E-Bezpečí 2020, 5(1): Page 115-118. Univerzita Palackého v Olomouci. ISSN 2571-1679.
Online: https://www.e-bezpeci.cz/index.php?view=article&id=1859

UČITELÉ, NESDÍLEJTE NA ŠKOLNÍCH WEBECH ZÁZNAMY Z ONLINE VÝUKY, NA KTERÝCH DOCHÁZÍ K JEDNOZNAČNÉ IDENTIFIKACI DĚTÍ. VYSTAVUJETE JE TAK RIZIKU!

Kamil KOPECKÝ

Uzavření škol s sebou přineslo skokový přechod k online výuce, za který je třeba učitele pochválit. Ze dne na den se velké části z nich podařilo přenést velkou část vzdělávacích aktivit do online prostředí, začali tvořit vzdělávací materiály všeho druhu, organizovat online výuku, realizovat synchronní videokonference, z mnoha z nich se ze dne na den stali youtubeři a streameři. Dokázali tak, že přechod do digitálního vzdělávání není vůbec tak obtížný, jak se může stát. Online vzdělávání s sebou však kromě zjevných benefitů přineslo některá rizika. A právě na ně se podíváme v dnešním textu.

Velká část učitelů přenesla svou výuku do online aplikací a systémů, které slouží k běžné mezilidské komunikaci či přímo k online vzdělávání. Své žáky pak často přiměli, aby si v daných aplikacích vytvořili své účty, prostřednictvím kterých budou s učitelem komunikovat. Opomněli však, že **aplikace mají své věkové limity** a také na to, že od loňského roku v ČR platí Zákon o zpracování osobních údajů č. 110/2019, který v paragrafu 7 říká: **Dítě nabývá způsobilosti k udělení souhlasu se zpracováním osobních údajů v souvislosti s nabídkou služeb informační společnosti přímo jemu dovršením patnáctého roku věku.** Jinými slovy, pokud si dítě chce založit účet na službě zpracovávající osobní údaje (což je drtivá většina komunikačních

nástrojů a služeb), **samo to nesmí udělat až do 15 roku a mělo by o to vždy žádat rodiče**. Škola by tedy měla požádat rodiče o souhlas s tím, že bude jejich dítě využívat služby, které pro ně nejsou věkově určeny. Typickým příkladem je např. aplikace WhatsApp, která má věkový limit 16 let. Tu by např. neměly bez souhlasu rodičů žáci základních škol vůbec používat. Správné řešení je např. jít cestou GSuite či Office 365, ve které má škola nainstalován školní vzdělávací systém a sama spravuje účty svých žáků - samozřejmě se souhlasem rodičů. **Školám však nedodržení veškerých regulí nelze plošně vyčítat, bylo třeba reagovat okamžitě, rychle, ze dne na den byly vhozeny do zcela nové situace a musely zásadně proměnit svou výuku.** Nyní je však dostatek času zajistit, aby bylo vše v pořádku i v rámci právního rámce.

Další problém je obecně **sdílení záznamů a snapshotů/screenů z videopřednášek a videochatů na webech škol**. Je třeba uvědomit si, že by školy měly chránit osobní údaje svých žáků před možným zneužitím, což se děje např. v případě fotografií tříd, u kterých by neměl náhodný návštěvník www stránek školy rozpoznat, které dítě se na fotografii jak jmenuje (tj. nedochází k jednoznačné identifikaci dítěte) apod. Bohužel v případě zveřejnění záznamů či snapshotů z videokonferencí a videochatů **dochází k velmi přesné identifikaci dítěte** - k dispozici je jméno, příjmení, fotografie obličeje, dokonce vybavení domácnosti (pokojíčku, kuchyně apod.). Kromě samotné identifikace tyto **záznamy zdůrazňují sociální rozdíly mezi dětmi**, které se odráží právě na vybavení bytu/domu v pozadí, a mohou tak děti vystavit nechtěné pozornosti spolužáků a dalších osob, která se může odrazit např. přesdílením záznamů do prostředí sociálních sítí, agresí, či vážnější kyberšikaně. Na problém dále upozorňujeme v našem streamu zde.

Řada škol se online výukou prostřednictvím videokonferencí chlubí, což je zcela v pořádku. **Škola by však měla vždy dbát na to, aby při zveřejňování těchto záznamů nedocházelo k jednoznačné identifikaci dětí a aby se zveřejněním souhlasili rodiče**. Je otázkou, jak při uzavření škol tento souhlas zajistit - cestou jsou např. školní informační systémy Bakaláři, Edookit apod., do kterých mají rodiče přístup a mohou souhlas

potvrdit. O zveřejnění těchto záznamů by měl rodič vždy vědět a být o nich školou informován, pravidla GDPR se na ně jednoznačně vztahují.

(Ukázka ze stránek jedné ZŠ, na které najdeme na jednom místě přesnou identifikaci desítek žáků.)

Na tomto místě je třeba **rozbít opětovně mýtus o online predátorech, kteří si tímto způsobem vyhledávají děti, které pak mohou kontaktovat. Stejně tak neplatí, že pokud dítě tráví více času v online prostředí, snadněji je tzv. predátory "loveno".** Jde o mýty a fabulace novinářů, realita je jiná.

"Je velkým omylem myslet si, že pokud dítě začne pouze více využívat online komunikaci (např. chatovat), může se stát obětí sexuálních predátorů. ***Rizikem není četnost, ale typ služeb, kde ke komunikaci dochází.*** *Tzn. pokud bude dítě komunikovat na službách určených pro dospělé (seznamování, erotika, zábava), je zvýšená pravděpodobnost možnosti setkání se se sexuálně motivovanou komunikací,"* vysvětluje major Václav Písecký, vedoucí oddělení kyberkriminality OIK SKPV pražské policie.

Zvýšené množství osobních údajů dětí v online prostředí má

spojitost především s online agresí (posmíváním, dehonestováním…), s kyberšikanou, s reakcemi spolužáků či dalších osob, ne však s online predátory!

Závěrem je třeba školy pochválit za to, jak se většina z nich dokázala přes všechny potíže se situací vyrovnat. Zároveň však opětovně apelujeme: **Prosím, nesdílejte na svých webových stránkách či školních profilech na sociálních sítích nic, co by mohlo vést k jednoznačné identifikaci vašich žáků! A pokud ano, pouze s výslovným souhlasem jejich rodičů.**

Pro E-Bezpečí
Kamil Kopecký
Pedagogická fakulta Univerzity Palackého v Olomouci