

ROZHLED V DIGITÁLNÍM SVĚTĚ



POHLED DO ONLINE ÉRY

Rozhovor s Sedlakova Legal, Výhody a nevýhody online obsahu, Konec televize? Jaká je cena, kterou platíme? Kyberšikana

V dnešní, rychlé době dokáží lidé konzumovat obrovské množství obsahu. Kvůli tomu se ale mnohdy stává, že se utopíme v množství informací, které moderní svět nabízí. Také velmi často stojíme před dilematem – koupit či objednat, to je oč tu běží. Ne vše je přitom zdarma tak, jak to vypadá. Jaká je cena, kterou platíme za brouzdání po internetu?

Redakce Digitálního rozhledu se zaměřuje právě na problémy, před kterými můžete vy, milí čtenáři, stát jako konzumenti obsahu. V našem prvním vydání jsme se rozhodli, přiblížit obsah na internetu, a dokonce jsme si připravili i rozhovor s psychologem Kamilem Kopeckým.

Obsah

Rozhovor se Sedlakova Legal

Výhody a nevýhody online obsahu aneb přijdeme o televizi navždy?

Jaká je cena, kterou platíme? Zdarma to rozhodně není

Kyberšikana aneb rozhovor s expertem

Rozhovor se Sedlakova Legal

V naší redakci máme rádi kvalitní rozhovory. A tak nám přijde skvělé začít právě rozhovorem. Na paškál jsme si vzali společnost Sedlakova Legal, která je jednou z největších právnických firem na trhu. Její dva pracovníci, Jiří Hradský, specialista na whistleblowing a technologie a Roman Tomek, specialista na GDPR a nemovitosti, společně odpověděli na naše zapeklité otázky.

Děkujeme firmě SEDLAKOVA LEGAL za rychlé odpovědi.

Adam: Je nějaký právní postih, který hrozí za konzumování obsahu online (příkladem jsou portály jako bývalé Ulož.to, Bombuj)?

Jiří & Radek: Právní postih hrozí jak uživatelům, tak samotným provozovatelům takových portálů. Tito provozovatelé jako platformy musí zajistit, že obsah, který sdílí, není získán nelegálně apod. Samozřejmě v určitých případech může hrozit také postih jednotlivcům, kteří obsah nahrávají, zejména, pokud nahrají například dětskou pornografii nebo jiný trestný či autorskoprávní obsah. I z důvodu nových právních předpisů, zejména nově účinného DSA tak třeba portál Ulož.to přešel do zcela jiné formy fungování (dnes již nejsou viditelné zveřejněné dokumenty).

Právní postih může spočívat například v náhradě škody, případně v nutnosti takový nelegální obsah stáhnout z dané platformy.

A: Už jste se někdy v praxi setkali s takovým soudním případem a postihem?

J&R: V minulosti je asi nejznámější rozhodnutí z roku 2021 ve věci HellShare/HellSpy. V roce 2014 Česká národní skupina Mezinárodní federace hudebního průmyslu podala žalobu proti těmto portálům z důvodu nekalé soutěže. Velmi zjednodušeně obdobné portály musí kontrolovat, že obsah, který je nahráván na jejich platformy neporušuje například autorskoprávní obsah, pokud za něj HellShare/HellSpy nabízí uživatelům odměnu. Jinými slovy, samotná platforma byla odpovědná za nahraný obsah, protože poskytovala uživatelům odměnu.

V praxi se mimo jiné také často řeší samotné nároky vůči jednotlivým uživatelům, kteří obsah nahrávají. V takovém případě se často požaduje zejména stažení daného obsahu.

A: V rámci online světa se dost mluví o úniku dat. Jak můžeme (s)právně postupovat, pokud dojde k úniku dat o nás?

J&R: Pokud dojde k úniku dat, je zejména potřeba dobře klasifikovat, jaká data utekla. Pokud se například jedná o osobní údaje, musí nás dle GDPR správce, který naše osobní údaje zpracovává upozornit v případech, kdy by nám hrozilo vysoké riziko zneužití či jiných incidentů. Jako subjekty údajů máme právo na informace o tom, co se s osobními údaji stalo



osobních údajů.

a na základě toho pak můžeme činit další relevantní rozhodnutí. Pokud stojíme na straně samotného správce, tedy osoby, která osobní údaje získává a dále zpracovává, musíme takový únik dat oznámit jako bezpečnostní incident dozorovému orgánu, kterým je v oblasti ochrany osobních údajů Úřad pro ochranu

A: Jak si myslíte, že se liší reklamační právo u věcí koupených online a v prodejně? Jsou tam nějaké kličky?

J&R: Po právní stránce v reklamaci jako takové rozdíly nejsou, hlavní je ta, že v případě kamenné prodejny jsou na kupujícího kladeny větší nároky ohledně prokázání, že zboží koupil (tedy je třeba mít alespoň účtenku), to u e-shopu odpadá, protože je vše evidováno v systému. Z praktického pohledu ale může být reklamační právo zboží koupeného online složitější, s ohledem na dostupnost prodejce. V případě kamenné prodejny jsem schopen se vždy zkontaktovat s někým, s kým lze řešit, ale v případě e-shopu toto může být problém, zejména u e-shopů ze zahraničí.

A: Vnímáte nějaké nedostatky ve spotřebitelském právu, které jsou za Vás důležité?

J&R: Zde velmi záleží na úhlu pohledu. Pokud bych se na věc díval jako spotřebitel, tak zde žádné zásadní nedostatky nevidím, naopak mi v některých ohledech přijde ochrana spotřebitele až příliš vysoká. Naopak pro podnikatele jsou podmínky v některých situacích již poměrně přísné, zejména v oblasti odstoupení od smlouvy. Spotřebitel totiž může odstoupit bez udání důvodu do 14 dní od koupě zboží, po tuto dobu ale může zboží vyzkoušet a používat. Podnikatel si sice může započíst případnou „škodu“, která tímto užíváním vznikla, ale ta může být obtížně vyčíslitelná (třeba drobné škrábance, poškozený obal apod.). Zároveň mu nikdo nezaplátí náklady s tím spojené, tedy že musel zboží zabalit, poslat, následně přijmout zpět, vrátit platbu, zkontrolovat vrácené zboží a další kroky.

Autor: Adam Král

Zdroj: e-mailová komunikace



Výhody online obsahu aneb proč byste měli být online?

Jak jsme již zmiňovali v naší předmluvě, uživatelé v dnešní době konzumují obrovské množství obsahu. A my tak mnohdy nevíme, jak se s tím vším naložit.

Náš redakční tým se rozhodl, zaměřit se hlavně na aspekty online obsahu jako takového. Jaké výhody uživatele čekají? Čtěte dál! Na levé straně najdete výhody online obsahu, na pravé pak nevýhody

Je libo špetku čehokoliv?

Určitě to znáš. Sedíš u televize, v ruce nějaké to občerstvení a ovladač. Celý kinematografický svět máš před sebou. Kamarád ti doporučil „fakt super“ seriál a ty jen čekáš na to, až budeš mít možnost ho zhlédnout. A moc dlouho čekat nemusíš, protože nekonečný zástup služeb má tvoje záda.

Mezi největší výhody online obsahu bychom tak zařadili rychlost. V minulých dobách jste museli čekat na to, až nějaký redaktor napíše článek, otiskne ho do místních novin a vy si ho koupíte. Takové čekání v dnešní době nenajdete a vše máte k dispozici takřka okamžitě.

Nižší náklady

Na svém počítači či mobilním telefonu můžete mít cokoliv okamžitě. V jedné sekundě si naladíte Netflix, HBO, ale i televizi a internetové články, to vše vás vyjde jen na pár stovek měsíčně. Nemusíte přitom čekat na to, až skončí obrovské zástupy reklam.

Zajímavosti

Věděli jste, že internet byl poprvé v České republice použit v roce 1991 v květnu? Byli jste v tu dobu na světě?

První televize pak do České republiky přišla v roce 1953, černobílá. Barevných obrazců se diváci mohli dočkat o dvacet let později, roku 1973. Jaký je váš nejoblíbenější televizní pořad?

Závislost

Alkohol, cigarety, ale i další návykové látky, to jsou známé věci. Na co se ale v poslední době zapomíná je závislost na sociálních sítích a televizi. Vystavení můžete být takzvanému FOMO efektu (strach z toho, že vám něco unikne), nebo z nutnosti být stále online.

I zde se jedná o závislost, kterou byste měli konzultovat se svým lékařem a psychologem. V první řadě je nutné začít to léčit a nechat si pomoc. Stát se to může všem, přesto jsou nejvíce v ohrožení mladí lidé z generace Z.

Ztráta sociálního zázemí

Proč byste vlastně chodili ven v době, kdy máte vše na dosah ruky? To je něco, co si spousta mladých lidí řekne a velmi často se stane, že nevylezete z domu po zbytek týdne či dne.

Jakou cenu platíme za používání internetu?

Jak říká jeden ze známých českých tvůrců, „internet je pozoruhodné místo“. V dnešní době se totiž můžeme setkat s obrovským množstvím obsahu, což jsme si řekli i o pár stránek zpátky.

Za používání internetu ale platíme obrovskou cenu. „To ale přece není možné, internet používám zadarmo“, slyším vás zvolat. Je to ale skutečně tak? Jistě, platíte měsíční poplatek za internet a zařízení, na kterém si tyto články, videa a další prohlížíte. Nebezpečí je ale mnohem více, než se zdá.

Kybernetické útoky & zločiny

Kybernetický zločin zahrnuje nelegální aktivity na internetu s cílem neoprávněně získávat, modifikovat nebo poškozovat elektronická data a informace. Klíčové oblasti zahrnují ransomware, phishing, krádež identity, útoky na firmy, kyberšpionáž, botnety a kybernetická želízka. Ochrana zahrnuje používání bezpečnostních opatření, jako jsou antivirové programy, firewally a šifrování dat

Dezinformace

Dezinformace jsou zdaleka nejnebezpečnějším nástrojem na internetu. Lži, pomluvy a v poslední době i deep-faky, to je něco, před čím se musíte mít na pozoru.

Znáte to, vidíte článek na internetu o tom, že do Česka míří nacisté z Ukrajiny, kteří povraždí vaše příbuzné, pak na vás vyskočí další o látkách, které vás ublíží, ale pak vlastně zjistíte, že to vůbec není pravda. Na příkaz tzv. hoaxu se můžete podívat níže.

Jak se tak dezinformacím bránit? Stačí si vše ověřovat. Má článek moc chyb? Podivný obrázek? Používá spousty vykřičníků? S největší pravděpodobností to bude hoax.

Autor: Adam Král

Zdroj: iDnes.cz



Kyberšikana aneb rozhovor s expertem

S nějakým druhem šikany se v dnešní době setkal snad každý z nás. V posledních letech ale narůstají případy tzv. kyberšikany, tedy soustavného, agresivního chování vůči jedinci na internetu. Náš redakční tým oslovil psychologa Kamila Kopeckého.

Adam: Kyberšikana je široký pojem. Co všechno si pod ním můžeme představit? Co kyberšikana je a co není?

P. Kopecký: Kyberšikana se často míchá s běžnou agresí, se kterou se na internetu setkávají jak děti, tak dospělí. Ti samozřejmě mají zkušenost s různými druhy nadávek, urážek a dehonestujícími komentáři. Aby šlo o kyberšikanu, musí platit několik podmínek.

Agrese musí být opakovaná, to zesiluje i její dopad, a člověk ji musí vnímat jako ubližující. Jinými slovy, pokud někomu pošlu sprostou esemesku „Ty krávo“, je to sprosté a vulgární, je to agrese, ale není to kyberšikana. Je to v tu chvíli jen agrese, která teprve může v kyberšikanu přerůst.

Kyberšikana má na oběť měřitelný dopad – ať už v rovině psychické, behaviorální či fyziologické. Logickým znakem také je, že v rámci kyberšikany jsou využívány moderní komunikační technologie jako internet, mobilní telefony a tak podobně.

A: Je ještě nějaký znak, který je pro kyberšikanu typický?

K: Přidal bych například zdánlivou anonymitu. U běžné šikany vždy víme, kdo útočí. U kyber formy si mnoho pachatelů myslí, že jsou neodhalitelní, protože útok probíhá pomocí anonymního profilu nebo přezdívky.

Z vlastní zkušenosti i výsledků výzkumu mohu říct, že ve většině případů kyberšikanu je agresor z okolí dítěte, ze stejné třídy nebo školy. Většinou se dá také vysledovat, kdo to byl.

A: Jak konkrétně se může kyberšikana projevat? Jak to poznám?

K: Forem je velmi mnoho. Verbální kyberšikanu si můžeme představit jako urážky, nadávky či nepěkné přezdívky, které o dítěti šíří například jeho spolužáci – a to především v prostředí sociálních sítí či skrze WhatsApp nebo Messenger.

U kyberšikany ve formě šíření fotografií se bavíme třeba o tom, že spolužáci vyfotí jiného spolužáka v nějaké dehonestující situaci přímo ve škole, například o přestávce na záchodě, a potom to začnou šířit internetem.

Velmi nebezpečná forma už je šíření vyloženě intimních materiálů, například obnažených fotografií. K tomu obvykle dochází, jakmile začnou děti navazovat partnerské vztahy. Bavíme se o sextingu – vzájemné sdílení intimních materiálů se stalo v posledních letech poměrně běžnou součástí romantických vztahů. Děti si však bohužel neuvědomují, že ty nemusí trvat věčně a po rozchodu se jejich intimní materiály mohou stát nástrojem agrese a útoku, mohou být zneužity k vyhrožování, vydírání nebo poškození pověsti.

Další nebezpečnou formou může být bodyshaming, tedy agrese, při které oběť urážíme kvůli vzhledu. A kyberšikana bývá spojena také s prostředím počítačových her, ve kterém se dostáváme k vyloženě podvodnému chování. Pro děti je herní prostředí velmi důležité, investovaly do něj hodně času, energie, někdy i peněz.

A bohužel se setkáváme se situacemi, kdy od dítěte někdo vyláká přihlašovací údaje do online herního účtu, změní na něm heslo a původního majitele pak útočník vydírá a za obnovení přístupu požaduje finanční prostředky, případně vyhrožuje, že celý účet s veškerým obsahem smaže.

A: Na svých webových stránkách uvádíte, že za prvních deset let vaší existence jste řešili necelé čtyři tisíce případů. Kdo a s čím se na vás nejčastěji obrací?

Aktuálně máme v poradně 6566 případů a z toho čtyřicet až padesát procent tvoří děti v nouzi. Děti se na nás obrací obvykle tehdy, když už je jejich problém skutečně vážný a bojí se o něm říct třeba rodičům nebo učitelům.

A: Můžete uvést příklady situací, které řešíte nejčastěji?

Přes sedmdesát procent případů se týká úniku intimních materiálů, třeba fotografií či videí, do online prostředí. Například nám napíše třináctiletá dívka, že se na internetu seznámila s klukem, kterému poslala svoje „nudesky“, jenže po odeslání jí začal vydírat a vyhrožovat, že fotky zveřejní a rozšíří, pokud nesplní jeho podmínky.

Typickými platformami, na kterých k tomu dochází, jsou Snapchat a Instagram, občas nám přijde také nějaký incident z TikToku. Řešili jsme

třeba případ třináctileté Beátky, točila na TikToku různá taneční videa a neznámý muž, podle fotky a jejího komentáře sympaťák, jí napsal, že se mu to líbí a jestli by nenatočila něco jen pro něj. Poté začal psát, že je krásná, že se mu líbí.

Mimochodem, přehnaná chvála je jeden ze znaků, že něco není v pořádku. Takto může začínat kybergrooming, kdy vás chce pachatel vylákat na osobní schůzku. Každopádně Beátka natočila pro „sympaťáka“ intimní video a rozjela se spirála vyhrožování – pokud mu nebude točit další videa, pak vše zveřejní.

Třináctileté dítě obvykle nepůjde dobrovolně tyto incidenty nahlásit přímo na policii, často to neřekne ani rodičům, protože jde o velmi citlivé a intimní téma. U rodičů se děti bojí reakce – že budou reagovat podrážděně, křičet, zakáží jim používat konkrétní aplikace.

Z pohledu rodiče je důležité dítěti nabídnout především pomocnou ruku a potlačit tyto podrážděné, i když pochopitelné reakce. Pokud totiž bude rodič reagovat podrážděně a restriktivně, dítě už za ním příště nepřijde.

A: Jak bych se na internetu měl chovat, abych byl v bezpečí? Jaké zásady mám dodržovat?

K: Jedním z opatření je určitě v online prostoru nesdílet citlivé materiály. Co se týče citlivých fotek, čím méně toho sdělujeme, tím lépe. Je nesmysl, že bychom nemohli sdílet absolutně nic, jde o to, aby ty fotky nebyly zneužitelné proti nám. A to ani v budoucnu. Může jít například o fotky z večírků, kde někdo opilý leží na stole. Takový snímek pak může ohrozit třeba uchazeče o zaměstnání.

Dalším opatřením může být nedávat si do přátel neznámé lidi. A potom bych se úplně vyvaroval sdílení intimních fotografií ve vztazích. Skutečně nikdy nevíte, kde to skončí.

A nesmíme zapomenout ani na technická řešení, ať už jde o dvoufázové zabezpečení účtů, bezpečné heslo a tak dále.

Autor: Adam Král

Zdroj: e-mailová komunikace s panem Kopeckým



Kamil Kopecký je pedagogem na Univerzitě Palackého v Olomouci. Řídí několik projektů a jeho specializací jsou rizikové formy komunikace v online prostředí, ochrana osobních údajů, ale i IT technologie. Pana Kopeckého jsme oslovili na základě článku Deníku N a doptali se ho na pár otázek.

Tiráž

Redakce Digitální rozhled



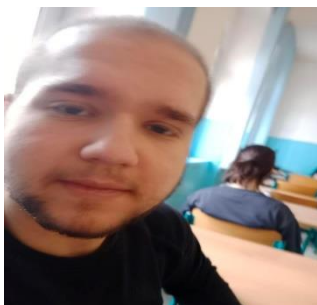
Adam Král

Šéfredaktor



Šimon Kubíček

Editor



Jaroslav Mihalík

Grafický designér