Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu

Radim Polčák* – František Kasl – Pavel Loutocký*** – Jakub Míšek**** – Václav Stupka*****

Abstrakt: Rostoucí význam informačních technologií se mimo jiné projevuje i potřebou průběžně upravovat dílčí charakteristiky mechanismu právní regulace. Cílem takových úprav je zajištění stabilní efektivity práva. V tomto textu je proveden rozbor dvou relativně nových regulatorních metod, které se postupně prosazují v právu informačních technologií a jsou založeny na použití tzv. performativních a chytrých pravidel. Článek tyto metody krátce vysvětluje a následně jejich užití demonstruje na pozitivních i problémových příkladech z oborů kybernetické bezpečnosti, ochrany osobních údajů a on-line řešení spotřebitelských sporů.

Klíčová slova: performativní pravidla, chytrá regulace, kybernetická bezpečnost, ODR, osobní údaje

Úvod

Informační technologie nabízí bezprecedentní potenciál k virtualizaci[1] právně relevantních společenských fenoménů. Způsobilost informačních technologií k totální transformaci společenských vztahů dokonce vedla k tomu, že pojem „virtuální" v běžném jazyce prakticky ztotožňujeme s pojmem „digitální" nebo „on-line".[2]

Význam virtualizace, k níž dochází v důsledku postupující penetrace společnosti informačními a komunikačními technologiemi, pro právo každopádně nespočívá v zásadní novosti doprovodných jevů. Skutečně nových otázek pro právo totiž vzniká jen velmi málo.[3] Namísto toho je právo zaměstnáváno nutností adaptovat své instrumentárium tak, aby bylo způsobilé technicky zvládnout nejrůznější „tvary změněné do nových těl".[4]

* Doc. JUDr. Radim Polčák, Ph.D., vedoucí Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: Radim.Polcak@law.muni.cz.

** Ing. Mgr. František Kasl, Ústav práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: Frantisek.Kasl@law.muni.cz.

*** JUDr. Pavel Loutocký, BA (Hons), vedoucí právního oddělení Centra pro transfer technologií. E-mail: loutocky@ctt.muni.cz.

**** Mgr. MgA. Jakub Míšek, Ústav práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: Jakub.Misek@law.muni.cz.

***** Mgr. Václav Stupka, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: Vaclav.Stupka@law.muni.cz.

1 Pojem virtualizace, který užíváme od antiky, označuje technologicky determinovanou změnu formálních aspektů určitého fenoménu při současném zachování jeho podstaty. Účelem virtualizace je zbavit se problémů spojených se starou formou, přičemž problémy související s novou formou mají být méně závažné. Podrobněji k pojmu viz monografii LÉVY, P. *Becoming Virtual – Reality in the Digital Age*. New York: Plenum Trade, 2002.

2 Takové chápání tohoto pojmu však není zcela adekvátní, neboť virtualizace nemusí nutně probíhat jen za užití informačních technologií. Virtuální je potřeba vnímat jako protiklad k aktuálnímu – srov. POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, s. 7.

3 Existují dokonce názory, že postupující penetrace společnosti informačními technologiemi nevyžaduje žádnou zvláštní pozornost právní vědy – srov. např. EASTERBROOK, F. Cyberspace and the Law of the Horse. *The University of Chicago Legal Forum*. 1996, roč. 1996, s. 207.

4 Tento obrat použil Ovidius v úvodu svých Proměn – viz NASO, P. O. *Proměny*. Praha: Odeon, 1969, s. 17. Vedle fyzických proměn, o nichž pojednává tato fenomenální báseň, se velmi dobře hodí i k označení proměn, jimiž prochází různé právní formy – podrobněji viz POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, s. 8.

1. Složitost technologie a rozmanitost aplikací

Největšími výzvami ve shora popsaném směru jsou relativní technická a funkční složitost informačních a komunikačních technologií a diverzita jejich aplikací.

I nejjednodušší počítač je technicky natolik složitou strukturou, že jeho skutečné fungování není do důsledku schopen pochopit ani profesionál. Nabízelo by se logické normativní řešení postavené na relevantním argumentu, že totiž člověku nepatří do rukou technologie, jejíž fungování není schopen pochopit. Takové řešení by zřejmě spočívalo v tom, po čem svého času volali někteří informatici, že by totiž přístup k informačním a komunikačním technologiím měl být podmíněn prokázáním technické způsobilosti člověka s těmito technologiemi nakládat.

Myšlenka „řidičáku na počítač" byla sama o sobě logická, neboť u vysoce složitého systému, jehož provoz může uživateli nebo třetím osobám způsobit značnou škodu, je zřejmě na místě požadovat prokázání schopnosti základním způsobem jej ovládat (to i bez pochopení technické podstaty jeho fungování) – byla ale z pochopitelných důvodů odsouzena k neúspěchu. Ve výsledku by totiž vedla k zákazu jdoucímu bez pragmaticky prokazatelných důvodů přímo proti základům lidské přirozenosti.[5] Na ambici požadovat po člověku zvládnutí jím užívané technologie jsme navíc postupně rezignovali i v jiných oblastech mimo ICT. K získání klasického řidičáku tedy již dnes není třeba detailní znalost fungování osobního automobilu – to prostě proto, že současné vozy jsou konstrukčně natolik složité, že normální člověk by jejich konstrukční finesy jednak nepochopil a jednak by mu ani případné jejich pochopení nebylo nic platné.

Technická a funkční složitost informačních technologií není problematická jen z hlediska požadavků na uživatele. Deficit chápání vnitřních mechanismů fungování i relativně banálních technologií logicky ztěžuje i práci právotvůrce. Neschopnost právotvůrce přizpůsobit pozitivní regulaci konkrétním parametrům příslušných technologií přitom není dána jen jeho neschopností tyto technologie dokonale poznat, ale též relativně rychlou jejich reprodukcí. Legislativní cyklus neumožňuje zajistit efektivitu právních předpisů jejich konkrétní adaptací na aktuální stav techniky proto, že reprodukce práva je řádově pomalejší než reprodukce informačních technologií. Řešením pak bývá spolehnutí se na schopnosti praxe podřadit nové technologické jevy přímo nebo analogicky pod rozsah obecných právních pojmů.

Populárnímu požadavku na to, aby právo anticipovalo technický vývoj a neklopýtalo za technickým pokrokem, se v tomto textu nemůžeme podrobněji věnovat. Stojí však každopádně za připomenutí, že vždy, pokud se právo o něco takového pokusilo, nedopadlo to ve výsledku dobře.[6]

K výše uvedeným složitostem ještě často přistupuje doposud bezprecedentní subjektivní pluralita.[7] U běžné společenské transakce, jakou je např. nákup knihy v kamenném knihkupectví zaplacený hotovostí, je subjektivní situace relativně transparentní. Je to

---

5 Pro člověka není přirozenější činnosti, než je informační aktivita. Informace je podstatou fungování živých organismů a člověk je tím pádem z podstaty nucen vyhledávat a rozvíjet nástroje, které mu usnadňují tvorbu, zpracování nebo komunikaci dat – srov. POLČÁK, R. *Internet a proměny práva*, s. 37.

6 Příkladem může být právní úprava zaručeného elektronického podpisu. Právo v tomto případě předběhlo dobu a upravilo podmínky k užití technologie, u níž se předpokládalo masivní rozšíření mezi širokou veřejnost. Namísto právem předpokládaného nahrazení vlastnoručního podpisu si však společenský vývoj v tomto případě šel vlastní cestou a zaručeného elektronického podpisu tak dnes až na výjimky používá jen ten, kdo z nějakého důvodu musí.

7 Podrobněji viz např. POST, D. Governing Cyberspace. *Wayne Law Review*. 1996, roč. 43, s. 155.

prostě vztah člověka s obchodníkem. Virtualizovaná obdoba této transakce však může mít ze subjektivního hlediska nepoměrně složitějších charakter. Typicky jsou totiž subjektem tohoto vztahu ještě poskytovatelé různých služeb informační společnosti, tj. např. poskytovatel veřejně dostupné služby elektronických komunikací, poskytovatel místního připojení, provozovatel zprostředkovatelské platformy, subjekt zpracovávající data o zákaznících, subjekt zajišťující bezpečnost platformy, poskytovatel platební brány, vydavatel elektronického platebního prostředku aj.

Rozptyl aplikací je jako druhý ze shora zmíněných faktorů pro právo nepříjemný z toho důvodu, že často fakticky brání efektivní regulaci prostřednictvím konkrétních behaviorálních pravidel. Standardní mechanismus právní regulace je totiž založen na tom, že právotvůrce volí strukturu a obsah konkrétních pravidel kódovaných do formy pozitivního práva podle projektovaného typického případu jejich užití. Výsledná pozitivní úprava má co nejefektivněji pokrýt případy spadající pod příslušný standard, přičemž nestandardní situace řešíme, je-li to možné, za užití zásad, analogie apod.[8]

Z výše uvedeného plyne, že virtualizace společenských vztahů je vzhledem k efektivitě právní regulace zatížena tím, že předmětným technologiím pořádně nerozumí právotvůrce ani jejich uživatel. K tomu ještě přistupuje taková rozmanitost různých aplikací, která jednak vylučuje povědomí na straně právotvůrce (tj. právotvůrce si nedokáže ani představit, jak mohou různé budoucí aplikace vůbec vypadat) a kromě toho i brání tvorbě efektivních pravidel mapovaných na konkrétní parametry příslušných technických řešení.

2. Virtualizace metody právní regulace

Z dosavadních zkušeností se zdá, že s výše popsanými problémy nelze hnout v tom směru, že by se uživatel nebo právotvůrce naučil chápat technické mechanismy fungování příslušných technologií nebo že by se snížila míra rozmanitosti jejich aplikací. Naopak lze očekávat, že odstup člověka od technologie dále poroste[9] a že současně poroste i zmíněná aplikační diverzita.[10] Právo přitom (naštěstí) nedisponuje nástroji k tomu, aby tyto trendy zvrátilo.[11]

K tomu, aby si právo alespoň zachovalo efektivitu svého regulačního mechanismu, je třeba odpovídajícím způsobem adaptovat na shora zmíněné výzvy metodu právní regulace.[12] Projevem virtualizace v právu se tak stávají pokusy o nové regulatorní přístupy, které mají jednak kompenzovat uvedené funkční deficity a jednak se snaží využít možností informačních technologií k zavedení doposud nedostupných regulatorních nástrojů. Z první kategorie nových přístupů se budeme v tomto textu dále věnovat tzv. perfor-

8 Srov. ZETSCHE, D. A. – BUCKLEY, R. P. – BARBERIS, J. – ARNER, D. W. Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. *Fordham Journal of Corporate and Financial Law*. 2017, roč. 23, č. 1, s. 31.

9 Tento pohyb lze pozorovat na příkladu osobních počítačů. Zatímco měl v devadesátých letech každý uživatel dokonalý přehled alespoň o tom, jaký procesor nebo jakou paměť má ve svém systému, dnes jsou tyto parametry často lhostejné i profesionálům.

10 Tento trend je důsledkem flexibility technických řešení umožňujících uživatelům velkou míru individualizace jejich zařízení. U prvních generací telefonů standardu GSM tak měl uživatel možnost individualizovat si své zařízení maximálně volbou barevného krytu, zatímco dnes prakticky nelze v praxi nalézt dva mobilní telefony s totožným softwarem.

11 Srov. SAXBY, S. The Role of Government in National/International Internet Administration. In: AKDENIZ, Y. – WALKER, C. – WALL, D. (eds). *The Internet, Law and Society*. Harlow: Pearson Education Limited, 2000, s. 3.

12 Tento požadavek je z metodologického hlediska čistě pragmatický a vychází z praktické zkušenosti s reálnou efektivitou práva v rychle se měnícím prostředí – k různým důvodům užití pragmatické metody v takových případech viz monografii THOMAS, E. W. *The Judicial Process*. Cambridge: Cambridge University Press, 2005.

mativním pravidlům (*performance-based rules*). Z druhé kategorie se dále zaměříme na chytrá pravidla (*smart rules*).

Pojem performativních pravidel označuje regulatorní techniku motivující regulované subjekty k tvorbě vlastních konkrétních pravidel chování.[13] Subjekty, k nimž právní regulace směřuje, zpravidla nejsou jednotliví lidé, ale tzv. definiční autority, tj. subjekty reálně provozující příslušné technologie.[14] Tento mechanismus právní regulace je založen na předpokladu, že k lidskému jednání, které je předmětem právní regulace, vždy dochází zprostředkovaně, tj. prostřednictvím nějaké technologie. Provozovatel této technologie, kterého též označujeme teoretickým pojmem definiční autority, má na výsledné jednání uživatele určující vliv, neboť jej díky totální technické kontrole může prakticky libovolně usměrňovat.[15]

Co do podstaty fungování mají performativní pravidla blízko k teleologickým normám. Stanoví totiž velmi obecně definovaný cílový stav, k němuž má směřovat jednání regulovaného subjektu. Odlišnost performativních pravidel od teleologických norem spočívá v tom, že performativní pravidlo zavazuje regulovaný subjekt k tomu, aby si za stanoveným účelem vytvořil vlastní konkrétní pravidlo chování (normu). Norma autonomně vytvořená na základě performativního pravidla je formalizována do podoby vnitropodnikového pravidla, typického ujednání ve smlouvě nebo dokonce počítačového kódu (k tomu viz dále) a tato její forma je pak i předmětem vrchnostenské kontroly a sankce. Regulovaný subjekt tedy nemůže splnit požadavek performativního pravidla jen tím, že se sám nějakým způsobem chová, ale plní jej prostřednictvím své vlastní relativně autonomní normotvorby postihující nejen jeho chování, ale především chování subjektů pod jeho technickou „jurisdikcí" (tj. uživatelů jeho služeb, zaměstnanců apod.).[16]

Performativní pravidla stojí, kromě shora zmíněného předpokladu týkajícího se významu definiční autority, ještě na dalších premisách odpovídajících výše diskutovaným problémům právní regulace virtualizovaných společenských fenoménů. Předně předpokládáme, že definiční autorita má nejlepší povědomí o tom, jak vypadá příslušná technologie a jak ji co nejefektivněji nastavit k tomu, aby fungovala požadovaným způsobem. Uživatel ani vrchnost nikdy nedisponují takovou mírou poznání technologie, jakou má ten, kdo tuto technologii vyvinul nebo kdo ji profesionálním způsobem provozuje.[17]

Tatáž definiční autorita je rovněž nejlépe disponována k adekvátnímu a efektivnímu nastavení technologie odpovídajícímu požadavkům právní úpravy, tj. k nastavení, které v informačním systému nebo síti při vynaložení co nejmenších nákladů odpovídajícím způsobem usměrní chování uživatelů. Vedle technických kompetencí má k tomu definiční autorita i právní nástroje. Definiční autorita má totiž jako vlastník zpravidla ultimativní katalog práv k příslušnému systému nebo síti.

---

13 V odborné literatuře se tento pojem v minulosti nejčastěji vyskytoval v souvislosti s obchodováním na kapitálovém trhu, leteckou dopravou nebo kontrolou emisí – srov. COGLIANESE, C. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, roč. 50, č. 3, s. 525.

14 Podrobněji k pojmu definičních autorit viz POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 130.

15 Jedná se o variantu regulatorního mechanismu, v jehož centru stojí reálná aktivita určité instituce. Obecně ke koncepci institucionalistického normativismu viz základní monografii WEINBERGER, O. *Law, institution, and legal politics – Fundamental Problems of Legal Theory and Social Philosophy*. Dordrecht: Kluwer Academic Publishers, 1987, s. 154.

16 Srov. KESAN, J. P. Private Internet Governance. *Loyola University Chicago Law Journal*. 2003, roč. 35, č. 1, s. 87.

17 Historický vývoj fenoménu definičních autorit mapuje jeden z předních teoretiků práva informačních technologií Lawrence Lessig v monografii LESSIG, L. *The Future of Ideas – The Fate of the Commons in a Connected World*. New York: Vintage Books, 2002, s. 143.

Typicky efektivním řešením je v tomto směru implementace předmětného pravidla chování do kódu informačního systému nebo sítě.[18] Definiční autorita tedy v tomto regulatorním modelu bere obecně definované pravidlo chování, z něj vytváří partikulární konkrétní normu pro svůj systém a tuto normu pak přímo vkládá do funkčního kódu virtuálního prostředí. Adekvátní vyjádření normy kódem přitom zajišťuje takovou míru efektivity, že dokonce není třeba řešit alternativu k naplnění její dispozice (sankci) – systém totiž na technické úrovni (tj. na úrovni svého *de facto* přírodního zákona) nic takového jako nenaplnění dispozice reálně neumožňuje.

Druhou regulatorní technikou, která se objevila jako důsledek virtualizace společenských vztahů, je metoda chytrých pravidel. Nejde v tomto případě o pokus o kompenzaci přirozeně rostoucí neefektivity práva jako u performativních pravidel, ale o relativně nový, technologicky determinovaný způsob zvyšování efektivity stávajících konkrétních právních pravidel v reálném čase díky minimalizaci informačního deficitu vrchnosti.[19] Regulované subjekty tedy v tomto případě nejsou nuceny ke konkretizaci obecných pravidel ve formě autonomní normotvorby, ale pouze k tomu, aby vrchnosti poskytovaly v reálném čase informační servis o fungování příslušného systému nebo služby.

Obecně vzato není na chytrých pravidlech nic moc nového. Vrchnost se vždy pokoušela sjednat si co nejlepší informační servis, přičemž platilo, že čím důležitější je veřejný zájem, tím intenzivnější je snaha o jeho zajištění. V případě služeb informační společnosti však jde o posunutí této snahy na zcela novou úroveň díky tomu, že poskytovatelé služeb informační společnosti často disponují dokonale přesnými daty o veškerém jednání svých uživatelů. Díky tomu a díky přirozené monopolizaci některých služeb informační společnosti (typicky u vyhledávačů, kontraktačních platforem, služeb elektronických komunikací aj.) mohou mít orgány autoritativně aplikující právo dokonalý a vcelku snadný přehled i o nejmenších detailech fungování regulovaného substrátu.

Typickým příkladem využití chytrých pravidel je estonská regulace platformy Uber.[20] K tomu, aby mohla tato platforma v Estonsku působit, zavázala se, vedle dalších povinností, k předávání dat o ekonomické aktivitě řidičů estonské finanční správě. Díky tomuto informačnímu servisu má estonská finanční správa dokonalý přehled o tom, kdo a jak často si formou spolujízdy přivydělává a díky automatizované analýze dat pak může s vysokou mírou efektivity vést daňové řízení. Řidiči to samozřejmě dobře vědí a ti, kdo tuto formu výdělku standardně realizují (tj. nejedná se o nahodilou aktivitu, která by nebyla předmětem daňové povinnosti), z vlastní iniciativy si opatřují živnostenská oprávnění a podávají pravdivá daňová přiznání. Každému je totiž jasné, že daňová kontrola v tomto případě nemusí být selektivní a sankce nemusí být předmětem nahodilé smůly, ale že díky možnosti automatizovaného zpracování velkých datových objemů mohou být kontrola i sankce plošné a vysoce přesné.

V následujících částech podrobněji rozebíráme, jak se shora konstatované problémy související s komplexitou virtualizovaných právních vztahů projevují v partikulárních oblastech platného práva. Z oborů, kde již máme s fungováním performativních nebo

---

18 Lessig se v tomto směru proslavil tezí, že totiž (počítačový) kód je zákonem kyberprostoru argumentovanou původně v práci *Code and Other Laws of Cyberspace*, později po revizi vydanou jako LESSIG, L. *Code version 2.0*. New York: Basic Books, 2006.

19 Podrobněji k pojmu chytré regulace, který se poprvé objevil v oboru právní regulace finančních trhů, viz např. ZETSCHE, D. A. – BUCKLEY, R. P. – BARBERIS, J. – ARNER, D. W. Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation. *Fordham Journal of Corporate and Financial Law*. 2017, roč. 23, č. 1, s. 31.

20 Podrobněji k různým přístupům k řešení fenoménu Uber napříč Evropou viz srovnávací studii DEMASI, A. Uber: Europe's Backseat Driver for the Sharing Economy. *Creighton International and Comparative Law Journal*. 2016, roč. 7, č. 1, s. 73.

chytrých pravidel nějaké, byť velmi omezené zkušenosti, jsme vybrali problematiku kybernetické bezpečnosti, ochrany osobních údajů a on-line řešení spotřebitelských sporů.

3. Regulatorní model kybernetické bezpečnosti

Pojem kybernetické bezpečnosti byl uměle vytvořen za účelem vzniku relativně nové regulatorní agendy a označuje soubor pravidel k zajištění důvěrnosti, dostupnosti a integrity informačních a komunikačních technologií a dat.[21] K tomuto cíli směřují snahy jednotlivců, kteří si zabezpečují počítače hesly a firewally, organizací, které implementují dohledové nástroje a vytváří bezpečností týmy, i států, pro něž se bezpečnost informačních systémů a sítí stala základním faktorem ochrany práv, fungování veřejné moci i samotné státní suverenity.

Stát je co do schopnosti přímo ovlivnit bezpečnost svého kyberprostoru velmi omezen, a to především z toho důvodu, že většina informačních infrastruktur, včetně těch kriticky důležitých, je vlastněna a provozována soukromoprávními subjekty. Tyto faktické definiční autority navíc mohou být velmi různorodé povahy – může jít například o vlastníky fyzické telekomunikační infrastruktury, provozovatele datových úložišť, informačních systémů kritické infrastruktury či poskytovatele služeb informační společnosti. Kromě toho mají velmi různorodou a proměnlivou povahu i technologie, které jednotlivé definiční autority v rámci svých infrastruktur implementují.

Právní úprava kybernetické bezpečnosti je na úrovni EU tvořena především směrnicí o síťové a informační bezpečnosti[22] a na úrovni ČR pak zákonem o kybernetické bezpečnosti.[23] Performativní pravidla se zde uplatňují především u institutu bezpečnostních opatření. Těmi se ve smyslu zákona rozumí *„souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru“*,[24] přičemž tyto úkony mají provádět povinné osoby, tedy správci či provozovatelé příslušných informačních a komunikačních systémů.

Zákon obsahuje výčet základních kategorií organizačních a technických bezpečnostních opatření, který je dále rozveden prováděcím předpisem.[25] Specifikace bezpečnostních opatření vyhláškou však rovněž není zcela konkrétní a povětšinou se omezuje na konkretizaci problémových okruhů nebo minimálních technických standardů. Povinný subjekt je tedy pozitivním právem informován o tom, jakého cíle má dosáhnout, a obecně rovněž o tom, jaké prostředky k tomu má využít. Je však zcela na něm, jaký obsah dá příslušným pravidlům obsaženým ve svých vnitřních normách realizujících organizační opatření, respektive jaké technické nástroje využije k zajištění konkrétních technických opatření.

Tento regulatorní mechanismus pochopitelně není prost určitých úskalí. Problém především spočívá v tom, že povinný subjekt se snaží vlastní autonomní normotvorbou

21 Podrobněji k pojmu a jeho právní reflexi viz monografii POLČÁK, R. – HARAŠTA, J. – STUPKA, V. *Právní problémy kybernetické bezpečnosti*. Brno: Masarykova univerzita, 2016.

22 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Známá rovněž jako směrnice NIS.

23 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

24 Viz § 4 odst. 1 zákona o kybernetické bezpečnosti.

25 Viz vyhlášku č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

a implementací technických řešení dosáhnout souladnosti (*compliance*) s právním pravidlem, jehož konkrétní obsah mu není znám. Může pak dojít k tomu, že se v otázce *ad hoc* splnění zákonných požadavků rozejde představa regulovaného subjektu a příslušné vrchnosti – u nás především Národního úřadu pro kybernetickou a informační bezpečnost.

Vedle metodických materiálů a vrchnostenských konzultací[26] je možné k pokrytí tohoto typu právní nejistoty využít především oficiální certifikace, tj. vrchností uznaného *a priori* potvrzení souladnosti příslušného technického či organizačního řešení se zákonnými a podzákonnými požadavky. K jednotnému systému oficiálních certifikací pro informační bezpečnost směřuje aktuální návrh tzv. kyberbezpečnostního balíčku.[27] Podle studie pravděpodobných dopadů takového řešení[28] lze očekávat poměrně velkou poptávku po těchto certifikátech v soukromém i veřejném sektoru. Současné certifikační standardy typu ISO nebo *Common Criteria* totiž trpí jednak věcnou či místní partikularitou a jednak jim chybí dokonalé vrchnostenské uznání.[29]

Technika chytrých pravidel se v zákoně o kybernetické bezpečnosti projevuje především mechanismem poskytujícím vrchnosti v reálném čase přehled nad bezpečnostní situací v zájmových informačních systémech a komunikačních sítích, tj. především v kritické informační infrastruktuře, v systémech základních služeb, ve významných systémech a významných sítích. Správci příslušných systémů a sítí tedy mají povinnost detekovat výskyt kybernetických bezpečnostních událostí[30] a v reálném čase předávat data o zjištěných kybernetických bezpečnostních incidentech[31] vládnímu, respektive národnímu dohledovému pracovišti. Na základě nepřetržité analýzy bezpečnostní situace v zájmové infrastruktuře pak dohledová pracoviště generují vrchnosti podněty k metodice a regulatorní činnosti (např. k vydávání varování či protiopatření).

Česká republika má díky tomu, že zde byl model chytrých pravidel zaveden v této oblasti jako v prvním členském státě EU, relativně bohaté praktické zkušenosti. Ty například ukazují potřebu systémového řešení pro efektivní a přitom *de iure* proporcionální přenos dat o bezpečnostních incidentech mezi dohledovými pracovišti na jedné straně a zpravodajskými službami nebo orgány činnými v trestním řízení na straně druhé. Ukazuje se rovněž, že si dohledová pracoviště v praxi nevystačí jen s daty o bezpečnostních incidentech či zranitelnostech poskytovanými povinnými subjekty, ale že bude třeba vybavit je možností tato data aktivně vyhledávat např. formou forenzní analýzy napadených systémů nebo tzv. penetračního testování.

Praxe velkých korporací i orgánů veřejné moci provozujících větší informační systémy rovněž ukazuje, že je nanejvýš potřebné řešit z pohledu vrchnostenské kontroly synergii různých informačních povinností týkajících se bezpečnostních incidentů v informačních systémech. Podobný model chytré regulace založené na detekci a okamžité notifi-

---

26 Srov. § 20 písm. d) zákona o kybernetické bezpečnosti.

27 Srov. *Společné sdělení Evropskému parlamentu a Radě č. JOIN(2017) 450, Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, ze dne 13. září 2017*, [cit. 2018-09-13]. Dostupné z: <http://eur-lex.europa.eu/legalcontent/CS/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>.

28 Viz *Inception impact assessment on Proposal for a Regulation revising ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework*, 2017, č. ref. Ares(2017)3436811, [cit. 2018-09-13]. Dostupné z: <https://ec.europa.eu/info/law/betterregulation/initiatives/ares-2017-3436811_en>.

29 Částečnou reflexi soukromých certifikátů obsahuje např. příloha č. 6 k vyhlášce č. 82/2018 Sb.

30 Tou je dle § 7 odst. 1 zákona o kybernetické bezpečnosti událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

31 Incidentem je událost, která způsobí narušení bezpečnosti. Viz § 7 odst. 2 zákona o kybernetické bezpečnosti.

kaci bezpečnostních incidentů totiž obsahuje i úprava ochrany osobních údajů, ochrany utajovaných informací a částečně i práva elektronických komunikací. Na úrovni regulovaných subjektů se tedy přímo nabízí sjednocení detekčních a notifikačních procesů a tomu by měla odpovídat i schopnost veřejné moci příslušná hlášení jednotně přijímat a zpracovávat.

4. Regulatorní model ochrany osobních údajů

Ochrana osobních údajů je poměrně mladou oblastí právní úpravy, jejíž počátky jsou spojeny s rostoucím významem informačních technologií. Ačkoli navazuje na právní úpravu ochrany soukromí, se kterou sdílí stejný abstraktní cíl, kterým je ochrana osobnosti a soukromého a rodinného života člověka, výrazně se od ní odlišuje ve způsobu, jakým je regulace zajištěna. První zárodky specifické právní úpravy můžeme nalézat v 70. letech,[32] přičemž od počátků až do dnešní doby se jedná o okruh norem, které jsou do značné míry specifické pro evropské hodnoty a právní řády.[33] Přestože byly v roce 1990 na půdě Organizace spojených národů přijaty pokyny pro regulaci počítačem zpracovávaných osobních údajů,[34] většina významných světových právních řádů má po dlouhou dobu jen omezené ambice pro tuto oblast vytvářet vymahatelný regulatorní rámec srovnatelný s tím, který je po téměř tři desetiletí budovaný v evropském prostoru.[35] Často je to pak právě evropský právní rámec, a obchodní síla Evropské unie, které představují hlavní motivaci pro přijetí srovnatelných požadavků do právních řádů mimoevropských zemí.[36]

Právo na ochranu osobních údajů vychází z pragmatické nezbytnosti *ex ante* uplatňovaných obecných preventivních povinností při nakládání s údaji o určité či určitelné fyzické osobě. Cílem je zajištění prostoru, ve kterém je člověk schopen vykonávat kontrolu nad digitálním obrazem svého života.

Zásadní funkční rozdíl ochrany osobních údajů oproti ochraně soukromí spočívá v primárně preventivním charakteru právní regulace.[37] Pokud je s osobními údaji nakládáno

---

32 Především rezoluce Výboru ministrů Rady Evropy z let 1973 a 1974, které výrazně přispěly ke sjednocení legislativního přístupu a iniciovaly přijetí prvních specifických národních úprav. Blíže viz NOVÁK, D. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. Praha: Wolters Kluwer ČR, 2014, s. 8.

33 V evropském prostoru byla prvním zásadním mezinárodně právním dokumentem na úrovni Rady Evropy Úmluva Rady Evropy o ochraně soukromí z roku 1981. Srov. *Thirty years after, The OECD privacy guidelines*, 2011, [cit. 2018-09-13]. Dostupné z: <http://www.oecd.org/sti/ieconomy/49710223.pdf>.

34 Viz VALNÉ SHROMÁŽDĚNÍ. *Guidelines for the Regulation of Computerized Personal Data Files*. Organizace spojených národů, 1990 [cit. 2018-09-13]. Dostupné z: <http://www.refworld.org/pdfid/3ddcafaac.pdf>.

35 Významný je především kontrast s právním prostředím Spojených států amerických, kde v současné době neexistuje právní norma na federální či státní úrovni, která by zajišťovala srovnatelnou úroveň ochrany. To je však často odrazem odlišných hodnot a politických či regulatorních cílů a priorit daných států, kdy důraz na ochranu soukromí a osobních údajů obyvatel je v Evropské unii atypicky vysoký. Zcela odlišný přístup k ochraně soukromí a osobních údajů jednotlivce je v zemích jako Čína či Indie. Viz např. HODSON, H. Big brother is rating you (if you're Chinese). *New Scientist*. 2015, roč. 228, č. 3043, [cit. 2018-09-13], či JACOBSEN, E. K. U. *Unique Biometric IDs: Governmentality and Appropriation in a Digital India*. 2015, [cit. 2018-09-13]. Dostupné z: <https://gupea.ub.gu.se/handle/2077/38732>. Další poznámky k tématu viz SVANTESSON, D. The (uncertain) future of online data privacy. *Masaryk University Journal of Law and Technology*. 2015, roč. 9, č. 1, s. 130–131.

36 Příkladem lze odkázat na vývoj právní úpravy ochrany osobních údajů v Pákistánu. Viz HAYAT, M. A. Privacy and Islam: From the Quran to data protection in Pakistan. *Information & Communications Technology Law*. 2007, roč. 16, č. 2. V současné době má nějakou formu zákonné ochrany osobních údajů přes 120 zemí na světě. Viz GREENLEAF, G. Global Tables of Data Privacy Laws and Bills. *Privacy Laws & Business International Report*. 2017, č. 145.

37 U ochrany soukromí je prevence především nástrojem k omezení možné odpovědnosti. V případě ochrany osobních údajů existují prevenční povinnosti zcela nezávisle na možné odpovědnosti a uplatňují se i tam, kde žádný zásah do práv a tím pádem žádná odpovědnost reálně nehrozí. Srov. např. GELLERT, R. Understanding Data Protection as Risk Regulation. *Journal of Internet Law*. 2015, roč. 18, č. 11, s. 9 an.

v souladu s předem deklarovaným účelem a přitom zákonem předvídaným způsobem, je minimalizováno riziko zásahu do práv a zájmů člověka.

Na této zásadě stojí rovněž obecné nařízení o ochraně osobních údajů.[38] To mimo jiné přineslo i výslovné zakotvení principu odpovědnosti správce osobních údajů[39] spočívajícím v tom, že správce má přijmout přiměřená technická a organizační opatření, která budou odpovídat povaze možného rizika spojeného se zpracováním osobních údajů. Za stanovení konkrétní podoby regulatorních povinností tedy v tomto případě odpovídá povinný subjekt. Tento formát regulace vychází především ze skutečnosti, že hodnota a související riziko zneužití určitého osobního údaje jsou určitelné pouze na základě konkrétního kontextu jeho zpracování.

Právě v tomto bodě do značné míry tkví podklad pro kritiku současného přístupu k regulaci zpracovávání osobních údajů pro nedostatečnou právní jistotu povinných subjektů (tedy správců). Přestože jsou přijímány různé návodné či doporučující pokyny a stanoviska ze strany dozorčích orgánů či sektorových organizací, není vzhledem k výše popsané podstatě osobních údajů v zásadě možné poskytnout jednotlivým povinným subjektům konkrétní kvantifikovatelné parametry, na jejichž základě si mohou ověřit soulad vlastního řešení se zákonnými povinnostmi.

Zatímco v případě povinných subjektů podléhajících regulaci kybernetické bezpečnosti jde veskrze o velké subjekty se značnými finančními i odbornými kapacitami, v případě správců osobních údajů jde často též o malé obce nebo jednotlivé živnostníky mající z pochopitelných důvodů jen minimální povědomí o všech možných aspektech bezpečnosti svých datových toků. Tato situace pak otevírá prostor k u nás často se vyskytující naivní nebo perverzní aplikaci příslušných performativních pravidel.[40]

Nelze však z výše uvedeného dovodit závěr, že popsaný regulatorní přístup k ochraně osobních údajů na základě performativních pravidel je koncepčně nevhodný. V dnešním arzenálu právotvůrce se nenabízí vhodná regulatorní alternativa, která by tohoto cíle dosahovala účelněji a efektivněji. Vyšší jednoznačnost pravidel předchozí úpravy ochrany osobních údajů ve směrnici 95/46/ES, jejichž smysluplnost a vymahatelnost byla značně limitována, byla tedy nahrazena dočasným zvýšením právní nejistoty povinných subjektů, která však ve výsledku povede k větší racionalitě, užitečnosti a ekonomické a regulatorní efektivitě. Tato právní nejistota se nadto bude do budoucna s vysokou pravděpodobností postupně rozplývat v důsledku rozvoje různých performativních nástrojů, tj. vrchnostensky schválených kodexů, modelových smluvních ujednání nebo modelových podnikových pravidel. Za úspěšný bude pak možno model performativní regulace považovat tehdy, pokud budou mít tyto nástroje pro reálnou praxi povinných subjektů větší význam než rozhodovací praxe dozorových orgánů nebo soudní judikatura.

---

38 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), známé rovněž pod zkratkou GDPR z anglického *General Data Protection Regulation*.

39 Viz čl. 24 obecného nařízení o ochraně osobních údajů.

40 Jako příklad za všechny je možné uvést již klasickou anekdotickou historku, kdy byla ředitelce základní školy poskytnuta rada, aby přes nástěnku s osobními údaji umístila záclonku. Viz ENDRŠTOVÁ, M. Rodiče dostanou díky GDPR novou munici. Učitelé se budou bát udělat chybu. *iDnes*. 30. 3. 2018, [cit. 2018-09-13]. Dostupné z: <https://zpravy.idnes.cz/gdpr-narizeni-o-ochrane-osobnich-udaju-skoly-konference-udani-puy-/domaci.aspx?c=A180326_153705_domaci_nub>.

5. Regulatorní model on-line řešení spotřebitelských sporů

On-line řešení sporů (ODR – *online dispute resolution*) představuje v obecné rovině alternativní formu procesu smírného nebo sporného řešení právně problémových situací. Netrpí nedostatky tradiční listinné nebo osobní komunikace vedoucími k nákladnosti, časově náročnosti a s nimi související frustraci nebo dokonce celkové praktické nedostupnosti příslušné smírné nebo sporné procedury.[41] ODR zahrnuje tři dílčí aspekty: i) mechanismy pro řešení sporů (které jsou zpravidla mimosoudní), ii) využití moderních technologií k výměně dat mezi stranami sporu a iii) využití moderních technologií ke zpracovávání dat v rámci řešení daného sporu (ve smyslu softwarové asistence).[42] K tomu může ještě přistupovat přímé zapojení definiční autority způsobilé zajistit efektivní výkon dohodnutého nebo stanoveného výsledku příslušného sporu. Takto vymezený soubor nástrojů pro řešení sporů již prokázal, že je schopný řešit určité typy sporů o právo vysoce efektivně.[43] V některých případech, typicky u přeshraničních spotřebitelských sporů malé hodnoty, lze dokonce konstatovat, že proces řešení sporů prostřednictvím ODR není reálnou alternativou soudního řízení, ale jde prakticky o alternativu jedinou – mimo jiné i proto, že ODR zpravidla provozuje subjekt způsobilý fakticky vykonat, respektive sankcionovat příslušné rozhodnutí.[44]

Vhodným příkladem ODR je systém pro spory na aukční platformě eBay. Spory vznikající mezi uživateli, tj. prodávajícími a kupujícími, jsou na základě smluvních podmínek eBay (tj. zcela mimo zákonnou úpravu rozhodčího řízení či mediace) „rozhodovány" prostřednictvím ODR platformy a výsledné rozhodnutí je realizováno za pomoci platební platformy PayPal.[45] Díky vysoké efektivitě a dostupnosti ODR je tímto způsobem uzavřeno přibližně 60 milionů sporů ročně, což je zhruba 80 % všech sporů vzniklých při obchodování na platformě eBay.[46]

Systém ODR je v tomto případě *de facto* zcela nezávislý na národních právních úpravách dotčených států[47] a jeho provozování ze strany eBay tedy není důsledkem performativního pravidla. Systém však slouží stejnému účelu, který sleduje zákonná ochrana

---

41 Srov. CORTÉS, P. Online Dispute resolution for Consumers. In: WAHAB, M. A. – KATSH, E. – RAINEY, D. (eds). *Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*. The Hague: Eleven International Publishing, 2012, s. 140.

42 K obecné definici ODR jako mechanismu pro řešení sporů využívajícího ICT technologií více viz KAUFMANN-KOHLER, G. – SCHULTZ, T. *Online Dispute Resolution: Challenges for Contemporary Justice*. The Hague: Kluwer Law International, 2004, s. 6 an.

43 Viz KATSH, E. – RABOVICH-EINY, O. Lessons from Online Dispute Resolution for Dispute Systems Design. In: WAHAB, M. A. – KATSH, E. – RAINEY, D. (eds). *Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*, s. 56.

44 Možnost, že by rozumně myslící český spotřebitel, který se cítí poškozen na svých právech z nákupu v čínském e-shopu v hodnotě 15 dolarů, investoval desetitisíce korun do soudního sporu a následného uznání a výkonu soudního rozhodnutí v Číně, je z pochopitelných důvodů zcela nepravděpodobná.

45 Vedle transferu peněz je významným sankčním nástrojem též hodnocení obchodníka nebo zákazníka, tj. takzvané hvězdičky. I tuto hodnotu přitom plně kontroluje provozovatel platformy.

46 Srov. SUSSKIND, R. *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. Oxford: Oxford University Press, 2017, s. 70.

47 Namísto národní právní úpravy rozhodčího řízení nebo mediace se v tomto případě uplatní pouze obecné limity soukromého práva vztahující se k autonomii vůle kontrahentů (zde prodávajícího, kupujícího a zprostředkovatele). K tomu navíc přistupuje omezení odpovědnosti provozovatele platformy jakožto poskytovatele služby informační společnosti – k tomu srov. případ C-324/09 *L'Oréal SA a další proti eBay International AG a další* – a shora rozebraná skutečnost, že zhrzený uživatel (prodávající nebo kupující) zřejmě kvůli pár desítkám eur nebude žalovat eBay. Šance, že by se tento typ ODR reálně dostal pod sankci státního práva, je tedy minimální.

spotřebitele, a tento účel se mu v mnoha směrech daří naplňovat nesrovnatelně efektivněji (kdyby tomu tak nebylo, volili by zřejmě zákazníci jinou formu ochrany svých práv).[48]

Jednou z výhod systému eBay je vedle jeho technické a ekonomické efektivity též vysoce účinná implementace nástrojů chytré regulace. Systém totiž disponuje kompletními daty o předchozích transakcích a z nich vzniklých sporech, které následně využívá při automatizované asistenci s rozhodováním nových sporů. Úvodní fází řešení sporu tak je vzájemné jednání stran za asistence automatu užívajícího agregovaná data z obdobných transakcí. Díky kvalitě procesního nástroje a asistenčního automatu je přitom tímto způsobem urovnáno celých 90 % z celkového počtu řešených sporů.[49]

Tahounem vývoje ODR jsou od počátku nestátní on-line definiční autority, nejčastěji platformy.[50] Příslušná řešení tedy vznikají z praktické potřeby a ekonomických motivů.[51] To ale neznamená, že by státní moc na regulaci a využití tohoto způsobu řešení sporů měla zcela rezignovat. Dosavadní snaha o nastavení rámce ODR skrze soubor performativních pravidel však v této oblasti prozatím v zásadě ztroskotává zejména kvůli tomu, že nebyla právotvůrcem pochopena podstata a výhody ODR a daná pravidla tudíž nebyla vhodně nastavena.

Příkladem takové nevhodné úpravy je unijní právní režim pro řešení spotřebitelských sporů on-line.[52] Přestože jeho hlavním cílem byla snaha poskytnout spotřebiteli jednoduchý a efektivní nástroj schopný nabídnout řešení sporů vyplývajících především z elektronického obchodování, úprava je roztříštěná, komplikovaná a zavádí další paralelní řízení, které je zejména pro spotřebitele matoucí. ODR platforma, která slouží pro podání stížnosti spotřebitele proti obchodníkovi, pouze bez přidané hodnoty zprostředkovává výměnu informací mezi stranami a samotný spor je pak až následně řešen na národní úrovni v dalším procesu skrze standardní mechanismy mimosoudního řešení sporů podle práva příslušného členského státu. ODR platforma tedy v tomto případě působí jen jako lepší e-mailová aplikace a fakticky ani neplní funkci ODR, neboť v jejím rámci vůbec nedochází k samotnému řešení či rozhodnutí věci.

Performativní pravidla této unijní úpravy tak sice nastavila obecné parametry pro řešení spotřebitelských sporů skrze ODR mechanismy, svým přístupem však popřela základní předpoklady pro reálně funkční ODR systém.[53] Celý systém byl již od počátku nevhodně nastaven i proto, že není propojen s definičními autoritami, které by zajistily efektivní vymahatelnost daných řešení sporů skrze bezprostředně použitelné donucovací mechanismy. Důsledkem je, že fakticky dochází k úspěšnému vyřešení sporu v rámci této evrop-

48 Srov. RULE, C. Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing In Dispute Resolution. *University of Arkansas at Little Rock Law Review*. 2012, roč. 24, č. 4, s. 772 an.

49 Viz SCHMITZ, A. – RULE, C. *The New Handshake: Online Dispute Resolution and the Future of Consumer Protection*. Chicago: American Bar Association, 2017, s. 53.

50 Srov. KATSH, E. ODR: A Look at History – A Few Thoughts About the Present and Some Speculation About the Future. In: WAHAB, M. A. – KATSH, E. – RAINEY, D. *Online Dispute Resolution: Theory and Practice: A Treatise on Technology and Dispute Resolution*, s. 10 an.

51 Jedná se o tzv. *bottom-up* přístup. K tomu více viz LESSIG, L. *Code version 2.0.* New York: Basic Books, 2006, s. 3 a 6.

52 Právní úprava je zakotvena na základě směrnice Evropského parlamentu a Rady 2013/11/EU ze dne 21. května 2013 o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů) a nařízení Evropského parlamentu a Rady (EU) č. 524/2013 ze dne 21. května 2013 o řešení spotřebitelských sporů on-line a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (nařízení o řešení spotřebitelských sporů on-line).

53 Konkrétní požadavky jsou zprostředkovaně upraveny například v čl. 5 an. směrnice o alternativním řešení spotřebitelských sporů.

ské ODR platformy v méně než 1 % zahájených řízení (nemluvě o nechuti spotřebitelů toto řízení vůbec zahajovat).[54]

Závěr

Předmětem tohoto textu byla analýza nových forem fungování mechanismu právní regulace, s nimiž se setkáváme v důsledku rozvoje informačních technologií. Všímali jsme si v tomto směru především regulatorní metody používající performativních a chytrých pravidel. Z konkrétních forem aplikace obou typů pravidel jsme se zaměřili na případové studie z oboru kybernetické bezpečnosti, ochrany osobních údajů a on-line řešení spotřebitelských sporů.

Shora rozebrané příklady předně ukazují, že volba regulatorní metody pomáhá výsledné efektivitě právní úpravy. Její úspěšná aplikace je však v každém případě podmíněna materiální korespondencí zvoleného regulatorního mechanismu s obsahem a subjektivní orientací příslušných pravidel. Primárním adresátem performativního či chytrého pravidla tedy má být definiční autorita a integrální jeho komponentou má být prostor pro realizaci její autonomní vůle. Adresát performativního či chytrého pravidla tedy má dostat prostor k autonomní interní normotvorbě (u performativního pravidla) a/nebo k autonomní volbě nástroje a postupu pro shromažďování dat z cílového substrátu (u chytrých pravidel). Pouze za takového předpokladu může model performativního či chytrého pravidla ve výsledku fungovat a využívat všech možných výhod, které tato regulatorní technika nabízí.

Z výše provedeného výkladu nepřímo vyplývají i další obecné závěry týkající se aktuálních směrů v právní regulaci informační společnosti. Evidentní je především trend rostoucí a státem tolerované, nebo dokonce podporované relativně autonomní normotvorné aktivity soukromoprávních subjektů. Ve shora zmíněných odvětvích i v dalších oborech práva informačních technologií se tak v rostoucí míře setkáváme s penetrací „otevřené textury platného práva“[55] normami majícími soukromý původ. Dokonce existují obory, v nichž se praktikující právník s pozitivním právem státního původu setká jen minimálně nebo zcela vůbec.[56]

Důsledkem právě popsaných jevů je, opět nejen ve shora sledovaných odvětvích, změna celkové orientace mechanismu právní regulace z odpovědnosti k tomu, co lze označit *a priori* souladností, prevencí nebo nejlépe anglickým termínem nemajícím odpovídající český ekvivalent, tj. *compliance*. Původně právní agenda, jejímž ultimativním motivem bývala odpovědnost povinného subjektu, se tedy postupně mění na agendu organizační směřující k *a priori* naplňování různých standardů. Oproti standardní prevenci se přitom *compliance* liší jednak v tom, že příslušné povinnosti jsou přímo a konkrétně upraveny,

---

54 Srov. *Report from the Commission to the European Parliament and the Council on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes*. 2017, č. ref. COM(2017) 744 final, [cit. 2018-09-13], s. 7. Dostupné z: <https://ec.europa.eu/info/sites/info/files/first_report_on_the_functioning_of_the_odr_platform.pdf>.

55 Pojem otevřené textury používá ve svém díle Herbert Hart. Označuje jím situaci, kdy je formálně určitý systém pozitivního práva tvořený jazykovými výrazy obsahově doplňován z vnějších zdrojů – srov. HART, H. *The Concept of Law*. Oxford: Clarendon Press, 1994, s. 123.

56 Příkladem je právo doménových jmen, kde má podstatná část reálně používaného právního rámce (typicky úprava registrace a užívání doménových jmen s generickými doménami první úrovně) charakter *soft law* tvořeného tzv. doménovými autoritami. Podrobněji viz HOSTAŠ, P. Doménová jména. In: POLČÁK, R. a kol. *Právo informačních technologií*. Praha: Wolters Kluwer, s. 273.

a jednak v tom, že jejich existence je absolutně nezávislá na potenciálních odpovědnostních následcích. Povinnosti ke *compliance* je tedy nutno plnit i v případech, kdy žádná odpovědnost reálně nehrozí.

V právu samozřejmě nejde o nic nového. Na modelu *compliance* tradičně stojí například protipožární ochrana, úprava provozu různých dopravních prostředků nebo bezpečnost práce. Determinace společenských vztahů složitými technologiemi a jiné shora popsané důsledky virtualizace tedy jen vytvářejí přirozený tlak na to, aby byl podobný model zaveden též v dalších odvětvích, jakými jsou například ochrana osobních údajů nebo kybernetická bezpečnost.

Tento posun s sebou nese i řadu více či méně problematických doprovodných jevů. Tlak na ekonomickou efektivitu vede mimo jiné k tomu, že především soukromoprávní korporace nahrazují v těchto regulatorních agendách právníky lacinějšími a tvárnějšími specialisty bez právního vzdělání. Způsobilost řady *compliance* procesů k formalizaci a typizaci motivuje rovněž povinné subjekty k investicím do automatizovaných řešení zahrnujících například autonomní filtry, detektory incidentů, kontrolní systémy nebo autonomní generátory oficiální komunikace (typicky hlášení o zjištěných incidentech). Tyto subsidiární efekty paradigmatických změn popsaných v textu výše však již dalece přesahují rozsah tohoto stručného pojednání.

Virtualization of Legal Relations and New Regulatory Methods in Positive Law

Radim Polčák – František Kasl – Pavel Loutocký – Jakub Míšek – Václav Stupka

Abstract: Growing importance of information technologies brings also the need for continuous updating of particular features of the mechanism of legal regulation. The purpose of such updates is to provide for stable efficiency of law. This text analyses two relatively new regulatory methods in cyberlaw based on performative rules and smart rules. The paper shortly explains these methods and demonstrates their use on examples from cybersecurity law, personal data protection and on-line resolution of consumer disputes.

Key words: performance-based rules, smart rules, cybersecurity, ODR, personal data