Právo IT

Skripta práva informačních technologiích pro čtvrtý ročník oboru Kybernetická bezpečnost.

Úvod

Úvod

Právo IT v současné době nabývá na důležitosti. Skripta postupně proberou témata místní působnost práva na internetu, odpovědnosti poskytovatelů služeb informační společnosti, práva k datům a softwaru, elektronické dokumenty, doménová jména, data veřejného sektoru, ochranu soukromí a osobních údajů, regulaci elektronických komunikací a také kyberbezpečnost a kyberkriminalitu.

> Doporučená literatura k předmětu: POLČÁK, R., Právo informačních technologií, Wolter Kluwer, 2018.

Identita oboru

Jelikož se jedná o poměrně novou oblast práva, je poměrně logické, že jsme mohli sledovat přechod od obecných otázek k problémům mnohem konkrétnějšího charakteru. Mezi původní otázky, které tato problematika zahrnovala můžeme vidět zejména základní axiomy tohoto oboru (například informační život člověka, právní povaha informačního automatu apod.). Nicméně problémy, kterými se zabývá současné právo informačních technologií jsou vysoce specializované a patří mezi ně například právo na užití autorských děl online, soukromoprávní odpovědnost za újmu způsobenou autonomními systémy aj. Ve světle tohoto již v podstatě nelze nikoho označit odborníka na právo informačních technologií, ale maximálně například na odborníka na obchodní právo v kyberprostoru, jelikož současně s rozvojem technologií narůstá objem potřebných znalostí a již není v silách jednoho člověka je obsáhnout všechny.

Rozmach jednotlivých podoborů je způsoben jednak stále větším množstvím odborných poznatků v této oblasti a jednak množstvím bezpečnostních hrozeb, které kyberprostor skýtá. Problémem je však vedlejší efekt tohoto rozmachu, a tedy to, že se stále více zapomíná na fundamentální myšlenky oboru práva informačních a komunikačních technologií, původně určujících společný základní směr vývoje těchto v dnešní době již více, či méně nezávislých podoborů.

V oblastech, které se v právu objevují jako nové, obvykle například reagující na technologický vývoj v dané oblasti se však vyskytují po právní stránce značné potíže. Je zapotřebí vytvořit základní parametry příslušné právní agendy, která se danou problematikou zabývá. Příkladem nám může být a například lidská orientace v prostoru. Ve městě, kde se nám nabízí jako orientační znaky například zavedené názvy ulic, domů, stanic dopravních prostředků hromadné dopravy, ukazatele směru, nebo třeba významných kulturních, společenských aj. center málokdy využijeme například orientaci podle slunce, nebo podle kompasu jednoduše proto, že jednak není dostatečně přesná a

jednak je v tomto prostředí, které přímo přetéká různými orientačními body naprosto zbytečná a neefektivní. Nicméně když se ten samý člověk ztratí například v horách, bez signálu mobilního telefonu, bude se muset spolehnout na slunce, kompas, mapu, lišejníky na stromech, tedy na úplně základní navigační pomůcky, prvky a záchytné body.

Metoda

V problematice práva obecně rozeznáváme mezi třemi základními metodologickými přístupy. Vzájemně je můžeme rozlišit například prostřednictvím trojice účelů práva, jak je formuloval Gustav Radbruch,4 tj.:

– spravedlnost,

– právní jistota,

– praktická užitečnost.

Spravedlnost je základním kamenem přirozenoprávní metodologie, která stojí na předpokladu, že platnost práva lze dovodit ze souladu s objektivně existující spravedlností. Rozdíl mezi jednotlivými přirozenoprávními přístupy se liší v pohledu na to, co je důvodem existence objektivní spravedlnosti (může jít například o Vyšší moc, přirozenost, nebo lidský intelekt). Vlastní teorii má i obor páva informačních technologií. Důvodem platnosti právního pravidla je zde jeho soulad s definiční normou. Jako výhodu přirozenoprávního pojetí práva můžeme vnímat bezesporu snahu o materiální soulad s apriorními parametry příslušného prostředí, ať už se jedná o sociální systém, metafyzickou strukturu, přírodní situaci, nebo prostor, vytvořený uměle za pomoci informačních a komunikačních technologií. Nicméně zjevnou nevýhodou tohoto přístupu je zejména neschopnost jedince objektivně identifikovat tyto apriorní parametry. Z tohoto vyplývá jednak nedosažitelnost dokonalého systému pravidel, které by byly schopné dokonale zrcadlit příslušný přirozený řád věcí. Nicméně ještě vážnějším nedostatkem tohoto přístupu k právu je jeho subjektivita, která je důsledkem odlišného náhledu na realitu (resp. Na její určitou část) u každého jednoho z nás.

Virtualizace

Máme za prokázané, že s vytvořením nového prostředí, kde život nachází svůj domov, nevznikly právu žádné originální výzvy a právo i nadále plní svou, Platónem definovanou funkci, a tedy, že se jedná o nástroj k řešení přirozeného konfliktu. Kybernetika, informační filozofie a všechny důsledky překotného vývoje informačních a komunikačních technologií v druhé polovině minulého století tím pádem právu nepřinesly nové výzvy, ale pouze motivovaly k dalšímu vývoji v souvisejících právních oblastech.

Pojem virtuality a virtualizace není v obecné filozofii zdaleka nový. Jeho původ sahá až do doby antického Řecka, kdy se virtualizace začala uplatňovat jako standardní forma totální formální abstrakce. Virtualizací je totiž obecně vzato proces, kdy zůstává zachována podstata nějakého (prakticky libovolného) fenoménu, přičemž dochází k zásadní změně jeho formálních znaků.

Virtualizovaný fenomén pak díky změně formy vykazuje i přes zachování své podstaty jiné vlastnosti, což se projevuje na jeho praktickém fungování.

Právo jako informační systém

Informační a komunikační technologie sice nepřinesly právu nic zásadně nového, ale rozkrytí jejich filozofické podstaty významně obohatilo právní teorii, filozofii a zprostředkovaně i právní praxi.

Velkým a objektivně neřešitelným problémem práva jako takového (nikoli jen práva informačních technologií) přitom je skutečnost, že mezi daty a informací není žádná logická souvislost. Data tedy sice mohou za příznivých okolností indukovat informaci – to, zda k informaci došlo, však nelze nikdy s jistotou předpovědět. Ideálním ilustrativním příkladem fungování informace je právo. Pohledem kybernetiky je právo nástrojem přirozeně vyvinutým za účelem organizace společnosti a člověka, tj. jde o informační systém. Na příkladu formalizovaných právních pravidel je přitom možno velmi dobře demonstrovat shora konstatovanou nesouvislosti mezi údajem a informací. Můžeme totiž sice intuitivně nebo na základě zkušenosti odhadovat, jak který zákon zafunguje v praxi. Nikdy ale nejsme schopni s jistotou říci, zda zákon skutečně zorganizuje společnost, zda zafunguje jako šum anebo dokonce zda nepovede jeho aplikace k dezorganizaci (chaosu).

Definiční autority

Právo ve světě informačních technologií (stejně jako v podstatě všechno v tomto světě) nemůže fungovat bez člověka. V dnešní době již nejde pouze o armádní síť, jak internet začínal, ale můžeme pozorovat, že informační technologie vytváří sociální prostor, kde se mohou spojit lidé z opačných koutů světa bez nutnosti fyzického kontaktu.

Prostředí informačních technologií jako takové je pak tvořeno a dozorováno různými subjekty (tyto subjekty označujeme jako definiční autority). Tyto autority pak vytváří tzv. definiční normy.

Performativní pravidla

Tento model je v systému práva poměrně novým. Jedná se z pohledu pozitivistické teorie o právní anomálii, neboť nevychází z předpokladu duality regulujícího a regulovaného subjektu.

Regulatorní mechanismus performativních pravidel cílí v konečném důsledku na chování člověka účastnícího se života v informačních sítích. Formálně však právní pravidla nesměřují k těm, jejichž chování mají ultimativně regulovat, ale k definičním autoritám. Performativní pravidlo tak má charakter obecně (až teleologicky) definované povinnosti ukládající definiční autoritě vytvoření a technickou implementaci konkrétních pravidel, přičemž jejich obsah je ponechán úvaze definiční autority v návaznosti na parametry příslušného systému nebo sítě. Různé definiční autority mohou na své fyzické nebo logické infrastruktuře dle svého uvážení implementovat obsahově zcela různá pravidla, jejichž fungování však vede k témuž cíli.

Působnost práva na internetu

Úvod a cíl kapitoly

Tato kapitola se zabývá problematikou působnosti práva na internetu v soukromoprávních vztazích s mezinárodním (přeshraničním) prvkem, tedy primárně právním odvětvím mezinárodního práva soukromého.

Vznik a existence internetu a volný pohyb osob (offline i online) ovlivňují nejen společnost samotnou, ale i normativní systémy regulace. Od počátku devadesátých let mění internet pojetí přenosu dat, sdílení informací, času a prostoru. Dnes už se nerozhodujeme, zda do kyberprostoru vstoupíme. Dnes už tam (bez ohledu na naši vůli) žijeme.

Cílem této kapitoly je proto na základě obecných úvah týkajících se charakteristických znaků internetu a jeho vlivu na mezinárodní právo soukromé a principu teritoriality analyzovat konkrétní pravidla pro určení práva rozhodného a mezinárodní příslušnosti soudů v soukromoprávních vztazích s mezinárodním prvkem, které vznikají na internetu.

Ve druhé podkapitole vymezíme charakteristické znaky internetu, a jakým způsobem ovlivňují mezinárodní právo soukromé a procesní. Toto právní odvětví je úzce spojeno s principem teritoriality, kterému se věnujeme ve třetí podkapitole. Tyto teoretické úvahy a obecná východiska jsou ve čtvrté podkapitole konkretizována výkladem vlivu internetu na smluvní a mimosmluvní závazkové vztahy s mezinárodním prvkem, resp. vlivu na pravidla pro určení práva rozhodného a mezinárodní příslušnosti soudů. V páté, předposlední kapitole, se věnujeme možnému budoucímu vývoji v oblasti geolokace a práva, ochrany a přístupu k datům, práva být zapomenut a působnosti práva v jiných, z pohledu dosahu internetu zajímavých, právních odvětví.

Charakteristické znaky internetu a jejich význam z pohledu působnosti práva

Internet je prostorem neomezeným státními hranicemi a zásadně nezávislý na státním území. Pravidla mezinárodního práva soukromého jsou na druhou stranu založeny právě na principu teritoriality a vazby jednání k území určitého státu, kdy státní hranice vymezují limity moci a suverenity státu. Jsou-li data zveřejněna na sociálních sítích, jsou v zásadě „nezničitelná“.

Neexistuje jedno mocenské centrum. V této souvislosti je nutné zmínit postavení organizace ICANN, a hlavně globálních korporací typu Facebook, Google, Amazon apod., které významně ovlivňují moc zákonodárnou, výkonnou i soudní.

Dynamika technologického vývoje převažuje nad legislativní rychlostí úpravy právních vztahů, které jsou jí ovlivněny, a to jak na úrovni národní, tak regionální (typicky EU) i mezinárodní.

S ohledem na uvedené vlastnosti internetu je otázkou, nakolik mohou být stávající právní normy aplikovány na právní vztahy vznikající v prostředí internetu. V této věci můžeme uvést tři přístupy.

Pro překlenutí problémů spojených s jejich aplikací je nutné je nově interpretovat. Normy platného práva tak získávají nový obsah.

Můžeme uvažovat i o třetím přístupu, který je založen na tvrzení, že specifické prostředí internetu vyžaduje přijetí nových právních norem pro právní vztahy vznikající online v prostředí počítačových sítí. Problémy při aplikaci stávajících právních norem nelze překlenout interpretací a je nezbytné přijmout řešení na úrovni legislativní.

Internet a evropské mezinárodní právo soukromé a procesní

V dnešní realitě činností prováděných prostřednictvím internetu je téměř vždy možné dohledat právní vztah s mezinárodním prvkem.

Internet má významný vliv na omezení dosahu pravomoci států a jejich schopnosti regulovat právní vztahy vznikající na internetu. Tato otázka úzce souvisí s principem teritoriality a suverenity v mezinárodním právu soukromém.

 # Princip teritoriality v mezinárodním právu soukromém (a veřejném)

Jeho důsledkem je to, že stát může své veřejné moci podrobit osoby a věci, které se na jeho území nacházejí.

 # Internet a jeho vliv na právní úpravu soukromoprávních vztahů s mezinárodním prvkem

Normy mezinárodního práva soukromého a procesního by měly zajistit právní jistotu a být předvídatelné pro účastníky těchto právních vztahů.

Pro určení rozhodného práva v soukromoprávních vztazích s mezinárodním prvkem jsou stěžejní kolizní normy. Většina hraničních určovatelů obsažených v kolizních normách je ukotvena k území státu, kde došlo k právně významné skutečnosti.

Vybrané aspekty internetu a jeho dopad v evropském mezinárodním právu soukromém

Z pohledu řešení soukromoprávních vztahů s mezinárodním prvkem s dosahem na území EU jsou stěžejní tyto předpisy:

Nařízení Brusel Ibis, Nařízení Evropského parlamentu a Rady (ES) č. 864/2007 ze 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (dále jen Nařízení Řím I) a Nařízení Evropského parlamentu a Rady (ES) č. 864/2007 ze dne 11. července 2007 o právu rozhodném pro mimosmluvní závazkové vztahy (dále jen Nařízení Řím II).

Tyto předpisy a v nich použité kolizní normy a procesní kritéria jsou předmětem interpretační činnosti Soudního dvora EU. Jedním z problémů spojených s působností práva na internetu, resp. aplikací těchto předpisů je, že dosud neexistuje dostatečný počet rozhodnutí Soudního dvora EU, která by vnesla více světla do některých problematických oblastí.

Rozhodnutí Soudního dvora EU, která se přímo týkají kolizních norem a procesních kritérií při aplikaci na právní vztahy vznikající online, je možné rozdělit do tří okruhů: smluvní závazkové vztahy (online spotřebitelské smlouvy a online podnikatelské smlouvy), online porušení osobnostních práv včetně pomluvy, a online porušení práva duševního vlastnictví (smluvní a mimosmluvní aspekty).

Vliv internetu na kolizní a procesní problematiku smluvních závazkových vztahů

Zpravidla řešeny národními právními řády, které mohou být ovlivněny vzorovými zákony, nebo unifikovanými předpisy na úrovni mezinárodních organizací nebo EU.

Pro určení práva rozhodného pro smluvní závazkové vztahy s mezinárodním prvkem jsou relevantní tato ustanovení:

Nařízení Řím I: volba práva (článek 3); náhradní hraniční určovatel v případě neexistence volby práva (článek 4); materiální a formální platnost smlouvy (článek 10, resp. článek 11) a speciální úprava spotřebitelských smluv (článek 6).

Pro určení mezinárodní příslušnosti soudů ve sporech vyplývajících ze smluvních závazkových vztahů s mezinárodním prvkem jsou relevantní tato ustanovení Nařízení Brusel Ibis: obecná

příslušnost (článek 4 a bydliště žalovaného); tzv. alternativní příslušnost (článek 7 odst. 1 a místo plnění, resp. místo dodání nebo místo poskytnutí služeb) a speciální příslušnost pro spotřebitelské smlouvy [článek 17 odst. 1 písm. c) a zaměřování činnosti].

 # Online smlouvy uzavírané mezi podnikateli

Pokud doložky o volbě práva nebo volbě sudiště nejsou mezi stranami sjednány, je nutné určit právní režim transakce a místo sudiště samostatně. Tyto otázky jsou zajímavé zejména z procesního hlediska. Nařízení Brusel Ibis obsahuje alternativní pravidlo pro založení mezinárodní příslušnosti soudů ve sporech vyplývajících ze smluvních závazků v článku 7 odst. 1. Základním kritériem je místo plnění, resp. místo dodání nebo místo poskytnutí služeb. Je-li uzavřena smlouva online na internetu, míst plnění může být mnoho. Pro účely aplikace článku 7 odst. 1 Nařízení Brusel Ibis je nutné nejdříve kvalifikovat smluvní typ. Nejčastějšími smluvními typy jsou smlouva kupní a smlouva o poskytnutí služeb. Z hlediska +elektronického obchodu je pak nutné rozlišit, zda se jedná o kupní smlouvu na „hmotné“ nebo „digitální“ zboží, resp. smlouvu o poskytnutí „hmotných“ nebo „digitálních“ služeb.

Zboží může být objednáno online, ale doručeno fyzicky (například hardware k počítači). Zde je místo dodání poměrně jasné, lze jej ukotvit k území určitého státu. Předmětem smlouvy ovšem může být zboží, které je koupeno elektronicky a existuje pouze v digitální podobě (např. koupě elektronické knihy nebo počítačového softwaru). V tomto případě bude místo dodání obtížné určit. Podobný problém lze identifikovat u služeb, např. vytvoření webové prezentace. Opět se nabízí otázka, kde je místo poskytnutí takové služby.

 # Online spotřebitelské smlouvy

Díky internetu je pro spotřebitele poměrně snadné nakupovat virtuálně po celém světě a vstupovat do právních vztahů s mezinárodním prvkem. Spotřebitelská smlouva může být nejen uzavřena prostřednictvím internetu, ale i plněna online (například nákup a stahování digitálního obsahu, jako je hudba, filmy nebo hry) a placena online prostřednictvím bankovního převodu nebo platby kreditní kartou.

Kolizní normy pro určení práva rozhodného pro spotřebitelské smlouvy nalezneme v článku 6 Nařízení Řím I. Pravidla pro založení pravomoci soudů pro spotřebitelské smlouvy jsou upravena v článcích 17 až 19 Nařízení Brusel Ibis.

Z hlediska uzavírání smluv na internetu jsou pro určení rozhodného práva (v případě neexistence volby práva) a příslušného soudu (v případě neexistence prorogační dohody) klíčové pojmy spotřebitel, spotřebitelská smlouva a především kritérium zaměřování činnosti podnikatele na stát spotřebitele, které je uvedeno jak v článku 6 odst. 1 písm. b) Nařízení Řím I, tak článku 17 odst. 1 písm. c) Nařízení Brusel Ibis.

Vliv internetu na kolizní a procesní problematiku mimosmluvních závazků

Internet umožňuje téměř neomezené sdílení dat a projevů výsledků tvůrčí duševní činnosti. S tímto vývojem ovšem také roste počet přeshraničních sporů v případech mimosmluvních závazkových vztahů. Z hlediska vlivu internetu jsou nejzajímavější a nejčastější případy v oblasti porušení osobnostních práv včetně pomluvy a porušení práv vyplývajících z duševního vlastnictví.

 # Kolizní a procesní problematika porušení osobnostních práv včetně pomluvy na internetu

Osoba, která žaluje na poškození svých osobnostních práv, může postupovat podle základního pravidla dle článku 4 Nařízení Brusel Ibis a podat žalobu v členském státě, kde má žalovaný bydliště (tedy osoba, která informaci poškozující pověst vydala, zpravidla vydavatel). U těchto soudů může poškozená osoba podat žalobu na náhradu veškeré způsobené újmy. Poškozený může také alternativně dle článku 7 odst. 2 Nařízení Brusel Ibis žalovat u soudů místa, kde je znám a kde došlo k újmě na jeho pověsti. U soudů těchto států může ovšem žádat pouze poměrnou výši náhrady podle rozsahu újmy, která mu na území těchto států vznikla.

V místě centra svých zájmů může poškozená osoba žalovat na celou újmu, která jí v tomto místě vznikla.

 # Kolizní a procesní problematika porušení práv vyplývajících z porušení práva duševního vlastnictví na internetu

Ve vztahu působnosti práva na internetu a ochrany duševního vlastnictví se mezinárodní právo soukromé zabývá především relativními subjektivními právy – smluvními a mimosmluvními závazkovými vztahy spojenými s uplatňováním a ochranou práva duševního vlastnictví.

Kolizní problematika u práva duševního vlastnictví jako takového nevzniká. Tato premisa vychází z podstaty práv duševního vlastnictví jakožto absolutních práv, která působí proti všem a jsou ovládána pravidlem lex loci protectionis. Kolizní problematika naopak vzniká u smluvních a mimosmluvních závazků s těmito právy souvisejícími.

Budoucí vývoj

Jedním z možných způsobů, jak překonat problémy spojené s teritoriální povahou práva, je využívání geolokačních, resp. geoidentifikačních technologií. Na půdě Evropské unie bylo přijato Nařízení Evropského parlamentu a Rady (EU) 2017/1128 ze dne 14. června 2017 o přeshraniční přenositelnosti online služeb poskytujících obsah v rámci vnitřního trhu. Nařízení se použije od 20. března 2018 a jeho cílem je umožnit spotřebitelům, kteří zaplatili za online služby poskytující obsah ve své zemi, přístup k těmto službám při cestách do jiných členských států EU. Druhým významným předpisem je návrh Nařízení Evropského parlamentu a Rady o řešení zeměpisného blokování a jiných forem diskriminace na vnitřním trhu kvůli státní příslušnosti, místu bydliště či místu usazení zákazníků a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES. Cílem tohoto návrhu je posílit postavení spotřebitelů na vnitřním trhu EU a omezit jejich diskriminaci založenou na jejich lokalizaci.

Shrnutí

Online prostředí umožňuje relativně snadno vstupovat do soukromoprávních vztahů s mezinárodním prvkem. V takovém případě je stěžejní určení, kde se budeme v případě sporu soudit a jakým právem se právní vztah řídí. Tyto otázky řeší mezinárodní právo soukromé.

Z našeho pohledu je zásadní, jaké hodnoty jsou při tvorbě právních norem preferovány; zda právní jistota a předvídatelnost, či flexibilita přijatého řešení.

Právo je teritoriální a zejména kolizní a procesní normy zásadně ukotvují právní vztah k území určitého státu. Problematické aspekty teritoriality jsme ilustrovali pomocí tří rozhodnutí, ve kterých národní soudy přijaly velmi extenzivní interpretaci vazby území k jednání, ke kterému došlo na internetu. Z tohoto důvodu byla tato tři rozhodnutí, byť teoreticky zajímavá, prakticky nevykonatelná.

Odpovědnost ISP

Odpovědnost ISP

Z hlediska teoretického či strukturálního se může zdát, že není důvodu k jakkoli specifickému řešení tohoto problému ve vztahu k nějaké zvláštní skupině subjektů. Není totiž žádného podstatného rozdílu mezi podnikatelem a podnikatelem v oboru ICT, respektive mezi poskytovatelem nějaké služby a poskytovatelem služby informační společnosti. Ať jde o subjektivní či objektivní odpovědnost civilní, o odpovědnost ve správním právu, či dokonce odpovědnost trestní, nemáme strukturální důvod odlišovat poskytovatele služeb informační společnosti od ostatních osob.

Systémový problém dopadů různých odpovědnostních kategorií na poskytovatele služeb informační společnosti se tedy neprojevuje v úrovni abstraktní či teoretické, ale vyplyne až z pragmatického zkoumání skutečného fungování těchto služeb. Předně totiž jde o služby poskytované v bezprecedentním rozsahu, tj. ve značné frekvenci a k užitku velkého množství různých druhů uživatelů. Druhým, a snad ještě důležitějším rysem těchto služeb, je jejich faktická podstata spočívající v technickém zajištění uživatelských informačních transakcí. Služba jako taková v tomto případě zpravidla neurčuje ani neovlivňuje obsah příslušné informační transakce, ale funguje pouze jako médium, přičemž konkrétní podobu příslušné transakce určuje uživatel.

Vyloženě problematickými pak jsou z pohledu poskytovatele služby informační společnosti objektivní typy právní odpovědnosti, u nichž zavinění nehraje roli. Jde přitom často právě o ty druhy porušení právních povinností, k nimž může v prostředí informačních sítí docházet velmi často – typicky např. o rušení osobnostních práv, práv duševního vlastnictví, práv plynoucích z ochrany osobních údajů aj. V takových případech není třeba zkoumat zavinění těch, kdo společným jednáním způsobili škodlivý následek, a jedinou obranou poskytovatele služby informační společnosti může být (vedle obligátní, avšak nikoli příliš užitečné vyšší moci) poněkud problémová argumentace, že příslušný škodlivý následek vlastně vůbec nezpůsobil.

K právě uvedenému přistupuje ještě specifický rys českého soukromého práva, které systematicky nerozeznává primární a sekundární odpovědnost. Na rozdíl od práva trestního, které typicky rozlišuje různé druhy účasti na protiprávním jednání (např. návod, pomoc apod.) nemá naše soukromé právo kategorie pro to, co se anglickými termíny označuje jako „secondary“, „contributory“ či „vicarious liability“. Český občanský zákoník totiž pracuje pouze s pojmem solidární odpovědnosti, která může být v odůvodněných případech rozdělena mezi povinné subjekty dle míry jejich zavinění.

Vedle faktické anonymity je na internetu běžné též to, co jsme výše poněkud nepřesně označili za anonymitu právní. Jedná se o situaci, kdy rušitel sice může být ztotožněn, ale jeho fyzická lokalizace činí prakticky nemožným vést proti němu spravedlivý proces. Lze tak sice teoreticky

podat v České republice na internetového diskutéra z Barmy žalobu na ochranu proti nekalosoutěžnímu jednání, avšak žádný rozumný člověk se k tomu zřejmě z pragmatických důvodů neodhodlá. Pokud už by se snad zadařilo dotyčného obeslat a úspěšně dospět až k rozsudku, neexistuje záruka, že tento bude v zahraničí uznán a. Vedle vystavení poskytovatele služby pasivní legitimaci pokaždé, kdy dojde k protiprávnímu jednání uživatele, je dalším strašidelným faktorem hraniční. Na jeho základě lze totiž uplatnit postih proti škodnému jednání v místě, kde došlo ke škodlivému následku, a použít k tomu místní právo. Znamená to, že poskytovatel přeshraničně dostupné služby informační společnosti nemá dokonce ani jistotu ohledně toho, ze které země a podle jakého práva může přijít riziko postihu.

Vývoj právní úpravy odpovědnosti ISP

V Evropské unii ani nelze očekávat sjednocení interpretační praxe judikaturou bez toho, aniž by v předmětné věcné působnosti existovala primární nebo sekundární unijní legislativa. Jedinou prakticky dostupnou možností řešení tohoto problému tak bylo přijetí společné unijní úpravy, která zajistí potřebnou jistotu a efektivitu, to však bez sjednocování příslušných odpovědnostních titulů. Tak vznikla směrnice Evropského parlamentu a Rady 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu na vnitřním trhu označovaná krátce jako směrnice o elektronickém obchodu nebo jen zkratkou ECD (e-commerce directive).

Do českého práva se specifická úprava odpovědnosti poskytovatelů služeb informační společnosti dostala až v roce 2004 právě harmonizací shora cit. směrnice zákonem č. 480/2004 Sb., o některých službách informační společnosti. Český právotvůrce zvolil v tomto případě standardní, avšak nepříliš šťastné řešení harmonizace formou převzetí normativních formulací přímo ze směrnice. Problém výsledného produktu spočívá jednak ve skutečnosti, že primárním adresátem norem založených směrnicí jsou členské státy, zatímco adresátem zákona mají být konkrétní osoby.

Relativně malá frekvence užití zákona č. 480/2004 Sb. byla u nás dána též skutečností, že jen velmi málo relevantních poskytovatelů služeb informační společnosti typu hosting mělo nebo má v České republice obecný soud. Pokud už u nás takoví poskytovatelé služeb jsou, obvykle mají implementovány takové “compliance” procedury, které je za využití omezujících ustanovení zákona č. 480/2004 Sb. efektivně brání před postihem. Na rozdíl například od Německa nebo Estonska se v naší právní praxi zatím ani nevyskytly dostatečně kreativní přístupy, které by zákonné omezení odpovědnosti dokázaly relativizovat nebo zmírnit.

Základem právní úpravy odpovědnosti ISP je pojem poskytovatele služby informační společnosti. Jeho vymezení, resp. vymezení pojmu služby informační společnosti, se však nenachází v samotné směrnici o e-commerce, ale bylo původně obsaženo ve směrnici č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění novelizační směrnice č. 98/48/ES.

Směrnice č. 98/34/ES byla později nahrazena novou úpravou ve směrnici (EU) č. 2015/1535 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti. Nová směrnice (EU) č. 2015/1535 sice dále obsahuje definici pojmu služby informační

společnosti, ale jeho obsah se oproti předchozí úpravě mírně změnil.

Služby typu mere conduit, caching

Zákon č. 480/2004 Sb. ve shodě se směrnicí o e-commerce rozdělují poskytovatele služeb informační společnosti na tři základní skupiny, a to:

1) Prostý přenos (mere conduit), tj. ve smyslu zákona služba spočívající v „přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací“.

2) Ukládání do vyrovnávací paměti (caching), tj. ve smyslu zákona služba spočívající v přenosu „automaticky dočasně meziukládaných informací“.

3) Shromažďování informací (hosting), tj. ve smyslu zákona služba spočívající v „ukládání obsahu informací poskytovaných uživatelem“.

Poskytovatelé služeb typu mere conduit mají odpovědnost omezenu § 3 odst. 1 zákona č. 480/2004 Sb. následovně:

Poskytovatel služby, jež spočívá v přenosu informací poskytnutých uživatelem prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací, odpovídá za obsah přenášených informací, jen pokud

a) přenos sám iniciuje,

b) zvolí uživatele přenášené informace, nebo

c) zvolí nebo změní obsah přenášené informace.

Poskytovatel služby informační společnosti prvního typu nemůže odpovídat (civilně, správně ani trestně) za protiprávní jednání svého uživatele, dokud takovému poskytovateli nelze přičíst předmětná data nebo jejich komunikaci. Jestliže se tedy příslušný ISP prvního typu (např. telekomunikační operátor) na protiprávní komunikaci nijak nepodílí a pouze k ní poskytne svoji infrastrukturu, je jeho odpovědnost podle českého práva vyloučena.

Toto ustanovení dopadá především na situace, kdy data mají původ mimo dosah jurisdikce příslušného členského státu, avšak protiprávní důsledky jejich existence se v tomto státě nějakým relevantním způsobem projeví. Typickým příkladem může být dětská pornografie či nacistická nebo komunistická nenávistná propaganda umístěná na serveru mimo Českou republiku. V takovém případě mají orgány autoritativní aplikace práva příslušného členského státu ztížen či dokonce znemožněn právní postih, v jehož důsledku by došlo k odstranění protiprávních dat. Pokud by byli poskytovatelé služeb typu “mere conduit” zcela vyňati z dosahu sankčních norem příslušného členského státu, byla by veřejná moc vzhledem k dostupnosti protiprávních dat zcela bezmocná.

Ukládání do vyrovnávací paměti („caching“)

1. Členské státy zajistí, aby v případě služby informační společnosti spočívající v přenosu informací poskytovaných příjemcem služby nebyl poskytovatel služby odpovědný za automatické dočasné přechodné ukládání, které slouží pouze pro co možná nejúčinnější následný přenos informace na žádost jiných příjemců služby, pokud:

a) poskytovatel služby informaci nezmění;

b) poskytovatel služby vyhoví podmínkám přístupu k informaci;

c) poskytovatel služby dodržuje pravidla o aktualizaci informace, která jsou stanovena způsobem obecně uznávaným a používaným v průmyslu;

d) poskytovatel služby nepřekročí povolené používání technologie obecně uznávané a používané v průmyslu s cílem získat údaje o užívání informace;

Oproti shora zmíněnému případu poskytovatelů služeb typu mere conduit se u služeb typu “caching” nejedná o přenos dat, ale o jejich ukládání. Na rozdíl od hostingu však v tomto případě nejde o konkrétní službu spočívající v zajištění dostupnosti uživatelských dat, ale o automat zvyšující efektivitu komunikačních linek tím, že v lokalitě se zvýšeným zájmem uživatelů provádí “en bloc” replikaci dat z původního cílového místa.

Vedle přičitatelnosti předmětných dat poskytovateli služby typu cache se omezení odpovědnosti neuplatní ještě v případech vadné replikace(zrcadlení) cílového místa. Tato víceméně technická výjimka z omezení odpovědnosti dopadá především na případy, kdy je na původním cílovém místě (zrcadleném serveru) provedena úprava dat a cache (zrcadlící server) tuto úpravu odpovídajícím způsobem nereflektuje. Poskytovatel služby typu caching tak může podle práva příslušného členského státu odpovídat za protiprávnost uložených (resp. zrcadlených) dat například tehdy, pokud původní cílové místo odstraní protiprávně publikovaná data, cache toto odstranění nereflektuje, a protiprávně zveřejněná data jsou zde tím pádem stále dostupná. Odpovědnostní limit poskytovatelů služeb typu caching každopádně nepředstavuje v právu informačních a komunikačních technologií nijak široce reflektovanou problematiku. Soudy členských států tak doposud nemusely řešit žádné složité případy a ani Soudní dvůr zatím neměl důvod se touto otázkou zabývat.

Hosting

Členské státy zajistí, aby v případě služby informační společnosti spočívající v ukládání informací poskytovaných příjemcem služby nebyl poskytovatel služby odpovědný za informace ukládané na žádost příjemce, pokud:

a) poskytovatel nebyl účinně seznámen s protiprávní činností nebo informací a ani s ohledem na nárok na náhradu škody si není vědom skutečností nebo okolností, z nichž by byla zjevná protiprávní činnost nebo informace, nebo

b) poskytovatel, jakmile se o tomto dozvěděl, jednal s cílem odstranit tyto informace nebo k nim znemožnit přístup.

Otázka omezení odpovědnosti posledního typu poskytovatele služby informační společnosti, tj. hosting, je v současné praxi s přehledem nejčastější a z hlediska soudní praxe stále frekventovanější. Důvodem je vedle bezprecedentního významu tohoto typu služeb též především obecná změna adresování normativního tlaku oprávněných subjektů z jednotlivých rušitelů právě na poskytovatele služeb.

Nástup služeb typu peer-to-peer. Tyto služby si získaly velkou oblibu a generují podstatný ekonomický efekt. Autorské právo, namísto toho, aby zisk z obliby těchto služeb směřoval k původcům jejich hodnoty (autorům), se omezuje na prosté snahy o zákaz jejich používání.

Hlavními rušiteli práv duševního vlastnictví jsou u služeb typu peer-to-peer uživatelé, kteří umožňují ostatním užívat svůj mediální nebo jiný obsah. Zjednodušeně řečeno, největší piráti zároveň jsou ochotni za příslušný obsah nejvíce platit.

Některé služby informační společnosti typu hosting obsahují vlastní funkcionality nebo dokonce celé komplexní aplikace řešící oznamování protiprávního jednání svých uživatelů. Příkladně na diskusních serverech nebo sociálních sítích se tak lze setkat s tlačítky „nahlásit“, která lze použít právě pro oznámení protiprávnosti příslušnému poskytovateli služby. Takové řešení je možno považovat za vhodné a vcelku efektivní, neboť příslušnému ISP umožňuje rychle řešit standardní případy. Z pohledu právního postavení třetí osoby dotčené protiprávním jednáním uživatele je však poněkud problematické – neposkytuje totiž zpravidla důkaz komunikace příslušného oznámení poskytovateli služby. V případech, kdy osoba dotčená na právech předpokládá problémy při iniciativním řešení svého nároku ze strany ISP (tj. nevěří v aktivitu příslušného ISP), je tedy vhodné zaslat příslušnému ISP oznámení o protiprávnosti ještě jiným způsobem umožňujícím pozdější důkaz ohledně času, kdy bylo oznámení ve smyslu § 5 odst. 1 písm. b) učiněno.

Filtrování

Jedním z obecně problematických momentů české harmonizace omezení odpovědnosti ISP pak je ustanovení § 6 zákona č. 480/2004 Sb. následujícího znění:

Poskytovatelé služeb uvedení v § 3 až 5 nejsou povinni

a) dohlížet na obsah jimi přenášených nebo ukládaných informací,

b) aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace.

Český zákonodárce přepsal do zákona obecné harmonizační ustanovení čl. 15 vylučující možnost členských států založit aktivní povinnost poskytovatelům služeb informační společnosti všech tří typů monitorovat své uživatele. Zatímco směrnicový požadavek na to, aby členské státy nezatěžovaly ISP povinností monitorovat uživatele je zcela legitimní, je jeho česká implementace přinejmenším pozoruhodná – zákonodárce zde totiž expressis verbis říká, že osoby soukromého práva (zde ISP) nemají určitou povinnost.

Samozřejmě platí, že zákon právní povinnosti zakládá a obecně je subjektům mimo orgánů veřejné moci dovoleno činit vše, co zákon nezakazuje. V tomto případě jako by však zákonodárce na tuto základní ústavní maximu pozapomněl a jal se vyjmenovávat, jaké povinnosti naopak regulovaný subjekt nemá. Jediný význam § 6 spočívá v tom, že pokud už snad české právo někde založí příslušným ISP povinnost monitorovat své uživatele, tato negativní zákonná formulace takovou povinnost explicitně ruší nebo omezuje.

Čl. 15 však nepředstavuje problém pouze pro českého právo tvůrce. Jedná se totiž o ustanovení, které prakticky brání členským státům v zavedení nástrojů pro a priori obsahovou kontrolu uživatelských dat.

Na první pohled se může zdát, že v případě čl. 15 jde pouze o konkrétní implementaci lidskoprávního zákazu cenzury například ve smyslu čl. 17 odst. 3 Listiny základních práv a svobod. Ve skutečnosti však kategorická formulace čl. 15 omezuje právo tvůrce v možnostech zavést poskytovatelům služeb informační společnosti obecnou povinnost aktivně omezovat své uživatele v protiprávním jednání.

Kontraktační platformy

Kontraktační platformy jsou v podstatě služby postavené na uživatelském obsahu, resp. na uživatelské aktivitě. Sekundárním objektem právních vztahů souvisejících s provozem platforem jsou tedy data podobně, jako je tomu u většiny ostatních služeb informační společnosti. Od ostatních uživatelských služeb informační společnosti (tj. služeb UGC – user-generated content) typu hosting se však významně odlišují tím, že primární objekt těchto vztahů nemá se službami informační společnosti zpravidla nic moc společného a jejich dominantní účel tedy má od technické podstaty samotné služby zcela odlišný charakter.

Rozdíl mezi klasickou hostingovou službou informační společnosti založenou na uživatelském obsahu (tj. službou UGC) a platformou lze vysvětlit třeba na příkladu sociálních sítí. Zatímco primárním účelem sociální sítě, jakou je například Facebook, je komunikace uživatelských dat, primárním účelem platformy typu aribnb, Uber nebo Bookatiger je poskytnutí služby, která s uživatelskými daty přímo nesouvisí, tj. ubytování, přepravy nebo úklidu domácnosti.

Víceméně tradiční charakter transakcí, které ve svém souhrnu tvoří sdílenou ekonomiku, dává dojem, že z právního hlediska prakticky není co řešit. Jde totiž pořád o zprostředkování, prodej a koupi, poskytnutí služby (úsluhy, posluhy) aj. Virtualizace sdílené ekonomiky však v tomto případě přináší právu závažnou výzvu danou bezprecedentní kombinací formálních novot příslušných sdílených transakcí a jejich souhrnného ekonomického významu. Stručně řečeno jsou tradiční

transakce z hlediska své formy a vzájemné kombinace natolik jiné a jejich výskyt je natolik významný, že je třeba věnovat tomuto jevu zvláštní pozornost.

Tím, co dnešní sdílenou ekonomiku ze subjektivního a funkčního hlediska zřetelně odlišuje od všeho, s čím máme doposud v právu nějakou zkušenost, je především povaha a relativní význam zprostředkovatele. V podmínkách informační společnosti je jím služba, kterou označujeme jako platformu sdílené ekonomiky nebo prostě jen jako platformu.

Platforma se od klasického zprostředkovatele liší především tím, že kompletně kontroluje příslušnou transakci. Vedle výběru a spojení nabídky a poptávky totiž obstarává též definici smluvních podmínek, poskytuje právní a technickou dokumentaci, zprostředkovává související vzájemnou komunikaci stran, zajišťuje finanční vypořádání (zpravidla formou elektronického platebního prostředku nebo elektronických peněz) a dokonce zajišťuje komplexní systém pro řešení případných sporů o plnění.

Z transakčního hlediska je dodavatel (poskytovatel služby) v permanentním komplexním právním vztahu s platformou a podobně je v takovém právním vztahu též odběratel (či zákazník). Hlavním závazkem z těchto vztahů na straně platformy však není přímo zprostředkování příslušné transakce (prodeje, poskytnutí služby apod.), ale provoz a údržba virtuální identity. Platforma kompletně kontroluje fungování obou typů virtuálních identit (poskytovatele služby i spotřebitele) a za užití různých sofistikovaných nástrojů se snaží dosáhnout uzavření smluv na hlavní plnění (tj. kupní, nájemní, přepravní nebo jiné smlouvy).

Strany mají sice možnost svobodně projevit svoji vůli, ta je však obecně omezena pouze na volbu ohledně uzavření či neuzavření smlouvy. Konkrétní smluvní podmínky jsou v tomto případě diktovány platformou a možnost jejich alternace na základě vůle stran je buď zcela minimální, nebo se týká jen otázek majících z podstaty specifický charakter. Online tržiště tedy příkladně dávají prodávajícím možnost zvolit artikl a cenu, zatímco přepravní platformy typicky umožňují pouze volbu trasy (nikoli už ceny) a úklidové platformy dávají zákazníkovi pouze možnost zvolit si z předdefinovaných forem plnění za fixní cenu. Forma poskytnutí služby, dodací podmínky, sankce ani jiné standardní součásti smlouvy nemohou být mezi stranami předmětem jednání či odchylné dohody. Typicky u přepravních služeb pak dokonce kontrahenti v době uzavření smlouvy ani vzájemně neznají svoji pravou totožnost, v některých případech dokonce nemají ani možnost odmítnout transakci (resp. jim při odmítnutí hrozí sankce).

Výše uvedená nemožnost jednat o smluvních podmínkách samozřejmě opět nepředstavuje pro soukromé právo nic zásadně nového. Tuto situaci dnes dostatečně řeší úprava adhezních smluv, přičemž právo zde logicky chrání slabší stranu. V případě platforem však problém spočívá v tom, že určit slabší stranu předmětného závazkového právního vztahu může být poměrně složité, neboť na obou stranách může vystupovat spotřebitel, resp. nikoli profesionál. Nadto nelze přehlédnout ani skutečnost, že podmínky adhezní smlouvy v tomto případě nevytváří ani nenavrhuje žádný z kontrahentů. Těžko tedy za této situace uplatňovat například pravidlo, dle kterého je neurčitost smluvního ujednání přičítáno k tíži toho, kdo takové ujednání poprvé použil; v tomto případě totiž všechna ujednání vymyslel a použil zprostředkovatel, který však vůbec není stranou realizační smlouvy.

Evropské právo má zatím důkladnou zkušenost především s klasifikací odpovědnosti online tržišť typu eBay nebo Aukro. Ta jsou, technicky vzato, rovněž platformami, neboť realizačními transakcemi jsou zde mezi uživatelská koupě a prodej. Od ubytovacích nebo přepravních platforem se však online tržiště výrazně odlišují větší mírou autonomie na straně navrhovatelů realizačních smluv (tj. prodávajících) – prodávající má totiž kompletní volnost nejen v samotné otázce, zda něco chce prostřednictvím platformy prodat, ale též za jakých podmínek.

Vyhledávače

Vyhledávače jsou podobně jako kontraktační platformy v podstatě službou UGC (user-generated content), protože jejich obsah tvoří uživatelská data. V porovnání s platformami však vyhledávače na jedné straně nedefinují práva a povinnosti realizačních transakcí, takže vztah mezi vyhledávačem a uživatelem jeho služeb je z právního hlediska mnohem volnější. Na straně druhé však vyhledávače hrají daleko aktivnější roli při zpracování a transformaci uživatelských dat. Uživatelé jejich služeb, ať jde o nabídku dat z cílových míst nebo poptávku po nich, mají totiž velmi malý vliv na to, jakým způsobem budou jejich data zpracována.

Při pohledu na silně monopolizovanou strukturu vyhledávacích služeb by se mohlo zdát, že celý následující výklad vztahuje se u nás prakticky pouze ke službám dvou relevantních poskytovatelů, a to seznam.cz a google.cz. Přestože je obecný trh vyhledávačů u nás obsazen právě uvedenými tržními dominanty, nejde o výlučné poskytovatele tohoto typu služeb. Vyhledávače totiž můžeme najít například i v rámci sociálních sítí nebo online tržišť.

Doménou, v níž vnitro platformní vyhledávače fungují, není celý internet, a jejich dosah je tedy omezen pouze na data zpracovávaná příslušnou platformou. Funkce těchto vyhledávačů je však z pohledu uživatelů z obou stran (nabídky dat i poptávky po nich) obdobná jako u obecných vyhledávačů, protože platformní vyhledávače pomáhají uživateli zorientovat se v jinak ohromném a nepřehledném množství dat. Především velké platformy si přitom vyhledávací funkce v rámci svých domén pečlivě hlídají před obecnými vyhledávači typu Google nebo Seznam – to proto, aby mohly z vyhledávacího monopolu v rámci svého prostředí ekonomicky těžit.

Příkladem právě uvedeného mohou být populární obchodní a spotřebitelská online tržiště provozovaná koncernem Alibaba – jde o služby Aliexpress, Tmall Global, alibaba.com a Lazada. Podstatnou část jejich příjmů tvoří, kromě provizí z realizovaných transakcí, především poplatky vybírané za optimalizaci vyhledávání. Zjednodušeně řečeno tedy Alibaba nevydělává jen na uzavřených obchodech, ale zvláštní zisky mu přináší též provoz vyhledávače, který v rámci této platformy používají zákazníci k tomu, aby našli požadované zboží nebo službu.

Podobně jako ve shora diskutovaném případě online tržišť je i v případě vyhledávačů jejich klasifikace jako ISP především otázkou míry jejich aktivního působení ve vztahu k uživatelským datům. Poskytovatel služby informační společnosti třetího typu (tj. hosting) totiž může požívat výhod omezení odpovědnosti vzhledem k protiprávnímu jednání svých uživatelů pouze tehdy, pokud tato služba skutečně ukládá uživatelská data, tj. pokud její skutečná činnost odpovídá definici čl. 14 směrnice o e-commerce, resp. § 5 zákona č. 480/2004 Sb.

Při právní klasifikaci vyhledávačů však je třeba zohlednit ještě jednu podstatnou skutečnost, a to, že uživatelská data často zpracovávají bez jakéhokoli přičinění příslušných uživatelů. Vyhledávače totiž automaticky prohledávají svoji doménu a získaná data pak nabízejí formou zpracovaných odkazů zájemcům o vyhledání konkrétních cílových míst. Pokud si tedy někdo příkladně vytvoří novou webovou prezentaci, obecný vyhledávač tuto prezentaci sám bez dalšího najde, zpracuje a nabídne svým uživatelům ve formě odkazu.

Je pochopitelně možné argumentovat, že pokud někdo dává nějaká data veřejně na internet, činí tak zřejmě proto, aby se kdokoli mohl s těmito daty seznámit. Vyhledávač pak vlastně bez nároku na protiplnění podniká kroky ke zvýšení popularity příslušného cílového místa a zvyšuje pravděpodobnost, že se potenciální zájemce dostane k tam umístěným datům.

U nás bude zřejmě zvláštní charakter plně automatizovaného zpracování dat vyhledávačem považován ve vztahu k protiprávním datům obsaženým na cílovém místě za „důvod hodný zvláštního zřetele“ ve smyslu § 2915 odst. 2 občanského zákoníku a povede k rozdělení odpovědnosti za výsledný škodlivý následek. Podobnou logikou, jakou naše soudy již dříve aplikovaly na postavení národní doménové autority jako účastníka škodného jednání spočívajícího v protiprávní registraci a užívání doménového jména, tedy dojde ve výsledku k tomu, že odpovědnost vyhledávače bude v takovém případě zřejmě omezena na povinnost odstranit link na cílové místo, jehož správce porušuje právní povinnost.

Shrnutí

V této kapitole jsme se věnovali problematice odpovědnosti poskytovatelů služeb informační společnosti. Otázku odpovědnosti či spoluodpovědnosti ISP jsme označili za základní problém celého odvětví práva informačních a komunikačních technologií, neboť se dotýká prakticky všeho právně relevantního dění v prostředí informačních sítí.

V návaznosti na zákonnou klasifikaci mere *conduit* – *hosting* – *caching* jsme provedli výklad ke standardním formám omezení odpovědnosti ISP v soukromém, správním a trestním právu a konstatovali jsme některé technické a obsahové defekty české harmonizační úpravy. Z regulatorních nástrojů jsme se podrobně věnovali otázce filtrování, která dominuje současnému judikaturnímu a legislativnímu diskursu.

Z konkrétních druhů poskytovatelů služeb informační společnosti jsme se zaměřili na internetové platformy a vyhledávače. V obou případech jde o subjekty, jejichž regulatorní aktivita má bezprostřední a zásadní dopad na dění v prostředí informačních sítí. Vedle právní kvalifikace těchto subjektů ve struktuře zákonných ISP jsme diskutovali výhody a rizika jejich proaktivní role při realizaci práva. Vedle detekce a eliminace různých důsledků protiprávního jednání uživatelů jsme se zabývali rolí platforem jako plátců nepřímých daní nebo jako sběračů hodnotných dat pro potřeby chytré regulace.

Práva k datům

Práva k datům

Data jsou v informatice údaje zaznamenané v digitální (číselné) podobě určené k počítačovému zpracování. Data (např. číslo, text, obrázek, zvuk) jsou zapsána (kódována) v podobě posloupností čísel (bajtů) a uložena např. v operační paměti počítače nebo na záznamovém médiu (pevný disk, CD, paměťová kata) Stejným způsobem je v paměti vedle dat uložen i sled instrukcí tvořící počítačový program, který určuje, jak má počítač data zpracovávat. Pojem data je často libovolně zaměňován s pojmem informace, nicméně v rámci teorie informace formulované kybernetikem Norbertem Wienerem jsou data prostým záznamem hodnot, a informace se z nich stávají až po jejich výkladu v kontextu s využitím znalostí.

Informace jsou data prezentovaná v takovém kontextu, který dává smysl a význam. Informace tedy slouží ke zpracování, skladování nebo přenášení dat. Například číslo 120/80 patří mezi data, pokud jej ale ozřejmíme jako dnešní ranní krevní tlak pacienta v milimetrech rtuťového sloupce, již je z něj užitečná informace.

Právo je multidimenzionální fenomén a vícevýznamový výraz, který je nutno definovat ve všech jeho rovinách neboli dimenzích. Nelze jeho definici tedy zúžit pouze na jeho normativní význam, ač především v této rovině je chápán nejčastěji, tedy ve smyslu soustavy právních norem, tj. pravidel chování (příkazů, zákazů nebo dovolení), kterými se řídí lidské spolužití a které jsou uznávané nebo přímo stanovené státem.

> Práva k datům se rozdělují na dvě skupiny, a to absolutní právo k datům a relativní práva k datům.

Obecně může absolutní práva působící erga omnes, a tedy s tím korespondující povinnosti třetích stran, založit jen zákon. Tím může být jednak občanský zákoník, ale i jiné zvláštní předpisy práva soukromého, jako např. předpisy upravující právo duševního vlastnictví. Občanský zákoník zakotvuje absolutní majetková práva věcná, tedy k věci. Aktuální národní právní úprava je postavena na širokém pojetí věci v právním smyslu, kdy se jí rozumí vše, „co je rozdílné od osoby a slouží potřebě lidí“, což zahrnuje jak věci hmotné, tak nehmotné. Věci nehmotné zahrnují práva, jejichž povaha to připouští, a jiné věci bez hmotné podstaty. Práva mohou být věcí nehmotnou pouze, pokud se jedná o práva majetková a převoditelná a nebrání-li tomu jejich povaha, tedy pokud se např. nejedná o práva osobnostní. Nehmotné statky mohou být věcmi nehmotnými (tedy jiné věci bez hmotné podstaty) pouze pokud se k nim vztahují převoditelná majetková práva. Ty nehmotné statky, které jsou předmětem osobnostních nebo smíšených práv, nemohou být věcmi.

Neexistence absolutních majetkových práv k datům jako takovým neznamená, že by nešlo zajistit ochranu dat relativně, tedy ve vztahu k jiným osobám. Smluvní ochrana je v praxi paradoxně možná i preferovaným způsobem ochrany dat. Důvodem je mj. i to, že smluvně založená práva k užití dat nepodléhají zákonným výjimkám a omezením typu dovolené rozmnožování pro soukromé užití, či dovolené nepodstatné vytěžování databáze. V souladu se zásadou smluvní volnosti si strany mohou sjednat povinnosti ve vztahu k datům inter partes – typicky např. povinnost chránit data před jejich zpřístupněním jiným osobám nebo např. povinnost poskytovat přístup k datům. Porušení sjednaných povinností lze sankcionovat stanovením smluvní pokuty. Vhodné je pak v dané smlouvě i sjednat, že uhrazení smluvní pokuty nevylučuje právo věřitele domáhat se náhrady škody, která vznikla porušením této smluvní povinnosti. Specifickou relativní ochranu poskytuje i právní ochrana proti nekalé soutěži, kterou musí členské státy Pařížské unijní úmluvy zajistit na základě čl. 10bis této Úmluvy. Národní úprava obecně zakazuje jednání, která jsou realizována v hospodářském styku v rozporu s dobrými mravy soutěže a jsou způsobilá přivodit újmu jiným soutěžitelům nebo zákazníkům. Právem reprobované tak je jakékoli nakládání s daty, které naplní podmínky této generální klauzule. Relativní ochrana datům může být právem proti nekalé soutěži poskytována i pokud netvoří obchodní tajemství, tedy i když by nebyla naplněna pojmenovaná (zvláštní) skutková podstata nekalé soutěže porušování obchodního tajemství.

Vzhledem k nehmotné podstatě dat je právo duševního vlastnictví intuitivně prvním ochranným režimem, který je vzhledem k ochraně dat, resp. užitku z nich, zvažován. V následujícím výkladu bude věnována pozornost dvěma specifickým odvětvím práva duševního vlastnictví, která lze využít při ochraně kvalifikovaných dat, a to autorskému právu a právům souvisejícím a zvláštnímu právu pořizovatele databáze. Naopak pozornost nebude věnována právům průmyslovým, která mohou data chránit pouze ve velmi omezené míře nebo vůbec. Známkové právo chrání data způsobilá grafického označení, která nesou určitý význam, tedy jsou způsobilá odlišit výrobky a služby, proti jejich kvalifikovanému užití v obchodním styku. Ostatní průmyslová práva jsou k ochraně dat jako takových nevyužitelná. Například v případě snahy získat patentovou ochranu pro data by byla taková přihláška zamítnuta, neboť data jako taková nejsou technickým řešením, které by šlo považovat za vynález. Patent by ale mohl být, při splnění všech podmínek patentovatelnosti, udělen např. na vynález, který s daty inherentně pracuje, jako např. způsob shromažďování, evidence a zpřístupnění dat. Obdobně nemá smysl uvažovat o ochraně dat průmyslovým vzorem, neboť se vůbec nejedná o způsobilý předmět ochrany. Těmto právům průmyslovým se v kontextu ochrany dat právem duševního vlastnictví nebudeme dále věnovat.

Při diskusi právní ochrany dat nelze opominout ani veřejnoprávní aspekt dané problematiky. Neoprávněným nakládání s daty lze naplnit více skutkových podstat trestných činů, nejčastěji pak trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací. První odstavec ustanovení § 230 zákona č. 40/2009 Sb. chrání důvěrnost dat, druhý pak jejich integritu a dostupnost. V případě jednání dle druhého odstavce není k jeho trestnosti vyžadováno neoprávněné získání přístupu k datům (tedy porušení důvěrnosti), ten může být naopak i legální, jako např. na základě pracovní či jiné smlouvy. Postihovány, ale mohou být úmyslné aktivity vztahující se k datům samotným, jakými jsou jejich neoprávněné užití, manipulace s nimi, či jejich falšování. Jak již uvedl Nejvyšší soud, jedná se v případě neoprávněného užití dat o ryze formální, abstraktně ohrožovací, delikt, kdy je postihováno samotné užití dat bez dalšího, které nemusí vést k nějakému objektivnímu výsledku na předmětu útoku (tedy počítačovém systému, nosiči informací, resp. datech). V základní, nekvalifikované, skutkové podstatě jím ani nemusí být

způsobena škoda či jím pachatel ani nemusí získat prospěch. Neoprávněnost užití je nutno dovodit z porušení jiných norem, jako např. ustanovení o ochraně osobnosti, autorských práv, či obchodního tajemství. Protiprávní je i takové užití, které je činěno bez vědomí a souhlasu oprávněné osoby, či v rozporu se stanoveným účelem. Neoprávněné je též nedovolené kopírování dat na jejich jiný nosič, jakož i jakákoli manipulace s nimi.

Výše diskutovaná absolutní, ani relativní práva k datům ze své podstaty reálně nezabrání neoprávněnému nakládání s nimi. Poskytovaná právní ochrana působí logicky až ex post. Osoba, do jejíchž práv bylo takovým neoprávněným jednáním zasaženo, může sice uplatňovat příslušné nároky, fakticky ale není schopná takovému neoprávněnému „užití“ zpřístupněných dat, resp. z nich plynoucího informačního užitku, zabránit. Kontrolu nad daty lze ale efektivně založit využitím adekvátních technických prostředků, jako např. šifrováním nebo kontrolou přístupu k datům. Samy tyto technické prostředky požívají za specifických podmínek veřejnoprávní ochrany. Na základě § 230 odst. 1 zákona č. 40/2009 Sb. je totiž možno trestněprávně postihovat již samotné překonávání takových bezpečnostních opatření, po jejichž překonání získá pachatel nedovolený přístup k počítačovému systému nebo k jeho části. Trestný je již úmyslný hacking sám o sobě, není tedy potřeba, aby měl pachatel úmysl způsobit škodu či újmu, získat prospěch nebo či se tím připravoval na spáchání jiného trestného činu.

Ochrana počítačových programů

Ochrana počítačových programů

Rozvoj informační společnosti by v současné podobě nebyl možný bez prostředků pro automatizované zpracování dat, které nám umožňují pracovat s daty ve výrazně větších objemech a výrazně efektivněji než v minulosti. Nástroje, kterými se v současnosti toto automatizované zpracování realizuje, zahrnuje právní řád primárně pod koncept počítačového programu.

Vnímáme-li počítačový program jako sérii instrukcí, kterou lze spustit na počítači, může tato série instrukcí nabývat různé vnější jevové podoby podle toho, jak jsou jednotlivé instrukce vyjádřeny. Má-li být počítačový program spuštěn na konkrétním zařízení, musí být instrukce vyjádřeny v tzv. strojovém kódu, tedy zakódovány tak, aby jim rozuměl daný stroj (typicky procesor příslušného zařízení). Počítačový program ve strojovém kódu proto představuje sekvenci instrukcí pro procesor daného zařízení, vyjádřenou formou jedniček a nul, a je pro člověka zpravidla nečitelný. Pokud naopak chceme počítačový program vytvářet či upravovat, popisujeme instrukce typicky v tzv. zdrojovém kódu, tedy jejich zápisem v programovacím jazyce. Programovací jazyk vyjadřuje instrukce způsobem srozumitelným pro člověka, ale současně umožňuje jejich pozdější převod do strojového kódu.

Zatímco převod počítačového programu ze zdrojového do strojového kódu je běžnou úlohou, rekonstrukce zdrojového kódu, máme-li k dispozici pouze kód strojový, je často obtížná, ne-li nemožná (zvláště v případě komplexních počítačových programů). Dostupnost zdrojového kódu tak významně ovlivňuje možnost počítačový program dále upravovat či rozvíjet. Jeho nedostupností však není vyloučena faktická možnost z dostupného strojového kódu odvozovat některé informace o tom, jak je počítačový program vystavěn, případně rekonstruovat část zdrojového kódu daného programu.

Pro hlubší pochopení právní úpravy software je nutné též vnímat, jakým způsobem počítačové programy vznikají. Počítačové programy dnes v převážné míře vytváří týmy, nikoli jednotlivci, přičemž tyto týmy často zastřešuje komerční společnost nebo jiná právnická osoba, kterou budeme dále nazývat dodavatelem software. Současně nový software často vzniká rozvojem existujícího softwaru nebo alespoň za využití obecně použitelných stavebních bloků zdrojového kódu. Vytvářený software tak zpravidla není jedním monolitickým celkem, ale skládá se z jednotlivých relativně samostatných modulů, které lze využít samostatně nebo je v budoucnu začlenit do jiného softwaru.

Ochrana počítačových programů autorským právem

Aby počítačový program dosáhl ochrany autorským právem, musí být původní v tom smyslu, že je autorovým vlastním duševním výtvorem. Jestliže počítačový program dosáhne požadovaného standardu originality, je chráněn jako dílo literární, a to bez ohledu na formu svého vyjádření. Ochrana tedy pokrývá vyjádření počítačového programu v podobě strojového kódu, zdrojového kódu i všech jejich mezistupňů. Stejně jsou rovněž chráněny přípravné koncepční materiály vznikající při vývoji počítačového programu, ke kterým budou typicky patřit modely architektury software, funkční specifikace apod. Chráněna tedy není funkcionalita počítačového programu, ale pouze její objektivní vyjádření v podobě příslušného kódu.

Ochrana zaměstnaneckého díla

Jestliže zaměstnanec vytvoří počítačový program ke splnění svých pracovních povinností, a neexistuje-li mezi zaměstnavatelem a zaměstnancem odlišná dohoda, zaměstnavatel vykonává k takovému programu svým jménem a na svůj účet autorova majetková práva.

Pokud mezi zaměstnancem a zaměstnavatelem neexistuje odlišná dohoda, zaměstnavatel má oprávnění počítačový program vytvořený zaměstnancem dále měnit, spojovat jej s počítačovými programy vytvořenými jinými osobami a uvádět jej na trh pod vlastní firmou bez zvláštního souhlasu.

Autorskoprávní ochrana počítačových programů rovněž podléhá zákonným výjimkám a limitacím. Především se na počítačové programy nevztahuje obecná výjimka pro dočasné rozmnoženiny autorského díla pro jeho oprávněné užití. Oprávněný uživatel je oprávněn zkoumat principy, na kterých je počítačový program založen, převádět jej ze strojového do zdrojového kódu, vytvořit si jeho záložní kopii či program, či odstraňovat jeho chyby, přičemž pouze poslední jmenované právo lze smluvně vyloučit.

Patentovatelnost počítačových programů

Autorské právo chrání vyjádření ve zdrojovém či strojovém kódu, nikoliv však samotnou funkcionalitu. Tu je možné chránit patentovým právem. Počítačové programy však nejsou považovány za vynálezy, a tak jsou patenty udělovány na tzv. vynálezy uskutečňované počítačem.

Koncept vynálezů uskutečňovaných počítačem umožnil patentovat vynálezy zahrnující počítač, počítačovou síť nebo jiné naprogramovatelné zařízení, kde jeden nebo více prvků byly uskutečněny počítačovým programem. Podmínkou ochrany je však technický přínos vynálezu pro stav techniky, pokud je posouzen jako celek.

Později byl do tohoto pojmu zahrnut počítačový program sám o sobě nebo nosič obsahující počítačový program. Podmínkou je schopnost programu vyvolat dodatečný technický účinek, mimo interakci mezi programem a hardwarem, na kterém je spouštěn.

Počítačový program jako obchodní tajemství

Obchodním tajemstvím rozumíme „konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení“. Při aktivní ochraně ze strany tvůrce, popř. příslušného uživatele a běžné nedostupnosti v příslušné komunitě může tuto definici naplňovat rovněž počítačový program. Nároků z porušení obchodního tajemství se pak lze domáhat jak vůči tomu, kdo obchodní tajemství neoprávněně zpřístupnil jinému, tak vůči tomu, kdo obchodní tajemství takto zpřístupněné neoprávněně využil, popř. se může jednat rovněž o trestný čin.

Smluvní a předsmluvní ochrana počítačových programů

Historicky nejstarším nástrojem smluvní ochrany počítačových programů je takzvaná dohoda o mlčenlivosti, která typicky zavazuje zákazníka k tomu, aby nezpřístupňoval samotný počítačový program, případně i související materiál a informace o fungování software, třetím osobám. Avšak prokazatelnost neoprávněného šíření dané informace bývá obtížně prokazatelná.

I v případech, kdy dohoda o mlčenlivosti není sjednána, může být počítačový program chráněn v obdobném režimu ze zákona. To je uplatněno např. v rámci procesu kontrakce ještě před uzavřením smlouvy, a to i v případě, že k uzavření smlouvy nedojde.

Smluvním nástrojem ochrany počítačového programu může být také konkurenční doložka.

Počítačové programy a právo proti nekalé soutěži

Nástrojem relativní ochrany počítačového programu může být rovněž právo nekalé soutěže.

V praxi jsou nekalosoutěžní nároky ve vztahu k počítačovým programům nejčastěji vznášeny společně s nároky z porušení autorských práv, tedy pro naplnění soudcovské skutkové podstaty porušení norem soukromého práva. Podmínkou jejich přiznání je kumulativní naplnění znaků nekalosoutěžního jednání, tedy jednání v hospodářském styku, rozpor s dobrými mravy soutěže a

způsobilost přivodit újmu jiným soutěžitelům nebo zákazníkům. V případě skutečného zásahu do autorských práv budou tyto znaky typicky naplněny, přičemž výsledné nároky jsou pak obdobné jako ve vztahu k porušení práv autorských.

Zhotovování a licencování komerčních počítačových programů

Klíčovým nástrojem právní dispozice s komerčními počítačovými programy jsou v praxi nástroje smluvního práva. Smlouvy musí obsahovat obecné náležitosti, jako zejména její určitost a dostatečné vymezení jejího předmětu pomocí dostatečně definovaných pojmů. Způsob úpravy se odlišuje podle toho, jak je financován vznik příslušného počítačového programu a jak chce jeho tvůrce limitovat další šíření.

 # Standardní software

- jeho vznik je financován jeho autorem, resp. zaměstnavatelem autora

- je nabízen na trhu širšímu okruhu možných zákazníků

- nástrojem dispozice s ním je licenční smlouva

V takové smlouvě, je třeba vymezit, jakého programu se týká, jaká je jeho funkcionalita, k jakému účelu má program sloužit a rozsah licence – územní, časový a množstevní. Je také vhodné smlouvu ošetřit k budoucím verzím programu.

Smlouvy obsahují ustanovení o odpovědnosti za vady, které se rozdělují na faktické a právní.

- Faktické vady – spočívají v nevhodné či nedostatečné funkčnosti počítačového programu, nedostatku jeho jiné vlastnosti přímo nesouvisející s funkčností

- Právní vady - spočívají v zatížení software nárokem jiné osoby v rozporu s příslušnou smlouvou, na základě které byl software pořízen

Dle obecného režimu odpovědnosti za vady musí být za úplatu poskytnutý program bez vad - odchýlení od sjednaných vlastností či nevhodnost k výslovně stanovenému účelu. Proto je, alespoň základní vymezení vlastností licencovaného počítačového programu či odkaz na toto vymezení, vhodnou součástí příslušné licenční smlouvy. Na bezúplatně poskytnutý počítačový program se tato odpovědnost ze zákona nevztahuje, nesmí však obsahovat úplatně poskytované služby (např. uživatelská podpora).

Na základě vadného plnění se lze domáhat:

- Je-li vad odstranitelná - opravy počítačového programu, přiměřené slevy z ceny

- Není-li vada odstranitelná a program nelze řádně užívat - přiměřené slevy z ceny, zákazník může odstoupit od smlouvy

Odlišná je situace v případě poskytování software spotřebiteli – osobě jednající mimo souvislost se svým podnikáním. Spotřebitel je vždy slabší stranou a současně vůči němu nelze omezit práva z vadného plnění nebo na náhradu újmy.

 # Software na zakázku

- Jeho vznik je financován zákazníkem – objednavatelem

- Je tvořen dle požadavků zákazníka

- Nástrojem dispozice je smlouva o dílo

Ve smlouvě je opět nutné vymezit specifikace předmětu plnění. Potřebná míra detailu této specifikace je však výrazně vyšší než u standardního software. Specifikace by měla pokrývat nejen funkční stránku počítačového programu, ale také parametry, které nejsou přímo spojeny funkcionalitou, ale mohou ji zásadně ovlivnit, např. hardwarové nároky či bezpečnostní parametry.

V případě, že zákazník potřebuje odbornou pomoc dodavatele programu, je pro smluvní strany výhodnější sjednat si smlouvu pouze s volnou specifikací, na základě které se dodavatel počítačového programu zaváže nejprve vypracovat detailní specifikaci programu. Zákazník ji poté musí akceptovat nebo může od smlouvy odstoupit.

Po zhotovení programu, dle podmínek zakázky následuje fáze akceptace zhotoveného počítačového programu, která je kritická jak z hlediska právního, tak z hlediska praktické funkčnosti počítačového programu. Po praktické stránce nabývá akceptace počítačového programu zpravidla podobu provedení tzv. akceptačních testů, které ověří soulad dodaného programu s klíčovými body specifikace.

Oblast odpovědnosti za vady počítačového programu vytvořeného na zakázku je na rozdíl od dodávky standardního softwaru jasnější. Dle občanského zákoníku má dílo vady, pokud neodpovídá smlouvě. Zároveň pokud zákazník převezme počítačový program bez výhrad, nepřizná mu soud právo na zjevné vady díla, pokud dodavatel namítne, že právo nebylo uplatněno včas. Pokud tedy smlouva nebude obsahovat jeho dostatečnou specifikaci, nebude zákazník zpravidla schopen vytknout dodavateli konkrétní vady.

Vedle obecné odpovědnosti za vady díla může být u dodání softwaru na zakázku sjednána záruka za jakost, která obrací důkazní břemeno - zákazník nemusí prokazovat, že program měl skrytou vadu již v okamžiku akceptace, ale dodavatel musí případně prokázat, že počítačový program si uchoval ujednané vlastnosti a vada vznikla jednáním zákazníka či třetí osoby.

Při dodávce software na zakázku má zákazník licenci k užití počítačového programu k účelu vyplývajícímu ze smlouvy, přičemž třetí osobě jej zákazník může poskytnout, jen pokud to bylo sjednáno.

Obvyklé je v takovém případě sjednání licence v neomezeném územním a množstevním rozsahu na neomezenou dobu, resp. na celou dobu trvání majetkových práv autorských k příslušnému počítačovému programu. Zpravidla je také sjednáváno právo zákazníka licenci postoupit třetím osobám, popř. jim udělit podlicenci. V závislosti na okolnostech konkrétního vztahu pak může být také sjednána licence výhradní, bránící dodavateli, aby sám počítačový program užíval a uděloval licenci dalším osobám odlišným od zákazníka.

V praxi je také významné oprávnění zákazníka software vytvořený na zakázku dále měnit, jež nemusí být automaticky součástí licence. Bez tohoto oprávnění se může dostat zákazník do situace, kdy nebude schopen provádět údržbu a rozvoj dodaného počítačového programu bez součinnosti nebo svolení původního dodavatele

Vedle samotného práva změn je pak v příslušných případech třeba si sjednat také právo na přístup ke zdrojovému kódu, který je pro úpravy po faktické stránce nezbytný. Vhodné je rovněž ošetřit kvalitu předávaného zdrojového kódu (např. zavázáním dodavatele, aby dodržoval konvence vývoje v příslušném programovacím jazyce), dostatečné komentáře uvnitř zdrojového kódu a současně dostatečnou dokumentaci funkčnosti software, jelikož dodavatel disponuje unikátním know-how o fungování softwaru.

Výše popsané způsoby smluvní dispozice se „standardním softwarem“ a „softwarem na zakázku“ představují modely pro typové situace. V praxi však nastávají situace, které nelze jednoznačně přiřadit k některému z výše popsaných modelů, a přesto je třeba pro konkrétní případ nalézt vhodnou smluvní úpravu. Příkladem může být dodávka standardního softwaru, jejíž součástí je však konfigurace příslušného počítačového programu, zapojení do procesů zákazníka a proškolení, popř. drobné či rozsáhlejší individuální úpravy či doplnění příslušného programu. Obvykle takový proces nazýváme implementací a pro jeho smluvní ošetření je třeba použít vhodnou kombinaci prvků úpravy pro dodávku standardního softwaru (rozsah licence) a prvků úpravy pro software na zakázku (způsob akceptace a řešení vad).

Licencování open source softwaru

V případě open source softwaru, který má být zpřístupněn k užití a dalším úpravám širší komunitě je smluvní úprava zcela specifická.

Proprietární software – uživatel má právo jen na užívání softwaru, nebo je jeho užití příslušným způsobem omezeno a nejsou k němu poskytnuty zdrojové kódy.

Free software - uživatel může software používat za jakýmkoliv účelem, studovat, jak pracuje, přizpůsobit ho svým potřebám, šířit dále jeho kopie a vylepšovat ho s tím, že tato vylepšení může následně zveřejňovat a dále šířit. Může být vymáhána povinnost sdílet úpravy provedené v programu s širší komunitou uživatelů

Pro usnadnění šíření open source softwaru vznikla řada typových licenčních podmínek, které se liší svými kritérii. Nejvýznamnějším kritériem je přítomnost tzv. copyleftové doložky, která vytváří povinnost upravený počítačový program šířit pod stejnými licenčními podmínkami, pod jakými je

šířen původní program.

Typy licenčních podmínek:

Silně copyleftové

- požadují, aby původní program a programy jej obsahující byly šířeny pod licenčními podmínkami původního programu

- garantují přístup ke zdrojovému kódu nabyvateli programu

- charakteristické licenční podmínky open source softwaru

Slabě copyleftové

- vyžadují šíření odvozených počítačových programů pod shodnými licenčními podmínkami a zpřístupnění jejich zdrojových kódů

- umožňují vytváření programů, které jsou propojené a šířené společně s původním programem aniž by měnily či používaly jeho zdrojový kód

- umožňují šíření takových propojených programů pod libovolnými podmínkami

- typické licenční podmínky softwarových knihoven

Necopyleftové

- neobsahují žádnou nebo obsahují velmi omezenou copyleftovou doložku

- ukládají pouze minimální omezení ve vztahu k dalšímu šíření programu

- program šířený pod necopyleftovými licenčními podmínkami tak lze použít i v rámci vývoje proprietárního softwaru bez rizika porušení licenčních podmínek původního programu

Služby související s počítačovými programy

Služby v oblasti ICT mohou být spojeny s dodávkou počítačového programu (např. jeho podpora, údržba apod.) nebo mohou být dodávány samostatně (cloud computing, telekomunikační služby). Mohou být smluvně regulovány tzv. inominátní smlouvou, která bývá často uzavírána jen jako součást jiné smlouvy, kterou doplňuje.

Jejími typickými prvky bývá:

- Definice služby (např. podpora software, odstraňování vad)

- Parametry služby (např. dostupnost, reakční doba, doba do odstranění vady)

- Způsob vyhodnocení

- Kreditace – forma sankce.

Elektronické dokumenty

Elektronické dokumenty

Předmětem této kapitoly je problematika elektronické formy dokumentu, jeho zabezpečovacích prvků a další souvisejících oblastí, jako je např. elektronické doručování či uchování elektronických dokumentů. S rozvojem informační společnosti stoupá i rozsah používání elektronických dokumentů, které jsou základními nositeli fixovaného stavu určité informace v daném časovém okamžiku.

Jako příklad lze uvést elektronické bankovnictví (založené na elektronických transakcích), které postupně nahrazuje použití tradičních bankovek. Ale i zde má dokument své místo v kontrolní roli výpisu z účtu, kdy zachycuje staticky proběhlou sekvenci transakcí a dokládá jejich pořadí, výši a další atributy. Neznamená to, že by se transakční přístup neměl prosazovat v operacích a úkonech, kde má své místo. V rámci celkového rozvoje elektronizace veřejné správy, tzv. e-governmentu, bývá přisuzován třetímu ze čtyř stupňů jeho rozvoje, kde má tedy velmi významné místo. Nikdy však nemůže nahradit zcela funkci dokumentů.

Elektronický podpis

Pokud má být elektronický dokument obecně použitelný, musí být elektronizovány také další instituty, které jsou v souvislosti s elektronickými dokumenty a elektronickými listinami používány. Tím jednoznačně nejdůležitějším je podpis, jehož praktické využití je skutečně široké. Jak velmi pregnantně uvádí R. Polčák, „právní účinky vlastnoručního podpisu mají čistě obyčejový charakter nejen v českém právu ale prakticky po celém světě – vlastnoruční podpis tak není definován zákonným právem a ani není nikde v psaném právu upravena domněnka projevu vůle. Formální adekvátnost podpisu tedy hodnotíme ad hoc zkušenostní intuicí a domněnka vyjádření vůle je otázkou velmi silné a téměř neoddiskutovatelné obyčejové normy“.

Za prvé je třeba identifikovat osobu, která podpis vytváří. U klasického podpisu nejde určitě o to, aby bylo jasně čitelné jméno podepisující osoby, ale o to, aby zde bylo jedinečné spojení mezi vytvořeným podpisem a podepisující osobou. U vlastnoručního podpisu je tato vlastnost zajištěna fyzickými schopnostmi podepisující osoby. V elektronické podobě může být aplikováno více způsobů, jak této vlastnosti docílit. Typicky se využívá znalost určitého tajného kódu (hesla) v obdobné funkci jako je např. PIN u bankovní platební karty.

Druhou podstatou je vytvoření podpisu jako vyjádření vůle. Znamená to, že podpis určitého elektronického dokumentu nemůže být vytvářen automatizovaně, ale pouze na přímý a jasný pokyn podepisující osoby.

Třetím bodem je to, že se nelze zprostit odpovědnosti za podepsaný text, což může být aplikováno pouze za podmínky, že se podepisující osoba mohla před vlastním podepsáním s textem seznámit. Toho se v elektronické podobě mnohdy dosahuje poměrně komplikovaně a neostře, protože elektronický dokument je vždy zprostředkovaně zobrazen na zobrazovacím zařízení pomocí nějakého nástroje, počítačového programu.

Vývoj využití elektronických dokumentů

Využití informačních a komunikačních technologií je v soukromém sektoru vždy napřed oproti veřejné správě. Je to dáno mnoha faktory obecně omezujícími či vymezujícími rozvoj elektronizace veřejné správy. Není tedy divu, že stejně tak to dopadá s právními předpisy v oblasti konkrétního využití elektronických dokumentů, jejichž přípustnost se v historii objevila mnohem později než jejich praktické použití v běžné neregulované praxi. První elektronické dokumenty a první pokusy elektronické komunikace prostřednictvím e-mailů, které lze v historickém kontextu považovat za první elektronické dokumenty, se datují do 60. let 20. století. Rozvoj komunikace prostřednictvím elektronické pošty nastal mnohem později, až v 90. letech.

Právní úprava elektronických dokumentů

Aktuální definice elektronického dokumentu je uvedena v nařízení č. 910/2014, i když podle anglické verze tohoto nařízení jde spíše o definici elektronického záznamu. Podle této definice se elektronickým dokumentem rozumí „jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka“. Citované nařízení je právním předpisem, který je závazný v celém rozsahu a přímo použitelný ve všech členských státech Evropské unie. Z hlediska elektronických dokumentů a jejich praktických použití jde skutečně o stěžejní předpis, i když po zdlouhavých diskusích, které provázely jeho přijetí, v něm zbylo k elektronickým dokumentům skutečně málo. Pouze uvedená obecná definice a dále jeden článek obsahující jen jeden odstavec. Avšak tento odstavec obsahuje důležité ustanovení zakazující, aby pouhý fakt elektronické podoby dokumentu byl použit jako zdůvodnění odmítnutí jeho přijetí jako důkazu v soudním anebo správním řízení.

Autenticita elektronických dokumentů

Z hlediska praktického použití elektronických dokumentů v případech, kdy jsou nositeli informace, která má důkazní hodnotu nebo vychází z právních závazků anebo obchodních vztahů dané organizace, je třeba se zabývat jejich autenticitou. Ta se typicky zajišťuje pomocí různých elektronických zabezpečovacích prvků, jako je elektronický podpis, elektronická pečeť anebo elektronické časové razítko. Jde o obdoby způsobů, jimiž je zajišťována autenticita listinných dokumentů, kde funguji instituty jako vlastnoruční podpis, razítko nebo pečeť. Autenticita elektronických dokumentů úzce souvisí s jejich důkazní spolehlivostí.

Aby mohl elektronický dokument obsahovat zaznamenání projevu vůle, musí existovat možnost, jak jej elektronicky podepsat. Zopakujme, že právní účinky podpisu mají sice čistě obyčejový charakter, ale jde o velmi silnou a téměř neoddiskutovatelnou obyčejovou normu. Vlastnoruční podpis je výsledkem uplatnění návyku získaného v podobě individuálního a relativně stálého písemného projevu, který spočívá ve vypracování složitého systému podmíněných reflexů závislých na stupni procvičování. Na rozdíl od vlastnoručního podpisu, pro který nejsou stanovena žádná explicitní pravidla, je jeho elektronická varianta přesně popsána, a to nařízením č. 910/2014. V definici pravidel pro elektronický podpis je podstatné dodržování maximální technické neutrality.

Nařízení č. 910/2014 rozlišuje čtyři úrovně elektronického podpisu, které se liší mírou své důvěryhodnosti. Nejnižší úrovní je elektronický podpis bez přívlastku.

Zaručený elektronický podpis je druhou úrovní elektronického podpisu, u kterého je již vyžadováno technické zabezpečení důvěryhodnosti, avšak stále ještě není požadována důvěryhodnost údajů uvedených v připojeném certifikátu. Článek 26 nařízení č. 910/2014 konkrétně stanoví pro zaručený elektronický podpis čtyři konkrétní pravidla, která tento podpis musí splňovat. Předně je jednoznačně spojen s podepisující osobou. Druhým požadavkem je, že umožňuje identifikaci podepisující osoby, přičemž touto identifikací se dle čl. 3 odst. 1 cit. nařízení rozumí používání osobních identifikačních údajů v elektronické podobě, které jedinečně identifikují určitou fyzickou či právnickou osobu nebo fyzickou osobu zastupující právnickou osobu. Je třeba zdůraznit onu jedinečnost, nikoliv však jednoznačnost. Ta již vyžadována není, přičemž důsledky tohoto přístupu budou zmíněny dále.

Doručování elektronického dokumentu

Elektronické dokumenty jsou nejen uchovávány na záznamových mediích, ale také přenášeny prostřednictvím elektronické komunikace. Elektronická komunikace ale nemusí vždy znamenat přenos elektronických dokumentů. Každá data v elektronické podobě ještě neznamenají elektronický dokument. Ten musí splňovat celou řadu různých podmínek, přičemž tou nejdůležitější je neměnnost. Na druhou stranu způsobů, jimiž může být elektronický dokument přenášen, je více. Můžeme je rozdělovat podle různých hledisek. Z právního pohledu je nejdůležitější členění dle stupně důvěryhodnosti a možností prokázat, že daná komunikace proběhla, mezi jakými subjekty proběhla a kdy proběhla. Mezi nejznámější a nejpoužívanější způsoby patří: Elektronická pošta, datové schránky, transakční portály.

Konverze forem a formátů elektronického dokumentu

Dokument jako ucelená neměnná jednotka by dle své definice v zákoně č. 499/2004 Sb. neměla být závislá na konkrétní formě. Stejně tak jsme to ukázali pro písemnou formu právního jednání. Listinná i elektronická forma má být rovnocenná, pokud jedna i druhá zachovává principy, které tvoří skutečný základ jednotlivých právních institutů. V mnohých případech může

elektronická forma dokonce poskytovat vyšší záruky než forma listinná. Vzpomeňme například jednu ze základních vlastností zaručeného elektronického podpisu – je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat. Takové zabezpečení vlastnoruční podpis pro listinné dokumenty v žádném případě neposkytuje. Existují dvě možnosti konverze, a to autorizovaná a převod podle zákona o archivnictví.

Uchovávání elektronických dokumentů

Přístup k uchování, ukládání a ochraně elektronických dokumentů je odlišný od listinných dokumentů. Primární rozdíl je v tom, že když je chráněn listinný dokument, je chráněn nosič, když je chráněn digitální dokument, jsou chráněna data. Uchování elektronických dokumentů je spojeno též se zajištěním věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a zajištěním čitelnosti. Uchování elektronických dokumentů je tak spojeno zejména s následujícími druhy rizik: rizika spojená s datovými formáty, rizika spojená s technickým nosičem, rizika spojená s omezenou platností elektronických zabezpečovacích prvků.

Pro nejtypičtější statické textové dokumenty a statické kombinované textové a obrazové dokumenty je určen datový formát Portable Document Format/Archive (PDF/A). Norma PDF/A byla vytvořena právě pro účely dlouhodobé archivace elektronických dokumentů. Jinými slovy jde o veřejnou normu, která specifikuje takové datové objekty v rámci formátu PDF a taková pravidla jejich popisu, které odpovídají potřebám dlouhodobého archivování a zachování nezávislosti na hardwaru, na operačním systému a na konkrétní aplikace.

Doménová jména

Doménová jména

Cílem této kapitoly je popsat problematiku týkající se doménových jmen především v rámci soukromoprávních vztazích. Každý den se uživatel internetu potýká s jejich existencí, při každé stránce na prohlížeče přistupujeme na nějaké doménové jméno, ale problematika, která se za nimi odehrává, a to nejen z technické stránky věci nemusí být tak jednoduchá, jako se na první pohled zdá.

Abychom se mohli zaobírat právní problematikou doménových jmen, tak je nutné první pochopit, co jsou vlastně doménová jména zač z technického hlediska a jak fungují. Počítače a jiná technická zařízení komunikující v počítačových sítích jsou označeny unikátními numerickými (např. 77.75.74.80) nebo alfanumerickými (např. 2a02:0598:3333::3) adresami IP protokolu (Internet Protocol), jako datového protokolu používaného pro přenos dat. K usnadnění obsluhy těchto zařízení se pak IP adresy prostřednictvím doménového DNS systému (Domain Name System) nahrazují tzv. doménami, které představují uzavřený virtuální prostor v počítačové síti. Domény tak v prvé řadě slouží k tomu, aby popis uvedeného prostoru v počítačové síti byl pojmenován způsobem, který je zapamatovatelný pro člověka.

> Doménový systém je hierarchický. Doménové jméno se skládá z TLD (top level domain), která identifikuje v záznamech, které registry je dané doménové jméno vedené, a SLD (second level domain), které v těchto záznamech identifikuje jeho unikátní záznam. www, které je součástí doménového jména se nazývá third-level domain (Subdomain).

Domény jako předmět právních vztahů

Domény jsou soukromoprávním předmětem právních vztahů s povahou nehmotných věcí. Práva k nim jsou relativními majetkovými právy, jež souvisí s využíváním služeb elektronických komunikací, nikoliv právy absolutními (např. věcnými právy a právem dědickým). Disponibilním předmětem právních vztahů k doménám je tak pohledávka ze smlouvy o registraci domény.

Domény v českém právním řádu

Domény, jejich správa a právní proces jejich registrace není nijak v českém právním řádu upravován. Ovšem to neznamená, že pro TLD .cz nevychází žádné nařízení. TLD .cz proto analogicky vychází z nařízení správních orgánů EU platných pro TLD doménu .eu. Internetové

adresy včetně domén dle § 28 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích, nepodléhají veřejné správě adres Českým telekomunikačním úřadem, takže doménová jména nepodléhají státní regulaci. Správcem domény CZ je na základě smluvních závazků s ICANN (Internet Corporation for Assigned Names and Numbers) sdružení CZ.NIC z.s.p.o.

Vznik SLD z pohledu práva

Doména vzniká až zápisem unikátní platné sekvence písmen do seznamu domén příslušného správce, nikoliv dříve – pouze samotný zápis představuje konstitutivní akt. Z právního hlediska doména vzniká uzavřením registrační smlouvy, ve které se správce zavazuje doménu zaregistrovat a budoucí držitel domény se zavazuje zaplatit registrační poplatek.Uzavřením smlouvy a zápisem do registru vzniká osobě, která si doménu zaregistrovala (běžně držitel) právo doménu držet a užívat ji. Smlouva je smlouvou nepojmenovanou a běžně se uzavírá distančním způsobem. Smlouva je zpravidla na dobu určitou, ale běžně lze prodloužit zaplacením registračního poplatku na další období.

Zánik SLD z pohledu práva

Doména může trvat jen po dobu, po kterou trvá její registrace v seznamu domén

Trvání registrace v seznamu domén je podmíněno trváním smlouvy o registraci domény a ovlivňují je technické podmínky, např.:

- Funkčnost a platnost DNS záznamů

- Placení poplatků registrace

- Případně bydliště na území státu, který doménu spravuje

Držitel může doménu kdykoliv zrušit, na což se pohlíží jako jednostranné ukončení smlouvy o registraci domény, čímž dojde k zániku domény. Zánik domény v tomto smyslu však neznemožňuje komukoliv, včetně původního držitele, doménu znovu zaregistrovat

Převod a zástava SLD

Doména může být předmětem převodu. Právně je převod domény nakládáním s pohledávkou věřitele na majetkové plnění poskytované správcem domény nejvyšší úrovně jako dlužníkem. Při převodu domény má správce povinnost udržovat registraci za stávajících podmínek, stejně jako u "klasického" nakládání s pohledávkou. Doména může být stejně jako běžné pohledávky v souladu s občanským zákoníkem předmětem zástavy. Záznam o zástavě se neprovádí v DNS systému správce, který pro tento úkon není uzpůsoben, je však možnost zástavní právo zapsat do rejstříku zástav vedený Notářskou komorou ČR.

Exekuce domény

Doména druhé úrovně, resp. pohledávka ze smlouvy o registraci domény, může být i předmětem výkonu rozhodnutí či exekuce. Převod domény z důvodu exekuce neznamená převod práv k případným obchodních názvů nebo ochranným známkám obsažených v doménovém jméně, což by mohlo vést k soudnímu rozhodnutí, kde nabyvateli takové domény bude kvůli těmto ochranným známkám zakázáno doménu používat. Takový soudní závěr je však extrémní, jedná se o velmi doslovný výklad právních předpisů, který je potencionálně v rozporus § 2 odst. 3 občanského zákoníku

Kolize s právy třetích osob

Doména zaregistrována tomu, kdo o ni jako první požádá, ale při registraci se neprovádí kontrola, zdali doména nekoliduje s právy třetích osob (ani to není možné). Může existovat pouze 1 doména se stejným zněním, ale může existovat více osob, nebo ochranných známek stejného znění. Ochrana práv třetích osob je řešena až poté, kdy byla doména zaregistrována. Může dojít k paralelní kolizi mezi jednou doménou a více právy třetích osob. Registrace domény kolidujících s jinými doménami v důsledku překlepů či neznalostí jazyka, se označuje jako typosquatting. (wwwbnw.cz | bmw.cz; gogle.com | google.com)

Odpovědnost za porušení práv třetích osob

Odpovědnost za porušení práv třetích osob, ke kterému dojde v důsledku registrace domény, nese primárně její držitel. Odpovědnost za porušení práv, k němuž dojde v důsledku užívání domény, pak může nést držitel domény nebo její uživatel provozující na předmětné doméně internetové stránky, pokud není totožný s držitelem. Nelze získat absolutní právo k doméně, a to ani vítězstvím soudního sporu.

 # Doména může být v kolizi s:

1. Jménem fyzické osoby

- Ke kolizím dochází především u veřejně činných osob (umělců, politiků…)

- Např. spory: (dagmarahavlova.cz, kjkrowling.com)

2. Názvem právnické osoby

- Název právnické osoby je v ČR unikátní

- Neoprávněné používání názvu právnické osoby je protiprávní

- V případě že práva k doméně vzniknou před vznikem ochranné známky či před zápisem obchodní firmy do obchodního rejstříku, držitel domény má právo ji dále využívat.

- V rámci ochrany názvu právnických osob je poskytována i ochrana názvům veřejnoprávních korporací, např. obcí (ostrava.cz)

3. Ochranou známkou

- Může existovat více ochranných známek stejného znění pro různé druhy výrobků nebo služeb

- Ochranná známka se zapisuje a je chráněna vždy jen pro určité geografické území

- Posuzuje se, zdali majitel stránky těží z ochranné známky (spor atomic.cz)

- Posuzuje se, jestli přidáním dalšího textu k ochranné známce dochází ke kolizi (shopbmw.cz je v kolizi s ochranou známku BMW), (balonky-praha.cz není v kolizi s balonky.cz)

4. S právy na ochranu před nekalosoutěžním jednáním

- Nekalou soutěží je jednání v rozporu s dobrými mravy soutěže, za účelem přivodit újmu jiným soutěžitelům nebo zákazníkům.

- Za jednání v rozporu s dobrými mravy se považuje chování, které by mohlo zkreslit společenskou funkci soutěže.

- Za nekalosoutěžní tak může být považováno

-- Registrování domény kolidující s ochrannou známkou či názvem

-- Užití takovéto domény k prezentaci konkurenčního výrobku

Řešení sporů týkajících se domén

Jako spory týkající se domén (tzv. doménové spory) se označují spory o vlastnictví domén, nebo spory týkající se porušování práv existencí či užíváním domén.

 # Řešení sporů obecnými soudy

Protože spory o domény vyplývají z poměrů soukromého práva, je ve všech těchto sporech dána pravomoc obecných soudů.

U sporů o domény, které jsou vyvolány kolizí domén a práv na označení či práv z nekalé soutěže, je dána věcná příslušnost krajských soudů.

U ostatních sporů o domény, tedy např. u sporů, které jsou vyvolány kolizí domén a jména či příjmení fyzické osoby, nebo sporů o vlastnictví domény, je dle § 9 odst. 1 zákona č. 99/1963 Sb.

dána věcná příslušnost okresních soudů.

Proti zahraniční osobě tak lze podat žalobu ve sporu týkajícím se domény u českého obecného soudu v případě, že se bude jednat o doménové jméno registrované v doméně nejvyšší úrovně CZ, neboť pak má tato zahraniční osoba v České republice majetek.

Ve věcech konfliktu domén s některým z popsaných práv tak lze takovou zahraniční osobu žalovat u soudu v České republice, a to nejčastěji u soudu dle sídla žalobce, neboť ke škodné události bude nejčastěji docházet právě u žalobce.

Ve věcech konfliktu domén s některým z popsaných práv tak lze takovou zahraniční osobu žalovat u soudu v České republice, a to nejčastěji u soudu dle sídla žalobce, neboť ke škodné události bude nejčastěji docházet právě u žalobce.

 # Alternativní řešení sporů

Řešení sporů týkajících se domén v soudním řízení před obecnými soudy naráží na problémy s jurisdikcí obecných soudů. Není sporu o tom, že tuzemský obecný soud bude mít pravomoc rozhodovat spor o doménu registrovanou v doméně nejvyšší úrovně CZ mezi dvěma tuzemskými subjekty. Tuto pravomoc však nebude mít v případě sporu o některou z generických domén nejvyšší úrovně mezi tuzemským navrhovatelem a cizozemským odpůrcem.

Z těchto důvodů je ve sporech týkajících se domén obvyklé řešení těchto sporů prostřednictvím alternativního (mimosoudního) řešení sporů, označovaného též jako ADR (Alternative Dispute Resolution). Alternativní řešení sporů je tak dostupné pro řešení sporů týkajících se domén registrovaných v generických doménách nejvyšší úrovně, v doméně nejvyšší úrovně EU, v řadě národních domén nejvyšší úrovně a konečně i v doméně nejvyšší úrovně CZ.

Dokumenty upravující alternativní řešení sporů tvoří součást smluvní dokumentace akceptované při registraci domény (u generických domén nejvyšší úrovně, případně domény CZ a některých dalších národních domén nejvyšší úrovně), případně se jedná o právní předpis, jak je tomu v případě domény nejvyšší úrovně EU.

 # Alternativní řešení sporů o generické domény

Alternativní řešení sporů o domény registrované v generických doménách nejvyšší úrovně probíhá na základě tzv. UDRP (Uniform Domain Name Dispute Resolution Policy) dokumentu vydaného organizací ICANN.

Zlá víra při registraci nebo užívání domény může být dle UDRP prokázána tehdy, jestliže:

- budou prokázány okolnosti nasvědčující tomu, že držitel domény spornou doménu zaregistroval nebo získal především za účelem prodeje, pronájmu nebo jiného převodu na navrhovatele

- doména byla zaregistrována s cílem zabránit tomu, aby vlastník ochranné známky mohl promítnout tuto známku do domény

- doména byla zaregistrována především za účelem narušení obchodních aktivit osoby, která je v postavení soutěžitele vůči držiteli sporné domény

- držitel domény se jejím užíváním úmyslně pokouší za účelem obchodního prospěchu přilákat uživatele Internetu na svou vlastní webovou stránku

Alternativní řešení sporů o domény EU

Alternativní řešení sporů o domény registrované v doméně nejvyšší úrovně EU je realizováno na základě Nařízení Komise (ES).

Ochrana spotřebitele na internetu

Ochrana spotřebitele na internetu

Odvětví elektronického obchodu patří k nejrychleji rostoucím na světě. Zejména spotřebitelům nabízí v online prostředí obrovský výběr produktů a služeb, a podtrhuje tak význam potřeby specifického přístupu v dané oblasti. Neustále rostoucí počet uživatelů internetu má pak vliv na růst podnikání v tomto odvětví. V důsledku toho je elektronický obchod nejběžnější formou vnitrostátního i přeshraničního nakupování v EU. V první části této kapitoly se tak zaměříme na problematiku ochrany spotřebitele při uzavírání distančních smluv. Jedním z hlavních cílů ochrany spotřebitele je poskytnout mu rovněž v online prostředí dostatečné záruky pro kvalitní obchodování, a podpořit tak jeho důvěru. Při uzavírání smluv v oblasti elektronického obchodování se ochrana spotřebitele projevuje především v tom, že je třeba jej dostatečně informovat (nejenom charakteristikách zboží, ale rovněž o prodejci, konkrétních specifikách smluvního vztahu, možnosti ukončit smlouvu atd.), dbát o zvýšenou ochranu jeho práv a rovněž mu poskytnout možnost jednoduše řešit vzniklé spory. Hlavním důvodem zvýšené ochrany spotřebitele (nejen v online prostředí) je nerovné postavení zúčastněných stran – podnikatelé jsou na rozdíl od spotřebitelů dobře informováni a vystupují obecně v silnější pozici.

V případě elektronického obchodování v online prostředí se asymetrické postavení může projevit ještě více vzhledem k jednoduchosti výměny informací a provedení dané transakce. Může tak dojít ke zneužití postavení více informovaných a zkušených subjektů na úkor subjektů méně informovaných. Základní mechanismy, kterými je možné zabránit zneužití silnějšího postavení v online prostředí, jsou, kromě obecných mechanismů ochrany spotřebitele, zejména zvýšená předsmluvní informační povinnost spotřebitele, zvýšená ochrana v případě vadného zboží a možnost odstoupit od smlouvy bez udání důvodu. Rovněž je specificky upravena problematika sjednávání smluv formulářovým způsobem.

Elektronický obchod (zejména za situace, kdy je jednou ze stran spotřebitel) nicméně poskytuje velkou výzvu tradičním metodám řešení sporů, neboť se jej účastní strany, které se nachází na různých místech (a často i v různých státech). Spotřebitelům je proto vhodné poskytnout adekvátní nástroje pro řešení jejich sporů v online prostředí. Použití tradičních soudních mechanismů pro spory vzniklé v tomto prostředí je kvůli nízké hodnotě transakcí a fyzické vzdálenosti mezi stranami často nepohodlné, nepraktické, časově náročné a drahé (a případně i zcela nedostupné). Tím, že právní úprava této problematice nevěnovala dostatek pozornosti, informační společnost začala hledat a posléze využívat alternativní způsoby, jak dané spory co nejefektivněji a nejvhodněji řešit.

Aktuální právní úprava ochrany spotřebitele při uzavírání distančních smluv

Přestože se v rámci této kapitoly budeme primárně věnovat právní úpravě smluv uzavíraných distančním způsobem, je nutné zdůraznit, že na tuto problematiku rovněž dopadají ustanovení obecně se vztahující k uzavírání spotřebitelských smluv (bez specifikace způsobu jejich uzavírání). Ta jsou systematicky řazena před ustanovení upravující distanční způsob uzavírání spotřebitelských smluv; relevantní ustanovení tedy rozebíráme dále.

Spotřebitel je v rámci soukromého práva definován v § 419 občanského zákoníku jako člověk, který uzavírá smlouvu s podnikatelem nebo s ním jinak jedná mimo rámec své podnikatelské činnosti nebo mimo rámec samostatného výkonu svého povolání. České soukromé právo pak vychází z předpokladu rozumného a informovaného spotřebitele, který je schopen posoudit důsledky svých činů. Základním předpokladem pak je, že spotřebitel je osoba, která má dostatek informací, aby mohla zodpovědně rozhodnout o tom, zda smlouvu uzavře, nebo ne.

Smlouvy uzavírané spotřebitelem

Obecně je právní úprava ochrany spotřebitele související s uzavíráním spotřebitelských smluv upravena § 1810 a násl. občanského zákoníku. Základní premisou, ze které občanský zákoník v této oblasti vychází, je fakt, že k ujednáním, která se odchylují od zákona v otázkách ochrany spotřebitele, se nepřihlíží. Zakázána jsou tak ujednání, která zakládají významnou nerovnováhu v neprospěch spotřebitele. V případě nutnosti výkladu smlouvy je pak třeba vždy přistoupit k interpretaci pro spotřebitele příznivější. Ustanovení týkající se ochrany spotřebitele (ať už obecná, nebo související s uzavíráním distančních smluv) jsou tak dle Melzera jednostranně kogentní. Odchýlení se od normy v neprospěch slabší strany, jejímž účelem je ochrana této slabší strany, vede zásadně k relativní neplatnosti. Zakázáno je rovněž, aby podnikatel požadoval další platby po spotřebiteli bez jeho souhlasu. Podnikatel je ale vždy umožněno zvolit přístup, který je ve prospěch spotřebitele nad rámec zákonných požadavků. Jedná se tedy o obecné zajištění transparentních podmínek, pokud jde o rozsah sjednaného plnění a jeho cenu. V rámci posílení postavení spotřebitele je mu umožněno za určitých podmínek odstoupit od smlouvy sjednané s podnikatelem bez udání důvodu a bez dalšího postihu. Takovým postihem mohou být například i zvláštní náklady, které spotřebitel uplatněním práva na odstoupení od smlouvy vyvolá; mezi takové ale nelze řadit náklady spojené se samotným prováděním smlouvy. Jedná se typicky o náklady spojené s vrácením zboží nebo náklady na komunikaci s podnikatelem. Podnikatel však nemůže požadovat v souvislosti s odstoupením od smlouvy úhradu nákladů, které mu vzniknou v souvislosti s ním. Stejně tak nemůže stanovit podmínky pro odstoupení od smlouvy, které vyvolají zvláštní náklady.

V přístupu ke spotřebiteli se však nelze omezit jen na stanovení zákazů silnější straně a stále intenzivněji chránit stranu slabší. Je nutno také spotřebitele náležitým způsobem informovat a vzdělávat a tím zvyšovat standard jeho ochrany. Zákonodárce se toho snaží dosáhnout zejména rozsáhlou informační povinností podnikatele v předsmluvní fázi. Ustanovení § 1811 občanského zákoníku vyjmenovává informace, které musí být spotřebiteli sděleny. Účelem není, aby podnikatel sepsal výčet informací, ale aby skutečně spotřebitele srozumitelně informoval. Je tak vyloučena povinnost spotřebitele informovat v případě smluv týkajících se záležitostí každodenního života, ale rovněž smluv o dodání digitálního obsahu na hmotném nosiči. Sdělované informace musí být jasné a průměrnému spotřebiteli, sdělení musí mít čitelný obsah a musí být jasně formulováno. Taxativně jsou informace vymezeny jako informace praktické (týkající se osoby podnikatele či předmětu smlouvy) a informace právní (možnost odstoupení od smlouvy, práva plynoucí z vad zboží).

Rozsah informační povinnosti však má negativní dopady na spotřebitele, který je postupně zahlcen více údaji, než jaké je schopen zpracovat (vzhledem k časové náročnosti a případně jeho nechuti). Poskytnuté informace je tak nutno vždy poměřovat s uvedenými principy (jasnost, srozumitelnost, přehlednost). České právo výslovně nezakazuje podnikateli poskytovat dodatečné (dobrovolné) informace, pokud splňuje tyto hlavní podmínky. Dodatečné informace nicméně nesmí mást spotřebitele a odvádět pozornost od povinně zveřejňovaných informací.

Smlouvy uzavírané spotřebitelem distančním způsobem

Na distanční smlouvy jsou obecně kladeny specifické požadavky, jelikož jejich uzavírání přináší spotřebiteli některé nevýhody. Účelem právní úpravy je tak kompenzovat fakt, že spotřebitel nemá možnost si fyzicky prohlédnout zboží, blíže se s ním seznámit a informovat se více o jeho vlastnostech. Právě zvláštní úprava ochrany spotřebitele v případě uzavírání distančních smluv se snaží tento nedostatek zmírnit.

Právní úprava obsažena v občanskému zákoníku neobsahuje legální definici pojmu smlouva uzavíraná distančním způsobem; definice je nicméně obsažena v čl. 2 odst. 7 směrnice o právech spotřebitelů. Z ustanovení § 1820 občanského zákoníku lze nicméně vyvodit, že se jedná o smlouvy, které je možno uzavřít bez současné fyzické přítomnosti stran a při kontraktaci byl použit prostředek pro komunikaci na dálku. Distanční smlouva tak musí splňovat tři základní podmínky: (i) jedná se o smluvní ujednání, (ii) smlouva je uzavřena bez fyzické přítomnosti smluvních stran a (iii) jsou využity prostředky komunikace na dálku. Nezáleží na tom, jakým způsobem došlo k plnění samotného závazku (tedy například, jak bylo zboží převzato), ale jakým způsobem byla sjednána smlouva.

Ustanovení týkající se uzavírání smluv distančním způsobem obsažená v § 1820 až 1840 občanského zákoníku se nicméně nezaměřují pouze na online prodej (tedy uzavírání smlouvy elektronickými prostředky). Obecně se vztahují i na uzavírání smluv po telefonu či smluv uzavíraných mimo obchodní prostory podnikatele. Dále v textu se však zaměřujeme jen na

uzavírání spotřebitelských smluv elektronickými prostředky, jelikož ty jsou v současné době v rámci dané oblasti zdaleka nečastější. V případě definice elektronických prostředků je pak možné inspirovat se § 2 písm. c) zákona o některých službách informační společnosti, který je definuje zejména jako síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronickou poštu.

Informační povinnost v souvislosti s uzavíráním smluv distančním způsobem

Na distanční uzavírání smluv dopadá zvláštní režim informační povinnosti vůči spotřebiteli. Pro podnikatele je tak stanoven dodatečný soubor informací týkajících se vzdáleného prodeje. V případě sjednání smlouvy prostřednictvím prostředků komunikace na dálku tak podnikatel spotřebiteli sdělí nejen obecné informace (dle § 1811 odst. 2 občanského zákoníku), ale rovněž údaje dodatečně vymezené v § 1820 odst. 1 občanského zákoníku a v případě využití elektronických prostředků pak rovněž informace vymezené v § 1826 občanského zákoníku. Tato informační povinnost musí být splněna před uzavřením smlouvy nebo před tím, než spotřebitel učiní závaznou nabídku; hlavním účelem je tak poskytnout spotřebiteli dostatečné informace o celém smluvním procesu.

Informace poskytnuté spotřebiteli lze rozdělit do čtyř hlavních kategorií: (I) informace týkající se platby, (II) informace o závaznosti smlouvy (např. minimální doba, po kterou je spotřebitel vázán smlouvou), (III) informace o odstoupení od smlouvy (možnosti odstoupení, podmínky odstoupení, způsob, jakým by měl spotřebitel postupovat) a (IV) informace o mimosoudním řešení sporů včetně uvedení orgánu, na který je možno se obrátit. Občanský zákoník však nestanoví formu takové informace (vzhledem k šíři a rozdílnosti způsobů distančního sjednávání smluv se nemusí jednat o písemnou formu). Podnikatel ale musí být schopen prokázat, že takovou informační povinnost splnil a informace poskytuje trvale. Informace tak mohou být spotřebiteli například zaslány elektronickou poštou.

Nad rámec výše uvedeného je pro případ uzavírání smluv elektronickými prostředky v § 1826 stanoveno, že je třeba rovněž uvést údaje o technickém zpracování smlouvy, o jejím uložení, různých jazykových verzích a případných kodexech chování, kterými může být podnikatel vázán. Spotřebitel by také měl být seznámen zejména s jednotlivými technickými kroky, které vedou k uzavření smlouvy. Měl by mu být tedy objasněn proces uzavírání smlouvy elektronickými prostředky a rovněž sděleno, kdy a jak dochází k uzavření smlouvy a jakým jednáním je vázán. V rámci těchto informací by měl být spotřebitel rovněž informován o tom, kdy se zavazuje objednávku zaplatit a jakým způsobem může opravit a zkontrolovat uvedené údaje. Tato úprava je tak zaměřena typicky na smlouvy, které jsou uzavírány mezi spotřebitelem a elektronickým obchodem.

Porušení informační povinnosti může mít různé důsledky. Podnikatel má povinnost pokrýt vzniklou škodu, pokud je dohoda se spotřebitelem nepřiměřená (a navíc taková dohoda nemá na spotřebitele žádný závazný účinek, pokud se jí spotřebitel explicitně nedovolává). Pokud podnikatel

neposkytuje spotřebiteli informace o nákladech na dodání nebo vrácení, o daních či dodatečných poplatcích, není spotřebitel povinen tyto náklady hradit. Spotřebitel je pak povinen zaplatit pouze poměrnou část nákladů, pokud byly závazky ze smlouvy již částečně splněny. spotřebitele o jeho možnosti odstoupit od smlouvy je sankcionováno prodloužením lhůty k odstoupení od smlouvy o jeden rok. takovém případě také spotřebitel neodpovídá za znehodnocení zboží nebo zhoršení jeho kvality od převzetí po navrácení podnikateli., který spotřebitele chybně informuje, hrozí i veřejnoprávní sankce dle zákona o ochraně spotřebitele. Je zakázáno používat nekalé praktiky při prodeji, porušit zákaz či porušit informační povinnost.

Obchodní podmínky

Vzhledem k tomu, že v případě distančního prodeje zboží či nabízení služeb (nejtypičtěji pak formou elektronickou), je obvyklé, že podnikatel oslovuje velký počet potenciálních zákazníků (což vede k uzavírání velkého počtu obdobných smluv). Zákonem je mu k tomu poskytnut adekvátní nástroj pro unifikaci smluvního ujednání ve formě obchodních podmínek. Využití obchodních podmínek nicméně může fakticky omezit možnost slabší strany změnit smluvní ujednání – konkrétní podmínky jsou jí vnuceny (jedná se o tzv. smlouvy uzavírané adhezním způsobem)., Mnohdy se pak zejména spotřebitel s obsahem takové smlouvy (a obchodních podmínek) ani neseznámí. Uzavírání smluv adhezním způsobem však nemusí být nikterak škodlivé (či protizákonné), jelikož to samo o sobě neznamená, že by taková smlouva obsahovala zneužívající ustanovení. Adhezní smlouva totiž může být (a měla by být) vyvážená a může odpovídat tomu, co by si strany ujednaly i individuálně. pak zavádí vyvratitelnou domněnku toho, že formulářové smlouvy (tedy zejména obchodní podmínky) je nutno považovat za smlouvy uzavírané adhezním způsobem, jelikož slabší strana typicky nedisponuje skutečnou příležitostí (faktickou možností) smluvní (obchodní) podmínky ovlivnit.

Obchodní podmínky mají obvykle obecný charakter, jsou navrženy jednou ze smluvních stran a jsou zpravidla užívány při obchodování. podmínky mají obvykle podobu psaného textu. Pro závaznost obchodních podmínek není nutné, aby splňovaly požadavek písemné formy, jelikož samy o sobě nemusí být podepsány. Je však nutno je se smluvním ujednáním náležitě provázat (například odkazem) a spotřebitel s nimi musí být skutečně seznámen. V případě, že obchodní podmínky nejsou v souladu se samotnou smlouvou, považuje se za platné ustanovení takové, které je zakotveno ve smlouvě. Pokud druhá strana (bez ohledu na to, jestli se jedná o spotřebitele či nikoli) nemohla určité překvapivé ujednání v obchodních podmínkách rozumně očekávat, bez jejího výslovného je pak dané ujednání neúčinné.,

Obsah obchodních podmínek je možno změnit i po uzavření samotné smlouvy, což bývá typické v případě, že vzniká mezi stranami dlouhodobý závazek (jedná se například o opakované plnění). Možnosti pro změnu obchodních podmínek jsou totožné s podmínkami pro změnu smlouvy. Proto musí být vždy naplněny stejné předpoklady, jakými jsou zejména souhlas druhé strany a stanovení konkrétních mechanismů pro změnu. Dojde-li tedy k jednostranné změně obchodních podmínek, má spotřebitel právo zvážit, jestli změněné podmínky bude akceptovat, nebo závazek bez sankce vypoví. Strany mají rovněž možnost sjednat způsob, jakým může dojít ke změně podmínek, a možnost přijetí změny tak lze učinit například konkludentně. K tomu, aby se nové znění

obchodních podmínek stalo součástí uzavřené smlouvy (a není nikterak sjednán mechanismus pro změnu obchodních podmínek), nepostačuje, aby strana, která nové znění navrhla, oznámila jejich změnu a požadovala, že pokud druhá strana nesdělí nesouhlas do určité doby, platí změna za schválenou. V takovém případě je třeba sjednat smlouvu novou.

Závazky ze smluv uzavřených distančních způsobem

V případě, že dojde k uzavření smlouvy, stávají se předsmluvní informace součástí smlouvy, jsou tedy závazné a smluvní strany je mohou změnit pouze po vzájemné dohodě a jen ve prospěch spotřebitele. To ale neznamená, že informace musí být součástí smlouvy – i v případě jejich absence v obsahu smlouvy jsou mezi stranami závazné. V případě změny obsahu smlouvy oproti informacím sděleným spotřebiteli před jejím uzavřením musí být odchylky výslovně uvedeny (nestačí tedy předložit jen změněnou smlouvu) a odsouhlaseny. Pokud k takovému výslovnému sdělení změn (odchylek) oproti původním informacím vůči spotřebiteli nedojde, neznamená to, že by se taková smluvní ujednání stala neplatnými – v rámci smluvního vztahu se použijí ta ujednání, která jsou pro spotřebitele výhodnější. Po uzavření smlouvy je pak podnikatel povinen vydat spotřebiteli vyhotovení smlouvy tak, aby mu byly dostupné informace o vzájemných ujednáních a bylo tak zlepšeno jeho postavení při případných sporech. Formu vyhotovení smlouvy je nutno vykládat v kontextu konkrétního způsobu uzavírání smlouvy, jelikož pro ni nejsou předepsány specifické požadavky.

Specifická situace nastává v případě neobjednaného plnění spotřebitelem. Pokud podnikatel dodá zboží spotřebiteli, aniž by si jej spotřebitel objednal, nastává fikce poctivé držby spotřebitele. Spotřebitel pak takto dodané zboží není povinen vracet ani za něj platit. Účelem dané úpravy je ochrana spotřebitele před nežádoucím obtěžováním ze strany podnikatele. V případě omylu podnikatele by ale takováto fikce neměla nastoupit.

Odstoupení od smlouvy uzavřené distančním způsobem

V případě, že dojde k uzavření smlouvy, stávají se předsmluvní informace součástí smlouvy, jsou tedy závazné a smluvní strany je mohou změnit pouze po vzájemné dohodě a jen ve prospěch spotřebitele. To ale neznamená, že informace musí být součástí smlouvy – i v případě jejich absence v obsahu smlouvy jsou mezi stranami závazné. V případě změny obsahu smlouvy oproti informacím sděleným spotřebiteli před jejím uzavřením musí být odchylky výslovně uvedeny (nestačí tedy předložit jen změněnou smlouvu) a odsouhlaseny. Pokud k takovému výslovnému sdělení změn (odchylek) oproti původním informacím vůči spotřebiteli nedojde, neznamená to, že by se taková smluvní ujednání stala neplatnými – v rámci smluvního vztahu se použijí ta ujednání, která jsou pro spotřebitele výhodnější. Po uzavření smlouvy je pak podnikatel povinen vydat spotřebiteli vyhotovení smlouvy tak, aby mu byly dostupné informace o vzájemných

ujednáních a bylo tak zlepšeno jeho postavení při případných sporech.

V případě, že dojde k uzavření smlouvy, stávají se předsmluvní informace součástí smlouvy, jsou tedy závazné a smluvní strany je mohou změnit pouze po vzájemné dohodě a jen ve prospěch spotřebitele. To ale neznamená, že informace musí být součástí smlouvy – i v případě jejich absence v obsahu smlouvy jsou mezi stranami závazné. V případě změny obsahu smlouvy oproti informacím sděleným spotřebiteli před jejím uzavřením musí být odchylky výslovně uvedeny (nestačí tedy předložit jen změněnou smlouvu) a odsouhlaseny. Pokud k takovému výslovnému sdělení změn (odchylek) oproti původním informacím vůči spotřebiteli nedojde, neznamená to, že by se taková smluvní ujednání stala neplatnými – v rámci smluvního vztahu se použijí ta ujednání, která jsou pro spotřebitele výhodnější. Po uzavření smlouvy je pak podnikatel povinen vydat spotřebiteli vyhotovení smlouvy tak, aby mu byly dostupné informace o vzájemných ujednáních a bylo tak zlepšeno jeho postavení při případných sporech. Formu vyhotovení smlouvy je nutno vykládat v kontextu konkrétního způsobu uzavírání smlouvy, jelikož pro ni nejsou předepsány specifické požadavky. V případě prodeje využívajícího elektronickou kontraktaci je pak nutno spotřebiteli poskytnout potvrzení o uzavření smlouvy a její znění na trvalém nosiči. Tato povinnost se rovněž vztahuje na nutnost poskytnutí znění všeobecných obchodních podmínek. Důkazní břemeno, že náležité znění smlouvy bylo poskytnuto, pak leží na podnikateli.

V případě, že spotřebitel odešle s využitím nástroje pro komunikaci na dálku, musí podnikatel obdržení takové objednávky potvrdit. Zákon však nestanovuje konkrétně, že se musí jednat o stejný nástroj, který využil spotřebitel; přes to však spotřebitel typicky očekává, že v případě elektronicky uzavřené smlouvy bude objednávka potvrzena stejnou formou. Účelem dané úpravy nicméně je, aby byl spotřebiteli poskytnut dostatečný důkaz o doručení jeho objednávky. V daném případě se ale jedná o špatnou implementaci směrnice o elektronickém obchodu, ve které je stanoveno, že podnikatel má příjem objednávky potvrdit elektronickou cestou.

K prostředkům typicky souvisejícím s ochranou spotřebitele v případě uzavírání smluv distančním způsobem náleží možnost jednostranně ukončit smluvní závazek zpravidla ex tunc slabší stranou bez udání důvodu a bez jakéhokoli postihu v rámci stanovené čtrnáctidenní lhůty. Jedná se tak o kompenzaci toho, že v případě distančního prodeje je pro spotřebitele obtížnější důkladně se seznámit s konkrétními vlastnostmi výrobku. V daném případě se tak jedná nikoli o sankci pro podnikatele, ale o výhodu poskytnutou spotřebiteli, aby se se zbožím mohl ve větší míře seznámit ve chvíli, kdy zboží fyzicky drží. V případě, že spotřebitel není v rámci předsmluvních či smluvních informací poučen o možnosti odstoupit od smlouvy sjednané distančním způsobem do čtrnácti dní, prodlužuje se tato lhůta (tedy možnost odstoupit od smlouvy) na jeden rok a čtrnáct dní. Pokud spotřebitele podnikatel o této lhůtě dodatečně informuje, počne běžet standardní čtrnáctidenní lhůta od okamžiku informování.

Budoucí vývoj

Prodej zboží a poskytování služeb online stále vzrůstá. V rámci evropské politiky pro jednotný digitální trh tak Evropská komise přijala strategii pro harmonizaci pravidel v oblasti prodeje zboží online a poskytování digitálního obsahu. Tato iniciativa se promítla zejména do návrhu dvou směrnic:

(i) směrnice o některých aspektech smluv o prodeji zboží online a jinými prostředky

(ii) směrnice o některých aspektech smluv o poskytování digitálního obsahu.

Hlavním účelem těchto dvou je zvýšit ochranu spotřebitelů v online prostředí a obecně podpořit oblast elektronického obchodování. Za hlavní problém je v současnosti považována stále roztříštěná právní úprava v oblasti spotřebitelského elektronického obchodování, která obecně odrazuje zúčastněné strany.

Hlavním cílem směrnice o některých aspektech smluv o poskytování digitálního obsahu je sjednotit právní úpravu smluvních vztahů, které se týkají poskytnutí digitálního spotřebiteli, jelikož pro ně v současné chvíli neexistuje společná právní regulace a přístup jednotlivých členských států se do jisté míry liší. Směrnice pak například specifikuje, za jakých okolností není digitální obsah v souladu se smlouvou (tedy, kdy je považován za vadný), jaká je možnost změny digitálního obsahu, jaké jsou možnosti nápravy v případě plnění, které není v souladu se smlouvou, či možnosti ukončení smlouvy (i například dlouhodobé).

Aktuální právní úprava řešení spotřebitelských sporů online

Zakotvení mimosoudního řešení spotřebitelských sporů, jako vhodného nástroje pro řešení sporů z elektronického obchodování, vychází primárně z evropské právní úpravy – ze směrnice o alternativním řešení spotřebitelských sporů a nařízení o řešení spotřebitelských sporů online. V první části této kapitoly se tak budeme věnovat představení jednotlivých mechanismů, které z této právní úpravy vyplývají. V případě, že dojde k porušení vzájemného ujednání mezi stranami a ty individuálně neuspějí v urovnání sporu, měl by právě tento režim spotřebiteli poskytnout vhodnou možnost pro řešení sporů s podnikatelem. Ve většině případů je totiž nereálné, aby spotřebitel daný spor řešil soudní cestou. V druhé části se pak zaměříme na konkrétní dopady evropské právní úpravy na tu českou a v závěru na kritiku poskytnutého řešení.

Směrnice o alternativním řešení spotřebitelských sporů

Jedním ze základních problémů možnosti řešit spory mimosoudně v rámci EU byla rozdílnost nabízených ADR (alternative dispute resolution) mechanismů v jednotlivých členských státech. V některých je totiž tradice řešení sporů tímto způsobem poměrně silně zakotvena (zejména ve státech západní Evropy a v severských státech), v postkomunistických státech pak není téměř žádná (a zejména ve spotřebitelských sporech je v rámci závazné fáze obecně vnímána spíše negativně – případně je zcela vyloučena). Mimosoudní řešení sporů tak bylo obecně v minulosti často územně omezeno, nebylo dostupné ve všech členských státech a mnohdy bylo limitováno jen na specifické oblasti.

Směrnice však v rámci harmonizace právních úprav neposkytuje soubor konkrétních pravidel (jak to v případě ODR činí například Třetí pracovní skupina Komise OSN pro mezinárodní obchodní právo), , ale stanovuje hlavní zásady a minimální standardy pro poskytování mimosoudního rozhodování spotřebitelských sporů v jednotlivých členských státech.

Směrnice o alternativním řešení spotřebitelských sporů měla být implementována členskými státy do jejich právních řádů nejpozději 9. 7. 2015; v České republice se tak stalo až s účinností k 28. 12. 2015 na základě zákona č. 378/2015 Sb., kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů a některé další zákony.

Nařízení o řešení spotřebitelských sporů online

Směrnice o alternativním řešení spotřebitelských sporů je v případě možnosti řešit spory mimosoudně online doplněna nařízením o řešení spotřebitelských sporů on-line. Tyto dva legislativní nástroje tak tvoří vzájemně propojené řešení. Cíl nařízení o řešení spotřebitelských sporů online je v zásadě jediný – zřízení platformy pro řešení sporů online a poskytnutí ODR. Tato platforma (ODR platforma) by měla být jednotným virtuálním kontaktním místem pro spotřebitele a podnikatele v případě, že chtějí řešit své spory mimosoudně online. ODR platforma je tedy internetovou stránkou, která umožňuje stranám elektronický přístup k řešení sporů ve všech jazycích členských států. Spotřebitele a podnikatele, kteří mezi sebou vedou spor, pak může ODR platforma v případě, že s tím zúčastněné strany souhlasí, propojit s konkrétním subjektem alternativního řešení sporů.

Data a informace veřejného sektoru

Data a informace veřejného sektoru

- Data vs. Informace

- Veřejná správa a samospráva – velké množství dat

- Příklady:

-- Statistická data

-- Kartografické informace

-- Meteorologické informace

-- Právní informace

-- Jízdní řády

-- Katastr nemovitostí

-- Zdravotnické informace

-- Informace veřejných knihoven

-- Výsledky výzkumu a vývoje

-- Údaje z rejstříků, o nakládání s veř. prostředky, o zaměstnancích veř. sektoru, údaje zpravodajských služeb

-- ...

- Data a informace veřejného sektoru

-- Přístup k informacím veřejného sektoru

-- Základní politické právo

-- Princip publicity veřejné správy

-- Výkon veřejné moci

- Opakované užití informací veřejného sektoru

o Ekonomický aspekt

o Akcent v oblasti soukromého práva

o Otevřená data – vysoká efektivita

Právo na informace – mezinárodní kontext

· Řeší primárně přístup k informacím

· Všeobecná deklarace lidských práv (1948)

o Čl. 19 - právo na svobodu projevu zahrnující právo jakýmikoli prostředky vyhledávat, přijímat a rozšiřovat informace a myšlenky

· Mezinárodní pakt o občanských a politických právech (1966)

o Podobně jako v případě Všeobecné deklarace lidských práv – právo na informace jako předpoklad a součást práva na svobodu projevu

· Úmluva Rady Evropy o ochraně lidských práv a základních svobod (1950)

o Ratifikováno 1992

· Doporučující dokumenty Rady Evropy

o Např. Rezoluce a doporučení Poradního shromáždění Rady Evropy o masmédiích a lidských právech, o deklaraci Výboru ministrů Rady Evropy o svobodě projevu informací ze dne 29. 4. 1982

o Obsahují základní principy práva na informace

§ Každá osoba má právo obdržet informace uchovávané státními orgány

§ Žadatel o informace není povinen prokazovat důvody své žádosti

§ Přístup k informacím má být uplatňován na principu rovnosti

§ Informace mají být poskytnuty v přiměřené lhůtě

§ Státní orgán musí sdělit důvody odepření informací

§ Zamítnutí žádosti musí být přezkoumatelné.

· Úmluva Rady Evropy o přístupu k úředním dokumentům (CETS č. 205; Tromsø, 18, června 2009)

o Zaručuje přístup k úředním dokumentům (= všem informacím zaznamenaným v jakékoli podobě)

§ Minimální povinné subjekty dle Úmluvy - orgány státní správy a samospráv, orgány zákonodárné moci, orgány soudní moci a fyzické a právnické osoby, pokud vykonávají správní pravomoc

o V současné době ratifikovalo 10 států Rady Evropy

§ Např. Finsko, Estonsko, Litva, Maďarsko a Černá hora

§ ČR zatím ne

Poskytování informací

· Na žádost

o § 4a

§ Je-li informace poskytována na základě žádosti, poskytuje se ve formátech a jazycích podle obsahu žádosti o poskytnutí informace, včetně k ní se vztahujících metadat, pokud tento zákon nestanoví jinak. Povinný subjekt není povinen měnit formát nebo jazyk informace ani vytvářet k informaci metadata, pokud by taková změna nebo vytvoření metadat byly pro povinný subjekt nepřiměřenou zátěží; v tomto případě vyhoví povinný subjekt žádosti tím, že poskytne informaci ve formátu nebo jazyce, ve kterých byla vytvořena. …

§ Možnost poskytnout prostřednictvím aplikačního rozhraní (API)

o Poplatky za poskytnutí nesmí překročit nutně vynaložené náklady

· Zveřejněním

o Povinné

§ Př. § 5 odst. 1 z. č. 106/1999 Sb.

§ Každý povinný subjekt musí pro informování veřejnosti ve svém sídle a svých úřadovnách zveřejnit na místě, které je všeobecně přístupné, jakož i umožnit pořízení jejich kopie, tyto informace:

· a) důvod a způsob založení povinného subjektu, včetně podmínek a principů, za kterých provozuje svoji činnost,

· b) popis své organizační struktury, místo a způsob, jak získat příslušné informace, kde lze podat žádost či stížnost, předložit návrh, podnět či jiné dožádání anebo obdržet rozhodnutí o právech a povinnostech osob,

· c) místo, lhůtu a způsob, kde lze podat opravný prostředek proti rozhodnutím povinného subjektu o právech a povinnostech osob, a to včetně výslovného uvedení požadavků, které jsou v této souvislosti kladeny na žadatele, jakož i popis postupů a pravidel, která je třeba dodržovat při těchto činnostech, a označení příslušného formuláře a způsob a místo, kde lze takový formulář získat,

· …

§ § 5 odst. 5 Povinné subjekty, které vedou a spravují registry, evidence, seznamy nebo rejstříky obsahující informace, které jsou na základě zvláštního zákona každému přístupné, jsou tyto informace povinny zveřejňovat v přehledné formě způsobem umožňujícím i dálkový přístup. Na tyto subjekty se pro tento účel nevztahuje povinnost zamezit sdružování informací podle zvláštního právního předpisu.

o Dobrovolné

§ § 5 odst. 7 ZInf:

§ Povinný subjekt může informace podle odstavce 1 zveřejnit i dalšími způsoby a s výjimkami uvedenými v tomto zákoně může zveřejnit i další informace.

Opětovné užití informací veřejného sektoru

· Pro efektivitu je třeba zajistit vhodný přístup k datum

o Otevřená data

o Open API

Povinné subjekty dle z. 106/1999 Sb.

· § 2 odst. 1: státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce

· § 2 odst. 2: subjekty, kterým zákon svěřil pravomoc rozhodovat o právech a povinnostech osob, v rozsahu výkonu této pravomoci

Veřejné instituce

· Novela č. 39/2001 Sb. – cíl: zajistit aplikaci na veřejnoprávní media

· Intenzivní soudní praxe:

o Všeobecná zdravotní pojišťovna (Nález Ústavního soudu ze dne 16. 1. 2003, sp. zn. III. ÚS 671/02)

o Fond národního majetku (Nález Ústavního soudu ze dne 27. 2. 2003, sp. zn. III. ÚS 686/02)

§ 4 znaky veřejné instituce

· (i) veřejný účel instituce

· (ii) její zřízení státem

· (iii) vznik orgánů instituce státem

· (iv) státní dohled nad činností instituce

· Státní podnik Letiště Praha (Nález Ústavního soudu ze dne 24. 1. 2007, sp. zn. I. ÚS 260/06)

o 5. Znak

§ (v) určení, zda instituce vzniká na základě veřejného nebo soukromého práva

o Základní kámen pro rozhodovací praxi NSS

· Chaps

o IDOS – data – Seznam.cz

o Chaps: Nejsme povinný subjekt, nic nedáme

o Správní kolečko:

§ Rozhodnutí MD (Ministerstva dopravy ze dne 16. 1. 2012 č. j. 220/2011- 030-Z106/10)

§ Rozsudek KS v Brně (7. 6. 2013 č. j. 62 A 26/2012-129)

§ Kasační stížnosti (27. 9. 2013 č. j. 5 As 57/2013-16)

§ Ústavní stížnosti (II.ÚS 3669/13)

o ÚS - Ano! – přenesení výkonu veřejné správy –povinný subjekt v rozsahu přeneseného úkolu

o (ÚOHS – pokuta Chaps 2 199 000 Kč, snížena na polovinu v rozkladu)

Otevřená data

· způsob poskytování informací veřejného prostoru

· úplná,

· snadno dostupná,

· strojově čitelná,

· používající standardy s volně dostupnou specifikací,

· zpřístupněna za jasně definovaných podmínek užití dat s minimem omezení,

· dostupná uživatelům při vynaložení minima možných nákladů.

· 5 stupňů

· Posílení transparentnosti a kontrola veřejné správy

· Zefektivnění veřejné správy

o Zejména při existenci propojených dat

· Datová žurnalistika

· Lepší služby

· Nové ekonomické příležitosti

· Zdroj nových služeb

· Jak to celé funguje?

o Veřejná správa poskytne PSI ve formě otevřených dat -> Nezávislý vývojář nad nimi postaví aplikaci

Ochrana autorského práva

· Pouze, když autorské právo svědčí třetí osobě

· Úřední dílo! (§ 3 Aut. Z.)

· Ne databázové parvo

· § 11 odst. 2 písm. c) z. 106/1999 Sb.

o „Povinný subjekt informaci neposkytne, pokud by tím byla porušena ochrana práv třetích osob k předmětu práva autorského nebo práv souvisejících s právem autorským.“

· Zákonná licence užití díla pro úřední účel dle § 34 z. č. 121/2000 Sb., autorský zákon

· Př. 1 – Právní analýza vypracovaná externím subjektem

o Rozsudek NSS ze dne č. j. 3 As 55/2014-33

o V projednávané věci je tedy třeba na základě smlouvy o dílo, příp. licenční smlouvy, uzavřené mezi žalovaným a advokátní kanceláří ověřit, zda byl žalovaný oprávněn požadovanou právní analýzu stěžovatelce poskytnout, aniž by porušil autorská práva jejího zpracovatele.

· Př. 2 – Mapy criminality

· Pokud je povinný subjekt oprávněn k rozmnožování, rozšiřování a sdělování – je povinen poskytnout

Soukromí

· § 8b:

o (1) Povinný subjekt poskytne základní osobní údaje o osobě, které poskytl veřejné prostředky.

o (2) Ustanovení odstavce 1 se nevztahuje na poskytování veřejných prostředků podle zákonů v oblasti sociální, poskytování zdravotních služeb, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření a státní pomoci při obnově území.

o (3) Základní osobní údaje podle odstavce 1 se poskytnou pouze v tomto rozsahu: jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků.

· Ustálená praxe NSS:

o Např. 8 As 55/2012-62 ze dne 22. 10. 2014

o Informace o platech zaměstnanců placených z veřejných prostředků se podle § 8b zákona č. 106/1999 Sb., o svobodném přístupu k informacím, zásadně poskytují.

o Povinný subjekt neposkytne informace o platu zaměstnance poskytovaném z veřejných prostředků (§ 8b zákona č. 106/1999 Sb., o svobodném přístupu k informacím) jen výjimečně, pokud se tato osoba na podstatě vlastní činnosti povinného subjektu podílí jen nepřímo a nevýznamným způsobem a zároveň nevyvstávají konkrétní pochybnosti o tom, zda v souvislosti s odměňováním této osoby jsou veřejné prostředky vynakládány hospodárně.

· Protest – ÚOOÚ

- Argument: Neproporcionální
- Řešení – neuvádět jména s výjimkou vrcholových pozic

Osobnost a soukromí

Osobnost a soukromí

Lidská osobnost je projevem identity člověka. Náhled na podstatu a pojem člověka obsahuje řadu poloh, které zahrnují filozoficko-teologické koncepty založené na starořeckém a křesťanském myšlení, biologické faktory popsané darwinismem, sociologické pojetí individua jako součásti primárnější a důležitější lidské společnosti či historickou dimenzi představující odraz dosavadního vývoje lidstva.

Dobrat se podstaty lidské identity a jádra jeho osobnosti je však cíl veskrze nedostižný, neboť jak uvádí Eduard Sprange, jehož filozoficko-teologické pojímání v západní civilizaci bylo historicky rozkolísáno po ose od „zdegenerované šelmy“ po „věrný obraz boha“ a v jehož nitru se současně prolíná „nesmrtelná duše“ se „záhadnou hrou vnitřních světů“, coby přihrádky osobnosti, které představují různé, ale provázané složky lidského já.

Jádro osobnosti lze z psychologického hlediska vyjádřit jako vyvíjející se systém duševních vlastností a tendencí jedince, ve kterých se odráží jeho charakterové rysy, schopnosti, nátura, postoje, a jiné, které se z podstatné části projevují lidským vědomím. Potřeba identity člověka je základní složkou jeho podstaty.

Prostředí kyberprostoru se v řadě ohledů odlišuje od reálného světa, což má s rostoucím významem virtuální přítomnosti pro většinu společnosti významné dopady na formování a realizaci osobnosti jednotlivců. Předně je v tomto prostoru omezeno množství informací sdílených v rámci interakce, která je tak oproti reálné mezilidské komunikaci ochuzena o nonverbální projevy a podpůrné smyslové vjemy. Tento aspekt je doplňován o prvek zdánlivé anonymity či přinejmenším nejistoty ohledně identity způsobený variabilitou virtuálních identit, který však může být v kontrastu s identifikovatelností zařízení a dalších podpůrných technických prvků online komunikace.

Lidská osobnost je různorodá a pestrá, zahrnuje prvky ctihodné a pozitivní, jakožto i odsuzované a potlačované. Toto polaritně strukturované napětí mezi vnitřními elementy člověka stojí za naším člověčenstvím, je hnacím motorem pokroku a změny. Pouze za přítomnosti úsilí nutně spojovaného s prosazováním morálních hodnot v nitru každého z nás jsme schopni docenit význam, který je těmto maximám přisuzován. Současně však tyto vnitřní rozpory mohou vést ke specifickému chování jednotlivce ve virtuálním prostoru, kde je člověk zdánlivě zbaven některých společenských či morálních mantinelů a je mu umožněno realizovat temnější stránky své osobnosti bez zjevného následku či trestu. Thomas Ploug ve své studii podotýká, že z morálně-etického hlediska lze možné příčiny tohoto posunu v hodnotách při jednání v online prostředí shledávat v interakci odcizujícího efektu technologií, absenci nonverbálních a smyslových vjemů či pocitu vzdálenosti a anonymity.

Nad rámec vnitřního vnímání vlastní podoby a projevů tohoto vnímání navenek je součástí osobnosti člověka i jeho jedinečná fyzická přítomnost. Tím, kým je, je i skrze svou specifickou stavbu těla, pohlaví, rasu, věk, vzhled, zdraví a další fyzické projevy. Soubor takto představených dílčích složek ve svém propojení vytváří osobnost člověka, kterou je namístě vždy vnímat v její ucelenosti a nedělitelnosti.

Pojem soukromí

Specifickou rovinou lidské osobnosti, která se široce prolíná s řadou výše zmíněných dílčích osobnostních práv, ale též se specifickou úpravou ochrany osobních údajů popisovanou dále, je rovina ochrany soukromí. Jak bude rozebráno v části poskytující přehled historického vývoje, řadí se tato spíše mezi později vykrystalizované složky právní ochrany osobnosti. Současně jde však o oblast s nejvíce dynamickým současným vývojem, který je silně ovlivněn rozmachem informačních a komunikačních technologií.

U soukromí jde o pojem, který se z pohledu práva vyvinul v rámci minulého století v podstatě ze dvou odlišných perspektiv. V americkém pojetí jde především o ochranu před zásahem a vměšováním se státu do soukromé osobní sféry člověka. Evropské pojetí naproti tomu původně vycházelo z širší potřeby ochrany cti a vážnosti, tedy z přiznání oddělení veřejného a soukromého nazírání na člověka.

Samota – Nejúplnější stav soukromí zde je jedinec oddělen od všech ostatních fyzických, psychologických či sociálních zásahů z vnějšku a nachází se ve svém vnitřním dialogu.

Stav intimity – jedince staví do malé skupinky, která umožňuje upřímné a uvolněné vztahy mezi členy.

Stav anonymity – Pokud se jedinec nachází na veřejně přístupném místě, ale zůstává „skryt v davu“, je ve stavu anonymity

Další pohled na soukromí přináší Daniel J. Solove, který shrnul tehdejší diskurs týkající se konceptu soukromí do šesti základních kategorií. První vnímanou složkou je právo být ponechán o samotě, o kterém bude bližší zmínka v pozdější části, která popisuje historický vývoj ochrany soukromí a prolínání jeho evropského a amerického pojetí. Druhou rovinu shledává v možnosti omezit přístup ke své osobě a bránit se nechtěnému přístupu ze strany druhých. Dále lze na soukromí nahlížet jako na tajemství a možnost skrýt určité záležitosti před druhými. Čtvrtým aspektem, který je reflektován ve zvláštní úpravě ochrany osobních údajů, je možnost výkonu kontroly nad informacemi o své osobě. Pátou rovinu soukromí Solove propojuje s obecným vnímáním ochrany osobnosti, jedinečnosti a důstojnosti člověka. Posledním, avšak nepominutelným prvkem je pak intimita neboli možnost kontroly intimních vztahů a přístupu k intimním aspektům života.

Komplexní náhled na vnímání soukromí z jiného úhlu pohledu přináší od devadesátých let Roger Clarke, který dělí soukromí jako takové do pěti dílčích dimenzí. Osobní či tělesné soukromí je z jeho pohledu otázkou tělesné integrity a váže se na problematiku souhlasu se zdravotními zásahy, odběry tkání či povinné vakcinace. Rovinu soukromí v chování a jednání váže ke všem aspektům

lidského chování, zvláště pak k těm, které jsou obecně přijímány jako citlivé, tedy např. otázky sexuálních preferencí, politických názorů či náboženského vyznání. Třetí rovinou je soukromí osobní komunikace, tedy zajištění možnosti komunikace mezi osobami přes různé komunikační kanály bez plošného sledování a odposlouchávání.

Další rovina se vztahuje na soukromí osobních údajů, které by se mělo projevovat kontrolou jedince nad údaji o jeho osobě a nad jejich zpracováváním. Pátou rovinou, kterou Clarke doplnil k předchozím v roce 2013 v důsledku vnímaného technologického a společenského vývoje, je soukromí osobního zážitku a zkušenosti. Význam této složky soukromí dle jeho názoru znepokojivě narůstá s rostoucí všudy přítomností profilování uživatelů digitalizovaných služeb, sahajícího od sledování polohy přes zaznamenávání aktivity na mediálních portálech po ukládání elektronické pošty.

Čtvrtým a nejkomplexnějším příkladem přístupu k pojetí soukromí, který je zde vhodné zmínit, je typologie vytvořená pod vedením Bert-Jaap Kopeš. Za využití předchozích klasifikací a údajů o ústavněprávní ochraně soukromí v devíti jurisdikcích západní kultury byl formulován model se dvěma dimenzemi. Jedna dimenze vychází z výše zmíněného Westinova pojetí soukromí a odlišuje míru intimity prostředí. Osa sahá od osobního prostoru, kde je soukromí vyjádřené samotou, po veřejný prostor, kde má soukromí podobu nenápadnosti. Druhá osa má pak dvě polohy reflektující základní pojetí přístupu k ochraně soukromí, tedy důraz na svobodu před zásahem vyjádřenou právem být nechán o samotě a důraz na svobodu určitého stavu značící prostor k rozvoji vlastní individuality. Prostor mezi těmito dimenzemi je vyplněn devíti základními typy soukromí, které zahrnují: tělesné soukromí; prostorové soukromí; soukromí komunikace; soukromí vlastnictví; soukromí informací; duševní soukromí; soukromí při rozhodování; sdružovací soukromí a soukromí chování.

Výpočetní technologie, internetové připojení a všeobecná digitalizace zásadně rozšířily možnosti vytvářet, shromažďovat, zpracovávat a sdílet údaje o nejrůznějších činnostech, vlastnostech, rysech či myšlenkách jednotlivce a tím narušovat či potlačovat některou z oblastí projevu soukromí jednotlivce. S růstem významu těchto operací se data stávají hlavní komoditou moderní digitální ekonomiky a je zřejmé, že pouhá incidenční následná ochrana skrze všeobecné osobnostní právo by byla nedostačující. Klíčovou roli tak získává paralelní preventivní právní úprava veřejnoprávního charakteru zaměřená na regulaci zpracování osobních údajů.

Ochrana osobnosti v čase

Počátky ochrany osobnosti lze vystopovat až k římskému právu. Vzhledem k dobové situaci byla nejprve omezena na ochranu tělesné integrity a následně rozšiřována na jiné formy urážky na cti (iniuria). S nástupem středověku a vlivem katolického křesťanství vzniká koncept obecné lidské důstojnosti, uznání schopnosti vlastního sebeurčení nebo předpoklad rovnosti všech lidí před Bohem. Pojetí civilněprávního všeobecného osobnostního práva však přináší až osvícenství skrze přirozenoprávní vnímání člověka jako rozumem nadané bytosti.

Pro české území lze počátky úpravy shledávat v přijetí Obecného zákoníku občanského a jeho následné recepci formou zákona č. 11/1918 Sb. do československého právního řádu. Přes absenci

výslovné úpravy osobnostních práv byla jejich obecná ochrana zakotvena skrze § 16, který přiznával každému člověku vrozená přirozená práva. Dobová právní doktrína oceňovala formulaci tohoto ustanovení pro jeho funkci všeobecné směrnice pro soudní rozhodování. Zároveň rozšiřovala jeho obsah např. o svobodu víry a vyznání či právo na osobní tajemství. Některé další složky osobnostního práva byly obsaženy v zákoně č. 218/1926 Sb., o právu autorském, v upravené právo na ochranu písemností osobní povahy a v § 34 právo k vlastní podobizně. Některé tradiční složky osobnostního práva však zůstaly upraveny trestněprávně, konkrétně zákonem č. 108/1933 Sb., o ochraně cti.

V důsledku složité politické situace během meziválečné a poválečné politice, nikdy nedošlo k přijetí ryze československé prvorepublikové kodifikace občanského práva, přestože došlo k jejímu vypracování . Zákon č. 141/1950 Sb., občanského zákoníku, přijatý za zcela odlišné politické situace a ideologie, atmosféry poválečných let, neobsahoval zákonnou úpravu všeobecného osobnostního práva, ačkoliv bylo při jeho přípravě čerpáno z návrhu meziválečné československé právní úpravy. Dílčí ochrana byla zachována jménu, příjmení a krycímu jménu fyzické osoby v § 22. Práva k osobním písemnostem a podobizně člověka upravoval § 95 a § 96 zákona č. 115/1953 Sb., autorský zákon, který v jejich rozsahu stanovil také postmortální ochranu a podmínky zpravodajské, umělecké a vědecké licence.

Ke kladnému vývoji došlo během přijetím zákona č. 40/1964 Sb., občanského zákoníku, který v § 11 poprvé obsahoval výslovnou úpravu všeobecného osobnostního práva jako jednotného práva. V rozšíření výčtu úpravě v autorském zákoně lze zřejmě sledovat reakci na technologický pokrok, kdy se záznamová zařízení jako diktafony, fotoaparáty či kamery začaly stávat běžnou součástí společenského dění. Postmortální ochrana byla rozšířena na všechny složky všeobecného osobnostního práva.

Po Sametové revoluci došlo v návaznosti na změnu politického režimu k dílčím novelizacím zákona č. 40/1964 Sb.. Přirozenoprávní základ osobnostního práva pak byl znovu zakotven přijetím Listiny základních práv a svobod v roce 1991. K hlavnímu vývoji prvorepublikové právní tradice došlo skrze soudní aplikaci práva, ve které byl reflektován nedávný společenský i technologický vývoj. Soukromoprávní úpravě osobnostních práv byla při aplikaci přiznávána významná role pro rozvedení a konkretizaci Listiny základních práv a svobod, který zabezpečoval respektování osobnosti fyzické osoby, ochranu jejích jednotlivých stránek a její všestranný svobodný rozvoj.

Právní úprava ochrany osobnosti a soukromí

Ochraně osobnosti nebo dílčím složkám všeobecného osobnostního práva je věnována celá řada mezinárodních úmluv. Historicky významný je vliv *Všeobecné deklarace lidských práv*, kde je v preambuli vyjádřena víra v základní lidská práva, v důstojnost a hodnotu lidské osobnosti. Následně je v článku *12* formulován zákaz svévolného zasahování do soukromého života, do rodiny, domova a korespondence a zároveň i ochrana před útoky na čest a pověst člověka. Deklarace sice sama o sobě nemá právní závaznost, jde však o klíčový zakládací dokument

Organizace spojených národů a jde i o vlivnou složku mezinárodního zvykového práva. Základní hodnoty deklarace byly následně rozvedeny a konkretizovány v *Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech*, které vstoupily pro Československou socialistickou republiku v účinnost dne 23. března 1976 formou *Vyhlášky ministra zahraničních věcí č. 120/1976 Sb.*

Následné nedodržování práv garantovaných v těchto dokumentech stálo u zrodu občanské iniciativy Charta 77. Z řady dalších významných mezinárodních dokumentů dotýkajících se práv člověka na ochranu jeho osobnosti je na tomto místě vhodné zmínit Úmluvu o otroctví, Mezinárodní úmluvu o odstranění všech forem rasové diskriminace, Úmluvu o odstranění všech forem diskriminace žen, Rámcovou úmluvu o ochraně národnostních menšin či soubor Úmluv Mezinárodní organizace práce.

Zásadním impulsem pro vývoj evropského pojetí ochrany lidských práv bylo v roce 1950 přijetí Úmluvy o ochraně lidských práv a základních svobod v rámci Rady Evropy. Tento mezinárodní dokument je jedním ze základních kamenů evropského přístupu k ochraně lidských práv a díky samostatnému kontrolnímu mechanismu v podobě Evropského soudu pro lidská práva umožnil vytvoření korpusu mezinárodní lidskoprávní judikatury, která je v mnoha ohledech více než vodítkem pro vývoj vnitrostátních úprav a rozhodovací praxe.

Výklad a aplikace Úmluvy jsou postaveny na souboru základních principů, které v mnohém odrážejí esenci tohoto rámce, tedy zajištění srovnatelné minimální úrovně lidských práv členských států Rady Evropy. Předně je sledována efektivita ochrany lidských práv, cílem je tudíž dosažení praktické a účinné realizace garantovaných práv. Dále se jedná o systém ochrany lidských práv, který působí subsidiárně k vnitrostátním systémům. Nosným výkladovým principem je požadavek nalézání spravedlivé rovnováhy mezi obecnými zájmy společnosti a ochranou základních práv jednotlivce. Text Úmluvy je současně nutno vnímat dynamicky, jako „živoucí instrument“, vyvíjející se v důsledku proměny společnosti. Dále je výkladu Úmluvy vlastní nalézání pozitivních závazků, tedy požadavků, aby smluvní strana (stát) něco učinila (především zajistila odpovídající ochranu práv dotčené osoby, např. skrze vnitrostátní systém soudnictví), nikoliv se pouze zdržela určitého jednání. Soud zároveň využívá konceptu prostoru pro uvážení, který omezuje zásahy soudu do praxe států pouze na zásadní nedostatky dodržování Úmluvy. Centrální pro výklad Úmluvy je v neposlední řadě koncept demokratické společnosti a princip vlády práva.

Česká a Slovenská Federativní Republika schválila Úmluvu 18. března 1992, čímž se stala součástí jurisdikce Evropského soudu pro lidská práva. Rozhodnutí štrasburského soudu mají nesporný vliv na přístup k výkladu lidských práv na vnitrostátní úrovni, což dosvědčuje řada rozhodnutí týkajících se přímo České republiky, jakožto i časté reference v judikatuře českých soudů.

V rámci unijního práva má dále stěžejní roli Listina základních práv EU. Svým obsahem Listina vychází do značné míry z Úmluvy o ochraně lidských práv a základních svobod a navazujícího judikaturního korpusu.

Na ústavněprávní úrovni zaujímá přední roli katalog lidských práv obsažený v Listině základních práv a svobod. Dílčí složky osobnostního práva prostupují řadou článků a vyzařují

nepřímo i z preambule. Tímto zakotvením osobnostních práv na nejvyšší úrovni českého právního řádu došlo k posílení jejich ochrany, která je podporována skrze rozhodovací činnost Ústavního soudu (a nepřímo též Evropského soudu pro lidská práva) a vedla ke zvýšenému standardu občanskoprávní reflexe těchto práv.

Ochrana osobních údajů

Ochrana osobních údajů

Veřejnoprávní ochrana osobních údajů je svým vývojem úzce propojena s mezinárodním vnímáním potřeby ochrany osobnosti, zvláště pak jejího soukromí. Je základní řada specifických práv subjektů údajů, jakými jsou: právo na informaci o zpracování, rozsahu zpracování, účelu zpracování nebo o jeho zpracovateli, právo na opravu či odstranění neoprávněně zpracovávaných osobních údajů. Ty se dají odvodit již z výkladu čl. 17 Mezinárodního paktu o občanských a politických právech.

Z Paktu však nelze bez dalšího dovozovat základní principy zpracování osobních údajů. Již dříve bylo možné jejich formulaci zaznamenat v pravidlech OECD (Organizace pro hospodářskou spolupráci a rozvoj) vydaných roku 1980. Obdobně jako pro ochranu osobnosti však pochází nadnárodní úprava významná pro české právní prostředí především z činnosti Rady Evropy. Úmluva č. 108 o ochraně osob s důrazem na automatizované zpracování osobních údajů byla přijata již v roce 1981. Pro Českou Republiku však nabyla platnosti až v roce 1981. Lze ji považovat za vůbec první detailněji zabývající se mezinárodní úpravu této problematiky.

Skrze tuto úmluvu byl položen základ národních právních předpisů, který následně umožnil snazší implementaci požadavků evropské směrnice č. 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Úmluva je považována za zásadní evropský předpis v této oblasti práva.

K 25. květnu 2018 vstoupil v účinnost Evropský reformní balíček pravidel pro zpracování osobních údajů, který reflektuje posun v prostoupení společnosti informačními a komunikačními technologiemi a reaguje na nově vzniklé výzvy. Cílila na harmonizaci a posílení ochrany osobních údajů a soukromí podle dosavadního právního rámce, přinesla tudíž řadu změn, ať již v celkové koncepci regulace a zajištění souladu s ní, tak v podobě nově upravených dílčích práv či povinností. Klíčové postavení nově jednotně zaujímá Obecné nařízení o ochraně osobních údajů č. 2016/679 (General Data Protection Regulation, dále jen „GDPR“), které je ve zvláštních oblastech doplněno dalšími evropskými právními předpisy či národní úpravou.

Účel úpravy

Zásahy do osobnostních či jiných základních práv a svobod skrze zpracování osobních údajů mohou nabývat různé intenzity. Může jít o různé formy narušení soukromí, resp. újmy na cti či vážnosti, např. skrze neoprávněné zveřejnění intimních informací o osobním životě či o preferencích, zálibách nebo jednání jednotlivce. Osobní údaje mohou být také využity pro profilování jedince skrze kombinaci údajů o jeho návycích, zájmech a slabostech za účelem jeho následného ovlivnění při jednání, rozhodování či tvorbě názorů.

Údaje ale mohou také sloužit k vydírání či manipulaci vybraných jedinců. Zřejmě nejzávažnější formou zneužití osobních údajů je pak tzv. krádež identity, kdy dojde k neoprávněnému převzetí jedné či více významných virtuálních identit jedince, které umožní narušiteli neoprávněně jednat jménem oběti a na její účet bez možnosti snadného odhalení.

Z důvodu tohoto nerovného postavení mezi subjekty údajů a subjekty zpracovávajícími jejich osobní údaje je v zájmu ochrany před zmíněnými zásadními zásahy do základních práv a svobod dotčených osob namístě uložit těmto subjektům,1924 aby při nakládání s osobními údaji zohledňovaly a bilancovaly vlastní ekonomické či společenské zájmy s riziky a dopady do sféry dotčených fyzických osob.

Základní zásady zpracování osobních údajů

Zpracování musí probíhat zákonným, korektním a transparentním způsobem pro vymezený a legitimní účel, přičemž rozsah zpracovávaných údajů tomu musí být přiměřený a osobní údaje mají být pokud možno přesné, případně opravitelné. Ukládání osobních údajů je přípustné pouze po nezbytnou dobu danou účelem zpracování a při veškerém nakládání s osobními údaji je nutno klást důraz na zajištění jejich náležitého zabezpečení zejména před neoprávněným zneužitím či náhodným narušením.

Tyto zásady jsou však rozšířeny o podstatný prvek, který posouvá koncepci úpravy k formě regulované samoregulace. Tím je výslovné zakotvení odpovědnosti správce za dodržování základních zásad zpracování a požadavek jeho schopnosti tento soulad doložit.

Požadavky na zákonné zpracování osobních údajů

Je nutno posuzovat kombinaci tří aspektů nakládání s osobními údaji. Je nutno určit účel, pro který dochází ke zpracování, nalézt či zajistit právní základ daného zpracování a vymezit okruh dotčených osobních údajů, který musí být přiměřený tomuto účelu a podložený právním základem. Obecné právní základy jsou upraveny v článku 6 GDPR.

Zpracování může být oprávněno nezbytností pro plnění smlouvy se subjektem údajů. Jeho nezbytnost lze také nalézat v plnění právní povinnosti uložené správci nebo v plnění úkolu ve veřejném zájmu či výkonu veřejné moci pověřeným správcem. Obsah těchto dvou kategorií právních základů může případně blíže vymezovat právo členského státu.

V omezené míře lze za podklad vnímat i nezbytnost zpracování pro ochranu životně důležitých zájmů fyzické osoby či ochranu oprávněných zájmů správce či třetí osoby. V druhém zmíněném případě je však nutno zohledňovat poměřování se zájmy či základními právy a svobodami subjektu údajů, především pokud se jedná o dítě.

GDPR naopak roli souhlasu do jisté míry zesiluje, když zavádí zvláštní požadavky na souhlas u zpracování osobních údajů dětí (mladších 13–16 let, podle národní úpravy). Jádrem úpravy je

požadavek, aby správce při snaze o získání souhlasu při poskytování služby informační společnosti (např. sociální sítě, online prodej, online herní platformy apod.) vyvinul přiměřené úsilí odhalit, zda zpracovávané osobní údaje přísluší dítěti pod zmíněnou věkovou hranicí, a v případě takového zjištění zajistil souhlas se zpracováním od osoby s rodičovskou odpovědností.

Tímto ustanovením je sledován chvályhodný záměr, jelikož je zřejmé, že dítě nízkého věku si je méně vědomo možných rizik a důsledků nakládání s jeho osobními údaji, zvláště pokud jde o profilování, marketingové účely či služby cílící na děti.

Mohou tím však vznikat jiná dříve pominutelná rizika a překážky. Předně je nutné ze strany správce zvažovat přiměřenou míru profilování uživatele, aby zjistil jeho věk.

Výše popsané dosud nebralo zřetel na skutečnost, že zpracovávané osobní údaje mohou mít různě citlivý charakter. Již od sjednání úmluvy č. 108 je přijímáno, že určité specifické kategorie osobních údajů vyžadují přísnější režim zpracování, který poskytuje dodatečné záruky ochrany před jejich zneužitím. Jedná se o údaje, které se váží k citlivým, intimním aspektům osobnosti či jednání jedince, které lze vzhledem k různým režimům dle GDPR dělit na pět kategorií

Obecné povinnosti správce a zpracovatele

Druhou rovinou k těmto povinnostem je pak potřeba vytváření záznamů, které v případě potřeby umožní správci doložit vnitřní procesy posuzování a bilancování předvídané nařízením a které dokumentují zavedená opatření a zdůvodnění jejich vhodnosti.

Je předvídáno, že řada správců pro mnoho forem zpracování bude spoléhat na jiný subjekt, který představuje v tomto ohledu zpracovatele. Po správci je tudíž vyžadováno, aby posuzoval vhodnost těchto poskytovatelů a vstupoval s nimi do právního vztahu pouze na základě smlouvy (příp. jiného právního aktu), která upravuje základní parametry zpracování a vzájemných práv a povinností, jak blíže vymezeno v článku 28 GDPR. Zpracovateli tak touto formou vzniká sekundární odpovědnost za soulad zpracování s právní úpravou, kterou nese především vůči správci. Je současně povinen jednat v mezích jeho pokynů a smí do zpracování zapojit dalšího zpracovatele pouze na základě písemného svolení správce, přičemž tímto nemůže snížit úroveň požadovaných záruk a povinností stanovených mu správcem.

Zabezpečení zpracování osobních údajů

Velká část rizik zpracování je spojena s únikem osobních údajů mimo sféru vlivu správce či zpracovatele a jejich následným neoprávněným zneužíváním a šířením. Nosnou premisou právní úpravy ochrany osobních údajů zajišťující prevenci proti těmto narušením zabezpečení osobních údajů je, že pokud správce či zpracovatel zpracovává osobní údaje, musí tak činit při zavedení vhodných technických a organizačních opatření přiměřených rizikům, která se váží k jejich náhodnému či neoprávněnému úniku, změně, zničení či zpřístupnění. Výchozím bodem pro určení potřebné úrovně zabezpečení je posouzení zpracování co do jeho povahy, kontextu,

rozsahu a účelu. V následujícím kroku je pak příhodné načrtnout možné rizikové scénáře a roztřídit je s ohledem na dostupné informace podle stupně závažnosti a pravděpodobnosti. Kategorie narušení zabezpečení lze dělit podle tradičního přístupu informační bezpečnosti na zásah do důvěrnosti údajů, do dostupnosti údajů a do integrity údajů.

Ohlašování případů porušení zabezpečení osobních údajů

Povinnost ohlášení se odvíjí od zjištění, zda porušení má za následek riziko pro práva a svobody fyzických osob. Na rozdíl od jiných režimů posuzování rizik v rámci GDPR se zde řeší konkrétní důsledky reálně nastalého porušení. Pro určení míry rizika hrají roli kritéria zahrnující především: formu porušení; povahu, citlivost a množství dotčených osobních údajů; identifikovatelnost jednotlivce z dotčených údajů; předpokládanou závažnost dopadů na jednotlivce; možný dopad na děti či jiné zvlášť zranitelné kategorie subjektů údajů; odhadované množství dotčených osob či případné specifické postavení správce.

Správce má povinnost ohlásit porušení zabezpečení Úřadu pro ochranu osobních údajů zásadně bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl. Pokud porušení zjistí zpracovatel, je povinen o něm bez zbytečného odkladu informovat správce (Minimální požadovaný obsah ohlášení je stanoven v článku 33 odst. 3 GDPR).

Má-li porušení natolik závažnou formu, že hrozí vysoké riziko pro práva a svobody fyzických osob, je správce povinen bez zbytečného odkladu oznámit porušení zabezpečení dotčeným subjektům údajů. Oznámení není nutné, pokud byly údaje subjektu zajištěny opatřením, které je činí nesrozumitelnými při neoprávněném přístupu

Každý případ porušení zabezpečení osobních údajů musí být správcem zdokumentován, výše popsané ohlášení dozorovému orgánu však není povinné pro případy, kdy riziko pro práva a svobody dotčených subjektů údajů není pravděpodobné.

Záměrná a standardní ochrana osobních údajů

Smyslem záměrné ochrany osobních údajů je pak od úvodní fáze procesu zpracování účinně chránit osobní údaje, např. formou pseudonymizace. Tímto procesem je podoba údajů skryta převedením na nepřímé identifikátory, které vyžadují ke ztotožnění s fyzickou osobou dodatečnou informaci, která je za vhodných opatření uchovávána odděleně.

Pověřenec pro ochranu osobních údajů

Pověřenec pro ochranu osobních údajů plní v rámci operací správce či zpracovatele několik význačných rolí, které směřují ke zkvalitnění nakládání s osobními údaji. Předně se jedná o specializovaného konzultanta, který má hluboké odborné povědomí o právní úpravě i praxi ochrany osobních údajů, a má tedy radit a poskytovat informace jak správci či zpracovateli, tak zaměstnancům, kteří provádějí zpracování osobních údajů. Zároveň se jedná o formu interního kontrolního orgánu či „hlídacího psa“, který v zájmu subjektů údajů a v rámci garantované funkční nezávislosti a absence střetu zájmů monitoruje soulad činností daného povinného subjektu s požadavky právní úpravy. Zatřetí pak pověřenec funguje jako kontaktní bod pro dozorový úřad či případně pro dotčené subjekty údajů.

Tato funkce může být zřízena libovolným správcem či zpracovatelem, některé významné subjekty ji však musejí zřídit mandatorně. Případný jmenovaný pověřenec může být jak interní zaměstnanec, tak poskytovatel služby formou outsourcingu.

Práva subjektu údajů

Obecné povinnosti správce směřující k usnadnění uplatňování práv subjektu údajů. Ten na ně musí upozornit srozumitelným, stručným a transparentním způsobem, poskytnout náležitou součinnost k jejich realizaci a zásadně v měsíční lhůtě informovat subjekt o formě vyřízení jeho žádosti včetně odůvodnění.

Správce odpovídá za kontrolu oprávněnosti požadavků, jelikož poskytnutí informací (osobních údajů) o subjektu údajů neoprávněné třetí osobě na základě její žádosti představuje porušení zabezpečení zpracování osobních údajů.

Výchozím právem subjektu údajů je právo na informace. To má dvě formy, podle toho, zda jsou osobní údaje získány přímo od subjektu údajů nebo od třetí osoby. Při získávání údajů přímo od subjektu údajů je v podstatě nutné mu v okamžiku získání poskytnout přehled o základních parametrech užití údajů, tedy např. účelu zpracování, totožnosti a kontaktu na správce či okruhu dalších subjektů, kterým správce získané osobní údaje bude předávat.

Specifické právo na informace se vztahuje k profilování a automatizovanému individuálnímu rozhodování, o kterém je pojednáno v sekci patnácté této části. Subjekt údajů musí být předně důsledně informován o svých právech. Pro tyto účely bude zřejmě v převážné míře odkazováno na webové stránky správce poskytující tuto informaci.

Specifickou formou práva na kopii údajů, nově zavedenou GDPR, je právo na přenositelnost údajů. To se váže na ztíženou změnu poskytovatele informační služby v situacích, kdy je požitek ze služby vázán na soubor osobních údajů poskytnutý uživatelem (např. komunikační platformy sociálních sítí či jiné služby, kde významným prvkem je, že si uživatel vytváří specifickou virtuální identitu).

Vzhledem k tomu, že jednou ze zásad zpracování osobních údajů je požadavek jejich přesnosti a správnosti, má subjekt údajů také právo žádat opravu či doplnění nepřesných údajů. Současně dostalo v GDPR zakotvení judikaturně dovozené právo na výmaz (také označováno jako právo na zapomnění či právo být zapomenut). Jeho smyslem je možnost subjektu údajů domoci se v duchu

zásady minimalizace rozsahu a doby uchovávaných údajů odstranění osobních údajů, které již neslouží k přiměřenému či legitimnímu zpracování.

Právní ochrana subjektu údajů

Na podporu zmíněných práv a zmocnění jednotlivce k větší kontrole nad svými osobními údaji má subjekt údajů k dispozici prostředky právní ochrany. V první řadě jde o možnost obrátit se na dozorový orgán (především Úřad pro ochranu osobních údajů, ale případně i na orgán jiného členského státu) se stížností na porušení právní úpravy.2064 Tato stížnost má formu podnětu, ve zvlášť neupravených ohledech se tedy užije obecná úprava dle zákona č. 500/2004 Sb., správního řádu. Zde je také upravena procesní stránka ochrany před nečinností dozorového orgánu, kterou předvídá článek 78 GDPR. Ve srovnatelné formě přijímal a vyřizoval Úřad pro ochranu osobních údajů stížnosti dle dosavadní úpravy zákona č. 101/2000 o ochraně osobních údajů, v tomto směru tedy nedochází pro subjekt údajů k viditelným změnám. Subjekt údajů má mimoto právo i na účinnou soudní ochranu přímo proti správci či zpracovateli, který porušením nařízení zasahuje do jeho práv.

Činnost dozorového orgánu

Jelikož jde však v případě ochrany osobních údajů o veřejnoprávní úpravu, je její dodržování, bez ohledu na výše zmíněné nároky subjektu údajů, primárně vynucováno činností dozorového orgánu. Tím je již zmíněný Úřad pro ochranu osobních údajů, resp. ekvivalentní orgány jiných členských států. Působnost a pravomoci úřadu konkrétně upravuje národní legislativa, přesto lze v GDPR v článcích 51 až 59 dohledat obecné požadavky na úpravu členskými státy. Předně je vyžadována jeho nezávislost, dále je pak kladen důraz na spolupráci mezi úřady napříč Evropskou unií.

Zde stojí alespoň za zmínku role vedoucího dozorového úřadu. Tím je úřad příslušný pro jedinou nebo hlavní provozovnu správce či zpracovatele, přičemž ostatní dozorové úřady tento informují o stížnostech či řízeních proti danému subjektu a je na vedoucím dozorovém úřadu, aby rozhodl, zda se věcí bude primárně zabývat on či úřad oznamující.

Věci jsou zásadně řešeny na bázi spolupráce mezi dozorujícími orgány se snahou o jednotný postup a konsensus. Úřady tak vykonávají úkony na základě vyžádání úřadu z jiného členského státu, případně postupují v některých šetřeních či donucovacích opatřeních společně.

V rámci rozhodnutí či opatření s obecným dopadem je využíván mechanismus jednotnosti, kterým je především Evropský sbor pro ochranu osobních údajů, tedy útvar, který navazuje na fungování Pracovní skupiny podle článku 29 směrnice č. 95/46/ES (zjednodušeně označována WP29, z anglického Article 29 Working Party). Sbor je nově subjektem Unie s vlastní právní subjektivitou, jeho fungování se tedy oproti pracovní skupině formalizovalo a jeho pravomoci a působnost jsou rozšířeny. Podrobný popis však přesahuje možnosti této kapitoly.

Rozhodnutí o udělení správní pokuty je individuálním správním aktem, který je výsledkem správního řízení ve smyslu zákona č. 500/2004 Sb., správní řád, adresát má tedy možnost

instančního přezkumu v rámci činnosti Úřadu pro ochranu osobních údajů a případně následného přezkumu ve správním soudnictví podle zákona č. 150/2002 Sb., soudní řád správní. Nárok na právní přezkum vyplývá také přímo z ustanovení GDPR.

Vedle popsané funkce dozoru Úřad i nadále plní funkce vzdělávací, informativní a konzultační ve vztahu k oblasti ochrany osobních údajů. V GDPR je pak z těchto zdůrazňována především funkce iniciace a monitorování přípravy a dodržování odvětvových kodexů chování.

Nad rámec zmíněných rolí, které měl ve srovnatelné míře Úřad již na základě implementace směrnice 95/46/ES skrze zákon č. 101/2000 Sb., o ochraně osobních údajů, vyplývají z GDPR některé dodatečné pravomoci, které mají regulatorní povahu. Ty se týkají především nově zavedené koncepce mechanismů pro vydávání osvědčení o ochraně osobních údajů a zavedení pečetí a známek dokládajících soulad s požadavky nařízení. Ty mají být vydávány subjekty akreditovanými na základě prokázání nezávislosti, odborné znalosti a adekvátnosti vnitřních struktur a postupů.

Posouzení vlivu na ochranu osobních údajů

Pod pojmem profilování je zapotřebí vnímat libovolnou formu zpracování osobních údajů, které je prováděno automatizovaně a které současně spočívá v užití osobních údajů k hodnocení určitých osobních aspektů dotčených subjektů údajů. Za hodnocení je pak předně namístě považovat analýzu, klasifikaci či odhad nejrůznějších parametrů, sahajících od místa, kde se osoba nachází, přes její preference a zájmy až po její spolehlivost či pracovní výkonnost. Profilováním je tedy i prosté rozdělení osob podle pohlaví či věku, mnohem významnější jsou však pokročilé mechanismy, kterými za pomoci kombinace dostatečného množství zdánlivě běžných údajů (např. podrobné aktuální údaje o spotřebě elektrické energie v kombinaci s veřejně dostupnými údaji pro zjištění vybavení domácnosti a odhad ekonomické situace, příp. skrze dlouhodobé sledování polohy mobilního telefonu pro vyvození návyků a preferencí) lze získat intimní vhled do osobní sféry velkého množství fyzických osob.

> Profilování jako takové musí být na základě GDPR prováděno v souladu s požadavky na transparentnost, zákonnost, limitaci účelem, přesnost a minimalizaci údajů.

Předávání údajů do zemí mimo Evropskou unii

V rámci Evropské unie platí princip volného pohybu osobních údajů a smyslem GDPR rozhodně není omezovat toto směřování k jednotnému vnitřnímu digitálnímu trhu. S ohledem na požadavek zajistit adekvátní ochranu subjektům údajů z Evropské unie a absenci reálných hranic v

kyberprostoru je však nutné řešit záruky a omezení, které se vztahují na nakládání s osobními údaji, které se dostanou do sféry jiné země než členských států (např. jsou uloženy či zpracovávány na serverech, které se nacházejí mimo území Evropské unie, ačkoliv jde o údaje o fyzických osobách z Evropské unie).

Tyto nástroje lze zjednodušeně dělit na dvě kategorie. U první jde o činnost Evropské komise, která může na mezistátní úrovni vyjednávat a posuzovat obecnou úroveň ochrany určité třetí země a následně rozhodnout o odpovídající ochraně (dosud přijímaných dle článku 25 směrnice č. 95/46/ES, nově pak dle článku 45 GDPR).

Při absenci tohoto plošného nástroje pro předávání osobních údajů do třetí země jsou správci a zpracovatelé nuceni individuálně zajistit vhodné záruky, a to především pro vymahatelnost práv subjektů údajů a jejich účinnou právní ochranu.

Vedle standardních smluvních doložek mohou být vhodné záruky zajištěny právně závaznými a vymahatelnými nástroji mezi orgány veřejné moci, závaznými podnikovými pravidly, dodržováním schváleného kodexu chování, příp. osvědčeními na základě schváleného mechanismu, která obsahují vymahatelné závazky uplatňovat ve třetí zemi vhodné záruky a chránit práva subjektu údajů.

Specifické výjimky a zvláštní úprava

Je namístě zdůraznit, co již bylo zmíněno v úvodu tohoto pojednání o ochraně osobních údajů, tedy že právní rámec GDPR představuje pouze základní harmonizační předpis, často doplňován o specifickou úpravu. Tato specifická úprava je k nalezení mj. v připravovaném zákoně o zpracování osobních údajů a doprovodném zákoně, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů, které představují specifickou národní úpravu předvídanou GDPR. Jde především o zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu (s ohledem na svobodu projevu a informací),2142 přístup veřejnosti k osobním údajům v úředních dokumentech,2143 nakládání s národními identifikačními čísly (tedy s rodným číslem),2144 specifickým parametrům zpracování v rámci zaměstnaneckého poměru,2145 výjimek pro zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely,2146 zvláštní režim komplexních pravidel pro ochranu údajů uplatňovaných církvemi a náboženskými sdruženími2147 či zvláštní pravidla pro dozorovou činnost ve vztahu k subjektům podléhajícím služebnímu tajemství či srovnatelné povinnosti mlčenlivosti.

Významným alternativním režimem je pak především úprava ochrany osobních údajů a soukromí v prostředí elektronických komunikací. S ohledem na rozsah změn, které přináší GDPR, je i pro tuto oblast zapotřebí revize dosavadního režimu směrnice č. 2002/58/ES o soukromí a elektronických komunikacích .

Neopominutelnou odchylkou je pak nakonec již v na začátku zmíněný odlišný režim pro zpracování orgány veřejné moci za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů.

Právo elektronických komunikací

Právo elektronických komunikací

Historie

Ačkoli se samotný pojem začal vyvíjet už v dobách vzniku prvního telegrafu, samotné označení práva elektronických komunikací se začalo používat až od roku 2005, předchozím označením bylo právo telekomunikační. Zákon č. 151/1949 Sb., o Československé státní poště přinesl s účinností od 1. července 1949 zásadní změnu do telekomunikačního práva, jelikož dnem účinnosti tohoto zákona nabyl stát vlastnictví k telegrafním a telefonním zařízením připojeným na poštovní telekomunikační síť. Za zmínku stojí také, že v tomto zákoně zákonodárce poprvé použil pojem „telekomunikace“. V pozdějších dobách zákon o telekomunikacích zvýšil dohled a dozor státu v oblasti telekomunikací. Jak dále uvádí důvodová zpráva k návrhu zákona č. 72/1950 Sb., „Telekomunikační zařízení slouží účinně společnosti spějící k socialismu. Umožňují zvyšování produktivity práce a zvyšují životní úroveň pracujících.“, současně se však radioelektrická zařízení mohou též stát „nebezpečnou zbraní v rukou nepřátel lidu a jeho lidově demokratického státu, v rukou třídního nepřítele. Je proto třeba, aby telekomunikační zařízení byla v rukou státu, po případě aby jejich zřizování a provozování bylo státem řízeno.“. Po předpisech telegrafních tak následovaly normy telekomunikační, které teprve počátkem 21. století nahradila právní úprava elektronických komunikací.

Aktuální úprava elektronických komunikací

Základem aktuální právní úpravy elektronických komunikací stále zůstává původní předpisový rámec pro elektronické komunikace z roku 2002, který inicioval vznik základní právní normy práva elektronických komunikací na národní úrovni – zákona o elektronických komunikacích. Předpisový rámec tvořila rámcová směrnice doplněná čtyřmi zvláštními směrnicemi.

1. **Rámcová směrnice** (2002/21/ES): si kladla jako svůj cíl vytvoření harmonizovaného rámce regulace sítí a služeb elektronických komunikací, přiřazených zařízení a doplňkových služeb, vymezovala též definice pojmů, na které ostatní směrnice předpisového rámce odkazovaly, a stanovila základní úkoly národních regulačních orgánů

2. **Autorizační směrnice** (2002/20/ES) byla přijata s cílem harmonizovat a zjednodušit pravidla a podmínky pro udělování oprávnění v členských státech a tím vytvořit vnitřní trh v oblasti sítí a služeb elektronických komunikací. Mezi takovéto podmínky patřila např. práva na užívání rádiových frekvencí a čísel.

3. **Přístupová směrnice** (2002/19/ES) stanovila základy regulace přístupu k sítím elektronických komunikací a přiřazeným prostředkům a jejich vzájemného propojení, jejím cílem bylo dosažení trvalé hospodářské soutěže, interoperability služeb a prospěchu zákazníka.

4. **Směrnice o univerzální službě** (2002/22/ES) vymezila práva koncových uživatelů (vč. náležitostí smlouvy, informačních služeb, přenositelnosti čísel apod.) a stanovila jim odpovídající povinnosti podnikatelů zajišťujících sítě a poskytujících služby elektronických komunikací.

5. **Směrnice o soukromí a elektronických komunikacích** (2002/58/ES) navazovala na směrnici 95/46/ES a specificky pro oblast elektronických komunikací upravila zásady ochrany soukromí a osobních údajů.

K první dílčí změně předpisového rámce – úpravě směrnice o soukromí a elektronických komunikacích – došlo 15. března 2006 přijetím směrnice 2006/24/EES označované jako Data retention směrnice. Předmětem úpravy Data retention směrnice bylo založení povinnosti podnikatelů v sektoru elektronických komunikací uchovávat provozní a lokalizační údaje účastníků a uživatelů po dobu minimálně šesti měsíců pro účely jejich možného vyžádání orgány k tomu oprávněnými dle národních právních řádů. Kromě uvedených dílčích změn byl předpisový rámec, zejména s ohledem na technologický vývoj, několikrát novelizován, poprvé již po sedmi letech od svého schválení.

Regulace komunikačních činností

Regulaci pak zákon o elektronických komunikacích obecně vymezuje jako usměrňování činností a vztahů. Regulační činnosti dle něj zahrnují vydávání rozhodnutí, opatření obecné povahy a stanovisek a účelem takto vymezených činností je:

1. dosažení a udržení konkurenčního prostředí,

2. ochrana trhu elektronických komunikací,

3. ochrana uživatelů služeb elektronických komunikací.

Rámcová směrnice vymezuje také požadavky na vnitrostátní regulační orgány. Obecně směrnice zdůrazňuje požadavek technologicky neutrální regulace, vyhýbající se ukládání, či zvýhodňování použití konkrétního druhu technologie, leda by pro takovýto postup existovala odůvodněná potřeba (např. zvýšení účinnosti využití spektra). Přidělování rádiových frekvencí by však, obdobně jako přidělování národních číslovacích zdrojů, mělo být vždy založeno na objektivních, průhledných a nediskriminačních kritériích.

 # Regulační orgány vnitrostátní:

1. Český telekomunikační úřad (ČTÚ)

2. Úřad pro ochranu hospodářské soutěže (ÚOHS)

 # Regulační orgány EU:

1. Evropská komise

2. BEREC (The Body of European Regulators for Electronic Communications)

Práva a povinnosti podnikatelů, účastníků a uživatelů, ochrana spotřebitele

Rozsáhlou část úpravy práva elektronických komunikací, tedy i rozsáhlou část zákona o elektronických komunikacích, tvoří úprava práv účastníků a uživatelů a jim odpovídajících povinností podnikatelů, jakož i některých dalších povinností uložených podnikatelům. V praxi však řada povinností uložených poskytovatelům služeb ochraňuje nejen spotřebitele, ale jakéhokoli účastníka (resp. v některých případech též uživatele). Zákon o elektronických komunikacích vymezuje v Hlavě VII. přestupky, kterých se může dopustit jak právnická nebo podnikající fyzická osoba (v některých případech pouze subjekt se specifickým postavením – poskytovatel univerzální služby, podnik s významnou tržní silou apod.), tak rovněž nepodnikající fyzická osoba porušením povinností v zákoně stanovených. Přestupky projednává ČTÚ.

Ochrana údajů, bezpečnost sítí a služeb

Zákon o elektronických komunikacích věnuje zvýšenou pozornost otázkám bezpečnosti sítí a služeb elektronických komunikací a také zajištění důvěrnosti komunikací a ochraně osobních údajů, vč. údajů provozních a lokalizačních. Kromě obecné povinnosti zajišťovat bezpečnost a integritu své sítě a bezpečnost poskytovaných služeb ukládá zákon o elektronických komunikacích v zájmu zajištění bezpečnosti a integrity veřejných komunikačních sítí a bezpečnosti služeb elektronických komunikací podnikatelům zajišťujícím veřejnou komunikační síť a obdobně též poskytovatelům veřejně dostupných služeb elektronických komunikací také některé specifické povinnosti. Povinnosti poskytovatelů služeb vyplývající ze zákona o elektronických komunikacích zahrnují zejména:

1. zpracování vnitřního technicko-organizačního předpisu pro zajištění ochrany údajů a důvěrnosti komunikací,

2. informování dotčených účastníků o specifickém riziku porušení bezpečnosti sítě ve vztahu k ochraně údajů,

3. vytvoření vnitřních postupů pro vyřizování žádostí o přístup k osobním údajům uživatelů,

4. oznámení případů porušení ochrany osobních údajů ÚOOÚ a v případě závažnějšího porušení, naplňujícího kritéria stanovená zákonem, též oznámení těchto případů dotčené fyzické osobě.

Kyberkriminalita

Kyberkriminalita

Z hlediska práva lze tedy kyberkriminalitu zařadit do kategorie trestního práva, přičemž ji lze studovat z tří základních právních hledisek. Jednak z hlediska hmotněprávní úpravy, tedy z hlediska toho, co je za kyberkriminalitu považováno, jak jsou formulovány příslušné skutkové podstaty, na jaké aktivity se vztahují a jak jsou nastaveny trestní sazby. Z hlediska procesněprávního lze především posuzovat dostupnost a efektivitu procesních nástrojů, které trestněprocesní předpisy poskytují orgánům činným v trestním řízení k vyšetřování kyberkriminality, dopadení pachatele a zajišťování elektronických důkazů. A konečně z hlediska mezinárodního práva veřejného lze zkoumat limity mezinárodní justiční a policejní spolupráce při vyšetřování přeshraniční kyberkriminality a možnosti harmonizace právních úprav a implementace nových mechanismů pro mezinárodní součinnost a předávání důkazů.

Aktuální právní úprava kyberkriminality

Úmluva o počítačové kriminalitě představuje komplexní mezinárodní nástroj pro řešení problematiky kyberkriminality. Je rozdělena do čtyř kapitol, zahrnujících problematiku hmotného a procesního práva, stejně jako mezinárodní spolupráci.

Procesní část Úmluvy obsahuje úpravu procesních prostředků pro získávání a práci s elektronickými důkazy. Důvodem této harmonizace mimo jiné je, aby v rámci mezinárodní spolupráce měly signatářské státy jistotu, že dožadovaný stát bude disponovat vhodnými procesními prostředky pro realizaci vyžádaných úkonů. Tato část obsahuje nástroje jako:

– urychlené uchování uložených počítačových dat, neboli takzvaný freezing order, jímž mají být data u poskytovatelů služeb ochráněna před smazáním nebo změnou uživatelem, aby mohla být následně vyžádána jako důkazní prostředek;

– urychlené zachování a částečné zpřístupnění provozních dat, směřující ke stejnému cíli v případě provozních a lokalizačních údajů nezbytných pro identifikaci pachatele;

– příkaz k předložení, který orgánům činným v trestním řízení umožňuje požadovat od držitelů dat jejich poskytnutí pro potřeby trestního řízení;

– prohlídku a zajištění uložených počítačových dat, pro případ, kdy je nevhodné všechna data dožadovat a je efektivnější tato analyzovat přímo v zařízení nebo na datových nosičích poskytujících osob;

– shromažďování provozních dat v reálném čase, za účelem dohledání pachatele či důkazů o trestném činu; a

– odposlech obsahových dat prostřednictvím technických nástrojů umožňujících záznam obsahu elektronické komunikace.

■ porušení tajemství dopravovaných zpráv (§ 182 zákona č. 40/2009 Sb.

porušení tajemství listin a jiných dokumentů uchovávaných v soukromí (§ 183 zákona č. 40/2009 Sb.)

■ neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 zákona č. 40/2009 Sb.) ■ opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 zákona č. 40/2009 Sb.)

■ poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 zákona č. 40/2009 Sb.)

■ neoprávněné opatření, padělání a pozměnění platebního prostředku (§ 234)

■ výroba a držení padělatelského náčiní (§ 236

■ Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních

■ Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže

■ Balík zákonů upravující problematiku ochrany duševního vlastnictví

■ Zákon č. 127/2005 Sb., o elektronických komunikacích a jeho prováděcí vyhlášky

■ Zákon č. 480/2004 Sb., o některých službách informační společnosti

■ Nařízení EU č. 2016/679, obecné nařízení o ochraně osobních údajů

■ Zákony upravující právní povahu a nakládání s daty, elektronickými dokumenty, elektronickými podpisy apod.

Taxonomie kyberkriminality

Kyberkriminalita je z hlediska svých projevů velmi dynamickým fenoménem. Jak se rozvíjí informační komunikační technologie a vznikají nové způsoby jejich využívání a nové služby jejich prostřednictvím poskytované, vznikají také stále nové způsoby jejich zneužívání. Katalog aktivit, které lze považovat za kyberkriminalitu, tak nebude nikdy konečný – některé přestávají být díky novým bezpečnostním technologiím nebo zastaralosti postupů atraktivní, zatímco jiné vznikají a mechanismus jejich fungování třeba není dokonale zmapován.

Stíhání kyberkriminality

Odhalování, prověřování a vyšetřování kyberkriminality má svá specifika, díky kterým je nutné, aby orgány činné v trestním řízení disponovaly dostatečně kvalifikovaným personálem, který dokáže po technické stránce porozumět příslušným technologiím a volit takové procesní prostředky, které na jednu stranu umožní efektivní dohledání pachatele a zmapování příslušné trestné činnosti a na druhou budou v souladu procesní úpravou trestního řízení. Následující podkapitoly proto pojednávají o organizační připravenosti českých orgánů činných v trestním řízení pro řešení problematiky kyberkriminality a specificích trestního stíhání kyberkriminality z hlediska využitých procesních nástrojů a postupů.

Významným předpokladem pro efektivní zvládání kyberkriminality na straně orgánů činných v trestním řízení je dobrá orientace nejen v samotných technologiích, které jsou při páchání využívány, proti kterým je tato trestná činnost namířena, nebo které mohou představovat vhodný zdroj operativního nebo důkazního materiálu, ale také znalost procesních nástrojů, prostřednictvím kterých je možné přístup k relevantním datům a informacím získat.

Jelikož nelze aktuální procesní úpravu trestního řízení považovat za dokonalou a pro potřeby trestního řízení v případech kyberkriminality přívětivou, je často nutné za účelem dosažení kýžených výsledků pracovat s dostupnými nástroji poněkud kreativně. V podstatě v každém stadiu trestního řízení se objevují v případě kyberkriminality specifické prvky, v dalším výkladu se proto na ty významné zaměříme.

V případech kyberkriminality se velice často vyskytuje mezinárodní prvek, kdy se například pachatel nachází v jednom státě, informační systém, na který útočí nebo využívá k útoku, je v druhém státě a škoda vzniká ve třetím státě. V takových případech se předpokládá úzká spolupráce na mezinárodní úrovni mezi policejními a justičními orgány, která by navíc měla probíhat efektivně vzhledem k volatilitě elektronických důkazů. Existující mechanismy mezinárodní spolupráce v trestních věcech však často nejsou dostatečně efektivní, aby umožňovaly včasnou reakci na přeshraniční požadavky na realizaci procesních úkonů. Jelikož si tento stav mezinárodní společenství uvědomuje, vznikají různé nástroje směřující ke zefektivnění postupů. Ty zasahují jak do práva hmotného, tak procesního.

Elektronické důkazy

Jelikož je trestní řád i přes velké množství jeho novelizací poněkud zastaralým právním předpisem, je často nutné elektronické důkazní prostředky zajišťovat prostřednictvím nepříliš vhodných procesních nástrojů, použitých kreativně tak, aby pokryly i případy elektronických důkazních prostředků trestním řádem původně nezamýšlené. Proto jsou často elektronické důkazy zajištěny postupem v praxi netestovaným a legislativně a judikatorně nezachyceným, což vyvolává riziko, že by se mohl jeho prostřednictvím získaný důkaz stát v trestním řízení nevyužitelný. Jasné limity stanovuje § 89 odst. 3 zákona č. 141/1961 Sb., který za absolutně nepřípustný považuje takový důkaz, který byl získán nezákonným donucením. Důkazy však mohou být v trestním řízení absolutně či relativně neúčinné i z jiných důvodů – například v případě, že je orgánem činným v

trestním řízení zvolen nevhodný procesní prostředek k jejich zajištění. Takový postup totiž může být vyhodnocen jako podstatná vada postupu způsobující absolutní či relativní (může-li být taková vada odstraněna) neúčinnost získaných důkazů.

Druhým způsobem, kterým lze získat elektronické důkazy, je prostřednictvím dat získaných ze vzdálených úložišť nebo služeb. To lze opět provést několika způsoby. Prvním a nejjednodušším způsobem je získání informací volně dostupných v síti. Není-li překonáváno žádné bezpečnostní opatření, lze v podstatě bez dalšího přistupovat k obsahu dostupnému v prostředí internetu a pořizovat z něj důkazní prostředky.

Data, která mohou být neocenitelným zdrojem důkazů v trestním řízení, mohou být získávána také přímo od poskytovatelů informačních služeb. Při volbě procesního nástroje, prostřednictvím kterého budou data zajišťována, je třeba z hlediska trestního procesu zohlednit dvě základní hlediska.

Prvním hlediskem je charakter poskytovatele, od kterého data žádáme. Poskytovatelé informačních služeb se totiž dají rozdělit na dvě základní skupiny.

Získání elektronických důkazních prostředků je teprve prvním krokem v procesu dokazování prostřednictvím elektronických dat. Data jako taková mají díky svému charakteru jen minimální vypovídací hodnotu. Teprve ve chvíli, kdy jsou interpretována na informace, je možné začít hovořit o důkazu. Vzhledem k vlastnostem dat a elektronických zařízení je, jak je naznačeno výše, poměrně technicky náročné nejen vyhodnocovat jejich informační obsah, ale mnohdy jej i v sumě dat identifikovat. K těmto úkonům lze nicméně využívat více či méně technicky sofistikované nástroje pro forenzní analýzu.

Kybernetická bezpečnost

Kybernetická bezpečnost

Zavedení pojmu kybernetické bezpečnosti velmi dobře demonstruje samotný charakter práva jako normativního systému. V právu si tedy mimo jiné můžeme dovolit i konstrukci zcela nového fenoménu, který v reálném světě nemá obdobu – a to byl právě případ kybernetické bezpečnosti.

Počítačová bezpečnost nebo síťová bezpečnost představují dnes již tradiční obory aplikované kybernetiky. Kryptografie, která s těmito víceméně moderními disciplínami sdílí základní ideu, tj. ochranu dat.

Technické aspekty bezpečnostních řešení však představují jen jednu z komponent informační bezpečnosti. Dalšími součástmi obrazu informační bezpečnosti jsou aspekty etické, společenské, organizační či ekonomické. Uměle vytvořený regulatorní koncept kybernetické bezpečnosti si ve své české formě klade za cíl instrumentálně pokrýt především otázky technické a organizační.

Byť to může znít paradoxně, nepředstavuje hlavní problém regulatorního fenoménu kybernetické bezpečnosti skutečnost, že nic takového jako kybernetická bezpečnost vlastně reálně neexistuje. Daleko větším problémem je, že nevíme, co chápat pod pojmem „bezpečnost“.

Problém metaforičnosti pojmu bezpečnosti se vcelku výrazně projevuje například v ústavním právu. Zabýváme se otázkou, zda je příkladně vhodné v zájmu bezpečnosti zasahovat do lidské svobody, soukromí nebo vlastnictví. Posouzení je nadmíru složité či dokonce nemožné za situace, kdy není jasné, jaké konkrétní bezpečnostní výhody nám z příslušného omezení jiného práva vyplynou.

Pojmová neurčitost bezpečnosti se vedle ústavního práva projevuje třeba i v relativně nové oblasti mezinárodních vztahů označované jako kyberdiplomacie. Pokud totiž má být kybernetická bezpečnost předmětem mezinárodní spolupráce, je třeba příslušné nástroje stavět na stejné teleologii. Můžeme se tedy potýkat se skutečností, že různé národy si pod pojmem bezpečnosti mohou představovat něco úplně jiného.

Regulátorní koncept kybernetické bezpečnosti obsahově vyplněn i řadou dalších distributivních práv, která na první pohled nemusí mít s informačním životem člověka nic moc společného – může se totiž jednat o právo na spravedlivý proces, právo na zdraví, práva na práci apod. Všechna tato distributivní práva jsou součástí struktury kybernetické bezpečnosti proto, že jejich výkon je v důsledku penetrace společnosti informačními a komunikačními technologiemi v nějaké míře závislý na fungování informačních systémů nebo komunikačních sítí. Dostupnost služeb elektronických komunikací má tedy v dnešní době přímý vliv například na dostupnost zdravotní péče, sociálního zabezpečení nebo funkcionalit zajišťujících člověku důstojnou společenskou existenci.

Regulatorní fenomén kybernetické bezpečnosti lze řešit prakticky dvěma základními způsoby. První možností je taková kombinace technických a organizačních opatření, která ve výsledku zajistí identifikaci subjektu, který způsobil kybernetický bezpečnostní incident. Tento přístup můžeme sledovat například ve Spojených státech nebo v některých státech Jižní Ameriky a je nutně spojen s vyšší mírou expozice informačního soukromí v prostředí informačních sítí.

Právní úprava

Základem právní úpravy české kybernetické bezpečnosti je zákon č. 181/2014 Sb., který je proveden vyhláškami Národního bezpečnostního úřadu, resp. Národního úřadu pro kybernetickou a informační bezpečnost a Ministerstva vnitra. Do českého zákona č. 181/2014 Sb. je provedena i harmonizace prozatím jediného specializovaného sekundárního předpisu EU, kterým je směrnice (EU) č. 2016/1148 (směrnice NIS) a její prováděcí předpisy. Kybernetická bezpečnost však tvoří pouze část z právní úpravy informační bezpečnosti, resp. bezpečnosti informačních systémů a komunikačních sítí. Na bezpečnostní požadavky můžeme narazit i v dalších nespecifických odvětvích českého a evropského práva, jakými jsou například sektorová regulace elektronických komunikací nebo energetiky, úprava zdravotnické dokumentace, úprava bankovních a finančních služeb nebo obecná regulace ochrany osobních údajů nebo ochrany utajovaných informací. Všechny shora uvedené regulatorní nástroje jsou komplementární.

Povinné subjekty

Prvním okruhem otázek vyžadujících zvláštní pozornost je osobní působnost zákona č. 181/2014 Sb. Zákon v současné době pracuje s následujícími kategoriemi tzv. povinných subjektů:

– poskytovatel služby elektronických komunikací,

– subjekt zajišťující síť elektronických komunikací,

– orgán nebo osoba zajišťující významnou síť,

– správce informačního systému kritické informační infrastruktury,

– provozovatel informačního systému kritické informační infrastruktury,

– správce komunikačního systému kritické informační infrastruktury,

– provozovatel komunikačního systému kritické informační infrastruktury,

– správce významného informačního systému,

– provozovatel významného informačního systému,

– správce informačního systému základní služby,

– provozovatel informačního systému základní služby,

– provozovatel základní služby a

– poskytovatel digitální služby.

Všechny shora uvedené povinné osoby nemají ze zákona stejné postavení, ale zákon mezi nimi hierarchicky rozlišuje. Hierarchie daná důležitostí příslušné povinné osoby vzhledem k národní kybernetické bezpečnosti se projevuje i v kategorizaci povinných osob provedené § 3 zákona č. 181/2014 Sb. Zákon totiž u některých kategorií stanoví podmínku, že nespadají do některé hierarchicky vyšší. Logikou regulatorní hierarchie zákona lze tedy povinné subjekty rozdělit do následujících skupin:

– Kritická informační infrastruktura, tj. systémy a sítě nejvyšší důležitosti pro národní kybernetickou bezpečnost

– Významné sítě, tj. sítě provozované podle zákona o elektronických komunikacích

– Významné informační systémy, tj. vybrané informační systémy spravované orgány veřejné moci s vyšší mírou obecné důležitosti pro fungování státu nebo vyšší bezpečnostní expozicí.

– Základní služby, jejichž pojem zavádí směrnice NIS. Tato kategorie se týká základních společenských funkcionalit závislých na informačních sítích.

– Digitální služby jsou rovněž kategorií zavedenou směrnicí NIS. Poskytovatelé služeb spadající do této kategorie, tj. online tržiště, vyhledávače a poskytovatelé cloudových služeb.

– Služby a sítě elektronických komunikací, tj. činnosti spadající pod rozsah zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

Je to dáno vedle shora vyložené hierarchické struktury zákonných zájmů a z ní plynoucí míry zákonných povinností též potřebou stratifikace různých formálních rolí. V tomto smyslu rozlišujeme následující pojmy:

– správce systému nebo služby,

– provozovatel systému nebo služby,

– provozovatel základní služby,

– poskytovatel služby a

– subjekt, orgán nebo osoba zajišťující síť.

Obecné povinnosti – bezpečnostní opatření a bezpečnostní dokumentace

Jedním ze základních kamenů zákona o kybernetické bezpečnosti je požadavek na povinné osoby implementovat minimální standard zabezpečení příslušných systémů nebo sítí formou organizačních a technických opatření. Za tímto účelem zavádí zákon tzv. bezpečnostní opatření. Zákonná úprava bezpečnostních opatření je z legislativně-technického hlediska poněkud problematická, neboť nemá jednotnou terminologii ani systematiku. Některá bezpečnostní opatření tak jsou přímo zákonem definována kategoricky a velmi konkrétně, zatímco jiná mají jen velmi povšechnou zákonnou definici nebo diskutabilní normativitu. Týkají se totiž otázek vyložené technických, organizačních nebo i transakčních. Velká míra rozmanitosti bezpečnostních opatření je pro zákon č 181/2014 Sb. Z hlediska založení povinnosti k zavedení bezpečnostních opatření je klíčovým § 4 odst. 2 zákona č. 181/2014 Sb. Ve výše uvedené formulaci jsou klíčovými pojmy „zavést“ a „provádět“ označující povinnost nikoli pouze pořídit odpovídající zabezpečení nebo zavést organizační pravidla, ale také tato bezpečnostní opatření permanentně udržovat ve stavu odpovídajícím zákonným požadavkům. Této dichotomii odpovídá též specifická povinnost správců a provozovatelů systémů a sítí zařazených do kritické informační infrastruktury provádět kontrolu a audit příslušných bezpečnostních opatření založená § 5 odst. 2 písm. m) zákona č. 181/2014 Sb.

Dalším významným prvkem § 4 odst. 2 zákona č. 181/2014 Sb. je povinnost dokumentovat přijatá a prováděná bezpečnostní opatření. Zákon v tomto směru zavádí pojem bezpečnostní dokumentace a deleguje stanovení její mandatorní struktury na NÚKIB.

Operativní povinnosti – hlášení incidentů a opatření

Zákon o kybernetické bezpečnosti definuje v § 7 kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident následovně:

> (1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

> (2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti

> a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. Odlišení potenciality kybernetické bezpečnostní události a aktuality kybernetického bezpečnostního incidentu má samozřejmě pragmatický význam. Nevýhodou rozlišení mezi událostmi a incidenty je, na první pohled poněkud paradoxně, nižší efektivita přehledových a analytických operací na národní úrovni. Pokud tedy v zájmové infrastruktuře například dojde k výskytu masivního koordinovaného útoku, může mít vládní CERT problém s vyhodnocením jeho relevance a dopadu za situace, kdy je tento útok hlášen pouze částí povinných subjektů, tj. těmi s méně kvalitními bezpečnostními opatřeními. Podobně zkreslený pak může být obraz i z pohledu dalších bezpečnostních či policejních složek, typicky zpravodajských služeb nebo orgánů činných v trestním řízení.

Povinnost hlásit kybernetické bezpečnostní incidenty se u jednotlivých typů povinných subjektů realizuje následovně (opět využijeme namísto relativně složité zákonné struktury shora provedenou systematiku):

– Kritická informační infrastruktura, významné informační systémy a základní služby (resp. informační systémy základních služeb) hlásí všechny kybernetické bezpečnostní incidenty vládnímu CERT

– Významné sítě hlásí všechny kybernetické bezpečnostní incidenty provozovateli národního CERT (tj. v současné době CZ.NIC).

– Digitální služby hlásí pouze kybernetické bezpečnostní incidenty „s významným dopadem na poskytování […] služeb, pokud má [poskytovatel] přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu," a to provozovateli národního CERT.

– Služby elektronických komunikací nemají povinnost hlásit výskyt kybernetických bezpečnostních incidentů dle zákona č. 181/2014 Sb. (samozřejmě za předpokladu, že jejich poskytovatelé nebo správci sítí nespadají do některé z výše uvedených kategorií).

Varování

Varování je zákonnou formou jednostranného informování o tom, co zákon bez bližší definice označuje jako hrozbu v oblasti kybernetické bezpečnosti. Důvodem k vydání varování tedy může být libovolné zjištění o hrozícím narušení toho, co teorie informační bezpečnosti označuje za integritu, důvěrnost nebo dostupnost dat. Typickým příkladem hrozby zakládající právo a povinnost NÚKIB vydat varování může být odhalená bezpečnostní díra nebo tzv. exploit.

Reaktivní a ochranná opatření

Z hlediska použité regulatorní techniky se reaktivní a ochranná opatření zásadně liší od shora zmíněných varování. Jejich úprava v zákoně č. 181/2014 Sb. je totiž komplexní, tj. zákon definuje všechny jejich normativní parametry včetně rozsahu, formy nebo sankce. Z hlediska normativního tlaku zajišťujícího jejich efektivitu se tedy nemusejí tyto nástroje, na rozdíl od varování, spoléhat na systematické vazby k ostatním právním předpisům.

Dohledová pracoviště – CERT/CSIRT

K označení dohledových pracovišť se používají zkratky CSIRT (computer security incident response team) nebo CERT (computer emergency response team). Přestože se oba pojmy liší, jsou používány prakticky jako synonyma pro pracoviště, která vyhodnocují data o kybernetických bezpečnostních incidentech a obstarávají v závislosti na svém zařazení různé technické, forenzní, organizační či jiné bezpečnostní činnosti v rámci toho, co je označováno anglickým výrazem constituency (tj. příslušnost či působnost).

V českém právu kybernetické bezpečnosti je třeba řešit drobný terminologický problém, který vznikl v důsledku toho, že česká zákonná úprava předešla v čase směrnici NIS. Směrnice totiž používá výrazu CSIRT, zatímco zákon č. 181/2014 Sb. hovoří o CERT. Přestože směrnice nikde přímo tento termín nepoužívá, vžilo se pro dohledová pracoviště na úrovni členských států označení „národní CSIRT“. Terminologický oříšek pak spočívá v tom, že co je v hovorovém jazyce evropského práva kybernetické bezpečnosti označováno jako „národní CSIRT“, znamená v českém právu povětšinou „vládní CERT“.

Zákon č. 181/2014 Sb. rozeznává na národní úrovni dvě centrální dohledová pracoviště, a to již zmíněný vládní CERT a dále pak národní CERT. Vládní CERT je centrálním dohledovým pracovištěm pro Českou republiku a plní též většinu funkcí předpokládaných směrnicí NIS. Je zřízen jako odbor NÚKIB a jeho přímá působnost zahrnuje kritickou informační a komunikační infrastrukturu, základní služby a významné informační systémy. Znamená to, že správci nebo provozovatelé příslušných informačních systémů a sítí mají povinnost hlásit tomuto dohledovému pracovišti výskyt kybernetických bezpečnostních incidentů a být s tímto pracovištěm v kontaktu prostřednictvím povinně předávaných kontaktních údajů.

Skutečnost, že národní dohledové pracoviště, resp. jeho provozovatel, kterým je aktuálně CZ.NIC, není při své činnosti svázáno limity zákonných zmocnění, se projevuje i v řadě dalších aktivit majících obecně pozitivní vliv na bezpečnost české informační a komunikační infrastruktury. Provozovatel národního CERT tak na bázi open source úspěšně vyvíjí a distribuuje vlastní router pro domácí nebo firemní použití nebo vydává odborné publikace zaměřené na problematiku kybernetické bezpečnosti.2475 V neposlední řadě umožňuje soukromoprávní povaha národnímu CERT účast v mezinárodních soukromých nebo akademických sítích dohledových pracovišť, do nichž mají obvykle orgány veřejné moci nebo státní bezpečnostní složky z různých důvodů žádný nebo jen velmi omezený přístup.

Odpovědnost za kybernetický bezpečnostní incident

Problematika odpovědnosti za kybernetický bezpečnostní incident je v prvním plánu vcelku jednoduchá. Odpovídá samozřejmě ten, kdo takový incident zavinil. V případě úmyslného útoku je tedy v první řadě odpovědný pachatel a u incidentů způsobených nedbalostí jde odpovědnost za tím, kvůli jehož kvalifikovanému opomenutí incident nastal.

Problémem reálného fungování práva kybernetické bezpečnosti však je v případě úmyslných útoku ztotožnění pachatele, k němuž i kvůli přeshraničnímu charakteru tohoto typu kyberkriminality dochází jen relativně zřídka. U nedbalostně zaviněných kybernetických incidentů, kde viníka sice nebývá těžké najít, bývá obvykle obtížné prokázat mu minimálně nevědomou nedbalost – konkrétně skutečnost, že o incidentu a možnosti zabránit mu vědět měl a mohl (a byl toho objektivně schopen). V řadě případů je rovněž problém s prokazováním míry zavinění či spoluzavinění. Typicky jde o situace, kdy má incident komplexní charakter a podílí se na něm více různých faktorů (kromě selhání člověka to může být třeba ještě bezpečnostní díra, nepředvídaná činnost autonomního systému, nahodilé faktory běžného síťového provozu apod.).

Otázka odpovědnosti za kybernetický bezpečnostní incident různých nikoliv odborných profesí je extrémně komplikovaná tím, že často technicky velmi složitá zařízení běžně obsluhují uživatelé, u nichž nemáme důvod předpokládat ani elementární povědomost o souvisejících bezpečnostních hrozbách. Tato situace je samozřejmě paradoxní, neboť technicky složité či nebezpečné nástroje mohou obvykle být kvůli různým právním omezením svěřeny pouze do rukou náležitě kvalifikovaných lidí. V případě často extrémně složitých informačních a komunikačních technologií je ale míra jejich penetrace současnou společností taková, že se jevu, kdy člověk denně pracuje s věcí, o jejímž reálném fungování vůbec nemá potuchy, nelze ubránit.

Problematika specifické odpovědnosti za kybernetický bezpečnostní incident je vedle civilistických a pracovněprávních úvah též předmětem diskuse v souvislosti se specifickou správněprávní úpravou kybernetické bezpečnosti, o níž pojednává celá tato kapitola. Nabízí se totiž legislativně vcelku jednoduché řešení spočívající v definici základních bezpečnostních povinností uživatelů služeb informační společnosti a jejich zajištění odpovídající sankcí ve formě přestupku nebo správního deliktu analogicky například s úpravou provozu na veřejných komunikacích. Ozývají se dokonce názory žádající větší míru veřejné kontroly přístupu k informačním a komunikačním technologiím implicitně obsahujícím větší destruktivní potenciál obdobně, jako je zavedena například formou řidičských oprávnění nebo pilotních průkazů.

K právě uvedenému je však třeba poznamenat, že jsme v žádném demokratickém právním státě správní kontrolu přístupu ke službám informační společnosti nebo specifickou správní odpovědnost za shora popsanou technickou nedbalost doposud nezaznamenali. Důvodem je velmi delikátní otázka ústavní proporcionality, která by se vedle zásahu do vlastnického práva dotkla například i práva na informační sebeurčení, svobody projevu nebo práva na soukromý život (jehož součástí je právo komunikovat prostřednictvím služeb informační společnosti).

Nejistota ohledně rozsahu zbavení trestní nebo jiné odpovědnosti za použití aktivních protiopatření vede k tomu, že jednotlivci a korporace zajišťující kybernetickou bezpečnost pro soukromý i veřejný sektor se snaží, pokud možno, nebýt nikde vidět. Špičkový expert na problematiku informační bezpečnosti chránící důležitý veřejný zájem tak namísto společenského uznání musí kvůli nejistotě možného postihu obvykle tajit své pracovní zařazení, a to dokonce někdy i před svými známými nebo vlastní rodinou.