BEZPEČNOST ICT VE VNITŘNÍCH PŘEDPISECH A ŠKOLENÍ ZAMĚSTNANCŮ[*]

PAVEL LOUTOCKÝ[**], KAMIL MALINKA[***]

ABSTRAKT

Cílem tohoto článku je prezentovat návrh, průběh a výsledky experimentu, jehož cílem bylo zjistit, jak zaměstnanci společnosti reagují na události, které jsou vymezené v rámci interní bezpečnostní politiky. V tomto kontextu se zabýváme v úvodu článku zejména právní stránkou související obecně s řízením zaměstnanců zaměstnavatele s využitím interních předpisů a pokynů zaměstnavatele tak, abychom prezentovali související právní rámec, který by měl být nutným základem pro efektivní dodržování interních předpisů. V této souvislosti tak vymezíme samotný pojem interního předpisu a požadavky na něj kladené právem (v kontrastu s interním pokynem); posléze prezentujeme relevantní rozhodovací praxi českých soudů. To by mělo posloužit k bližšímu pochopení mechanismů a nástrojů, jakými zaměstnavatel může řídit své zaměstnance při výkonu jejich pracovní činnosti. Obecný právní rámec pak dáme do souvislosti s výsledky experimentu. Účelem je tak ověřit hypotézu, že přestože právo stanovuje požadavky, které klade na řízení zaměstnance, jedná se jen o stanovení obecného rámce (což není a priori špatně), nicméně v praxi pak mnohdy dochází k nedostatečné a nekonkrétní úpravě dané problematiky, která nepokrývá všechny potřebné souvislosti. Velmi důležitým aspektem při implementaci pokynů zaměstnavatele je totiž v praxi zejména skutečnost, jak informace

[*] Tento článek vznikl díky podpoře Masarykovy univerzity v rámci projektu Experimentální výzkum chování uživatelů ICT v oblasti bezpečnosti perspektivou sociálních věd, práva a informatiky (MUNI/M/1052/2013).

[**] Autor je prezenčním doktorským studentem na Ústavu práva technologií PrF MU. Kontaktní e-mail je loutocky@mail.muni.cz.

[***] Autor působí v Divizi výpočetní a úložné infrastruktury - Ústavu výpočetní techniky FI MU. Kontaktní e-mail je malinka@ics.muni.cz.

efektivně předat zaměstnancům, u kterých je vyžadováno, aby se chovali v souladu s bezpečnostní politikou (jak prezentujeme na našem experimentu) či obecně v souladu s interními přepisy a pokyny zaměstnavatele. A právě tato otázka není detailněji právním rámcem reflektována. Daný experiment proběhl v rámci pobočky brněnské společnosti zabývající se vývojem softwaru. Tato společnost má cca 300 zaměstnanců. Jedním ze zajímavých zjištění byla mimo jiné i reálná neúčinnost doposud používaných vzdělávacích videí pro školení zaměstnanců a naopak viditelný účinek personalizovaného přístupu.

KLÍČOVÁ SLOVA

řízení zaměstnance, vnitřní předpisy, vnitřní pokyny, povinnosti zaměstnanců, vnitřní bezpečnost, školení zaměstnanců

ABSTRACT

The target of this article is to present the proposal, progress and the results of the experiment, which aimed to find out how company employees respond to the situations that are defined within the internal security policy. In this context, we are focused in the beginning on the legal aspects related to the general control of the employees using internal regulations and instructions of the employer to present related legal framework, which should be a necessary basis for effective compliance with internal regulations of the employer. We define the very concept of the internal regulations and its requirements (in contrast with internal instruction); then we present relevant decisions of the Czech courts. This should serve for better understanding of the mechanisms and instruments with which the employer can control its employees in the performance of their work. We will then put general legal framework in the context with the results of the experiment. The purpose is thus to verify the hypothesis that although the law provides the requirements for the control of its employees, it is just a general framework (which is not a priori wrong), but in practice, it often leads to inadequate and vague regulation of the issue and it does not cover whole area. In practice, very important question connected to the implementation of the employer's instructions is how to present the information to the employees, who are required to behave in accordance with the security policy (as it is shown in our

experiment) or generally in coherence with internal regulations and instructions of the employer. Such issue is not reflected in detail by the legal framework. The experiment took place in the branch of the company located in Brno, Czech Republic, which is focused on software development. The company has about 300 employees. One of the interesting findings was amongst the others that the training videos were inefficient for staff training, and vice versa there was visible positive effect of personal approach.

KEYWORDS

control of the employee, internal regulations, internal instructions, employees' obligations, internal security, training of the employees

1. ÚVOD

Interní bezpečnostní politika je často upravena v rámci organizace soukromých společností, ale i veřejných institucí. Základním cílem bezpečnostní politiky je vymezení povinností, jakým způsobem nakládat s daty, s fyzickým majetkem, stanovit procesy pro potřeby řešení bezpečnostních incidentů, definovat role a odpovědnost v rámci organizace, atp.

Bezpečnostní politika může být stručná, ale i velmi komplexní sada nástrojů, která do různých úrovní detailu popisuje očekáváné chování zaměstnanců, ale i např. technické požadavky na konfiguraci prostředků pro elektronickou komunikaci, ukládání dat, šifrování či požadavky na fyzickou bezpečnost. V každém případě je zaměstnancům prezentována v podobě interních předpisů či pokynů zaměstnavatele tak, aby mohla být v případě porušení rovněž po konkrétním zaměstnanci vymáhána a bylo tak zajištěno požadované chování jednotlivců na pracovišti.

V řadě případů prochází interní bezpečnostní politika nezávislým auditem, který potvrdí její úplnost. Struktura interní bezpečnostní politiky je pak definována standardem ISO/IEC 27001.[1]

Součástí procesu tvorby a zavádění bezpečnostní politiky v organizaci je školení zaměstnanců. Právě školení je jedním z efektivních nástrojů, jak

[1] ISO/IEC 27001 - Information security management [online]. *ISO* [cit. 6. 9. 2016). Dostupné z: http://www.iso.org/iso/iso27001

prokazatelně zaměstnance s konkrétními povinnostmi ve vztahu k zaměstnavateli seznámit a naplnit tak specifické zákonné požadavky, ale i požadavky zaměstnavatele. To, že prokazatelně (a dle zákonných požadavků) zaměstnavatel seznámí zaměstnance s povinnostmi vyplývajícími z pracovního poměru vůči zaměstnavateli, však ještě neznamená, že zaměstnanec bude opravdu takové požadavky respektovat či se jimi vhodně řídit.

Školení je dlouhodobý proces, při kterém je potřeba zaměstnancům srozumitelnou formou sdělit v konkrétním případě obsah bezpečnostní politiky stanovený vnitřním předpisem a tuto znalost prohlubovat. Procesy stanovené bezpečnostní politikou lze dále rovněž pravidelně testovat a zaměstnancům tak vytvořit prostředí, jak konkrétní situace „zažít". Zde se dostáváme k podstatě našeho experimentu. Pro zaměstnance je bezpečnostní politika většinou „nutné zlo" a školení zůstává často bez většího dopadu na konkrétní a odborné znalosti zaměstnance. Je tedy dobré se zamýšlet nad formou školení, jeho délkou, četností a také nad dalšími akcemi, které zaměstnancům přiblíží informace ve skutečném pracovním procesu. Je rovněž ale vždy nutno pamatovat na stanovený právní rámec, který upravuje kontrolu nad zaměstnancem a plnění jeho pracovních povinností.

V tomto článku se nejprve zaměříme na požadavky, které klade zákoník práce[2] na to, aby mohly být pro zaměstnance interní pokyny a předpisy závazné a v případě jejich porušení mohly být činěny adekvátní kroky. Posléze právní požadavky srovnáme s experimentem, na čemž se pokusíme prezentovat, že v praxi jsou požadavky kladené zákoníkem práce nedostatečné a negarantují náležitou kvalitu chování zaměstnance.

2. VYBRANÉ PRÁVNÍ ASPEKTY ŘÍZENÍ ZAMĚSTNANCŮ

Specifickým rysem charakteristickým pro oblast pracovního práva je, že vedle právních předpisů jsou za pramen práva považovány rovněž kromě kolektivních smluv[3] též interní (vnitřní) předpisy a pracovní řád[4] (vnitro-

[2] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších přepisů (dále jen „zákoník práce" nebo „ZP").

podnikové právní akty)[5] vydávané zaměstnavatelem. Tak je tomu zejména v případě, kdy vnitřní předpis upravuje *„mzdová, platová práva či ostatní práva zaměstnance v pracovněprávních vztazích, nebo rozvádí ustanovení zákoníku práce* (zejména v otázkách pracovněprávních nároků – pozn. autor)*, popř. zvláštních právních předpisů podle zvláštních podmínek u zaměstnavatele.*“[6] Vnitřní předpis je chápán jako jednostranný akt zaměstnavatele, kterým ukládá konkrétní povinnost osobě podřízené.[7] Vnitřní předpis dopadá na nevymezený okruh adresátů (resp. je omezen generálně jen na osoby podřízené zaměstnavateli či vedoucímu zaměstnanci) a stanovuje zaměstnancům povinnosti více či méně konkrétně.[8]

Otázkou však je, zda lze za vnitřní předpisy považovat rovněž takové akty řízení,[9] které souvisí se samotnou organizací pracovních postupů. V daném případě se nemusí jednat jen o konkrétní pokyn zaměstnanci, ale lze uvažovat i o aktech upravujících organizační strukturu zaměstnavatele, které se vztahují na širší skupinu osob (například řád pro oběh listinných dokumentů, atd.), či pokyny upravující technologické postupy.[10] Bělina

---

[3] K pojmu kolektivních smluv a obecně k problematice kolektivního pracovního práva více viz například GALVAS, Milan a kolektiv. *Pracovní právo.* 2. dopl. a přeprac. vyd. Brno: Masarykova univerzita, 2015, 825 s. ISBN 9788021080218. S. 719 a násl.

[4] Pracovní řád je možno chápat jako podmnožinu spadající pod vnitřní předpisy. Pracovní řád se jako specifický druh vnitřního předpisu liší především povinností, který ze subjektů jej vydává, s odkazem na § 303 odst. 1 ZP. Smyslem pracovního řádu je pak bližší rozpracování povinností zaměstnanců, které jsou zakotveny obecně v zákoníku práce a případně pak v souvisejících právních předpisech. Neupravuje však otázky související s obsahem vnitřního předpisu ve smyslu § 305 ZP.

[5] BĚLINA, Miroslav a kolektiv. *Pracovní právo.* 6. doplněné a podstatně přepracované vydání. Praha: C.H. Beck, 2014, 464 s. ISBN 9788074002830. S. 49.

[6] Ibidem.

[7] JAKUBKA, Jaroslav. *Vnitřní předpisy zaměstnavatele.* 1. vyd. Praha: ASPI, 2008, 196 s. ISBN 9788073573966. S. 20.

[8] Ke konkrétnímu rozčlenění druhů vnitřních předpisů více viz zejména JAKUBKA, Jaroslav. *Vnitřní předpisy zaměstnavatele.* 1. vyd. Praha: ASPI, 2008, 196 s. ISBN 9788073573966. S. 23-24.

[9] Aktem řízení máme na mysli zejména pokyny vedoucího zaměstnance či přímo zaměstnavatele. Vedoucí zaměstnanci jsou tak *„oprávněni stanovit a ukládat podřízeným zaměstnancům pracovní úkoly, organizovat, řídit a kontrolovat jejich práci a dávat jim k tomu účelu závazné pokyny.*“ § 11 ZP.

[10] HŮRKA, Petr a kolektiv. *Pracovní právo*. 2. upravené vydání. Plzeň: Aleš Čeněk, 2015, 575 s. ISBN 9788073805401. S. 102.

a Drápal k tomu uvádí, že *„vzhledem k tomu, že se právně jedná víceméně o akty řízení vyplývající z postavení nadřízenosti zaměstnavatele vůči zaměstnanci, lze se domnívat, že nikoli.“*[11] Daná kategorie aktů řízení spadá totiž svým charakterem pod individuální a individualizované pokyny zaměstnavatele (§ 301 a násl. ZP) a není důvod, aby na takové akty dopadaly náležitosti nezbytné pro vydání vnitřního předpisu, což ovšem není vyloučeno.[12] Kdyby tomu bylo jinak, uvádíme, že by to mimo jiné *de facto* znamenalo, že každý pokyn nadřízeného vůči podřízenému by musel být vydán písemnou formou tak, jak požaduje § 305 ZP pro vydání vnitřního předpisu.[13] To by v daném případě vedlo k absurdním situacím a zásadním způsobem omezovalo řízení a nutnou flexibilitu v rámci organizační struktury zaměstnavatele zejména v případě alespoň částečné individualizace pokynu. Je nutno vždy odlišovat konkrétní způsob, jak zaměstnance instruovat o jeho povinnostech vůči zaměstnavateli; tedy mezi „obecnými“ vnitřními předpisy a individualizovanými (interními) pokyny. V našem případě je však třeba zdůraznit, že interní bezpečnostní směrnice vydaná zaměstnavatelem (kterou se zabýváme v rámci experimentu) se vztahuje na neindividualizovanou skupinu zaměstnanců a svým charakterem tak spadá pod vnitřní předpis ve smyslu § 305 ZP.

Na základě § 4a odst. 2 a především § 305 ZP je v souvislosti s vydáním vnitřního předpisu možno odchýlit se od obecné zákonné úpravy a specifikovat vzájemné pracovněprávní vztahy vnitřním předpisem, který musí být dle zákoníku práce vydán písemně.[14] Je však třeba respektovat to, že vnitřním předpisem (a rovněž tak kolektivní smlouvou[15] či pracovněprávní

[11] BĚLINA, Miroslav, Ljubomír DRÁPAL a kolektiv. *Zákoník práce. Komentář*. 2. vydání. Praha: C.H. Beck, 2015, 1610 s. ISBN 9788074002908. S. 1184.

[12] Obdobně lze dovodit i z důvodové zprávy, kde je u vydání vnitřního předpisu uvedeno jen, že *„bude upravovat mzdová nebo platová práva včetně úpravy pracovních podmínek v pracovněprávních vztazích.“* Důvodová zpráva k zákonu č. 262/2006 Sb., zákoník práce. Sněmovní tisk 1153/0, část č. 1/8 [online]. Poslanecká sněmovna Parlamentu České republiky [cit. 15. 7. 2016). Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?O=4&CT=1153&CT1=0. S. 269-270.

[13] K tomu srov. například rozsudek Nejvyššího soudu ze dne 4. 9. 2012, sp. zn. 21 Cdo 2141/2011.

smlouvou mezi zaměstnancem a zaměstnavatelem) nelze zaměstnanci stanovit režim přísnější,[16] než jaký stanovuje zákon.[17]

Pro vnitřní předpis je pak stanoveno, že „*musí být vydán písemně, nesmí být v rozporu s právními předpisy ani být vydán se zpětnou účinností, jinak je zcela nebo v dotčené části neplatný.*“[18] Vydává se na dobu určitou, a to nejméně na dobu jednoho roku.[19] Po jeho vydání musí být zaměstnavatelem vnitřní předpis náležitě vyhlášen. Zákoník práce blíže nespecifikuje, jakým způsobem musí být vnitřní předpis vyhlášen. Lze se ale oprávněně domnívat, že vyhlášení musí být učiněno tak, aby se s ním měl zaměstnanec možnost seznámit obvyklým způsobem. Je pak již zcela na zaměstnavateli, jestli interní pokyn pouze například vyvěsí na místě obvyklém a k tomu určeném nebo proškolí své zaměstnance prostřednictvím pověřené osoby či formou zcela odlišnou (např. formou prezentace s lektorem, formou nahraných video-prezentací, dotazníků, atp.). Konkrétnější požadavky pak zákoník práce nestanovuje. Podstatné je, že zaměstnanec musí být s takovým interním aktem náležitě seznámen. To však dále nikterak negarantuje, že se s interním předpisem zaměstnavatel seznámil natolik, že jej bude schopen i vhodně a náležitě dodržovat.[20]

O vydání, změně či zrušení vnitřního předpisu pak zaměstnavatel své zaměstnance musí seznámit do 15 dnů od dne, kdy tak učinil, a pro za-

---

[14] „*Zaměstnavatel může vnitřním předpisem stanovit práva v pracovněprávních vztazích, z nichž je oprávněn zaměstnanec, výhodněji, než stanoví tento zákon. Zakazuje se, aby vnitřní předpis ukládal zaměstnanci povinnosti nebo zkracoval jeho práva stanovená tímto zákonem.*“ § 305 odst. 1 ZP.

[15] „*Vnitřní předpis má nižší právní sílu než kolektivní smlouva.*“ BĚLINA, Miroslav a kolektiv. *Pracovní právo.* 6. doplněné a podstatně přepracované vydání. Praha: C.H. Beck, 2014, 464 s. ISBN 9788074002830. S. 49.

[16] „*Odchylná úprava práv nebo povinností v pracovněprávních vztazích nesmí být nižší nebo vyšší, než je právo nebo povinnost, které stanoví tento zákon nebo kolektivní smlouva jako nejméně nebo nejvýše přípustné.*“ § 4a odst. 1 ZP.

[17] K tomu obdobně více viz JAKUBKA, Jaroslav. *Vnitřní předpisy zaměstnavatele.* 1. vyd. Praha: ASPI, 2008, 196 s. ISBN 9788073573966. S. 17.

[18] § 305 odst. 2 ZP.

[19] „*Vnitřní předpis týkající se odměňování může být vydán i na kratší dobu.*“ § 305 odst. 2 ZP.

[20] V případě porušení pak odkazujeme na další kapitolu tohoto článku, kde uvádíme konkrétní judikaturu v souvislosti s tím, kdy lze využít sankčních mechanismů vedoucích až například k ukončení pracovního poměru.

městnance je pak závazný ode dne, kdy se s ním v souladu s § 301 písm. c) ZP měl zaměstnanec povinnost seznámit. „*Vnitřní předpis musí být přístupný všem zaměstnancům zaměstnavatele a navíc má zaměstnavatel povinnost uschovat vnitřní předpis po dobu 10 let ode dne ukončení jeho platnosti.*“[21] Konkrétnější úpravu interního předpisu pak již samotný zákoník práce dále nerozvádí. Vnitřní předpis, který splňuje výše uvedené náležitosti, je pro zaměstnance závazný a ten se jím musí řídit.

2.1 ŘÍZENÍ ZAMĚSTNANCŮ Z POHLEDU ROZHODOVÁNÍ SOUDŮ

V rámci této kapitoly bude daná problematika související s řízením zaměstnance prostřednictvím vnitřních předpisů (ale i pokynů) dále rozvedena s využitím konkrétní rozhodovací praxe českých soudů, čemuž předcházela komplexní rešerše relevantní judikatury související se závazností interních předpisů a pokynů zaměstnavatele. Účelem je tak blíže čtenáři představit a vymezit danou problematiku a její dopady v praxi a prezentovat dostupné právní mechanismy, které může zaměstnavatel využít v případě, kdy dojde k porušení vnitřního předpisu nebo jeho pokynu.

Pracovní povinnosti jsou zaměstnanci stanoveny právními předpisy, vnitřním předpisem, pracovní smlouvou nebo přímo pokynem nadřízeného vedoucího zaměstnance. Jednotícím kritériem pro všechny druhy těchto povinností pak je, že vyplývají z pracovního poměru nebo jiného pracovněprávního vztahu k zaměstnavateli. Zaměstnavatel pak může po zaměstnanci požadovat plnění z pracovněprávních vztahů jen tehdy, stanoví-li to právní předpisy a jen za podmínek právními předpisy zakotvených.[22] Vnitřní předpis, kterým je konstituován nárok na plnění zaměstnancem, ačkoliv to obecně závazné právní předpisy neumožňují, je proto nutno považovat za

[21] BĚLINA, Miroslav, Ljubomír DRÁPAL a kolektiv. *Zákoník práce. Komentář*. 2. vydání. Praha: C.H. Beck, 2015, 1610 s. ISBN 9788074002908. S. 1187.

[22] V konkrétním případě byl pak zaměstnanec povinen hradit „adaptační příspěvek“, který byl financován ze mzdových nákladů, což bylo shledáno jako poškozující zaměstnance a v rozporu se zákonem. Rozsudek Nejvyššího soudu ze dne 23. 9. 2004, sp. zn. 21 Cdo 1040/2004. Přestože nejen toto rozhodnutí se dotýká ustanovení zakotvených ve zrušeném zákoníku práce (zákon č. 65/1965 Sb., ve znění pozdějších předpisů), vycházíme z premisy, že konkrétní interpretace jsou obdobně aplikovatelné rovněž na ustanovení zakotvená zákoníkem práce vzhledem k jejich sledovanému účelu.

neplatný a v rozporu se zákonem.[23] Předpisy vydané v rámci obecně závazných předpisů a na jejich podkladě (např. právě interní předpisy zaměstnavatele), jsou pak zaměstnanci povinni dodržovat jen tehdy, jestliže s nimi byli řádně seznámeni. Jednotícím kritériem pro všechny druhy pracovních povinností vyplývajících z pracovněprávního vztahu, jejichž porušení může být důvodem k rozvázání pracovního poměru, tedy je, že může jít jen o povinnosti stanovené právními předpisy nebo o právní povinnosti stanovené v jejich rámci. Konkrétní způsob seznámení se s interními předpisy není zákonem stanoven jinak, než že je nutno tak učinit obvyklým způsobem.[24] Vhodné mechanismy a způsoby tak právní úprava zcela ponechává na zaměstnavateli, u kterého důvodně předpokládá, že právě on je tím, kdo je schopný nejlépe kontrolovat své zaměstnance a má nejlepší předpoklad pro to, aby zvolil odpovídající nástroj.

Zaměstnanci jsou tak povinni plnit závazky, které jim byly uloženy (mj.) vnitřním předpisem nebo pokynem nadřízeného vedoucího zaměstnance. Nesplnění povinností z těchto smluvně převzatých závazků představuje porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci a mohou být tedy důvodem k rozvázání pracovního poměru.[25] Nelze však vycházet pouze z konkrétních zákazů (pokynů) a z v interních předpisech obecně stanovených povinností, které ukládají zaměstnancům závazky, ale rovněž ze závazků morálních a etických.[26] Porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci je ovšem výpovědním důvodem jen tehdy, bylo-li zaměstnancem zaviněno, a to úmyslně, vědomou nedbalostí nebo alespoň z nevědomé nedbalosti. Zaměstnanec pak odpovídá jen za takovou škodu, kterou skutečně způsobil on sám v přímé souvislosti s porušením pracovních povinností při plnění stanovených úkolů.[27] Není

[23] Rozsudek Nejvyššího soudu ze dne 22. 3. 2001, sp. zn. 21 Cdo 249/2000.

[24] Rozsudek Nejvyššího soudu ze dne 26. 10. 2006, sp. zn. 21 Cdo 182/2006.

[25] Rozsudek Nejvyššího soudu ze dne 17. 12. 2009, sp. zn. 21 Cdo 3323/2008 nebo rozsudek Nejvyššího soudu ze dne 21. 3. 2013, sp. zn. 21 Cdo 742/2012.

[26] Rozsudek Nejvyššího soudu ze dne 15. 12. 2011, sp. zn. 21 Cdo 3178/2010.

tak odpovědný za škodu, kterou způsobila třetí osoba či jiný zaměstnanec nebo dokonce sám zaměstnavatel.[28]

Zejména na základě ustanovení § 2 odst. 1 a dle § 301 a násl. ZP jsou zaměstnanci povinni plnit pokyny zaměstnavatele a vedoucích zaměstnanců.[29] Zaměstnanci jsou však povinni plnit jen takové pokyny, které nejsou v rozporu s právními předpisy.[30] Co se týče formy samotného pokynu, není relevantní, byl-li učiněn písemně nebo ústně, bez ohledu na svoji intenzitu (expresivnost), anebo na to, do jaké míry odpovídá jeho obsah pravidlům společenských konvencí. Pokyny[31] nelze chápat jako nějaké formalizované abstraktní poučování o pravidlech chování v situacích, které teoreticky mohou (ale nemusí) v budoucnu nastat (tedy nelze je chápat jen jako generalizovaná pravidla). Je nutno je rovněž chápat jako „*praktickou reakci, jejímž smyslem je usměrnit jednání podřízených tak, aby se vyhnuli možnému nebezpečí, které by v průběhu výkonu práce při jiném způsobu chování mohlo jinak reálně hrozit.*“[32] Závaznost a závažnost daného pokynu je ale třeba vždy poměřovat v souvislosti s konkrétní situací. Zaměstnanec si však pokyny uložené mu nadřízeným musí ověřovat jen tehdy, kdyby mu taková povinnost ověřovat pokyny nadřízeného byla uložena přímo pracovní smlouvou nebo vnitřním přepisem (či případně pokynem nadřízeného vedoucího zaměstnance).[33]

---

[27] „*Výše požadované náhrady škody způsobené z nedbalosti nesmí přesáhnout u jednotlivého zaměstnance částku rovnající se čtyřapůlnásobku jeho průměrného měsíčního výdělku před porušením povinnosti, kterým způsobil škodu.*“ § 257odst. 2 ZP.

[28] Rozsudek Nejvyššího soudu ze dne 18. 3. 2014, sp. zn. 21 Cdo 1245/2013 a rozsudek Nejvyššího soudu ze dne 26. 8. 2014, sp. zn. 21 Cdo 1174/2013.

[29] Vedoucím zaměstnancem je takový zaměstnanec, „*kterému je na základě pověření zaměstnavatele podřízen nejméně jeden další zaměstnanec, jemuž je v rozsahu pověření oprávněn průběžně a soustavně stanovit a ukládat pracovní úkoly, organizovat, řídit a kontrolovat jeho práci a dávat mu k tomu účelu závazné pokyny.*“ Rozsudek Nejvyššího soudu ze dne 19. 1. 2004, sp. zn. 21 Cdo 1527/2003.

[30] Rozsudek Nejvyššího soudu ze dne 15. 7. 2008, sp. zn. 21 Cdo 4467/2007 nebo obdobně rozsudek Nejvyššího soudu ze dne 18. 6. 2008, sp. zn. 21 Cdo 2991/2007.

[31] V konkrétním případě byly pokyny vztažené na zajištění bezpečnosti a ochrany zdraví při práci.

[32] Rozsudek Nejvyššího soudu ze dne 14. 8. 2014, sp. zn. 21 Cdo 2886/2013 a rozsudek Nejvyššího soudu ze dne 4. 9. 2012, sp. zn. 21 Cdo 2141/2011.

[33] Rozsudek Nejvyššího soudu ze dne 24. 10. 2001, sp. zn. 21 Cdo 3077/2000.

Zaměstnanec je dále na základě § 301 a násl. ZP povinen dodržovat povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci.[34] Porušením takové povinnosti se pak rozumí zaviněné porušení pracovních povinností, které jsou zaměstnanci stanoveny právními předpisy, smlouvou, interním předpisem či přímým pokynem nadřízeného.[35] Dané povinnosti však jednotně vyplývají ze zaměstnaneckého poměru.[36] Stanovení porušení takových povinností interním předpisem ale není pro soud závazné; ten vždy posuzuje rozpor chování zaměstnance komplexně v rámci zákonných ustanovení a v souvislosti s intenzitou, s jakou k porušení takových povinností došlo.[37]

2.2 PRÁVNÍ ÚPRAVA A ZKUŠENOSTI Z PRAXE

Z výše řečeného lze vyvodit, že právní úprava definuje nutné náležitosti pro řízení zaměstnance ve formě interních předpisů a případně pokynů. Konkrétněji pak specifické mechanismy neupravuje a dané ponechává ryze na zaměstnavateli. To ale (jak se snažíme prokázat dále) zapříčiňuje, že v rychle se rozvíjejících oblastech (a to konkrétně v oblasti informačních technologií), kde je nutno na případnou problematiku reagovat rychle, zákonné požadavky zcela neposkytují dostatečné mechanismy pro zaměstnavatele, jak efektivně respektovat jeho konkrétní (a rychle nabývající) požadavky zaměstnavatelem. Zákon by dle našeho názoru měl klást větší důraz na preventivní mechanismy (jak zaměstnance vhodně seznámit s interními předpisy), než na mechanismy sankční (které i na základě dostupné judikatury považujeme za již poměrně dobře rozvinuté). A právě oblast ICT bezpečnosti (která nám dále slouží pro konkrétní experiment) je v tomto velmi specifická, protože např. i odborníci na bezpečnost nejsou často schopni odolat některým specifickým nástrahám. Proto je cesta od vydání

[34] Tento pojem byl ve starém zákoníku práce označován jako „pracovní kázeň".

[35] Ústavní soud zdůraznil, že v zájmu zaměstnavatele je rozvést základní práva a povinnosti v interních předpisech a konkretizovat je zde. Nález Ústavního soudu ze dne 23. 11. 1999, sp. zn. II. ÚS 324/99.

[36] Rozsudek Nejvyššího soudu ze dne 6. 2. 2007, sp. zn. 21 Cdo 212/2006.

[37] Srov. rozsudek Nejvyššího soudu ze dne 19. 1. 2000, sp. zn. 21 Cdo 1228/99, rozsudek Nejvyššího soudu ze dne 14. 2. 2001, sp. zn. 21 Cdo 971/2000 a rozsudek Nejvyššího soudu ze dne 7. 4. 2009, sp. zn. 21 Cdo 896/2008.

instrukce týkající se „bezpečného chování“ k její samotné implementaci a k zajištění adekvátního chování zaměstnanců velmi dlouhá. Je nutné si uvědomit významnost té části, která se primárně zaměřuje na vysvětlení potřebných zásad chování zaměstnanců, jež si mohou, ale také nemusí uvědomovat, že nemají dostatečné znalosti, aby odolali všem bezpečnostním hrozbám, ale chtějí se chovat korektně. Experiment, který popisujeme v další části, lépe ukazuje tato specifika.

Pro úplnost, dalším souvisejícím problémem, kterému se věnoval Polčák, Říha a Malinka,[38] a z toho důvodu jsme jej již dále nerozváděli, je problém úplnosti a závaznosti směrnice versus její čitelnost. Aby byla vnitřní pravidla závazná, je třeba, aby byla úplná, což často vede ke znečitelnění celého textu a následně k jeho problematické interpretaci.

3. POPIS EXPERIMENTU

Experiment proběhl v rámci pobočky brněnské společnosti zabývající se vývojem softwaru. Tato společnost má cca 300 zaměstnanců. Vzhledem k tomu, že IT je hlavní oblastí podnikání společnosti, jejím jasným cílem je zaručit bezpečné IT prostředí. Proto je existující bezpečnostní politika doplněna mimo jiné o aktivní práci se zaměstnanci.

Konkrétní experiment probíhal ve spolupráci se společností už ve fázi přípravy. Před začátkem experimentu ve společnosti probíhala školení bezpečnostní politiky formou krátkých videí, která byla tematicky zaměřená na jednotlivé oblasti interní bezpečnostní politiky, a to zejména těch oblastí, se kterými se běžní zaměstnanci setkávají nejčastěji. Bezpečnostní politika je stanovena vnitřním předpisem organizace.

Proškolování zaměstnanců formou krátkých videí probíhalo každých 6 měsíců a bylo povinné. Každé z celkem šesti videí bylo přibližně osm minut dlouhé a na konci videa byl krátký kvíz, kdy zaměstnanec označil jednu z nabízených odpovědí. Pokud zaměstnanec správně odpověděl, bylo pro-

[38] POLČÁK, Radim, Zdeněk ŘÍHA a Kamil MALINKA. Právní aspekty interních směrnic – část I. *Data Security Management*, Praha: TATE International s.r.o., 2015, roč. 19, č. 2, s. 36-39. ISSN 12118737, nebo POLČÁK, Radim, Zdeněk ŘÍHA a Kamil MALINKA. Právní aspekty interních instrukcí – část II. *Data Security Management*, Praha: TATE International s.r.o., 2015, roč. 19, č. 3, s. 36-39. ISSN 12118737.

školení zaznamenáno jako úspěšné. Celkově tedy každý zaměstnanec strávil školením cca jednu hodinu každých šest měsíců.

V rámci změn ve způsobu proškolování zaměstnanců ve společnosti jsme navrhli tři různé formy školení:

1. forma stávajících videí;
2. forma prezentace osobou z IT/bezpečnostního týmu;
3. forma zaslání bezpečnostní politiky e-mailem k pročtení.

Stávající forma videí zůstala po nějakou dobu zachována, než byly společností připraveny prezentace se stejným obsahem, jako ve videích. Časově byla prezentace naplánována na 60 minut, abychom dodrželi přibližně stejný čas, který zabere zhlédnutí videí.

Poté co byly nové materiály připraveny, proběhly následující změny ve školení zaměstnanců. Abychom mohli zhodnotit efektivitu jednotlivých forem školení, zaměřili jsme se pouze na skupiny nově nastoupivších zaměstnanců:

1. ve druhém kvartálu v roce (Q2) byli noví zaměstnanci školeni formou videí;
2. ve třetím kvartálu v roce (Q3) byli zaměstnanci školeni formou prezentace;
3. ve čtvrtém kvartálu v roce (Q4) obdrželi zaměstnanci pouze e-mail s informací, kde lze bezpečnostní politiku (v textové formě) najít, pokud by si ji chtěli přečíst (zaměstnancům byl odeslán odkaz na interní směrnici). Neprobíhala tak žádná dodatečná forma školení, jako tomu bylo v prvních dvou případech.

Časovým rozdělením nových zaměstnanců vznikly 3 výše popsané skupiny, z nichž každá obsahovala přibližně 20-30 osob.

Pro potřeby zhodnocení efektivity výše uvedených forem školení jsme jako následný krok navrhli simulaci dvou reálných situací, se kterými se zaměstnanci mohou běžně setkat:

1. řízená interní phishingová kampaň;
2. neohlášená vzdálená instalace softwaru na pracovní počítač.

V průběhu těchto simulací byly zaznamenávány reakce zaměstnanců.

Řízená phishingová kampaň byla navržena tak, že všem novým zaměstnancům z Q2, Q3 a Q4 byl postupně rozesílán e-mail, který se tvářil jako interní, ale s podvrženým odesílatelem a odkazem na fotogalerii, kde se měly nacházet fotografie z firemní akce. Odkaz na fotogalerii byl podvržený, ale URL v textu měla podobu interní adresy. Sledovali jsme, kteří zaměstnanci své podezření na podvrženou e-mailovou zprávu oznámí podle procesu, který jim byl sdělen v rámci bezpečnostního školení.

Neohlášená vzdálená instalace softwaru na pracovní počítač spočívala v tom, že přihlášenému zaměstnanci na obrazovce vyskočilo a po pár vteřinách zase zmizelo černé okno terminálu s několika příkazy. Tato akce se zaměstnancům náhodně zobrazovala po dobu dvou dnů, abychom předešli situacím, kdy se stejné okno ve stejný okamžik otevře lidem, kteří sedí vedle sebe. Opět jsme sledovali, kolik zaměstnanců ohlásí definovaným způsobem podezřelé chování na své pracovní stanici.

3.1 VÝSLEDKY EXPERIMENTU

V rámci experimentu jsme rozdělili nově nastoupivší zaměstnance do tří skupin (viz tabulka níže) a provedli experimenty popsané v předchozí kapitole (řízená phishingová kampaň a vzdálená instalace SW). Z tabulky vyplývá očekáváný trend, kdy nejvíce zaměstnanců ohlásilo podvrženou e-mailovou zprávu, pokud prošli proškolením ve formě prezentace. Naopak neohlášenou vzdálenou instalaci SW, která se na cílovém počítači projevila ve formě „probliknutí“ terminálového okna, neohlásil nikdo ze zaměstnanců. Fakt, že zaměstnanci této události nevěnovali pozornost, si vysvětlujeme existencí startovacích skriptů při přihlášení do počítače. Ačkoli simulovaná instalace probíhala v náhodných časech, uživatelé si toho buď nevšimli nebo probliknutí terminálového okna přisuzovali startovacím skriptům. Ačkoliv kvůli počtu testovaných zaměstnanců nejsme schopni prokázat, že se jedná o statisticky významnou změnu, je rozdíl v efektivitě poměrně značný. Velmi zajímavým zjištěním dále byla srovnatelná účinnost školení formou videí s pouhým zasláním odkazu na interní směrnici v textové podobě do e-mailové schránky bez dalšího školení. Intuitivně jsme očekávali alespoň malý viditelný rozdíl.

Kvartál	Počet nováčků	Typ školení	Nahlášení instalace SW	Nahlášení phisingu
Q2	37	Video	0	9
Q3	45	Prezentace	0	17
Q4	42	Žádné školení	0	10

4. METODY PROHLOUBENÍ POVĚDOMÍ O BEZPEČNÉM CHOVÁNÍ

Jak jsme již nastínili v úvodní části článku, samotná existence bezpečnostní politiky nezajišťuje její dodržování (a znalost) ze strany zaměstnanců, což nám potvrdil i provedený experiment. Právní rámec je pak nastaven velmi abstraktně a ponechává tak zcela na zaměstnavateli, jak se s problémem minimálního respektování stanovených požadavků vypořádá. Poskytuje mu nicméně účinný nástroj v možnosti vypovědět pracovní poměr (či zvolit jiné sankční mechanismy) a tím tak nepřímo zaměstnance nutit k respektování jím stanovených pravidel. Vyvstává tedy otázka, jak toto povědomí u zaměstnanců více vybudovat a zejména pak udržovat.

Školení typicky probíhá na roční bázi – pokud vůbec – nebo jen u nově nastoupivších zaměstnanců. V průběhu pracovního poměru pak zaměstnanec neabsorbuje změny v bezpečnostní politice a jeho znalost obsahu tohoto dokumentu v čase klesá. Pokud poté nastane situace, která vyžaduje reakci definovanou v bezpečnostní politice, tak lze předpokládat, že taková reakce bude buď zcela špatná, nebo neúplná. Je tedy nutné zamýšlet se nad možnostmi pravidelného „připomínání“ bezpečnostní politiky a procedur, které jsou zde definované.

Je vidět, že ačkoliv je konkrétní politika v souladu se všemi předpisy, a navíc je implementováno i několik dodatečných mechanismů pro zajištění vhodné úrovně znalosti, je obtížné cíle dosáhnout. Z praxe známe několik metod, jak se mu alespoň přiblížit.

Organizace povědomí svých zaměstnanců nejčastěji prohlubují různými formami simulace nečekaných událostí. Každý se zřejmě již několikrát setkal s cvičným požárním poplachem. Pokud ale budeme uvažovat o prostře-

dí IT firem, které pracují s různě citlivými informacemi, tak budou tyto simulované události značně odlišné. Dále se pokusíme popsat nejčastěji simulované situace z prostředí IT firem.

Řízenou phishingovou kampaň jsme již zběžně popsali dříve v textu. Zde jsme sledovali, kolik zaměstnanců tento incident nahlásí požadovaným způsobem. Tuto simulaci je ale možné více automatizovat. Například pomocí nástroje Metasploit[39] lze kampaň připravit, řízeně rozeslat a pomocí prvků, které jsou vloženy do každého e-mailu sledovat, kdo zprávu jen otevřel, kdo kliknul na URL adresu nebo dokonce kdo zadal přihlašovací údaje na podvržené stránce. Je možné upravit i tzv. „landing page“, tedy stránku, která se uživatelům zobrazí, pokud kliknou na URL nebo zadají přihlašovací údaje na podvržené stránce. Takto lze uživatele informovat o tom, že se jednalo o řízený test, a tedy nehrozí žádné riziko. Součástí takové stránky je pak velmi často citace relevantní pasáže bezpečnostní politiky s popisem očekávaného chování ze strany uživatelů.

Většina IT organizací má ve své interní politice část věnovanou tzv. „clear desk policy“ (politika čistého stolu), která zaměstnancům nařizuje nenechávat na stole citlivé informace (např. vytisknutý e-mail, flash disky, autentizační tokeny, napsaná hesla nebo i např. nezabezpečený laptop přes noc). Zde je opět na místě zamyšlení, jakým způsobem tato nařízení kontrolovat a vynucovat. Běžný přístup spočívá v pravidelných kontrolách kanceláří a oznamování uživatelům, že na jejich stolech byly nalezeny věci v rozporu s touto politikou (instrukcí).

Sociální inženýrství je velmi účinnou metodou, jak otestovat a budovat v zaměstnancích přirozenou ostražitost vůči nestandardním situacím. Nejslabším prvkem bezpečnosti je (a vždy bude) lidský faktor. Pomocí vhodně zvoleného způsobu lze v dané souvislosti dosáhnout značných škod. Stačí si představit situaci, kdy přijde k zaměstnanci osoba s tvrzením, že je z IT (pro zvýšení důvěryhodnosti se může odvolávat např. na manažera IT týmu) a jde např. instalovat nové ovladače k tiskárně. Pokud poprosí zaměstnance o zadání hesla do systému a odemčení počítače, je velmi pravděpodobné, že se svým požadavkem uspěje. Takovýchto situací lze uvést

[39] Metasploit [online]. *Metasploit* [cit. 6. 9. 2016). Dostupné z: https://www.metasploit.com/

celou řadu – běžně např. vydávání se za IT, ostrahu nebo správu budovy, dodavatele zboží, nebo např. za osobu, která nalezla „zapomenuté“ USB disky.

5. ZÁVĚR

V článku jsme upozornili na poměrně velký odstup právního řádu od reálné praxe zejména v oblasti bezpečnosti IT. Ačkoliv je nutné mít definována pravidla, za jakých podmínek je konkrétní směrnice závazná a korektní, tato nejsou ve skutečnosti nápomocna dosažení zamýšleného cíle. Velmi důležitá je forma sdělení. To, co může být z pohledu práva zcela dostatečné, z pohledu IT bezpečnosti (ale rovněž i jiných oblastí) zdaleka neplní svůj účel. Proto je nutno mít při řešení specifické problematiky vždy na paměti, že právo poskytuje mechanismy pro úpravu daného jen základní a konkrétní nástroje ponechává na zaměstnavateli, který „svému“ prostředí rozumí více a je tak schopen jej vhodněji upravit.

Svá tvrzení jsme podložili experimentem z reálného prostředí, který ukázal, že osobní přístup při školení byl výrazně účinnější než anonymní vzdělávací videa (či generálně zaslaný email s odkazem na interní směrnici), jejichž účinek byl překvapivě mizivý.

Na předešlém jsme prezentovali obecný právní rámec, který poskytuje zaměstnavateli nástroje pro kontrolu zaměstnance. V případě řešení porušení závazků vyplývajících zaměstnanci z interních předpisů tak právo poskytuje až následný mechanismus, jak vynutit na zaměstnanci náležité chování, když primárně je na zaměstnavateli, aby interní vztahy reguloval on sám.

Rovněž je nutno upozornit na to, že ne vždy, kdy dojde k porušení interních instrukcí zaměstnancem, dochází nezbytně nutně k využití sankčních mechanismů poskytovaných zákoníkem práce či vyvozování od-

povědnosti zaměstnance.[40] Právní rámec tedy poskytuje základní limity a sankční mechanismy a ponechává zaměstnavateli poměrně široké možnosti, jakým způsobem kontrolovat chování svých podřízených, aniž by dané bylo stanoveno konkrétněji. To považujeme za vhodné, protože právě zaměstnavatel je primárně tím, u koho je předpokládáno, že bude mít nejlepší znalosti pro to, jakým způsobem své zaměstnance kontrolovat. Je tedy nutné apelovat na to, aby právě on zvolil účinné mechanismy nejen pro úpravu samotných vztahů mezi svými zaměstnanci, ale rovněž aby zvolil vhodné nástroje, jakým způsobem o konkrétních požadavcích své zaměstnance informovat. A právě (ne)vhodnost těchto nástrojů jsme hodnotili v rámci experimentu.

V případě, že i přes veškerou snahu dojde k vážnějšímu porušení interních předpisů (a interní mechanismy kontroly zaměstnavatele selžou), zákoník práce poskytuje sankční mechanismy, jakým způsobem dané pochybení řešit. Nejprve je tedy nutno, aby zaměstnavatel s vnitřními předpisy vždy vhodným způsobem zaměstnance seznámil, a to nikoli primárně ve smyslu nutnosti naplnění obecných požadavků kladených právními předpisy, ale právě proto, aby byly interní předpisy zaměstnanci efektivně dodržovány a respektovány a nedocházelo tak ke zbytečnému nedorozumění a pochybení ve smyslu nevhodného seznámení zaměstnance s interními předpisy (i když byly *de facto* splněny všechny zákonné požadavky). Cílem tohoto článku však nebylo navržení konkrétních nástrojů, jakými vhodně zaměstnance informovat o jeho interních povinnostech. To bude potenciálním předmětem našeho dalšího výzkumu.

[40] Opětovně upozorňujeme na výše uvedenou judikaturu a to zejména na rozsudek Nejvyššího soudu ze dne 18. 3. 2014, sp. zn. 21 Cdo 1245/2013, a rozsudek Nejvyššího soudu ze dne 26. 8. 2014, sp. zn. 21 Cdo 1174/2013, které stanovují, že při porušení povinností vztahujících se k zaměstnancem vykonávané práci je důvodem pro výpověď to, že porušení stanovených pravidel bylo zaměstnancem zaviněno úmyslně, vědomou nedbalostí nebo alespoň z nevědomé nedbalosti.

6. POUŽITÁ LITERATURA

6.1 MONOGRAFIE, ODBORNÉ ČLÁNKY, SBORNÍKY

[1] BĚLINA, Miroslav a kolektiv. *Pracovní právo.* 6. doplněné a podstatně přepracované vydání. Praha: C.H. Beck, 2014, 464 s. ISBN 9788074002830

[2] BĚLINA, Miroslav, Ljubomír DRÁPAL a kolektiv. *Zákoník práce. Komentář*. 2. vydání. Praha: C.H. Beck, 2015, 1610 s. ISBN 9788074002908

[3] GALVAS, Milan a kolektiv. *Pracovní právo.* 2. dopl. a přeprac. vyd. Brno: Masarykova univerzita, 2015, 825 s. ISBN 9788021080218

[4] HŮRKA, Petr a kolektiv. *Pracovní právo*. 2. upravené vydání. Plzeň: Aleš Čeněk, 2015, 575 s. ISBN 9788073805401

[5] JAKUBKA, Jaroslav. *Vnitřní předpisy zaměstnavatele.* 1. vyd. Praha: ASPI, 2008, 196 s. ISBN 9788073573966

[6] POLČÁK, Radim, Zdeněk ŘÍHA a Kamil MALINKA. Právní aspekty interních směrnic – část I. *Data Security Management*, Praha: TATE International s.r.o., 2015, roč. 19, č. 2, s. 36-39. ISSN 12118737

[7] POLČÁK, Radim, Zdeněk ŘÍHA a Kamil MALINKA. Právní aspekty interních instrukcí – část II. *Data Security Management*, Praha: TATE International s.r.o., 2015, roč. 19, č. 3, s. 36-39. ISSN 12118737

6.2 ELEKTRONICKÉ ZDROJE

[8] ISO/IEC 27001 - Information security management [online]. *ISO* [cit. 6. 9. 2016). Dostupné z: http://www.iso.org/iso/iso27001

[9] Metasploit [online]. *Metasploit* [cit. 6. 9. 2016). Dostupné z: https://www.metasploit.-com/

6.3 JUDIKATURA

[10] Nález Ústavního soudu ze dne 23. 11. 1999, sp. zn. II. ÚS 324/99

[11] Rozsudek Nejvyššího soudu ze dne 14. 2. 2001, sp. zn. 21 Cdo 971/2000

[12] Rozsudek Nejvyššího soudu ze dne 14. 8. 2014, sp. zn. 21 Cdo 2886/2013

[13] Rozsudek Nejvyššího soudu ze dne 15. 12. 2011, sp. zn. 21 Cdo 3178/2010

[14] Rozsudek Nejvyššího soudu ze dne 15. 7. 2008, sp. zn. 21 Cdo 4467/2007

[15] Rozsudek Nejvyššího soudu ze dne 17. 12. 2009, sp. zn. 21 Cdo 3323/2008

[16] Rozsudek Nejvyššího soudu ze dne 18. 3. 2014, sp. zn. 21 Cdo 1245/2013

[17] Rozsudek Nejvyššího soudu ze dne 18. 6. 2008, sp. zn. 21 Cdo 2991/2007

[18] Rozsudek Nejvyššího soudu ze dne 19. 1. 2000, sp. zn. 21 Cdo 1228/99

[19] Rozsudek Nejvyššího soudu ze dne 19. 1. 2004, sp. zn. 21 Cdo 1527/2003

[20] Rozsudek Nejvyššího soudu ze dne 21. 3. 2013, sp. zn. 21 Cdo 742/2012

[21] Rozsudek Nejvyššího soudu ze dne 22. 3. 2001, sp. zn. 21 Cdo 249/2000

[22] Rozsudek Nejvyššího soudu ze dne 23. 9. 2004, sp. zn. 21 Cdo 1040/2004

[23] Rozsudek Nejvyššího soudu ze dne 24. 10. 2001, sp. zn. 21 Cdo 3077/2000

[24] Rozsudek Nejvyššího soudu ze dne 26. 10. 2006, sp. zn. 21 Cdo 182/2006

[25] Rozsudek Nejvyššího soudu ze dne 26. 8. 2014, sp. zn. 21 Cdo 1174/2013

[26] Rozsudek Nejvyššího soudu ze dne 4. 9. 2012, sp. zn. 21 Cdo 2141/2011

[27] Rozsudek Nejvyššího soudu ze dne 6. 2. 2007, sp. zn. 21 Cdo 212/2006

[28] Rozsudek Nejvyššího soudu ze dne 7. 4. 2009, sp. zn. 21 Cdo 896/2008

6.4 PRÁVNÍ PŘEDPISY, DŮVODOVÉ ZPRÁVY

[29] Důvodová zpráva k zákonu č. 262/2006 Sb., zákoník práce. Sněmovní tisk 1153/0, část č. 1/8 [online]. Poslanecká sněmovna Parlamentu České republiky [cit. 15. 7. 2016). Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?O=4&CT=1153&CT1=0

[30] Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších přepisů

[31] Zákon č. 65/1965 Sb., zákoník práce, ve znění pozdějších předpisů
