazné naprogramování bariér proti automatizovanému algoritmizovanému slaďování cen (tedy proti koluzi).[83] Nelze dopustit, aby se kartelisté zbavili své odpovědnosti tím, že se prostě skryjí za počítačový program.[84]

Na druhé straně se ovšem musí připustit, že algoritmy se mohou vymknout kontrole a mohou do jisté míry začít žít svým vlastním životem, který se vzdaluje od role pouhého nástroje k porušování práva a který může svými výsledky překvapit i své autory.[85] Přitom mohou vyvinout vzorce neodhalitelné člověkem, přičemž obvykle neposkytují ani informace o průběhu rozhodovacího procesu; je to projev „černé skříňky“.[86]

Přijmout ovšem přísný přístup a přičítat veškeré důsledky tvůrci či uživateli algoritmu, by mohlo sice vést k jevově atraktivnímu odstranění mezer (hluchých míst) v odpovědnosti, ale i ke zmrazovacímu účinku – jedinou cestou úniku od odpovědnosti za dopady algoritmů by totiž bylo vyhnout se zcela jejich používání. To by ovšem bylo na újmu funkčnosti trhu a spotřebitelského blahobytu. Vhodnější by bylo využít instrumentária trestního i civilního práva, které bylo vyvinuto pro odstínění stupňů přičitatelnosti a míry zavinění.[87] Měl by se posuzovat rozumný standard péče a předvídatelnosti.[88] Nevyhnutelné budou požadavky na soutěžní *compliance* algoritmů včetně povinnosti dozoru a pravidelných kontrol programů z hlediska dopadu na soutěž. Autor koluzivního algoritmu by mohl být považován za odpovědného, byť by nebyl přímým účastníkem dohody.[89]

Funkcí zvláštních druhů odpovědnosti za následky použití rizikových technologií je především pragmatická distribuce zbytkových rizik v případech, kdy je nemožné (nebo rozumně neproveditelné) zjistit porušení povinnosti provozovatele nebezpečné technologie, ale škoda vznikla nepochybně v souvislosti s jejím provozem. Bylo by právně politicky neobhajitelné (nespravedlivé), kdyby škodu či újmu v podobných případech nakonec snášel ten, jemuž vznikla, a nikoliv ten, v rámci jehož činnosti vznikla, byť nelze dokázat, že ji způsobil či zavinil.

---

83 Algoritmy by tedy podle parafrázovaných slov komisařky pro soutěž M. Vestagerové měly před tím, než budou vpuštěny do života, projít právnickou fakultou (VESTAGER, M. Europe's chief regulator Margrethe Vestager on reining in tech: 'This is the biggest wake-up call we've ever had'. Dostupné z: <https://www.vox.com/2017/11/29/16712940/margrethe-vestager-european-commission-competition-regulation-recode-decode-kara-swisher-podcast>). Přístup 20. 8. 2019.

84 Narážíme ne jeden z projevů „společnosti černé skříňky“ (*black box society*); algoritmy zamýšlené jako rádci a pomocníci nás mohou zotročit a stát se nevyzpytatelným orákulem (SIMANOWSKI, R. Künstlliche Intelligenz: Aus dem Strudel der Algorithmen taucht das Orakel wieder auf. *Neue Zürcher Zeitung*. 13. 5. 2019). Poddat se předvídanému „digitálnímu panteismu“ není však evidentně přijatelná rada pro antitrustové orgány a pro soutěžní politiku digitální doby, i když by to bylo pohodlné a alibistické.

85 Byly popsány případy, že automatizovaně počítaná cena vstupenek do lyžařského resortu Colorado se odvíjí od automaticky hlášeného množství sněhu, nebo že nápojové automaty mění ceny za nápoje podle vnější teploty. To může ve spojení s „velkými daty“ vést k dokonale individualizované cenové diskriminaci. Nedostatek lidské kontroly vedl i excesům, jako že učebnice o ovocných muškách kvůli interaktivním cenovým automatům používaným Amazonem stála až 23, 7 mil. USD, nebo kdy naopak v důsledku chyby prodávaly United Airlines letenky za 5 USD (MEHRA, S. K. *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, s. 1323; 1336).

86 Hovoří se o samoučících algoritmech (*deep-learning algorithms*; srov. PICHT, P. G. *Competition (law) in the era of algorithms*, s. 404).

87 JANKA, F. S. – UHSLER, S. B. Antitrust 4.0 – *The Rise of Artificial Intelligence and emerging challenges to antitrust law*, s. 121 an.

88 Srov. Např. rozhodnutí SDEU ve věci *AC Treuhand AG v EC* (C-194/14 P, C 2015, bod 30).

89 Doktrína *hub and spoke*, viz případ *Treuhand*, ibidem.

Tvorba, nasazení a využívání algoritmů jakožto druhu „chytrých smluv" představuje poněkud odlišný případ. Ať už jsou či nejsou vývoj, nasazení a funkce algoritmů (včetně jejich strojového učení, respektive „samoučících" schopností) plně pod kontrolou jejich uživatele, případné protiprávní následky by se měly vždy přičíst k jeho tíži. V tom se situace úpravě důsledků používání rizikových technologií podobá. Na rozdíl od provozu zvlášť nebezpečného nebo škod způsobených provozní činností lze však v algoritmu jakožto sekvenčním sledu strukturovaných programovacích kroků[90] (včetně algoritmu „samoučícího") vždy dohledat vůli jeho autora, která se v onom sledu kroků projevila (třeba i nedbalostí v podobě zanedbání standardu opatrnosti a poskytnutí neadekvátního prostoru pro umělou inteligenci strojově se učící mimo předběžnou či následnou kontrolu inteligencí lidskou).

V této souvislosti je zřejmé, že právě např. cenové adaptivní („chytré") algoritmy „bez dohledu" jsou samy o sobě rizikové. Prostor pro indeterminismus samoučícího algoritmu (tedy pro jeho „nezávislé" zdokonalování) se otevře opět buď podle zadání objednatelem (a na jeho riziko), nebo je důsledkem vadného plnění programátora. Podle toho by se měly přičítat důsledky případné protiprávnosti vyplynuvší z takového indeterminismu.[91]

Přičitatelnost následků uživatelům algoritmů nevylučuje regresní postih vůči jejich tvůrcům a/nebo operátorům. Uživatel, pokud není sám programátorem algoritmu, přinejmenším určil tvůrci parametry, jež má algoritmus splňovat. Povedou-li k protiprávnosti ony sjednané rizikové parametry, nelze její důsledky přenést z uživatele algoritmu na programátora. Způsobí-li protiprávnost algoritmu a újmu programovací chyba algoritmu či nějaká jeho vlastnost nad rámec zadání (např. v důsledku tvůrčí hravosti či aktivismu programátora), měl by důsledky snášet programátor v rámci odpovědnosti za vady plnění uplatněné uživatelem. Je možné uvažovat o převzetí nebezpečí oběti, o slibu odškodnění, o smluvních doložkách či prohlášeních ve smlouvách uživatelů s programátory o souladu s právem (*compliance*) apod. Lze též sjednávat nebo i *de lege lata* veřejnoprávně ukládat transparentnost zdrojových kódů[92] i jejich prověřování. Roli v obsahové kontrole algoritmů coby předmětu plnění může samozřejmě kromě právních nástrojů hrát i programátorská a obchodnická etická samoregulace.

Předvídatelnost a možnost vyhnout se negativním následkům při rozumné péči a rozumné bdělosti a ostražitosti by se měly v dovozování případné odpovědnosti tvůrců a uživatelů algoritmů brát v úvahu velmi nuancovaně a individualizovaně, a nikoliv pohodlně a „sekýrnicky".[93] Algoritmům by se mohla přiznat jistá míra nezávislosti a u jejich tvůrců by se mělo zkoumat, zda věděli nebo měli vědět o inherentním riziku spojeném s algoritmy.[94] Exonerační důvody by neměly být vyřazeny jen proto, že je to z regulatorního hlediska pohodlnější a snáze „zadministrovatelné". Měly by se hledat méně kontroverzní cesty, nežli zvažovat zákaz jakéhokoliv jednání s potenciálně protisoutěžními

90 HARRINGTON, J. E., Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agents*, s. 17 an.

91 I deterministický algoritmus představuje pro běžného uživatele druh „černé skříňky". Získá-li algoritmus navíc adaptivní a zpětnovazební schopnosti označitelné jako strojové učení (takže ztratí onen striktní determinismus), lze jej označit jako *double blackbox*. Jeho průměrnému uživateli nezbývá než se uchýlit k jakési racionální rezignaci pod heslem „důvěra namísto porozumění." Srov. ibidem, s. 28.

92 Ibidem, s. 340 an.

93 Nezřídka se vyskytují názory, že by měla být zavedena objektivní odpovědnost za design algoritmu, který podnik používá (ŠMEJKAL, V. My nic, to roboti! Protikartelové právo a cenové algoritmy. *Antitrust*. 2017, roč. 8, č. 3, s. 85), jakož i odpovědnost za to, aby algoritmy byly naprogramovány způsobem znemožňujícím udržovat společnou cenu (*compliance by design*).

94 To platí především o tzv. *deep learning algorithms*.

tendencemi a bez vyrovnávacích tendencí prosoutěžních, byť by jednání nezakládalo dohodu v tradičním smyslu.[95]

Vodítkem může být obdoba nedogmatického a strukturovaného přístupu, který se uplatňuje při soutěžněprávním posuzování výměny citlivých obchodních informací. Samotné sdílení takových informací umožňujících nejistotu o budoucím konkurentově chování na trhu se pokládá za dohodu omezující soutěž.[96] A algoritmy plní přinejmenším tuto funkci sdílení citlivých informací, pokud nejdou ještě dál a nesnižují nejistotu o budoucím chování třeba i tím, že budoucí chování přímo „čtou“ předem a reagují na ně.

Byl navržen i jistý orientační soubor testů umožňujících identifikovat soutěžně nebezpečné algoritmy s větší pravděpodobností.[97] Nepřímým důkazem algoritmizované kartelové dohody by měla být existence tzv. „plus faktorů“: a) plánované a odvratitelné jednání; b) jednání usnadňuje koordinaci; c) usnadňuje ji tím, že vytváří záměrně závazky podle jednotného schématu; d) tyto závazky nelze ospravedlnit prosoutěžními důvody. Pokud by algoritmy naplnily tyto znaky, daly by se pokládat za koordinační ve své podstatě (*coordination by design*). Nenahradilo by to samozřejmě důkazy, ale signalizovalo by to přinejmenším „tmavě šedou zónu“, v níž se uživatelé algoritmů pohybují. Mohlo by to snad zúžit motivaci k dosahování nadsoutěžních zisků v prostoru mezi nezákonnou explicitní koluzí a zákonnou koluzí tacitní.

3.3 Chování v algoritmizovaném prostředí

Blockchainy spojené s cenovými algoritmy představují regulatorní výzvu podobnou kvadratuře kruhu. Decentralizace a transparentnost informací podporují fungování tržního mechanismu, ovšem jenom pokud se nezneužijí v jeho neprospěch. Jde doposud o „hru s ohněm“ nejen ze strany uživatelů blockchainů, ale i regulatorních orgánů. Opakuji, že zatímco jednostranné jednání v podobě cenového následování je ekonomicky zcela racionální a nelze je právně zakázat, dohoda o cenovém následování se přísně zakazuje; navenek jsou přitom nerozeznatelné.[98] Snížení nejistoty o budoucím chování na trhu musí být přitom důsledkem vzájemné komunikace mezi stranami, nikoliv prostého monitoringu trhu.[99] Cenové algoritmy nejsou nové ve své podstatě,[100] ale v obrovských možnostech svého zpracování na výkonných a propojených počítačích.[101]

---

95 Tento regulatorně přísný přístup hrozící falešnými pozitivy navrhuje GAL, M. S. *Algorithms as Illegal Agreements*, s. 117. Obávám se důsledků takové agresivní a předčasné nadregulace. K podobným tendencím srov. vtipné odlišné stanovisko prof. Musila k rozšiřování pojmu eventuálního úmyslu s využitím skvostné pasáže z raportu putimského četnického strážmistra Flanderky z výslechu „ruského špióna“ Švejka – sp. zn. III. ÚS 3255/13, body 34–35.

96 Srov. Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci – 2011/C 11/01. V recitálu 70 se např. konstatuje, že výhradní výměna informací může vést k uzavření trhu narušujícímu hospodářskou soutěž.

97 Viz GAL, M. S. *Algorithms as Illegal Agreements*, s. 110 an., 113 an.

98 WHISH, R. – BAILEY, D. *Competition Law*. 8. vydání. Oxford: Oxford University Press, 2015, s. 597.

99 KUPČÍK, J. Cenové následování v perspektivě digitálních trhů. *Obchodní právo*. 2018, č. 11, s. 408, s odkazem na stanovisko generálního advokáta ve věci *Wood Pulp*.

100 Do učebnic vstoupil např. velký americký elektrický tendrový kartel z padesátých let, jehož účastníci využívali pro určení vítězné nabídky mezi nabídkami krycími měsíční fáze (*Westinghouse Electric Corporation, GE Electric Company and Allis Chalmers Manufacturing Company, v the Judges of the US District Court, District of Utah, Central Division*, 311 F. 2d-10th Cir. 1962; PEREIRA, V. Algorithm-driven collusion: pouring water into new bottles or new wine into fresh wineskins? *European Competition Law Review*. 2018, No. 5, s. 215).

101 Tyto možnosti posouvají na vyšší úroveň i tzv. kartely *hub-and-spoke*. V případu *ETURAS* (Case C-74/14, 21. leden 2016) rozhodoval SDEU o postupu litevských spřežených na online trhu rezervačních služeb E-Turas. Litevský soutěžní úřad pokutoval

Nikoliv každé využití počítačů ve vztahu k tvorbě cen musí být závadné.[102] Využití počítačového monitoringu k replikaci ceny vedoucí firmy na trhu (prosté cenové následování) není kartelové právně relevantní. Otázka (důkazní) však je, jde-li skutečně jen a pouze o toto chování a o nic jiného. Stažení a zavedení cenového algoritmu je již spornější, protože snižuje (ne-li odstraňuje) nejistotu o chování konkurentů na trhu, což zakládá protiprávnost. Kontroverzní je též využití algoritmů získaných konkurenty a jejich dekódování, jež může vést k monopolistickým ziskům.

Cenové algoritmy umožňují tacitní koluzi, aniž by bylo potřeba se na tom předběžně domlouvat a aniž by to strany vůbec zamýšlely. Možnost koluze klesá s počtem účastníků a s počtem různých asymetrií, jako jsou náklady, tržní podíly apod.[103]

Může existovat jeden společný algoritmus pro více soutěžitelů, při jehož použití hrozí pravděpodobný konflikt se zákazem kartelů (typicky zakázaná dohoda *hub and spoke*), ale může se jednat i o více algoritmů reagujících jeden na druhého – v tom případě jde jen o cenové následování, které není důsledkem výměny informací mezi soutěžiteli a jež není zakázáno jako dohoda omezující soutěž. Ovšem subjekty využívající cenové algoritmy mohou porušit zákaz kolektivní dominance, pokud mají všichni přehled o všech.[104] Snazší možnost a vyšší pravděpodobnost nezákonné koluze prostřednictvím algoritmů nesmí znamenat jejich paušální apriorní omezení jakožto nebezpečného nástroje, protože na druhé straně přinášejí trhu velkou transparentnost a bleskovou reakci na vývoj na trhu, čímž působí prosoutěžně.[105] Cenové algoritmy vlastně mají funkce „mírotvůrce“: brání cenovým válkám; jsou schopny koluze, aniž by měly zakódovánu takovou instrukci a aniž by si vyměňovaly informace (komunikovaly spolu).

Usnadnění právně nezakázané tacitní koluze prostřednictvím cenových algoritmů je podle těchto liberálních přístupů do jisté míry mýtus. K mlčky učiněnému srozumění může dojít za určitých podmínek – srovnatelná velikost konkurentů a podobnost jejich nákladové struktury, podobnost sortimentu (homogenní produkce). V podobných situacích dochází k mlčenlivému srozumění již dnes, takže nejde o specifický „přínos“ algoritmů. Ono riziko je podstatně vyšší v případě, že algoritmy nejen monitorují, ale navíc spolu interagují, a dokonce se přitom i „samy“ učí. Slaďovací interaktivní záměr bude však v algoritmu znalecky zjistitelný. Podezřelé ze slaďovacího záměru bude používání stejných cenových algoritmů konkurenty.

---

cestovní agenturu Eturas (*hub*) za účast ve sladěných postupech týkajících se slev za rezervační služby. Eturas stanovil strop těchto slev a informoval cestovní kanceláře (*spokes*). Ty se neohradily a ani neoznámily postup soutěžnímu orgánu. Komunikace mezi uživateli online platformy vedla tedy k dohodě podobné klasické kartelové dohodě „v zakouřené místnosti“.

102 PEREIRA, V. *Algorithm-driven collusion: pouring water into new bottles or new wine into fresh wineskins?*, s. 221 an.

103 DENG, A. What Do We Know About Algorithmic Tacit Collusion? *Antitrust*. 2018, Vol. 33, No. 1, Fall 2018, s. 88, 90. Obecně koluzi usnadňuje především symetrie konkurentů, jejich menší počet, homogenita produktu, vyšší bariéry vstupu, transparentnost trhu, stabilita poptávky, malé a časté nákupy spotřebitelů. Identifikace takových relevantních trhů vypovídá ovšem jen o jejich náchylnosti ke koluzi účastníků, ale neříká nic o výslovné nebo tacitní koluzi. Navíc se algoritmy týkají jen cenových či množstevních kartelů, ale ne jiných druhů (rozdělení trhů, manipulace nabídek ve veřejném zadávání. Někteří soutěžitelé používají ceníky, jiní využívají obchodní zástupce zavázané k dané cenové politice, takže cesty k faktické cenové koordinaci mohou být různé.

104 KUPČÍK, J. *Cenové následování v perspektivě digitálních trhů*, s. 410.

105 Pokud např. společnost A vyhlásí slevovou akci a konkurent B (díky monitorovacímu a reaktivnímu algoritmu připojujícímu se k cenovým změnám konkurenta) poskytne tutéž slevu svým zákazníkům, ti mohou mít výhody ze slevy poskytnuté společností A, aniž by k ní za cenu transakčních nákladů museli přejít. Na druhé straně může tento mechanismus odrazovat od poskytování slev, na nichž by vlastně jejich vyhlašovatel nic nezískal (příklad uvádějí LEWIS, S. – RIDYARD, D. Automatic harm to competition? Pricing algorithms and co-ordination. *European Competition Law Review*. 2018, Vol. 39, Iss. 8, s. 342).

3.4 Algoritmy a diskriminace

Cenové algoritmy mohou být nebezpečné pro soutěž i pro blahobyt spotřebitelů nejen jako ideální nástroj sjednocování cen, ale i tím, že umožňují tzv. dokonalou cenovou diskriminaci na trhu,[106] která se již dnes může ve značné míře individualizovat.[107] Různé věrnostní programy poskytují obchodníkům velmi přesná a personalizovaná data o zákaznících a spotřebitelích, využitelná k individuálnímu marketingu. Sociální sítě typu Facebook prozrazují o uživatelích svým provozovatelům tolik, že mohou velmi snadno sestavit každému z nich osobnostní profil, jenž je komerčně skvěle využitelný.[108]

Vliv diskriminace na soutěž může ovšem být víceznačný.[109] Cílená diskriminace může zvýšit tržní výstup a snížit ceny pro určité skupiny zákazníků, ale i zvýšit je pro jiné. Cenovou diskriminaci mohou výrazně podpořit tzv. velká data.[110] Ta jsou způsobilá odhadnout velmi přesně cenový interval, respektive cenový strop, jejž je jednotlivý spotřebitel (či vybraný okruh spotřebitelů) ještě ochoten přijmout.[111] Velká data otevírají prostor selektivní cílené inzerci, a navíc umožňují individualizované zobrazení ve vyhledávačích. V takovém případě nemusí všichni spotřebitelé nutně obdržet při zadání téhož produktu stejné výsledky, ale různým lidem se poskytují k jejich (dez)orientaci na trhu různé „na míru přizpůsobené“ webové verze.[112]

Sledují se přitom stále častěji nejen „onlinové“ aktivity, ale i aktivity „offlinové“. Díky tomu se mohou vytvářet a „ladit“ osobní digitální profily každého zákazníka, s nimiž se pak dá s využitím metod behaviorální psychologie manipulovat a dá se tak přiblížit k maximálnímu využití ekonomického potenciálu každého zákazníka. Ač to zní na prvý

---

106 MCSWEENY, T. – O'DEA, B. The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement. *Antitrust*. 2017, Vol. 32, No. 1, Fall, s. 78 an; EZRACHI, A. – STUCKE, M. E. *Virtual Competition*. Cambridge, Massachusetts – London, England: Harvard University Press, 2016, s. 83 an.

107 Personalizovaná (individualizovaná) cenová diskriminace se liší od dříve běžné dynamické plošné diskriminace (při níž se jiné ceny uplatňují v předprodeji a jiné na poslední chvíli; jiné v mrtvých časech a jiné ve špičkových hodinách; jiné u čerstvého a jiné u staršího zboží atp.). Jde o přesun od statistického (plošně skupinového) přístupu k politice *ad personam*.

108 Srov. HENKEL, Ch. H. Facebook is phantastisch für die Demokratie. *Neue Zürcher Zeitung*. 21. 11. 2019. V rozhovoru se stanfordským profesorem psychologie M. Kosinskim se tu velmi expresívně kritizuje svatouškovství, s nímž se zakazuje využívat ve veřejné sféře některé osobní údaje občanů, byť by jim třeba mohly zachránit život, ale Facebook a Google je mohou používat, aby nám prodávali všemožné svinstvo (*„allen möglichen Mist“*).

109 Zákazníci jsou ochotni zaplatit za produkt podle odlišné poptávkové síly různou cenu, neboť se liší jejich tzv. rezervační cena, již jsou ochotni zaplatit. Producenti vytěží z diskriminačních prodejů více než při stejných cenách a navíc se zvýší spotřebitelský blahobyt, neboť zboží a služby si dopřejí i spotřebitelé, kteří by je za jednotnou cenu (pohybující se nad jejich cenou rezervační) nekoupili. Zvýšený výnos přispívá k rychlejší návratnosti fixních nákladů a k vyšší dynamické efektivnosti (což je jedno z hledisek spotřebitelského blahobytu); blíže BEJČEK, J. Cenová diskriminace a tzv. dvojí ceny v evropském a českém kontextu. *Právní fórum*. 2008, č. 5, s. 181.

110 Cenu pak díky nim bude záviset na řadě ukazatelů, jako je např. vlastnictví auta, nebo třeba i politické názory či jiné propojené ukazatele (MCSWEENY, T. – O'DEA, B. *The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement*, s. 77 an.). Je evidentní, že diskriminační kritéria nejsou produktem algoritmů či umělé inteligence, ale že je do algoritmů vnášejí jejich programátoři, kteří do nich kódují (třeba i mimo rámec technického zadání) svoje hodnotové představy, pozice a předsudky. Ty jsou implicitně obsaženy i v algoritmech adaptivních (se samoučícími schopnostmi). Algoritmy nejsou imunní ani vůči základním problémům diskriminace, při nichž se negativní a nepodložené domněnky mění v předsudky. Programují je totiž lidé, jejichž hodnoty se do softwaru promítají, ale jsou přitom skryty v „černých skříňkách“. Srov. též PASQUALE, F. *The Black Box Society*, s. 8, 38. Je jasné, že algoritmy nemají předsudky, pocity skupinové identity, konformity a jiná hodnotová omezení, pokud je do nich programátoři vědomě či nevědomě nevnesou (zatímco lidé je mají, aniž si to často vůbec uvědomují).

111 Tzv. rezervační cena. Kladný rozdíl mezi ní a cenou skutečnou je spotřebitelský nadbytek či přebytek (*consumer surplus*). Big data ve spojení s cenovými algoritmy umožňují „vyždímat každou minci pod úrovní rezervační ceny“, a to individualizovaně. Rezervační cena se vyjevuje typicky při aukcích, ale dá se extrapolovat i pomocí velkých dat a algoritmů.

112 EZRACHI, A. – STUCKE, M. E. *Virtual Competition*, s. 93.

pohled paradoxně a jako *oxymorón*, ocitáme se v éře masové individualizace, jež ruku v ruce s transparentností zákazníků umožňuje téměř dokonale diskriminovat každého z nás. Vzhledem k tomu, že vztah mezi obchodníky a zákazníky je zásadně asymetrický, tyto důsledky si zákazník nemusí ani uvědomit. Teprve budoucnost přiblíží odpověď na otázku, jestli (a popřípadě v jakém rozsahu) povede dokonalá cenová diskriminace k „vykořisťování bohatších", ke znehodnocení rozdílů v příjmech, k nivelizaci spotřeby a k demotivaci, což by možná změnilo i makroekonomické funkce trhu.[113]

Velká data propojená do plošných adaptabilních sítí podporují a zefektivňují nejen možnost vykořisťování tržní protistrany, a to zejména u tržně silných podnikatelů. To má dopady nejen na soutěžní prostředí, ale přímo i na blahobyt spotřebitele. Navíc v sobě skrývají hrozbu vylučovacího ohrožení nebo omezení soutěže, protože posilují tzv. *gatekeeper effect* ve prospěch stávajících účastníků na trhu, a obsahují tudíž výrazný monopolizační potenciál; i to je výzva pro právní ochranu soutěže.

Mimo rámec tohoto pojednání je rovněž otázka, zda by dokonale personifikovaná cenová diskriminace neporušovala zákaz diskriminace podle zákona o ochraně spotřebitele, respektive zákaz zneužití dominantního postavení podle zákona o ochraně hospodářské soutěže, pokud by diskriminujícím subjektem byl dominant na relevantním trhu.

Samozřejmě může sehrát korekční roli nasazení digitálních zákaznických či spotřebitelských analyticko-detekčních nástrojů, které odhalují cenové algoritmy tržní protistrany, personalizaci cenových nabídek a reklamy apod. Ty mohou kompenzovat rozdíly v tržní síle a případně vést k sebeobranným individuálním i kolektivním opatřením.

Závěr

Reakce soutěžní politiky na cenové algoritmy by měla být velmi uvážlivá a obezřetná,[114] dokud neexistuje jasný test k odlišení protisoutěžní dohody od mlčky učiněného srozumění, jež se navenek a ekonomicky nijak neliší, na rozdíl od diametrálně odlišného hodnocení právního.

Je možné zastávat extrémní stanoviska ve prospěch tvrdé (preventivní) regulace i proti ní, jakož i různé kompromisní polohy mezi krajními póly. Nerozhodují o nich jen věcné důvody a argumenty, ale také (ne-li především) osobní hodnotové nastavení jednotlivců

---

113 Tyto obavy jsou asi prozatím poněkud předčasné. Účinky cílené individualizované cenové diskriminace by byly mírnější díky samoregulaci trhu a informační zpětné vazbě. Cenově individuálně diskriminující obchodníky by velmi brzo začali odmítat zákazníci, již by patrně takovou diskriminaci nepokládali za férovou. Žádný zákazník navíc není tak naivní a není tak fatálně odkázán na internetové reklamy a vyhledávače, aby si (*ex post* i *ex ante*) nezjistil, za jakou cenu lze zboží běžně na trhu pořídit. Digitální transparentnost by fungovala jako negativní zpětná vazba. Zpětnovazebně působí digitalizace i v opačném směru. Negeneruje totiž pouze digitální obchodníky, ale formuje i digitální spotřebitele a zákazníky. Ti by se postupům proti sobě dokázali účinně bránit, neboť jsou (alespoň někteří) schopni identifikovat cenové algoritmy, respektive jejich nasazení a třeba i hromadně bojkotovat jejich uživatele. Navíc stále funguje a bude fungovat i konkurence klasických kamenných obchodů. V praxi se mimochodem mnoho příkladů reálné cenové diskriminace neobjevilo. Britský *Office for Fair Trading* dokonce nedávno konstatoval, že informace o jednotlivcích nevyužívají podnikatele k tomu, aby jim zvedli ceny (DOLMANS, M. – TURNER, J. – ZIMBRON, R. Pandora's box of online ills: We should turn to technology and market-driven solutions before imposing regulation or using competition law. *Concurrences*. 2017, No. 3, s. 6). Jiná bude určitě pozice běžného spotřebitele, a jiná situace institucionálního zákazníka. Pro běžného spotřebitele, který bude díky digitalizaci, velkým datům a algoritmizaci stále transparentnější a předvídatelnější, budou algoritmy naopak stále větší záhadou. Budou se patrně rozevírat nůžky mezi schopností algoritmů předvídat, jak se bude chovat zákazník, a na druhé straně sofistikovaností a neproniknutelností toho, co a jak s ním dovedou udělat algoritmy. K tomu srov. MARTINI, M. *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz*. Berlin: Springer Verlag, 2019, zejména s. 333 an.

114 LEWIS, S. – RIDYARD, D. *Automatic harm to competition? Pricing algorithms and co-ordination*, s. 343–344.

na rozhodujících pozicích, jejich osobní zkušenosti a z toho odvozený právně politický habitus.

Dá se pozorovat jistá bezradnost o dalším postupu vůči nové technologii dynamicky se vlamující do sfér, které tradičně počítaly jen s lidmi a s jejich autentickou osobní vůlí a psychologicky přirozenými reakčními schopnostmi. To platí i o antitrustovém právu. Někteří autoři varují, že koordinace prostřednictvím algoritmů je stále běžnější a že by se proto měl změnit původní náhled na apriorní zákonnost vědomého paralelismu. Poukazuje se na „důkazní paradox“, že tržní podmínky digitalizované ekonomiky bezprecedentně usnadňují komunikaci a koordinaci, ale současně velmi znesnadňují důkaz o explicitních dohodách, protože skutečná komunikace mezi partnery přestává být podstatná[115] a vlastně ani nemusí probíhat;[116] tento dopad má prý znamenat konec soutěžního práva, jak jsme je znali.[117]

Objevuje se i názor, že některé typy cenových algoritmů podporujících nadsoutěžní ceny (jako jsou samoučicí algoritmy stanovující cenu) by se měly zakázat automaticky (*per se*)[118] a že snad již nazrála doba, aby se zakázalo jakékoliv (*sic!*) chování s potenciálně protisoutěžní tendencí, jež nemá odpovídající prosoutěžní kompenzaci, a to ani kdyby takové chování nenaplňovalo znaky dohody v tradičním smyslu.[119] Vývoj doktríny a judikatury tímto směrem by předpokládal *ad hoc* analýzy jednotlivých algoritmů a zjišťování a poměřování těch jejich vlastností, které usnadňují koluzi, a těch, které naopak fungují prosoutěžně. To by bylo velmi náročné na expertízu i na předvídatelnost a právní jistotu soutěžitelů. Mohlo by to také v případě pochybností (které nelze vyloučit nikdy) odrazovat od používání i efektivních a prosoutěžních algoritmů.

Agresivnější přístup k získání nových pravomocí soutěžních úřadů a snaha vlamovat se nad rámec stávajících pravomocí soutěžních orgánů do algoritmů může mít zmrazovací efekt a může bránit rozvoji technologií včetně jejich nesporných kladných dopadů na trh a soutěž a v důsledku na blahobyt spotřebitele.

Lze očekávat a doporučit zdrženlivost jak v aplikaci klasických antitrustových nástrojů, tak i ve snahách získat nové pravomoci, byť by se prokázalo, že koordinované výstupy a používání algoritmů potenciálně korelují; je vhodné připustit, že klasické instrumentárium antitrustového práva nedosáhne na sporné případy, kdy mlčky dosažená koordinace chování vyústí v kolektivní výkon tržní moci.

Aktivismus spojený s pohodlným paternalisticko-restriktivním přístupem by mohl více uškodit než prospět. Cenové algoritmy jsou jen jednou z možných cest omezení soutěže, a to navíc jen cenové. Mají však i řadu pozitiv a mohou být zamýšleny poctivě a v dobré víře, aniž by nutně ochromovaly nezávislost v rozhodovacím procesu a vyřazovaly lidskou vůli. Mělo by se dopřát sluchu dynamičtějším necenovým teoriím újmy, vztahujícím se ke kvalitě (včetně ochrany soukromí) a inovacím, které by se neměly regulatorně apriorně zmrazit.

Obecná moudrost napovídá, že když člověk (určitě) neví, zda má něco udělat, tak to prostě udělat nemá. I v reakcích antitrustových úřadů na dosud málo probádaný fenomén

115 GAL, M. S. *Algorithms as Illegal Agreements*, s. 116–117.
116 Tak HARRINGTON, J. E., Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agents*, s. 22 an.
117 EZRACHI, A. – STUCKE, M. E. *Virtual Competition*, s. 211, 216 a porůznu.
118 Tak HARRINGTON, J. E., Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agents*, s. 48–49.
119 Tak GAL, M. S. *Algorithms as Illegal Agreements*, s. 117.

cenových algoritmů by měla platit obdoba Hippokratovy maximy „hlavně neuškodit"; nejdůležitější zásah může být i ten, který se neuskutečnil.[120] Proti preventivní ostražitosti a snaze připravit se doktrinálně i technicky na dobu, až se *science fiction* stane realitou a automatické systémy dosáhnou skutečného srozumění, tedy souzvuku myslí (*meeting of minds*),[121] nelze nic namítat.

Pokud však nezvítězí regulatorní pokora nad regulatorní paranoiou, aktivismem a možná i arogancí,[122] bude namístě obava, aby se s vaničkou nevylilo i dítě, tedy aby se regulátoři nedopustili tzv. falešných positiv (která vedou ke zbytečným obavám nebo intervencím). Regulatorní zásahy by se měly omezit na jasné případy nebo případy, u nichž se v drtivé většině projevují jednoznačně negativní dopady (analogie s *per se* zákazy typu tvrdých kartelů). Cenové algoritmy mohu ostatně být nejen nástrojem kartelizace, ale umožňují i nastavení k cenovému boji s konkurencí, vedoucímu ke snížení cen a ke zvýšení spotřebitelského blahobytu.[123] Kombinace cenových algoritmů s blockchainovou technologií snižuje identifikovatelnost účastníků v důsledku efektu neprůhlednosti (u soukromých blockchainů) a prohlubuje bezradnost antitrustových úřadů,[124] která by se mohla v nejhorším případě projevit jako snaha o restrikce a plošné pohodlné regulace blockchainů a cenových algoritmů.

Plošná regulatorní antitrustová infiltrace, jež byla snad jakž takž adekvátní v době průmyslové, se může míjet účinkem v době postindustriální a informatické. Bez ní jsou blockchainy neprůhledné, ale s ní by blockchainy (ty soukromé) ztratily atraktivitu a zčásti i samotnou použitelnost. Zvažovat by se dala možnost zavést mimořádná dozorová opatření antitrustových orgánů, které by mohly vstupovat do soukromých blockchainů a měly by přístup k dekódovacím klíčům. To ale v právním státě nelze činit preventivně a bez soudního dohledu. Technická logika blockchainů, v nichž neexistuje žádná třetí osoba v roli zmocněnce či opatrovníka, naráží na logiku antitrustového práva. Za robotizovaná narušení soutěže mohou teoreticky nést odpovědnost buď bezsubjektoví roboti (což nejsou ovšem ani soutěžitelé, ani podnikatelé[125]), nebo soutěžitelé („podniky" ve smyslu evropského práva); pokud ovšem nepřistoupíme na racionální, hodnotově-etickou a agnostickou rezignaci a nepřijmeme pozici, že by také nemusel nést odpovědnost nikdo.

---

120 MARDSEN, P. Who should trust bust? Hippocrates, not hipsters. *CPI Antitrust Chronicle*. 2018, April, s. 3. Dostupné z: <www.competitionpolicyinternational.com>.

121 Tak VESTAGER, M. Algorithms and Competition, Remarks by the European Commissioner for Competition at the Bundeskartellamt 18th Conference on Competition. Berlin, March 16, 2017. Dostupné z: <https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017_en>. Přístup 1. 3. 2019.

122 Pokora a zdrženlivost vesměs bývají odsouzeny spíše k vyčkávání a reakci na činy aktivních či arogantních…

123 Tak např. lucemburský soutěžní úřad rozhodl v čistě domácí kauze o povolení výjimky ze zákazu horizontálních cenových kartelů, protože uznal kladný dopad cenového algoritmu na spotřebitele. Algoritmus původně jen doporučoval maximální jízdné v taxících, ale ve skutečnosti určoval konečnou cenu pro zákazníka, jež se nedala vyjednáváním změnit. Přínosy spočívaly např. ve snížení počtu prázdných jízd a znečištění životního prostředí, jež jsou koneckonců ve prospěch spotřebitelů, kteří proto mají nakonec jízdné levnější a při kratším čekání na službu. Úřad dovodil přínos pro spotřebitele i nezbytnost omezení soutěže. Pokud by ceny nebyly fixovány, zákazníci by se obraceli na místně nejbližší taxi. Nebezpečí pro soutěž na trhu úřad neindikoval, protože příslušná platforma operovala jen na 26 % relevantního trhu. Jde o docela ojedinělý případ výjimky z horizontálního cenového kartelu, jehož zákaz se běžně posuzuje jako objektový, při němž se nemusí dokazovat škodlivost (*per-se*). Tento přístup také jistě nelze zobecnit (srov. MLL NEWS. 2018, 21.7. Dostupné z: <www.mll.news-com>).

124 MEHRA, S. K. *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, s. 375.

125 Úvahu o existenci chytrých robotů v postavení samostatných podnikatelů nebo zakladatelů a provozovatelů podniků se sklonem k protisoutěžnímu jednání, jež se vyplácí (ŠMEJKAL, V. *My nic, to roboti! Protikartelové právo a cenové algoritmy*, s. 85), můžeme podle gusta pokládat za vizionářskou, nebo třeba až fantasmagorickou.

Decentralizovaná podstata blockchainů se vzpírá vertikální povaze antitrustového práva, jež by se prý mělo také decentralizovat včetně antitrustových orgánů. Jinak někteří skeptičtí autoři věští antitrustovému právu z těchto důvodů smrt či ztrátu legitimity,[126] jiní[127] jsou méně dramatičtí, nicméně vyzývají k novému regulatornímu dialogu s použitím pravidla zdravého rozumu (*rule of reason*).

Zbývá už „jen“ dlouhá doba potřebná ke krystalizaci obsahu onoho pojmu – tedy co je ještě tzv. zdravé. Zejména se bude hledat hodnotově podmíněná hranice mezi užitkem blockchainů a algoritmů z hlediska soukromého na jedné straně, a případnými sociálními negativními dopady na straně druhé. Praxe zatím zaujímá spíše konzervativní a zdrženlivé stanovisko.[128]

Preemptivně prohibitivní přístupy k algoritmům (typu striktní až absolutní odpovědnosti za následky provozu zvláště nebezpečného) se v současnosti zvažují zatím jen teoreticky.[129] Nepokládám je za adekvátní, ale spíše za projev sklonu k přeregulaci s pravděpodobným zmrazovacím účinkem na rozvoj technologií, trhu i spotřebitelského blahobytu. Sklonu k „regulatornímu kvazireflexu“ preventivního automatického zákazu algoritmů („pro jistotu“) bychom neměli v této fázi vývoje podlehnout, pokud se dokonce otevřeně přiznává, že důkazy o spiknutí autonomních činitelů určujících a podporujících nadsoutěžní ceny nejsou v současnosti k dispozici, a pouze se varovně konstatuje, že existuje taková *možnost* a že pouze hrozí *nebezpečí*, že by se mohla stát všudypřítomnou realitou.[130]

126 SCHREPEL, T. Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox. *Georgetown Law Technology Review*. 2019, Vol. 3.2, 281, s. 336.

127 MEHRA, S. K. *Antitrust and the Robo-Seller: Competition in the Time of Algorithms*, s. 1375.

128 Srov. velmi aktuální společnou studii francouzského a německého soutěžního úřadu (AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT. *Algorithms and Competition*. Bonn – Paris. November 2019, s. IV – Executive Summary). Ta přiznává, že *„je předčasné vymezit, které potenciální typy interakce představují nezákonné chování“* a odlišit je od inteligentního přizpůsobování podmínkám na trhu.

129 Srov. MARTINI, M. *Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz*, s. 337 an.

130 Tak HARRINGTON, J. E., Jr. *Developing Competition Law for Collusion by Autonomous Price – Setting Agents*, s. 71.

Smartly Illicit "Smart" Contracts Between the Effectiveness of the Contractual Agenda and the Coded Illegality, Especially in the Protection of Competition

Josef Bejček

Abstract: Smart contracts based on software technology of blockchains are currently gaining ground as means of enhancing efficiency of closing and enforcing contracts and as a tool of speeding up and securing the contract agendas. On the other hand, their characteristics may tempt user to illegal use. They may pseudonymize (and anonymize, as a result) legal relations and enable illegal financial and other activities – admittedly being transparent and secure within groups of participants, but actually hidden and hardly to be disclosed from outside. The use of smart contracts to disguised collusion has been identified as one of the most dangerous recent challenges. It can substantially endanger both competition environment and consumer welfare. Very cautious approach to law making and (competition) policy making is advisable, so that the positive strengths of this new technology are not thwarted.

Key words: blockchain, smart contracts, collusion, pricing algorithms, economic competition