

# RIZIKOVÉ CHOVÁNÍ ŽÁKŮ ZÁKLADNÍ ŠKOLY A STŘEDOŠKOLSKÝCH STUDENTŮ PŘI PRÁCI S POČÍTAČEM A S INTERNETEM

---

*Petr KACHLÍK*

**Abstrakt:** *Výpočetní technika, počítačové sítě, mobilní telefony a další vyspělé informační a komunikační technologie (ICT) umožňují rychlou výměnu informací, přinášejí nové možnosti v zaměstnání, ve vědě, vzdělání, zábavě. Jejich neuvážené používání zejména dětmi a mládeží může vést k řadě zdravotních i sociálních poruch. Bylo provedeno kvantitativní výzkumné šetření, které proběhlo ve všech regionech ČR, při němž bylo formou anonymního dotazníku osloveno 1072 žáků z 26 škol (2. stupeň ZŠ a SŠ). Otázky se týkaly trávení volného času, práce s ICT, útoků vedených cestou ICT. Ukázalo se, že existuje nízký stupeň rodičovské kontroly, 30 % respondentů již bylo atakováno cestou ICT. Problematické situace řešilo s rodiči jen 5 % vzorku, více jak 50 % je ochotno zveřejnit po roční on-line komunikaci své osobní údaje. Je nezbytné posílení zájmu rodičů o volný čas dětí a jejich manipulaci s ICT, nastolení důvěry a brzké řešení problémů, ve škole je potřebné prohloubení informační gramotnosti žáků s důrazem na jejich osobní bezpečnost a netiketku.*

**Klíčová slova:** *bezpečnost, dotazník, hra, ICT, internet, počítač, prevence, riziko, student, škola, útok, volný čas, výzkum, zneužití, žák*

## Úvod do problematiky

Informační a komunikační technologie (ICT) se velmi rychle rozšířily z vojenského a akademického prostředí mezi běžné uživatele, získaly si obrovskou oblibu, slouží nejen při výkonu zaměstnání, ale i v domácnosti a při trávení volného času (Procházka, 2010).

Miliardy lidí po celém světě využívají mobilní telefony a internet ke komunikaci, při níž stačí vytočit číslo nebo kliknout myší. Přínosem internetu pro komunikační možnosti je umožnění informační dostupnosti a prostupnosti, interaktivnost při výměně zpráv a rychlost při zprostředkování kontaktu (Vybíral, 2000).

Historie celosvětové počítačové sítě započala v 50. letech 20. století, kdy bylo snahou Američanů držet krok se Sovětským svazem, který v té době již získal vojensky využitelné kosmické technologie. Panovala obava zejména z jaderného napadení, které by mohlo ohrozit velkou část území Ameriky a jejích spojenců, vyřadit z provozu obranné a komunikační systémy, jež byly centralizované. Pracovníci společnosti RAND (*Research ANd Development*) přišli tehdy s unikátním řešením – vybudováním sítě, která

nebude mít centrální uzel a v případě zničení některých linek může dopravit informace k příjemci jinými trasami (Kras, 2001).

Ve Spojených státech vznikla speciální vládní agentura ARPA (*Advanced Research Projects Agency*), která se zabývala pokročilými výzkumnými projekty a v roce 1969 spustila experimentální síť s názvem ARPANET. Síť se z původních 20 uzlů ryze vojenského a vládního typu (r. 1971) rozrostla na více než 200 uzlů (r. 1981) zahrnujících též akademické prostředí. Výpočetní technika té doby byla dostupná pouze velkým institucím, byla značně rozměrná, drahá a z dnešního pohledu málo výkonná, vyžadovala kvalifikovanou obsluhu. Poprvé se objevuje pojem „internet“, k síti se mohou připojit a využívat ji i komerční uživatelé. Od 80. let 20. století se počítač zmenšuje, roste jeho výkon a dostupnost pro veřejnost, je koncipován jako osobní, tedy „jednouživatelský“ (Blábolil, 1997). Od 90. let 20. století množství uživatelů internetu geometricky vzrůstá, každý rok se více jak zdvojnásobuje, nastává doba, která zásadním způsobem ovlivňuje chování lidstva – doba internetová. Dnešní celosvětová počítačová síť představuje globální kyberprostor – nepřeborný zdroj informací a myšlenek, do něhož může vstoupit několik miliard účastníků (Kras, 2001).

Dalším klíčovým mezníkem ve vývoji internetu je vznik celosvětové pavučiny stránek označované jako World Wide Web (WWW). Jde o způsob komunikace pomocí multimediálních a hypertextových odkazů, což učinilo webové prezentace uživatelsky i komerčně atraktivními. Dnes může prakticky každý uživatel na internetu publikovat své myšlenky (Blábolil, 1997). V r. 1992 byl nastartován projekt Mosaic, šlo o vývoj grafického webového prohlížeče (Kodýtek [on-line], 2006). Česká republika byla k internetu oficiálně připojena 13.2.1992. Zprvu disponovala 2 uzly (Praha, Brno) propojenými pevnou linkou, časem byla tato páteř rozšířena o další města, vznikly konkurenční projekty. Kapacita sítě nejdříve sloužila akademickým a nevýdělečným organizacím, od r. 1995 i komerční sféře, která poskytuje finance k dalšímu rozvoji a provozu (Zemánek, 2004).

V rámci internetové sítě mohou uživatelé využívat několika standardních služeb, nejčastěji jde o World Wide Web (WWW) – soustavu propojených hypertextových dokumentů, která poskytuje rozsáhlý informační virtuální prostor (Broža, 2004). Z dalších stojí za zmínku HTTP (Hyper Text Transfer Protocol) – strukturovaný text s odkazy na jiné stránky, texty, obrázky, zvuky, animace a jiné soubory (Říha, 1996), FTP (File Transfer Protocol) – nástroj k hromadnému přesouvání souborů, umístění grafiky, hudby a videa na webové stránky (Musil [on-line], 2003a). V případě elektronické pošty (e-mailu) se jedná o rychlou komunikaci mezi institucemi, podniky i soukromými osobami. Zprávy mohou obsahovat text, zvuky, obrázky, videa (Říha, 1996). E-banking (elektronické bankovníctví) nabízejí v současné době všechny banky. Prostřednictvím klientského čísla a hesla je možné okamžitě zjistit stav svého účtu a provádět různé bankovní operace v kteroukoliv hodinu a z jakékoliv vzdálenosti (Elektronické bankovníctví [on-line], 2010). IM (Instant Messaging) dovoluje přímou komunikaci na síti v reálném čase, News (UseNet, NetNews, NewsGroup) jsou tématicky zaměřené diskusní skupiny, kde je možné pročitat si příspěvky, reagovat na ně a zveřejňovat vlastní. Veškerý obsah je přístupný všem (Musil [on-line], 2003b). Služba Noviny urychluje přístup k informacím, které jsou přehledně tříděné do rubrik. Prakticky každý významnější tištěný titul má i svoji elektronickou mutaci, existují i tituly šířené výlučně

elektronickou cestou. Na příspěvky je možné reagovat, diskutovat k nim (Kras, 2001). Obchodování a nákupy (e-business, e-commerce, e-shop) představují rostoucí segment služeb internetu. V současnosti je možné nakupovat nepřebernou paletu zboží a služeb a platit přes internet nebo pomocí SMS zpráv. Zboží je většinou posíláno kurýrní službou nebo poštou na dobírku. (Vitovský, 2006) WAP (Wireless Application Protocol) zajišťuje provoz elektronických služeb optimalizovaných pro mobilní telefony, které pak umožňují na displeji totéž, co internetový prohlížeč. Televizní a rozhlasové vysílání šířené po internetu dovoluje zhlédnout většinu pořadů v přímém přenosu nebo po premiérovém odvysílání (Kras, 2001).

Přínosem rozlehlých počítačových sítí je sdílení informací bez ohledu na geografickou vzdálenost, informace jsou během vteřin k dispozici prakticky kterémukoliv účastníkovi sítě (Veřtát et al., 1993). Převratný rozvoj ICT ovlivňuje množství stránek lidského života: z jedné strany racionalizuje a usnadňuje nepřebernou řadu lidských činností, ze strany druhé poskytuje prostor pro páchaní trestných činů. Dnešní děti a mládež tráví u počítače stále více času, fenoménem internetu bývají doslova pohlceny. Podle celosvětového průzkumu agentury Media Metrix z roku 2000 se došlo k závěru, že na internetu surfují v 7,6 % děti od 2 do 11 let a teenageři v 11,9 %. Z výsledků se dá předpokládat, že v ČR je více než čtvrtina dětské internetové populace mladší 18 let. Téměř všechny děti mají v současné době přístup k internetu, část jejich života se tak odehrává ve virtuálním prostředí a ony tento fakt považují za přirozený a běžný. (Co dětem hrozí na internetu [on-line], 2010)

Při práci s počítačem a při pohybu na internetu hrozí dětem a dospívajícím řada rizik. K nejdůležitějším z nich patří:

- neopatrné a bezmyšlenkovité sdělování citlivých informací, při němž hrozí jejich zneužití; při propojení stop zanechaných v kyberprostoru lze i bez speciálních znalostí pomocí vyhledávačů sestavit profil konkrétního uživatele (Dočekal [on-line], 2010);
- komerční využití a zneužití dat dětí a mladých lidí získaných ze sociálních sítí, sestavení komplexního profilu osobnosti i její rodiny, tipování budoucích obětí trestné činnosti (Procházka [on-line], 2010);
- publikace a zneužití nevhodného obsahu na sociálních sítích, celosvětovou doménou je Facebook, který během několika let získal v prostředí českého internetu více než 2 milióny uživatelů (Dědiček, 2010);
- flaming, tedy útočné, urážlivé, nepřátelské jednání vedené prostřednictvím internetu, při kterém lze využít e-mailu, diskusních fór i chatu, vést plamennou diskusi bez logické argumentace s cílem urážet, zesměšňovat, útočit, dochází k porušování základních pravidel komunikace na internetu, tzv. netikety (Flame war [on-line], 2010);
- hacking: průnik do informačních systémů s cílem jejich prozkoumání a poznání funkce, obvykle bez změn jejich činnosti a dalších škod (Jirovský, 2007);
- cracking: průnik do informačních systémů s cílem získat data, změnit jejich obsah, funkci, obohatit se, páchat další trestnou činnost, speciálním případem jsou tzv. script-kiddies-dospívající s minimálními technickými znalostmi, kteří se zviditelňují prostřednictvím poškozování ICT. Je třeba také připomenout

porušování autorských práv a práv k duševnímu vlastnictví, kterých se uživatelé dopouštějí nelegální nabídkou počítačových programů a multimediálních souborů, odstraňováním či obcházením ochranných prvků v nich. (Rychnovský, 2005);

- phishing ("rhybaření"): forma podvodu na internetu, vylákání, získání a zneužití důvěry a osobních dat nezkušeného, naivního uživatele, např. přihlašovacích jmen, hesel, čísel účtů, PIN kódů, apod. (Phishing [on-line], 2010);
- cybergrooming: záměrné a manipulativní jednání s dětmi a mladistvými prostřednictvím internetu, nejčastěji chatu, e-mailu, seznamek a ICQ, které má v oběti vyvolat falešnou důvěru. Manipulátor (groomer) budí zdání, že dítěti naslouchá a rozumí, zároveň o něm sbírá co nejvíce informací, které pak užívá k vydírání, ubližování, při osobním setkání může dítě zneužít k pedofilním nebo teroristickým aktivitám (Cyber grooming [on-line], 2010);
- kybersex: hanlivá, vulgární internetová komunikace (slovo, text, fotografie, video) sexuálního charakteru, má různý rozsah a formy – např. flirtování, pornografické materiály, intimní návrhy, spycams, což je voyerismus nebo exhibicionismus přes webkameru (Až 25 miliónů lidí denně provozuje kybersex [on-line], 2010);
- pedofilie, pornografie: jejich propagace i obstarání jsou v prostředí internetu mnohem snazší (Weiss, 2002). Dětská pornografie představuje nejziskovější odvětví filmového průmyslu. (Milfiát, 2008; Vaničková, 2009). V řadě zemí není šíření pornografie ani trestným činem, ale díky nadnárodní povaze internetu jsou stránky s nelegálním obsahem viditelné i v zemích, kde je šíření pornografie trestnou činností (Matějka, 2002). Děti nejsou jen v pozici obětí, ale i vědomých či nevědomých dodavatelů citlivých materiálů a sexuálních služeb (Milfiát, 2008; Kožíšek, 2010; Viktora, Vokáč, 2010);
- SMS spoofing: všichni mobilní operátoři poskytují služby propojené s internetem, mj. lze posílat SMS zprávy, e-mail, prohlížet WWW stránky. Dítě, které většinou nenapadne ověřovat odesílatele přijaté SMS zprávy (může být anonymní a podvržená), se tak může dostat do nebezpečné situace (Klíma, 2005; SMS Spoofing [on-line], 2010);
- malware: souhrnné označení pro šíření škodlivých kódů (např. viry, červi, trojské koně), které mohou proniknout do počítačových systémů a poškodit je, distribuovat nevyžádanou reklamu, vykrádat nebo zpřístupnit citlivá data (Hlavenka, Samšuk, 1996; Kocman, Lohniský, 2005; Kuneš, 2006);
- spamming: nevyžádaná sdělení většinou reklamního charakteru, která jsou masově rozesílána především e-mailem, ale zaplevelují i diskusní fóra a sociální sítě, otevření spamu ohrožuje uživatele např. zavirováním počítače, přesunem na závadové stránky (Matějka, 2002);
- hoax (výmysl, podvod, mystifikace, novinářská kachna): jde o řetězové e-maily, které mají většinou charakter poplašných zpráv, obsahují např. varování před neexistujícími hrozbami, vyzývají příjemce k dalšímu masovému rozesílání (Únos dětí v obchodním domě [on-line], 2010);
- cyberbullying (kyberšikana): jde o násilné a ponižující aktivity jednotlivce nebo skupiny vůči slabšímu jedinci, který nemůže ze situace uniknout, není schopen se

účinně bránit (Vágnerová, 2004), v tomto případě se většinou jedná o nahrávání a publikaci videozáznamů nebo fotografií dětí a učitelů v diskreditujících situacích, je použito počítače, internetu či mobilního telefonu (Doubrava, 2010);

- cyberstalking: pronásledování, slídění s následným útočným chováním prostřednictvím internetu a mobilních telefonů, vedoucí k poškození oběti a demonstraci moci a síly útočníka (Kyberstalking [on-line], 2009);
- kyberterorismus, propagace násilí a agresivity: násilí se postupně stává součástí běžné zkušenosti, dokonce i tehdy, jde-li o násilí symbolické, prezentované v médiích, začíná být považováno společností za normální jev (Vágnerová, 1997). Podle Jirovského (2006) je kyberterorismus spojení kyberprostoru s terorismem, jde o aktuální globální hrozby, nezákonné aktivity namířené proti počítačům, počítačovým sítím a v nich uloženým informacím s cílem zastrašit nebo donutit k podpoře sociálních či politických cílů.
- propagace náboženských sekt a extrémistických hnutí: děti a mladí lidé jsou velmi ohroženou a vysoce ovlivnitelnou skupinou, vysoká anonymita internetového prostředí umožňuje prezentaci aktivit těchto skupin, nábor nových členů, mobilizaci jejich sponzorů (Šmahel, 2003);
- šíření ideologie čistě konzumního způsobu života, preference financí, úspěchu, egoismu a moci na úkor klasického hodnotového žebříčku (zdraví, rodina, vztahy, záliby) (Říčan, 2007);
- závislost na virtuálních drogách (netolismus či netomanie) a ICT, např. mobilu, chatu, sociálních sítích, internetu, počítači: u dětí a dospívajících vzniká závislost rychleji než u dospělých, zasahuje všechny atributy zdraví (Kalina [on-line], 2010), u závislosti dominuje psychická složka (Pokorný et al., 2002), jejímu vzniku napomáhá nejistá osobnost s nízkým sebevědomím a sebehodnocením a ztrátou reálných sociálních vazeb, může se objevit i tolerance (Vágnerová, 2004; Nešpor, 2000; „Závislost“ na internetu a boj proti ní [on-line], 2010).

Každý má právo internet využívat k dobrým věcem, jinou věcí je, že jej někteří jedinci zneužívají ve svůj prospěch a potěchu. Základní informovanost o prevenci a bezpečnosti by mělo dítě dostat především v rodině (Fischer, Škoda, 2009).

Bednář (2006) a Kühnelová (2011) uvádějí několik základních pravidel dodržení počítačové bezpečnosti:

- nestahovat žádné ilegální programy;
- používat legální a aktualizovaný operační systém, oficiální webové prohlížeče;
- neotevírat e-maily a přílohy, které nebyly vyžádány, pocházejí z neznámých adres;
- řádně prostudovat výstrahy a další zprávy, které souvisejí s činností počítače;
- nenavštěvovat problematické stránky, zejména s nabídkou pornografie, nelegálních programů a médií, jsou nejčastějšími nositeli virů;
- pro různé služby používat různá hesla, která budou delší (kombinace písmen, číslic, speciálních znaků);

- po skončení práce s webovými aplikacemi se řádně odhlásit a uzavřít všechna okna prohlížeče, zabránit se tak možnému vykrádání informací;
- do registračních formulářů zadávat minimum osobních informací;
- nikomu, jehož identitou si nejsme jisti, nesdělovat žádné osobní informace.

V prevenci rizikového chování dětí a dospívajících hraje stěžejní roli rodina, jež poskytuje zázemí potřebné ke společenské seberealizaci, je zdrojem zkušeností a vzorců chování, které nemůžeme získat v jiném prostředí (Fischer, Škoda, 2009). Rodina dítěte je klíčovým faktorem pro predikci rizikového chování, jako prevence rizikového vývoje se zdůrazňuje otevřená komunikace a význam pozitivních emočních vztahů v rodině, i zda a jaké jsou vztahy mezi rodiči a školou (Macek, 1999).

Děti je důležité od předškolního věku vychovávat tak, aby uměly třídít informace a naučily se posuzovat, co je pro ně škodlivé a co prospěšné. Je dobré být svým dětem stále nablízku a průběžně kontrolovat, které stránky navštěvují, dohodnout se, kolik dítě může strávit před obrazovkou času a dbát na dodržování pravidel. K ochraně dětí lze použít různých typů hlídacích programů (Hlídací pes 2002 [on-line], 2010).

Pokud se rodiče pro zakoupení takového programu rozhodnou, před jeho samotnou instalací je lepší s dětmi nejdříve promluvit a vysvětlit jim, že program není určený ke sledování potomka, ale k jeho ochraně. Děti by měly chápat, že existují metody, jak se nebezpečným situacím vyhnout, a rodiče chtějí znát vše, co se jim kdy přihodí. Je to právě neinformovanost, která činí děti zranitelnými (Elliottová, 2000).

Z pohledu transformace školního systému v návaznosti na procesy evropské integrace je zřejmé, že v současné době je potřeba reformovat vzdělávací programy na všech úrovních edukace na základě požadavků sociálně – tržní ekonomiky a připravit mladé lidi na možnost vstupu na flexibilní trh práce Evropské unie s dynamickými komunikačními dovednostmi a poznatky o využití moderních technologií včetně internetu (Lokšová, Lokša, 2003).

Jsme součástí informační společnosti, a proto se s těmito novými vlivy proměňuje prostředí, v němž se vzdělávání uskutečňuje. Značnou část znalostí v této oblasti získávají děti ve škole. Mění se výukové cíle, přizpůsobují se Školní vzdělávací programy a v konečném důsledku i celkové úlohy škol. Orientovat se ve světě informací, získat elementární dovednosti v ovládnutí výpočetní techniky a dosáhnout základní úrovně gramotnosti v užívání moderních technologií dokáží děti již od základních škol prostřednictvím vzdělávací oblasti Informační a komunikační technologie, která je povinnou součástí Rámcových vzdělávacích programů základního vzdělávání (*RVP ZV*). Tato vzdělávací oblast je pro získání kvalitního vzdělání a udržení tolik požadované konkurenceschopnosti na trhu důležitá. Získané dovednosti jsou v informační společnosti nezbytným předpokladem uplatnění na trhu práce i podmínkou k efektivnímu rozvíjení profesní i zájmové činnosti. Cílové zaměření směřuje k poznávání, porozumění digitálním médiím a všem tokům informací od samého vzniku, přenosu, zpracování až po praktické využití. Žáci se učí tvořivě myslet, porovnávat a třídít více informačních zdrojů, respektovat práva k duševnímu vlastnictví. Stěžejním cílem je zaujetí odpovědného, etického přístupu k nevhodným obsahům vyskytujícím se na internetu či jiných médiích (Vítková, 2004; *RVP ZV*, 2010).



Volným časem je myšlen čas, v němž si dítě může svobodně, na základě své nálady, zájmu a pocitu, volit činnost, jakou samo chce (Pávková et al., 2001). Každou volnočasovou aktivitu u dětí a mládeže nelze považovat za prevenci, je třeba vybírat a podporovat takové programy a koncepce, které budou plnit funkce regenerační, relaxační, výchovné, sociálně preventivní a kompenzační. Začlenění dítěte do volnočasové aktivity je poměrně složitý proces, u něhož je nezbytné, aby obsahoval faktory informační, motivační, ekonomické i sociální. V životě dětí i mládeže s nástupem informačních technologií došlo v oblasti volného času ke změnám. Sport a kultura se zkomercionalizovaly, dominantními médii se staly počítače, internet, televize, poslech reprodukováné hudby. Mnoho dětí neví, jak smysluplně využít svůj volný čas, proto podléhají nudě. Vlastní aktivity nahrazují televize a video. (Viehoffová, Reuysová, 2000) Je jasné, že v životě dětí a mládeže hrají digitální média důležitou roli a bylo by špatné jim je zakazovat či jiným způsobem je zatracovat. Je třeba mít na paměti, že čím jsou děti mladší a nevyzrálejší, tím větší mají média vliv na utváření názorů a postojů. Důležitým aspektem je výchova k rozvoji osobnosti dětí, osvojení si pozitivního sociálního chování, zdravého životního stylu a přirozeného odmítání všech forem porušování zákona. Nejzdravějšími volnočasovými aktivitami jsou sportovní a pohybové, které naplňují v mnoha oblastech zdravý životní styl, rozvíjejí socializaci a celou osobnost mladých lidí. Kvalitně vyplněný volný čas samozřejmě nevyřeší vše, ale zmenšuje pravděpodobnost, že dítě „sklouzne“ k nežádoucím jevům spojeným s počítačovými technologiemi a k sociálně patologickým jevům všeobecně, zároveň zvyšuje šanci, že dítě bude v něčem úspěšné. Při vytváření volnočasových aktivit není důležité množství, ale jejich skladba a kvalita (Hájek et al., 2008).

## Metodické poznámky

Hlavním cílem výzkumného šetření byla analýza rizikového chování a možností zneužívání informačních a komunikačních technologií ve vzorku dětí a mládeže.

K naplnění tohoto cíle byla zvolena metoda kvantitativního výzkumu. Bylo využito kritické analýzy odborných tištěných a elektronických informačních zdrojů a techniky anonymního dotazníku. Samotné dotazování proběhlo v rozmezí ledna až května 2010. Nejdříve bylo kontaktováno vedení vybraných základních a středních škol, jemuž byly sděleny základní informace o výzkumu, vždy se jednalo o jednu základní a jednu střední školu v každém krajském městě republiky (podrobněji viz tab. 1 a 2). Na základních školách byl dotazník určen pouze pro žáky druhého stupně.

Po získání souhlasu vybraných škol byl v každé z nich osloven pedagog, který byl pověřen rozděním i sběrem dotazníků mezi žáky a studenty v jednotlivých třídách, většinou se jednalo o učitele, který vyučoval předmět Informatika.

Respondentům bylo rozdáno celkem 1300 anonymních nestandardizovaných dotazníků, obsahujících celkem 35 položek s uzavřenou nabídkou odpovědí, z toho 29 s možností jednoznačné volby, 6 mnohoznačné volby. Na každou školu tedy připadlo 50 dotazníků, zpět se vrátily 1072 vyplněné formuláře.

Data z formulářů byla převedena do elektronické podoby, výstupy byly získány pomocí popisné statistiky za využití programu EpiInfo, v. 6.04 en (Dean et al., 1994).

Kraj ČR	Skupina respondentů					
	Dívky n = 525		Hoši n = 547		Celkem n = 1072	
	Počet	%	Počet	%	Počet	%
Karlovarský	45	8,6	38	6,9	83	7,7
Olomoucký	50	9,5	44	8,0	94	8,8
Plzeňský	37	7,0	46	8,4	83	7,7
Ústecký	36	6,9	43	7,9	79	7,4
Středočeský	42	8,0	60	11,0	102	9,5
Pardubický	42	8,0	43	7,9	85	7,9
Liberecký	39	7,4	40	7,3	79	7,4
Vysočina	42	7,8	42	7,7	84	7,7
Moravskoslezský	37	7,0	43	7,9	80	7,5
Jihočeský	38	7,2	33	6,0	71	6,6
Jihomoravský	40	7,6	40	7,3	80	7,5
Zlínský	38	7,2	40	7,3	78	7,3
Královéhradecký	39	7,4	35	6,4	74	6,9

Tabulka 1: Charakteristika respondentů z hlediska zastoupení jednotlivých krajů a pohlaví

Věková kategorie	Skupina respondentů					
	Dívky n = 525		Hoši n = 547		Celkem n = 1072	
	Počet	%	Počet	%	Počet	%
19 let a více	44	8,4	45	8,2	89	8,3
17–18 let	106	20,2	112	20,5	218	20,3
15–16 let	150	28,6	133	24,3	283	26,4
13–14 let	111	21,1	130	23,8	241	22,5
11–12 let	114	21,7	127	23,2	241	22,5

Tabulka 2: Charakteristika respondentů z hlediska věkových kategorií a pohlaví

Dotazníkového šetření se zúčastnili celkem 1072 respondenti; 525 dívek a 547 hochů. Celkově nejpočetnější zastoupenou skupinou byla věková kategorie 15–16 let, nejméně zastoupenou skupinou pak věková kategorie 19 let a více.

## Výsledky dotazníkového šetření

Výsledky jsou prezentovány pomocí tabulek absolutních a relativních četností získaných tříděním souboru dle pohlaví a doprovozených textovým komentářem. Drobné odchylky v relativních četnostech (desetiny procent) jsou způsobeny zaokrouhlováním číselných hodnot na jedno desetinné místo.



Čas strávený týdně u počítače	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
méně než 2 hodiny	0	0,0	0	0,0	0	0,0
3–5 hodin	16	3,0	3	0,5	19	1,8
6–10 hodin	44	8,4	17	3,1	61	5,7
11–15 hodin	100	19,0	58	10,6	158	14,7
16–20 hodin	151	28,8	159	29,1	310	28,9
více jak 20 hodin	213	40,6	310	56,7	523	48,8

Tabulka 3: Celkový čas strávený u počítače během týdne

Celkově respondenti tráví u počítače více jak 20 hodin týdně – 523 osoby (48,8 %), z toho je 213 dívek (40,6 %) a 310 hochů (56,7 %). Méně jak 2 hodiny týdně prakticky nikdo z respondentů nevedl.

Čas strávený týdně hraním počítačových her	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
méně než 2 hodiny	156	29,7	60	11,0	216	20,1
3–5 hodin	106	20,2	154	28,2	260	24,3
6–10 hodin	30	5,7	132	24,1	162	15,1
11–15 hodin	14	2,7	82	15,0	96	9,0
16–20 hodin	8	1,5	39	7,1	47	4,4
více jak 20 hodin	13	2,5	55	10,1	68	6,3
hry na počítači nehrají	198	37,7	25	4,6	223	20,8

Tabulka 4: Čas strávený týdně u počítačových her

Celkově respondenti hrají nejčastěji počítačové hry 3–5 hodin týdně (260 osob, 24,3 %). Počítačové hry vůbec nehraje 198 dívek (37,7 %); hoši hrají počítačové hry nejčastěji 3–5 hodin týdně (154 respondenti, 28,2 %). Z tabulky je patrné, že chlapci celkově hrají počítačové hry daleko častěji než dívky.

Čas strávený týdně surfváním na internetu	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
méně než 2 hodiny	19	3,6	2	0,4	21	2,0
3–5 hodin	54	10,3	34	6,2	88	8,2
6–10 hodin	90	17,1	63	11,5	153	14,3
11–15 hodin	110	21,0	118	21,6	228	21,3
16–20 hodin	107	20,4	132	24,1	239	22,3
více jak 20 hodin	143	27,2	197	36,0	340	31,7
vůbec nesurfují	2	0,4	1	0,2	3	0,3

Tabulka 5: Čas strávený týdně surfváním na internetu

Celkově respondenti nejčastěji surfují na internetu více jak 20 hodin týdně (340 osob, 31,7 %); z toho jde o 143 dívky (27,2 %) a 197 hochů (36 %).

Na otázku, zda rodičům vadí trávení volného času dětí u počítače, odpověděl pozitivně celkem 501 respondent (46,7 %); z toho byly 282 dívky (53,7 %) a 219 hochů (40 %). Na otázku, zda rodiče kontrolují, na jaké stránky se na internetu děti dívají, odpověděli pozitivně celkem 134 respondenti (12,5 %); z toho bylo 109 dívek (20,8 %) a 25 hochů (4,6 %). Rodiče nejčastěji kontrolují své děti ve věku mezi 11.– 12. rokem.

Čas strávený týdně komunikací na sociálních sítích	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
méně než 2 hodiny	2	0,4	2	0,4	4	0,4
3–5 hodin	20	3,8	16	2,9	36	3,4
6–10 hodin	60	11,4	30	5,5	90	8,4
11–15 hodin	96	18,3	102	18,6	198	18,5
16–20 hodin	113	21,5	136	24,9	249	23,2
více jak 20 hodin	187	35,6	247	45,2	434	40,5
takto nekomunikují	47	9,0	14	2,6	61	5,7

Tabulka 6: Čas strávený týdně komunikací na sociálních sítích

Respondenti nejčastěji komunikují na sociálních sítích více jak 20 hodin týdně, což zmínily 434 osoby (40,5 %); jde o 187 dívek (35,6 %) a 247 hochů (45,2 %). Sociální síť ke komunikaci vůbec nevyužívá 61 respondent (5,7 %), z toho 47 dívek (9 %) a 14 hochů (2,6 %).

Setkání s atakou přes mobilní telefon a počítač	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
vyhrožování	35	6,7	56	10,2	91	8,5
zesměšňování	71	13,5	86	15,7	157	14,6
urážení	76	14,5	84	15,4	160	14,9
zneužití účtu	54	10,3	57	10,4	111	10,4
foto, video, hlas	201	38,3	203	37,1	404	37,7

Tabulka 7: Ataky přes informační a komunikační technologie  
(respondenti mohli zaškrtnout více kladných odpovědí současně)

Respondenti se setkali se všemi nabízenými možnostmi ataků cestou ICT. Nejčastěji se jednalo o zneužití fotografií, video- a audiozáznamů zachycujících trapné či choullostivé situace a jejich prezentaci na některé ze sociálních sítí nebo webovém portále. Častěji byly oběti útoku prostřednictvím ICT vystaveny zesměšňování a urážkám. V celém souboru se s touto formou úroku setkala 86,1 % respondentů, 83,3 % dívek a 88,8 % hochů.

Obecně se s nepříjemnou situací související s užíváním ICT setkala celkem 170 respondentů (tj. 15,9 %); 79 dívek (tj. 15 %) a 91 chlapec (tj. 16,6 %). Dle věkové kategorie byl nejvíce zastoupen věk od 13 do 14 let – celkem 54 respondentů (tj. 31,8 %); nejméně kategorie 19 let a více – celkem 10 respondentů (tj. 5,9 %).

Řešení uvedených problémů s rodiči	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
vyhrožování	7	1,3	13	2,4	20	1,9
urážení	21	4,0	21	3,8	42	3,9
zesměšňování	31	5,9	26	4,8	57	5,3
zneužití účtu	21	4,0	27	4,9	48	4,5

Tabulka 8: Řešení ataků vedených cestou ICT s rodiči  
(respondenti mohli zaškrtnout více kladných odpovědí současně)

Společně s rodiči řešilo útoky cestou ICT 15,6 % respondentů, 15,2 % dívek a 15,9 % hochů. Nejčastěji se jednalo o zesměšňování a zneužití účtu na sociální síti.

Sdělení citlivých informací cestou internetu po krátké známosti	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
jméno	382	72,8	407	74,4	789	73,6
příjmení	117	22,3	127	23,2	244	22,8
bydliště (adresa)	25	4,8	28	5,1	53	4,9
číslo mobilu	33	6,3	38	6,9	71	6,6
identifikace školy	70	13,3	51	9,3	121	11,3
e-mail	118	22,5	115	21,0	233	21,7
Skype, ICQ	128	24,4	135	24,7	263	24,5
heslo e-mailu	0	0,0	0	0,0	0	0,0
PIN kód kreditní karty	0	0,0	0	0,0	0	0,0

Tabulka 9: Svěření osobních údajů a citlivých informací po krátké známosti po internetu (respondenti mohli zaškrtnout více kladných odpovědí současně)

V případě, že by respondenti znali osobu pouze krátce a jen z komunikace po internetu, prozradili by nejčastěji své jméno (uvedlo celkem 789 osob, tj. 73,6 %; 382 dívky, tj. 72,8 %; 127 chlapců, tj. 23,2 %), dále číslo Skypu a ICQ (celkem 263 osoby, tj. 24,5 %; 128 dívek, tj. 24,4 %; 135 chlapců, tj. 24,7 %). Nikdo z respondentů by neprozradil heslo ke svému e-mailovému účtu a PIN kód své kreditní karty.

Po roční známosti pouze z komunikace po internetu by situace vypadala obdobně (viz tab. 10): respondenti by nejčastěji prozradili své jméno (celkem 968 osob, tj. 90,3 %; 467 dívek, tj. 89 %; 501 chlapec, tj. 91,6 %). Druhou nejčastěji sdělenou informací by bylo číslo Skypu a ICQ (zminily celkem 792 osoby, tj. 73,9 %; 386 dívek, tj. 73,5 %; 406 chlapců, tj. 74,2 %). Opět by nikdo z respondentů neprozradil heslo ke svému e-mailovému účtu a PIN kód své kreditní karty.

Sdělení citlivých informací cestou internetu po roční známosti	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
jméno	467	89,0	501	91,6	968	90,3
příjmení	280	53,3	303	55,4	583	54,4
bydliště (adresa)	151	28,8	157	28,7	308	28,7
číslo mobilu	186	35,4	203	37,1	389	36,3
identifikace školy	241	45,9	270	49,4	511	47,7
e-mail	374	71,2	409	74,8	783	73,0
Skype, ICQ	386	73,5	406	74,2	792	73,9
heslo e-mailu	0	0,0	0	0,0	0	0,0
PIN kód kreditní karty	0	0,0	0	0,0	0	0,0

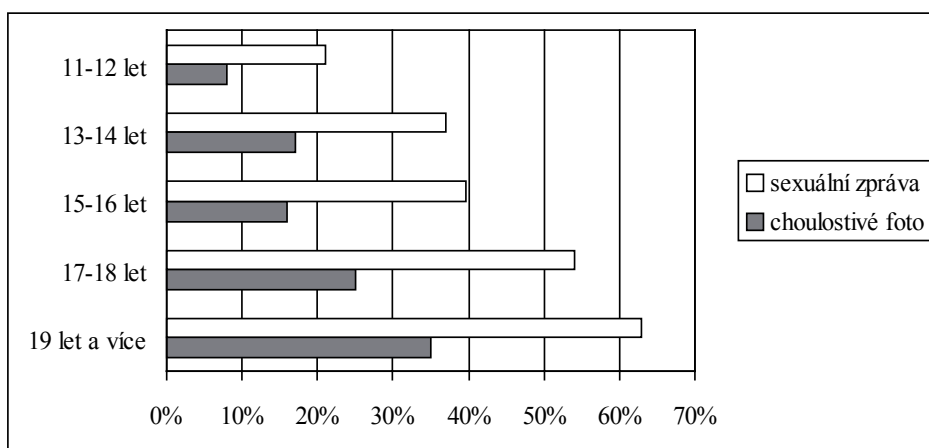
Tabulka 10: Svěření osobních údajů a citlivých informací po roční známosti po internetu (respondenti mohli zaškrtnout více kladných odpovědí současně)

Sdělení citlivých informací cestou internetu za úplatu	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
jméno	373	71,0	395	72,2	768	71,6
příjmení	69	13,1	73	13,3	142	13,2
bydliště (adresa)	16	3,0	14	2,6	30	2,8
číslo mobilu	32	6,1	27	4,9	59	5,5
identifikace školy	33	6,3	29	5,3	62	5,8
e-mail	108	20,6	117	21,4	225	21,0
Skype, ICQ	132	25,1	157	28,7	289	27,0
heslo e-mailu	0	0,0	0	0,0	0	0,0
PIN kód kreditní karty	0	0,0	0	0,0	0	0,0

Tabulka 11: Svěření osobních údajů a citlivých informací po internetu za úplatu (respondenti mohli zaškrtnout více kladných odpovědí současně)

Respondenti by svému komunikačnímu partnerovi, jehož znají pouze po internetu, za úplatu (dárek, peníze) nejčastěji prozradili své jméno (celkem 768 osob, tj. 71,6 %; 373 dívky, tj. 71 %; 395 chlapců, tj. 72,2 %). Druhou nejčastěji zveřejněnou informací by představovalo číslo Skypu a ICQ (uvedlo celkem 289 osob, tj. 27 %; 132 dívky, tj. 25,1 %; 157 chlapců, tj. 28,7 %). Nikdo z respondentů by neprozradil heslo ke svému e-mailovému účtu a PIN kód své kreditní karty.

Řada oslovených dětí se již setkala s obtěžováním intimního charakteru. Fotografii, kde je někdo částečně svlečený nebo nahý, dostali celkem 193 respondenti (tj. 18 %); 98 dívek (tj. 18,7 %) a 95 chlapců (tj. 17,4 %). Sexuálně laděnou zprávu dostalo celkem 425 respondentů (tj. 39,6 %) – 198 dívek (tj. 37,7 %) a 227 chlapců (tj. 41,5 %). Jak vyplývá z grafu č. 1, s rostoucím věkem stoupá i obtěžování intimního charakteru.



Graf 1: Obtěžování intimního charakteru dle věkové kategorie respondentů

Na schůzku dohodnutou cestou internetu by šli celkem 232 respondenti (21,6 %), z toho 105 dívek (20 %) a 127 chlapců (23,2 %). Dle věkové kategorie by se schůzkou nejčastěji souhlasili respondenti ve věku od 17 do 18 let (celkem 78, tj. 33,6 %).

Oznámení schůzky dohodnuté po internetu	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
sourozenci	97	18,5	149	27,2	246	22,9
rodičům	207	39,4	134	24,5	341	31,8
kamarádovi	149	28,4	173	31,6	322	30,0
nikomu	72	13,7	91	16,6	163	15,2

Tabulka 12: Oznámení schůzky dohodnuté po internetu

Dívky by se s plánovanou schůzkou nejčastěji svěřily rodičům (207, tj. 39,4 %), hoši kamarádovi (173, tj. 31,6 %). Pravdu o sobě na internetu píše celkem 219 respondentů (20,4 %); 101 dívka (19,2 %) a 118 chlapců (21,6 %). Většina respondentů vystupuje pod přezdívkou (celkem 805, tj. 75,1 %), z toho 395 děvčat (75,2 %) a 410 chlapců (75 %).

Prosbu o mlčení týkající se osoby – „že si spolu píšeme“ – obdrželo celkem 240 respondentů (tj. 22,4 %), z toho 110 dívek (21 %) a 130 chlapců (23,8 %). Nejčastěji šlo o děti ve věkové skupině 15–16 let.

Prosbu o mlčení týkající se obsahu – „co si spolu píšeme“ – obdrželo celkem 214 respondentů (tj. 20 %), z toho 110 dívek (21 %) a 104 chlapci (19 %). Opět šlo nejčastěji o děti ve věkové skupině 15–16 let.

Znalost některého z uvedených portálů	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
Alík	284	54,1	325	59,4	609	56,8
Libímseti	460	87,6	492	89,9	952	88,8
YouTube	514	97,9	544	99,5	1058	98,7
Hry.cz	221	42,1	329	60,1	550	51,3
Facebook	524	99,8	547	100,0	1071	99,9
Rajče	376	71,6	433	79,2	809	75,5
MySpace	201	38,3	241	44,1	442	41,2
XChat	338	64,4	386	70,6	724	67,5

Tabulka 13: Znalost některého z uvedených portálů (respondenti mohli zaškrtnout více kladných odpovědí současně)

Kromě 1 dívky prakticky všichni respondenti znají Facebook – 1071 osoba, tj. 99,9 %. Druhým nejnámějším portálem je YouTube – celkem 1058 osob, tj. 98,7 %, z toho 514 dívek (97,9 %) a 544 chlapci (99,5 %). Nejméně známým portálem mezi respondenty je MySpace – uvedly jej celkem 442 osoby, tj. 41,2 %, z toho 201 dívka (38,3 %) a 241 chlapec (44,1 %).



Účet založený na některém z uvedených portálů	Skupina respondentů					
	Dívky		Hoši		Celkem	
	Počet	%	Počet	%	Počet	%
Alík	101	19,2	106	19,4	207	19,3
Libímseti	188	35,8	166	30,3	354	33,0
YouTube	154	29,3	229	41,9	383	35,7
Hry.cz	25	4,8	71	13,0	96	9,0
Facebook	463	88,2	515	94,1	978	91,2
Rajče	124	23,6	148	27,1	272	25,4
MySpace	26	5,0	25	4,6	51	4,8
XChat	153	29,1	167	30,5	320	29,9

Tabulka 14: Účet založený na některém z uvedených portálů (respondenti mohli zaškrtnout více kladných odpovědí současně)

Nejvíce respondentů má založeno svůj účet na Facebooku – celkem 978 osob, tj. 91,2 %, z toho 463 dívky (88,2 %) a 515 chlapců (94,1 %). Nejméně respondentů má založeno svůj účet na portálu MySpace – 51 osoba, tj. 4,8 %, z toho 26 dívek (5 %) a 25 chlapců (4,6 %). U chlapců je druhým preferovaným portálem, kde mají založen svůj účet, YouTube ( uvedlo jej 229 chlapců, tj. 41,9 %). Obdobně děvčata uvedla jakou druhou možnost portál Libímseti (188, tj. 35,8 %). Ve věkové kategorii od 11 do 12 let má založen svůj účet na Facebooku celkem 240 respondentů (tj. 99,6 %).

Alespoň jeden z portálů, kde lze nahlásit závadový obsah, znají celkem 272 respondenti (25,4 %), z toho jde o 137 dívek (26,1 %) a 135 chlapců (24,7 %). Nejlépe informovaní jsou respondenti ve věkové kategorii od 15 do 16 let (celkem 68 osob, tj. 25 %).

Z pohledu trávení volného času nejvíce dětí sportuje 3 až 5 hodin týdně (333 respondenti, tj. 31,1%). Dívky sportují opět nejčastěji 3 až 5 hodin týdně (256, tj. 76,9 %), chlapci 6 až 10 hodin týdně (196, tj. 61,6 %).

Dívky nejčastěji navštěvují dva zájmové kroužky (116, tj. 22,1 %), do žádného zájmového kroužku nechodí 163 dívky (31 %). Hoši nejčastěji navštěvují 1 zájmový kroužek (264, tj. 48,3 %), zatímco do žádného kroužku nechodí 161 hoch (29,4 %).

Častý pocit nudy uvedlo celkem 220 respondentů (20,5 %), z toho bylo 126 dívek (24 %) a 94 chlapci (17,2 %). Většinu volného času tráví doma sám celkem 291 respondent (27,1 %), z toho bylo 157 dívek (29,9 %) a 134 chlapci (24,5 %). Nespokojenost se svým volným časem zmínilo celkem 260 oslovených (24,3 %), z toho 132 dívky (25,1 %) a 128 chlapců (23,4 %).

## Diskuse

Internet se stal během posledních 20 let běžnou součástí našeho života, využíváme jej ke vzdělávání, práci i zábavě. Vznikl také další nový fenomén – fenomén kyberprostoru, virtuální svět, kde se téměř každý z nás čas od času pohybuje a zanechává v něm svůj otisk. Hledáme-li nějaké informace, dostane se nám čím dál častěji odkazu, že „je to všechno na internetu“.

Se zdokonalováním ICT se postupně stírá hranice mezi reálným a virtuálním. Zejména děti jsou od útlého věku zvyklé přistupovat k počítači a k internetu a manipulaci s nimi vnímají jako naprostou samozřejmost, obdobně tomu je s mobilním telefonem. Bohužel si řada z nich neuvědomuje rizika, která jsou s těmito činnostmi spojená, což může vést k prozrazení mnoha informací důvěrného charakteru, a kromě úniku i k jejich zneužití. Nevyplácí se také absolutní důvěra v pravdivost publikovaných informací, kdy daní za jejich rychlé vyhledání a poskytnutí je mnohdy pochybná kvalita, prezentace nesprávných, lživých a nebezpečných názorů. Nedá se tedy automaticky ztotožnit, že vše, co najdeme na internetu, je správné, hodnotné a pravdivé. Vyplatí se vzájemné porovnávání informací získaných z několika různých zdrojů, doporučuje se preferovat zejména klasické tištěné materiály a servery, jejichž obsah je odborně recenzován.

Před publikováním jakýchkoli informací (zejména osobního charakteru) je třeba neopomenout pozorné přečtení pravidel a licenčních podmínek, což platí ve zvýšené míře při pohybu na sociálních sítích typu Facebooku. Bohužel, děti a dospívající je často přeskakují nebo ignorují, a tak se dopouštějí závažných chyb, které již nelze jednoduše vzít zpět, nebo jejich následky řešit právní cestou. Mnoho zde zveřejněných materiálů (fotografií, konverzací) by se lidé báli ukázat a říci svým nejbližším při komunikaci „z očí do očí“, nic jim ovšem nebrání je publikovat na síti, poněvadž nejsou pod přímým dohledem. To je však velký omyl – internet má „paměť“ a každý v něm více či méně zanechává své stopy. V extrémních případech může být jedinec zpětně identifikován a spojen s činnostmi, které na síti prováděl, odhaleny jeho zvyky, názory, spotřební a profesní chování, deviace. Tak, jako si ceníme své rodiny, zdraví, postavení, financí a úspěchů, bychom si měli cenit též svého soukromí, a to i ve virtuální podobě. Nedoporučuje se sdělovat více údajů, než je skutečně potřebné, a jen tomu, koho známe lépe než jen ze setkávání na internetu. Řada pachatelů trestné činnosti dokonale ovládá tzv. sociální inženýrství, není pro ně problém vzbudit důvěru oběti, manipulovat s ní; opatrnost, ověřování identity komunikačního partnera a mírně „paranoidní“ přístup jsou tedy plně na místě.

Před svou expanzí byl předchůdce internetu sítí vojenskou, vládní a neveřejnou, po svém otevření se velmi rychle rozšířil zejména do akademického sektoru. V současné době internet obsáhl prakticky celou planetu, jeho uživatelů je několik miliard. Významný podíl jeho kapacity je určen komerčním aktivitám, které také podstatně financují jeho další rozvoj a udržování. Průnik reklamy na internet je další daní za jeho služby. Na jedné straně vytváří konkurenční prostředí a tlak na přijatelný poměr ceny a kvality nabízených komodit, na straně druhé komplikuje řadě uživatelů běžný pohyb na síti, inzeruje výrobky a služby, které si nemohou „osahat“, jsou odkázáni pouze na solidnost obchodníka.

Žádný univerzální vyhledávač neobsáhne celý obsah internetu. Některé části sítí jsou běžným neprivilegovaným uživatelům záměrně nedostupné (utajované informace), jiné dovolují jen omezený průnik vyhledávacím robotům, které indexují zveřejněná data.

Cenzura obsahu internetu je sice v omezené míře možná, váže však značné technické a lidské kapacity. V globálním měřítku je prakticky neproveditelná, poněvadž toto médium je diverzifikované, vysoce dynamické, funguje bez ohledu na státní hranice, uživatelé preferují svobodnou výměnu informací a jakékoli zásadnější omezení není v jejich komunitách pozitivně přijímáno.

Rozumná míra cenzury na straně rodičů dětí a dospívajících je ale realizovatelná a žádoucí. Nejjednodušší je stanovení „pravidel hry“ a kontrola jejich dodržování. Internetové prohlížeče, ev. operační systém mají také možnost nastavení dětské pojistky (filtrace potenciálně nebezpečného obsahu a služeb, používání počítače jen v určité době), lze rovněž využít nástrojů třetích stran (speciálních hlídacích programů). V každém případě je vhodné, aby rodiče dítěti takovou skutečnost předem sdělili, probrali s ním účel takové ochrany, nepoužívali ji skrytě, „na zapřenou“. Rovněž je vhodné, aby se rodiče aktivně zajímali o to, co jejich potomek na počítači a na internetu dělá, jak využívá svůj mobilní telefon. I dítě má právo na své soukromí, je proto potřebné chovat se taktně, nezničit důvěru vzájemného vztahu a otevřenost komunikace.

Práce s ICT vyžaduje nejen odpovídající úroveň technické a informační, ale též mediální gramotnosti. Mediální výchova, tvorba, obhajoba a posuzování vlastních postojů, fakta o působení reklamy, jejich tricích a schopnosti jí čelit by měly být dítěti poskytovány již v rodině před začátkem povinné školní docházky, rovněž tak povědomí o informacích jako hodnotě, která má svou cenu, již je třeba umět odhadnout, chránit a vážit si jí.

Děti nejsou jen obětmi poškozenými zneužitím ICT, ale samy aktivně mohou takovým situacím napomáhat. Řada z nich dobře zná „svou taxu“, kterou mohou žádat za intimní fotografie, osobní schůzky nebo různé sexuální aktivity, vybírá si ji financováním kreditů na mobilní telefon, vstupenkami do her, sponzoringem ve formě oblečení, kosmetiky, módních doplňků, sportovních a dalších volnočasových aktivit, nebo přímo v hotovosti.

Každé svolení s komunikací přes webovou kameru nebo dokonce s osobní schůzkou je pro dítě potenciálně nebezpečné a mělo by být rázně odmítnuto. Každá nečekaná, nepříjemná nebo nezvyklá situace, která se dítěti přihodí při manipulaci s počítačem, internetem nebo mobilním telefonem, by měla být s důvěrou automaticky probrána s rodiči nebo jinou dospělou osobou dítěti blízkou (zákonný zástupce, pedagog, vychovatel).

Zanedbatelné není ani porušování autorských práv, jehož se dopouštějí osoby, které na internetu nelegálně vystaví a umožní šíření audiovizuálních děl a počítačových programů, ev. provedou odstranění ochrany v těchto souborech. Vlastní stažení takového obsahu uživatelem (zejména v případě zvuku a videa) obvykle trestné není, avšak jde o pohyb v „šedé zóně“. Navíc řada takto „upravených“ programů může napáchat značné škody (poškození nebo zničení dat, jejich vykrádání, zavírování počítače, sítě, atd.) a mít tragické následky (systémy kontroly a řízení, ale i domácí počítač s důležitými dokumenty, rodinnými fotografiemi a videi za několik let).

Příliš časté a dlouhodobé používání ICT může generovat řadu zdravotních problémů. Nejde pouze o závislostní chování s výraznou psychickou složkou, růstem tolerance, abstinencií příznaky, prokrastinací, oploštěním komunikace a bloky v případě „face to face“, ale též o nepravdivý výživový režim s nevhodnou a vynucenou polohou těla a vyšší zátěží páteře, očí a rukou, se zhoršením krevního oběhu zejména v dolní polovině těla, s hrozící nadváhou nebo obezitou.

Toužíme po mezilidské komunikaci a setkávání, paradoxně náš ale vymoženosti ICT mohou odcizovat, budeme-li se spoléhat výlučně na ně a pohrdneme-li reálným světem a reálným komunikačním parterem.

## Závěr

Byla realizována anonymní dotazníková studie na vzorku 1072 respondentů – žáků a studentů druhého stupně vybraných základních a středních škol ze všech krajů ČR.

Téměř polovina respondentů tráví u počítače více než 20 hodin týdně, třetina surfuje na internetu více než 20 hodin týdně. Nejčastější doba, kterou respondenti věnují hraní počítačových her, činí 3–5 hodin týdně, takto se chová čtvrtina souboru. Pětina oslovených počítačové hry vůbec nehraje. Na sociálních sítích se respondenti nejčastěji pohybují více než 20 hodin týdně (uvedlo 40 % souboru), tímto způsobem vůbec nekomunikuje 6 % vzorku.

Respondenti se setkali se všemi zásadními možnostmi ataků cestou ICT, zejména se jednalo o zneužití choulostivých obrazových a zvukových záznamů. Oběti útoku prostřednictvím ICT byly vystaveny především zesměšňování a urážkám, což uvedlo 86 % celého souboru. Jen 16 % oslovených dětí řešilo útoky cestou ICT společně s rodiči. Rodičům téměř poloviny dotazovaných vadí trávení volného času jejich potomků u počítače. Pouhých 13 % dětí většinou ve věku 11–12 let rodiče kontrolují, co na počítači a internetu dělají.

Téměř tři čtvrtiny respondentů by po krátké a výlučně internetové známosti prozradily komunikačnímu partnerovi své jméno, čtvrtina pak i číslo Skype a ICQ. Obdobně by situace vypadala po roční neosobní známosti, kdy by své jméno zveřejnilo 90 % dotazovaných, číslo Skype nebo ICQ téměř tři čtvrtiny. Tytéž informace by děti byly ochotné poskytnout i za úplatu.. Nikdo z respondentů by neprozradil heslo ke svému e-mailovému účtu a PIN kód své kreditní karty. Pětina respondentů o sobě na internetu zveřejňuje pravdivé údaje, tři čtvrtiny vystupují pod přezdívkou.

Přibližně pětina dětí se již setkala s obtěžováním intimního charakteru spojeným s obdržením choulostivé fotografie. Sexuálně laděnou zprávu dostalo přibližně 40 % souboru. Pětina oslovených nejčastěji ve věku 17–18 let by šla na schůzku dohodnutou přes internet. Dívky by o této schůzce informovaly rodiče, hoši kamaráda. Pětina dospívajících ve věku 15–16 let obdržela prosbu o mlčení týkající se komunikačního partnera nebo obsahu komunikace.

Prakticky všichni respondenti znají Facebook, téměř všichni portál YouTube. Nejvíce oslovených (92 %) má založen účet na sociální síti Facebook. Čtvrtina dětí a dospívajících ví, kde na internetu je možné nahlásit závadový obsah.

Internet nabízí demokratické prostředí s minimálními omezeními, které se stále rozvíjí a roste. Abychom dokázali plně využít jeho potenciálu, a nebyli přitom poškozeni, je nezbytné se neustále vzdělávat o způsobech efektivního vyhledávání a práce s informacemi, ale také o vlastní ochraně před hrozbami, které jsou se sítí a s dalšími ICT spojeny. Těžisko preventivního působení leží zprvu na bedrech rodiny a školy, později na osobní zodpovědnosti každého uživatele ICT za své chování.

## **RISK BEHAVIOR AMONG ELEMENTARY SCHOOL PUPILS AND HIGH SCHOOL STUDENTS WHILE WORKING WITH COMPUTERS AND THE INTERNET**

**Abstract:** Computer technology, computer networks, mobile phones and other advanced information and communication technologies (ICT) allow a rapid exchange of information and bring new opportunities in employment, science, education and entertainment. An ill-considered use of ICT by children and young people in particular may lead to many health and social disorders. Quantitative research carried out in all regions of the Czech Republic addressed 1072 pupils from 26 schools (elementary and high schools) in the form of an anonymous questionnaire. Its questions were related to their leisure time activities, work with ICT, and offensive behavior via ICT. The results have shown that there is a low level of parental control; 30 % of respondents have already experienced offensive behavior via ICT. Only 5 % of the sample have addressed their parents when dealing with a problematic situation, while more than 50 % of the respondents are willing to make their personal data public after one year of on-line communication. It is necessary to strengthen parents' interest in their children's free time and in how they handle ICT, as well as to build trust between the two parties and apply early solutions to problems. As for the school environment, it is necessary to deepen the information literacy of pupils with an emphasis on their personal safety and netiquette.

**Key words:** safety, questionnaire, game, ICT, Internet, computer, prevention, risk, student, school, offensive behavior, free time, research, abuse, pupil