VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

RIZIKA TIKTOKU Z POHLEDU KYBERNETICKÉ BEZPEČNOSTI A OCHRANY OSOBNÍCH ÚDAJŮ STUDENTŮ STŘEDNÍ ŠKOLY

Autor práce: Julija Didenko, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Julija Didenko, DiS

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Rizika TikToku z pohledu kybernetické bezpečnosti a ochrany osobních údajů studentů střední školy

Název bakalářské práce v anglickém jazyce: Risks of TikTok from the Perspective of Cybersecurity and Personal Data Protection of Secondary School Students

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): RNDr. Růžena Ferebauerová
Datum zadání bakalářské práce (měsíc, rok): listopad 2025

Cíl bakalářské práce:
Hlavní cílem bakalářské práce je vyhodnotit rizika spojená s používáním aplikace TikTok u studentů střední školy Trivis Praha z pohledu kybernetické bezpečnosti, právní ochrany osobních údajů a ochrany osobních údajů. Vedlejším cílem je navrhnout doporučení, která mohou přispět ke zvýšení bezpečnosti uživatelů této platformy, a to na základě vymezení teoretických východisek kybernetické bezpečnosti, právní ochrany osobních údajů a posouzení způsobů, jak studenti TikTok používají.

Student: Julija Didenko, DiS.	29.11.2025 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	15.12.25 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	15.12.2025 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2025 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.12.2025 *datum*	*podpis*

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce, RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

DIDENKO, J. Rizika TikToku z pohledu kybernetické bezpečnosti a ochrany osobních údajů studentů střední školy: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 73 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kybernetická bezpečnost, TikTok, ochrana osobních údajů, sociální sítě, studenti středních škol.

Bakalářská práce se zabývá problematikou rizik spojených s používáním sociální sítě TikTok z hlediska kybernetické bezpečnosti a ochrany osobních údajů u studentů střední školy. Teoretická část práce se zaměřuje na vymezení základních pojmů souvisejících s kybernetickou bezpečností, ochranou osobních údajů a legislativním rámcem upravujícím zpracování osobních údajů v digitálním prostředí. Dále popisuje fungování sociální sítě TikTok a nejčastější typy hrozeb, které mohou ohrozit bezpečnost a soukromí mladých uživatelů. Praktická část práce je založena na dotazníkovém šetření mezi studenty střední školy TRIVIS Praha, konkrétně studenty 1 a 2. ročníku, a zaměřuje se na zjištění úrovně povědomí o rizicích používání aplikace TikTok, způsoby zabezpečení uživatelských účtů a přístup studentů k ochraně osobních údajů. Na základě vyhodnocení získaných výsledků jsou navržena doporučení a opatření, která mohou přispět ke zvýšení kybernetické bezpečnosti a ochrany osobních údajů studentů při používání sociálních sítí.

ABSTRACT

DIDENKO, J. Risks of TikTok from the Perspective of Cybersecurity and Personal Data Protection of Secondary School Students: bachelor's thesis. České Budějovice: College of European and Regional Studies, 2026. 73 pp. Supervisor of the bachelor's thesis: RNDr. Růžena Ferebauerová.

Key words: cybersecurity, TikTok, personal data protection, social networks, secondary school students.

The bachelor's thesis addresses the risks associated with the use of the social network TikTok from the perspective of cybersecurity and personal data protection among secondary school students. The theoretical part focuses on defining basic concepts related to cybersecurity, personal data protection, and the legislative framework governing the processing of personal data in the digital environment. It also describes the functioning of the social network TikTok and the most common types of threats that may endanger the security and privacy of young users. The practical part of the thesis is based on a questionnaire survey conducted among students of the TRIVIS secondary school in Prague, specifically first- and second-year students. It focuses on identifying the level of awareness of risks associated with the use of the TikTok application, methods of securing user accounts, and students' approach to personal data protection. Based on the evaluation of the obtained results, recommendations and measures are proposed that may contribute to improving cybersecurity and personal data protection of students when using social networks.

Obsah

Úvod

V současné digitální době hrají sociální sítě významnou roli v každodenním životě mladé generace. Mezi nejpopulárnější platformy patří sociální síť TikTok, která je využívána především dětmi a dospívajícími ke sdílení krátkých videí, komunikaci a zábavě. Rychlý rozvoj této platformy a její masové využívání však s sebou přináší nejen nové možnosti, ale také řadu rizik spojených s kybernetickou bezpečností a ochranou osobních údajů.

Mladí uživatelé často nevěnují dostatečnou pozornost zabezpečení svých uživatelských účtů a ochraně osobních údajů, což je může vystavit různým hrozbám, jako jsou kybernetické útoky, zneužití osobních údajů, kyberšikana či manipulace ze strany cizích osob. Sociální síť TikTok navíc pracuje s rozsáhlým množstvím osobních dat, jejichž zpracování a ochrana vyvolává otázky nejen z hlediska kybernetické bezpečnosti, ale i z pohledu platné legislativy v oblasti ochrany osobních údajů.

Téma této bakalářské práce je proto zaměřeno na analýzu rizik spojených s používáním sociální sítě TikTok u studentů střední školy z hlediska kybernetické bezpečnosti a ochrany osobních údajů. Práce se soustředí na problematiku bezpečného chování mladých uživatelů v online prostředí a na úroveň jejich informovanosti o možných hrozbách, které mohou ohrozit jejich soukromí a bezpečnost.

Cílem bakalářské práce je vyhodnotit rizika spojená s používáním aplikace TikTok u studentů střední školy TRIVIS Praha a posoudit jejich povědomí o zásadách kybernetické bezpečnosti a ochrany osobních údajů. Součástí práce je rovněž snaha o formulaci doporučení a opatření, která mohou přispět ke zvýšení bezpečnosti studentů při používání sociálních sítí. Práce je rozdělena na teoretickou a praktickou část, přičemž teoretická část se zaměřuje na vymezení základních pojmů a legislativního rámce, zatímco praktická část je založena na dotazníkovém šetření mezi studenty střední školy.

1 Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je analyzovat rizika spojená s používáním sociální sítě TikTok u studentů střední školy z hlediska kybernetické bezpečnosti a ochrany osobních údajů. Práce se zaměřuje na identifikaci nejčastějších hrozeb souvisejících s používáním této platformy a na zhodnocení úrovně povědomí studentů o rizicích, která mohou ohrozit jejich bezpečnost a soukromí v digitálním prostředí. Vedlejším cílem práce je navrhnout doporučení a opatření, která mohou přispět ke zvýšení kybernetické bezpečnosti a ochrany osobních údajů mladých uživatelů sociálních sítí.

Metodika bakalářské práce kombinuje teoretický a empirický přístup k dosažení stanovených cílů. Teoretická část práce je zaměřena na rešerši odborné literatury, právních předpisů a odborných zdrojů vztahujících se k problematice kybernetické bezpečnosti, ochrany osobních údajů a fungování sociálních sítí, se zvláštním zaměřením na sociální síť TikTok. Teoretická část se dále věnuje vymezení základních pojmů, popisu mechanismů fungování platformy TikTok a identifikaci nejčastějších typů hrozeb, které mohou negativně ovlivnit bezpečnost a soukromí mladých uživatelů.

Empirická část práce je založena na kvantitativním výzkumu formou dotazníkového šetření realizovaného mezi studenty střední školy TRIVIS Praha, konkrétně studenty 1 a 2. ročníku. Cílem dotazníkového šetření je zjistit způsoby používání aplikace TikTok, úroveň zabezpečení uživatelských účtů, míru povědomí studentů o rizicích spojených s ochranou osobních údajů a jejich přístup k ochraně soukromí v online prostředí. Získaná data budou analyzována pomocí základních statistických metod, zejména absolutní a relativní četnosti, a přehledně prezentována prostřednictvím grafů. Výsledky šetření budou interpretovány v kontextu stanovených cílů práce a poslouží jako podklad pro návrh doporučení směřujících ke zvýšení kybernetické bezpečnosti a ochrany osobních údajů studentů při používání sociálních sítí.

2 Kybernetická bezpečnost

Kybernetická bezpečnost je definována jako soubor obecně uznávaných pravidel a postupů týkajících se bezpečného provozu informačních a komunikačních technologií. Hlavním účelem kybernetické bezpečnosti je chránit kyberprostor před narušením, zneužitím nebo poškozením. Základní právní rámec pro tuto oblast v České republice je definován zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, který pokrývá klíčové pojmy, bezpečnostní opatření v oblasti počítačových sítí, stejně jako postupy související s hlášením kybernetických incidentů. Dodržování těchto opatření je nezbytné nejen pro omezení dopadu kybernetických útoků, ale také pro jejich efektivní prevenci.[1]

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) na svých webových stránkách zdůrazňuje důležitost ochrany digitálních technologií a bezpečného fungování internetu. Navzdory tomu však podle tohoto úřadu přetrvává ve společnosti nízká úroveň povědomí o problematice kybernetické bezpečnosti, která je často podceňována a nesprávně chápána.[2] Z hlediska zajištění kybernetické bezpečnosti se jedná o nepříznivý stav, a to zejména s ohledem na skutečnost, že otázkám kybernetické a informační bezpečnosti je ve značném rozsahu věnována pozornost také v dokumentu Bezpečnostní strategie České republiky. Tento dokument zároveň upozorňuje na skutečnost, že i relativně malá skupina aktérů může způsobit strategicky závažné narušení kybernetického prostoru.[3]

V kontextu uvedených skutečností je zřejmé, že schopnost odolávat škodlivým aktivitám v kybernetickém prostoru úzce souvisí s úrovní vzdělání, znalostí a praktických zkušeností v oblasti kybernetické bezpečnosti. Zranitelnost jednotlivců i institucí je proto významně ovlivněna odbornou připraveností osob, které s informačními systémy pracují. Lze konstatovat, že míra odolnosti veřejných institucí vůči kybernetickým hrozbám odpovídá schopnosti jejich zaměstnanců těmto hrozbám účinně čelit.[4]

[1] ČESKO. *Zákon č. 264/2025 Sb., o kybernetické bezpečnosti.* In: *Sbírka zákonů České republiky.* 2025.
[2] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Vzdělávání. Online. Dostupné z: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/ [cit. 2026-01-02].
[3] MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. Bezpečnostní strategie České republiky 2023. Online. Dostupné z: https://mzv.gov.cz/file/5101086/Bezpecnostni_strategie_2023.pdf [cit. 2026-01-04].
[4] VALUCH, J. Kybernetické hrozby v kontexte medzinárodného práva a medzinárodnej bezpečnosti. Bratislava: Wolters Kluwer, 2019. ISBN 978-80-8168-931-2, s. 12.

Kyberprostor lze charakterizovat jako dynamicky se vyvíjející virtuální prostředí, které umožňuje nepřetržitý tok informací a přináší řadu přínosů. Zároveň však s sebou nese i specifická bezpečnostní rizika, mezi něž patří zejména anonymita. Ta může hrát významnou roli při narušování bezpečnosti informačních a komunikačních technologií a zneužívání dat.[5]

2.1 Vznik kyberprostoru

Vznik kyberprostoru je úzce spojen s rozvojem výpočetní techniky a počátky síťového propojení počítačů. První významný krok nastal koncem 60. let 20. století, kdy došlo k propojení několika univerzitních počítačů a ke vzniku zárodku sítě ARPANET. V této fázi vývoje nikdo nepředpokládal, že se síťové technologie rozvinou do podoby globální infrastruktury propojující miliony uživatelů. Tvůrci tehdejších komunikačních protokolů se soustředili především na funkčnost a spolehlivost přenosu dat, zatímco otázkám bezpečnosti nebyla věnována taková pozornost, jaká je kladena v současnosti. Slabiny těchto technologií se postupně staly cílem nelegálních aktivit, které se s dalším rozšiřováním sítí začaly výrazně projevovat.

Rozvoj informačních a komunikačních technologií probíhal mimořádně rychlým tempem, na které společnost nebyla dostatečně připravena. Technický pokrok výrazně předstihl schopnost společnosti přizpůsobit se novým podmínkám a vytvořit odpovídající právní, etický a morální rámec. Zatímco lidská společnost si po dlouhá staletí formovala své normy a pravidla postupně, prudký technologický vývoj ve druhé polovině minulého století způsobil, že tyto zavedené mechanismy přestaly odpovídat nové realitě. Výpočetní technika a telekomunikace se staly hybnou silou změn, které zasáhly nejen technickou oblast, ale i samotné fungování společnosti.

Lidské interakce byly historicky vždy založeny na přímém kontaktu ve fyzickém prostředí, kde komunikace probíhala jak na verbální, tak na neverbální úrovni. Vnímání druhého člověka bylo ovlivněno nejen obsahem sdělení, ale také jeho projevy, gesty a fyzickou přítomností. Postupným vývojem verbální komunikace a vznikem písemných forem sdělování však začalo docházet k oddělení komunikace od fyzického prostoru. Významným mezníkem byl rozvoj knihtisku, který umožnil masové šíření textu a přenesl

[5] SVOBODOVÁ, M., SCHEU, H. a GRINC, J. Listina základních práv Evropské unie: deset let v praxi – hodnocení a výhled. Praha: Auditorium, 2019. ISBN 978-80-87284-89-1, s. 148.

čtenáře do světa představ a imaginace. Přestože šlo o určitý krok směrem k virtuálnímu prostoru, jednalo se stále o jednostranný proces bez skutečné interakce.

Zásadní proměnu přinesl až nástup výpočetní techniky a internetu, které umožnily vznik interaktivního virtuálního prostředí. Kyberprostor se postupně stal samostatnou dimenzí lidského života, do níž se promítají všechny základní rysy současné společnosti. Stejně jako v reálném světě se zde objevují politické, ekonomické, kulturní i sociální aspekty a lidé v něm vystupují v různých rolích a identitách. Kyberprostor si zároveň vytváří vlastní pravidla fungování, která se ne vždy shodují s normami fyzického světa. Společnost je proto nucena tyto nové podmínky reflektovat, přizpůsobovat se jim a hledat způsoby, jak čelit novým formám rizik, které jsou s existencí kyberprostoru neoddělitelně spojeny.[6]

2.2 Vymezení kyberprostoru

Kyberprostor lze chápat jako specifické prostředí vznikající v důsledku rozvoje informačních a komunikačních technologií, které zásadním způsobem ovlivňují fungování současné společnosti. Jeho studium vychází především z analýzy technologických možností, jež člověku umožňují vytvářet nové formy komunikace, interakce a zpracování informací. Přestože jsou základy kyberprostoru úzce spjaty s oblastí informatiky a telekomunikací, jeho význam dalece přesahuje technickou rovinu a zasahuje i do společenských, psychologických a právních souvislostí.

Pojem kyberprostor se do širšího povědomí dostal zejména prostřednictvím kyberpunkové literatury, kde byl prezentován jako imaginární, avšak komplexní virtuální svět tvořený daty a informacemi. Tento obraz zdůrazňoval především propojení člověka s technologiemi a možnost pohybu v digitálním prostředí, které není omezeno fyzickým prostorem. Ačkoliv šlo původně o fikční pojetí, postupem času se termín kyberprostor začal používat i v odborném diskurzu a získal realističtější a přesněji vymezený význam.

[6] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2, s. 15.

V současném chápání je kyberprostor zpravidla definován jako soubor existujících počítačových sítí a komunikačních systémů, které umožňují přenos, ukládání a zpracování informací. Patří sem nejen internet jako nejrozšířenější forma digitálního prostředí, ale také systémy virtuální reality, online hry a další počítačem simulovaná prostředí. Kyberprostor tak představuje dynamický a neustále se vyvíjející prostor, ve kterém dochází k interakci mezi technologiemi a lidským chováním.

Rozvoj kyberprostoru úzce souvisí s historickým vývojem kybernetiky, informatiky a mikroelektroniky. Tyto obory položily základy pro vznik moderních digitálních technologií a umožnily masové rozšíření výpočetní techniky. Významným přínosem bylo také nové pojetí informace, které umožnilo její kvantifikaci a systematické zpracování. Díky tomu se technologie staly nedílnou součástí každodenního života a zásadně proměnily způsoby komunikace, práce i trávení volného času. Kyberprostor zároveň ovlivňuje kulturní a společenské procesy. V souvislosti s jeho rozvojem dochází k proměnám identity jednotlivce, vnímání reality i sociálních vazeb. Technologie přestávají být pouze nástrojem a stávají se prostředím, ve kterém se odehrává významná část lidské činnosti. Tyto změny se výrazně promítají zejména u mladších generací, pro něž je digitální prostředí přirozenou součástí jejich života.

Celkově lze konstatovat, že kyberprostor není pouze technickým fenoménem, ale komplexním společenským prostorem, který propojuje technologii, kulturu a lidské chování. Jeho chápání se v průběhu času vyvíjelo od fikční představy k reálnému a nepostradatelnému prvku moderní společnosti, jenž má zásadní dopad na fungování jednotlivců i celé společnosti.[7]

2.3 Bezpečnost informací (důvěrnost, integrita, dostupnost)

Bezpečnost informací je považována za jednu ze zásadních oblastí kybernetické bezpečnosti a úzce souvisí se zabezpečením informačních a komunikačních systémů v prostředí kybernetického prostoru. Zaměřuje se především na ochranu dat a informací před neautorizovaným přístupem, jejich zneužitím, ztrátou či poškozením. V odborných zdrojích je tento pojem nejčastěji definován pomocí tzv. bezpečnostní triády CIA, která

[7] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2, s. 17.

vymezuje tři základní pilíře informační bezpečnosti, jimiž jsou důvěrnost, integrita a dostupnost informací.[8]

Obrázek 1: Triáda CIA

Důvěrnost informací patří mezi klíčové principy informační bezpečnosti a jejím hlavním účelem je zabránit neoprávněnému přístupu k datům. Tento princip se zaměřuje na ochranu citlivých informací před jejich zneužitím a současně na zajištění jejich bezpečného využívání jak v rámci organizace, tak i mimo ni. Porušení důvěrnosti může vést k negativním důsledkům, mezi které patří například narušení soukromí jednotlivců, finanční ztráty nebo poškození dobrého jména organizace. K zajištění důvěrnosti se využívají jak technická, tak organizační opatření, například řízení přístupových oprávnění, autentizační mechanismy či šifrování dat.[9]

Integrita informací představuje požadavek na zachování jejich správnosti, úplnosti a neměnnosti v průběhu celého životního cyklu dat. Tento princip zajišťuje, že s informacemi není neoprávněně manipulováno, a to ani úmyslně, ani neúmyslně. Narušení integrity může vést k závažným následkům, například k chybným rozhodovacím procesům, nepřesným údajům nebo snížení důvěryhodnosti informačních systémů. Ochrana integrity je realizována prostřednictvím různých kontrolních mechanismů, mezi které patří například verzování dat, využívání digitálních podpisů nebo zaznamenávání provedených změn v systému.[10]

[8] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements [online]. Geneva: International Organization for Standardization, 2022. [cit. 2026-01-07] Dostupné z: https://www.iso.org/standard/27001
[9] Národní úřad pro kybernetickou a informační bezpečnost. NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost [online]. Praha: NÚKIB, datum publikování neuvedeno [cit. 2026-01-09]. Dostupné z: https://nukib.gov.cz/
[10] Aptien. What is Data Integrity? Aptien Knowledge Base [online]. datum publikování neuvedeno [cit. 2026-01-11]. Dostupné z: https://aptien.com/cs/kb/articles/what-is-data-integrity

Dostupnost znamená, že informace a systémy jsou pro oprávněné uživatele k dispozici ve chvíli, kdy je potřebují. Cílem je, aby služby fungovaly plynule a nedocházelo k častým nebo dlouhým výpadkům, které by narušily běžný provoz. Pokud dostupnost selže, projeví se to většinou okamžitě – uživatelé se nemohou přihlásit, pracovat s daty nebo využívat poskytované služby. Proto se klade důraz na opatření, která pomáhají výpadkům předcházet nebo je rychle řešit, například používání záložních systémů, rozložení zátěže mezi více serverů nebo automatické přepnutí na náhradní řešení při poruše. Důležitou součástí zajištění dostupnosti jsou také plány obnovy po havárii a plánování kontinuity provozu, které umožňují co nejrychlejší návrat k běžnému fungování i v případě vážných technických problémů nebo mimořádných událostí.[11]

2.4 Kriminalita v kyberprostoru

Současný vývoj výpočetní techniky je úzce propojen s procesy modernizace, automatizace a digitalizace, které jsou umožněny zejména rozvojem internetu. V návaznosti na tyto technologické změny se do praxe dostávají i nové formy virtuální reality, včetně její rozšířené podoby. Tyto technologie vytvářejí nové prostředí, které otevírá prostor nejen pro inovace, ale zároveň i pro vznik a rozvoj kybernetické kriminality. S tím souvisí rostoucí odpovědnost provozovatelů technologií, sítí a úložišť, ale také samotných uživatelů, kteří se mohou stát cílem útoků. Právě na ně je možné klást určité požadavky, a to jak prostřednictvím státní legislativy, tak i vnitřních pravidel a norem jednotlivých organizací, aby byly na možné útoky připraveny a dokázaly se jim účinně bránit.

Kriminalita v kyberprostoru je pojmově vymezena ve vztahu k tomuto specifickému prostředí, avšak její význam výrazně přesahuje jiné formy trestné činnosti související s výpočetní technikou, jako jsou například krádeže hardwaru, neoprávněné nakládání s příslušenstvím nebo nelegální kopírování a prodej softwaru. Z hlediska celospolečenského i mezinárodního představuje kybernetická kriminalita závažný problém, který se stal jedním z hlavních ohnisek boje proti organizovaným formám trestné činnosti a jejich důsledkům. Její dopady se neomezují pouze na jednotlivce, ale zasahují celé instituce, státy i nadnárodní struktury.

[11] O2 Czech Republic a.s. CIA triáda: důvěrnost, integrita a dostupnost. O2 CyberNews [online]. Praha: O2 Czech Republic a.s., datum publikování neuvedeno [cit. 2026-01-12]. Dostupné z: https://o2cybernews.cz/slovnik/cia-triada

Specifickým rysem kriminality v kyberprostoru je především snadná a rychlá realizace útoků, které mohou být prováděny prakticky odkudkoli na světě, kam dosahují internetové a komunikační sítě. S tím souvisí i značné obtíže při zajišťování stop a důkazů po útocích, stejně jako komplikované dokazování z pohledu trestního práva. Důkazní materiál bývá často omezený, obtížně dohledatelný a z hlediska soudního řízení mnohdy málo přesvědčivý. Tato skutečnost přispívá k rozšířenému přesvědčení o anonymitě pachatelů a jejich faktické beztrestnosti, která však ne vždy odpovídá realitě konkrétních případů.

S kriminalitou v kyberprostoru je zároveň spojena skutečnost, že její pachatelé často předbíhají platnou legislativu i schopnost státních orgánů na tyto činy adekvátně reagovat. Nedostatečná koordinace mezi jednotlivými státy, rozdílné právní úpravy a obranné strategie, stejně jako nadnárodní charakter této trestné činnosti, výrazně komplikují její potírání. Útoky nejsou vedeny pouze proti jednotlivcům nebo organizacím v rámci jednoho státu, ale často mají mezinárodní rozsah a mohou být namířeny i proti samotným státům či jejich blokům. To klade vysoké nároky na spolupráci mezi postiženými subjekty a vyžaduje neustálé přizpůsobování právních i bezpečnostních nástrojů aktuálním hrozbám.[12]

2.5 Internet

Internet je celosvětová síť propojených telekomunikačních a počítačových systémů, prostřednictvím nichž dochází k přenosu, sdílení a výměně informací mezi uživateli a zařízeními. Provozní architektura internetu je založena na standardizovaných komunikačních protokolech a technických normách, které umožňují spolupráci jednotlivých sítí a jejich fungování v rámci globálního komunikačního prostředí. Internet není řízen jedním centrálním subjektem, ale je tvořen soustavou vzájemně propojených sítí, jejichž decentralizované uspořádání přispívá k jeho flexibilitě, odolnosti a schopnosti dalšího rozvoje.[13] Na internet lze zároveň nahlížet jako na rozsáhlou globální počítačovou infrastrukturu, která umožňuje efektivní propojení a komunikaci mezi jednotlivými zařízeními.

[12] PORADA, Viktor a Karel RAIS a kol. Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: Pocta Vladimíru Smejkalovi. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-0, s. 116 – 117.

[13] SMEJKAL, Vladimír. Internet a § § §. 2. aktualizované a rozšířené vydání. Praha: Grada Publishing, 2001. ISBN 80-247-0058-1, s. 16-20.

Nejde přitom o jednotnou síť, ale o komplex mnoha menších sítí, jejichž hlavním smyslem je výměna dat mezi koncovými body.[14]

S rostoucím významem internetu v každodenním životě se postupně rozvíjí také nabídka služeb dostupných prostřednictvím webové infrastruktury. Na webové infrastruktuře vzniká řada služeb, mezi které patří například elektronická pošta, přístup k informačním zdrojům, publikování digitálního obsahu a elektronické komunikační služby využívané zejména v oblasti podnikání. Internet má zároveň významný sociální, ekonomický i právní dopad, který přesahuje jeho čistě technologickou funkci. S rozvojem internetové komunikace a šířením informací se objevují nové otázky související s ochranou osobních údajů, autorskými právy a odpovědností za zveřejněný obsah. Z těchto důvodů je internet nutné vnímat jako komplexní informační a komunikační systém, který výrazně ovlivňuje fungování moderní společnosti.[15]

[14] PAVLÍČEK, Antonín; GALBA, Alexander; HORA, Michal. Moderní informatika. 2. aktualizované a rozšířené vydání. Praha: Professional Publishing, 2017. ISBN 978-80-906594-6-9, s. 68–69.
[15] SMEJKAL, Vladimír. Internet a § § §. 2. aktualizované a rozšířené vydání. Praha: Grada Publishing, 2001. ISBN 80-247-0058-1, s. 20-22.

3 Kybernetické hrozby v online prostředí

Kybernetické hrozby představují v současném online prostředí stále výraznější riziko, které má zásadní vliv na zabezpečení informačních a komunikačních technologií, stejně jako na ochranu osobních a citlivých dat uživatelů. Dynamický rozvoj digitálních technologií, společně s rozšiřujícím se využíváním internetu a rostoucí závislostí společnosti na informačních systémech, přispívá k nárůstu počtu kybernetických útoků a ke zvyšování jejich technické náročnosti.

Důsledky těchto hrozeb se neomezují pouze na jednotlivce, ale významně zasahují také organizace soukromého i veřejného sektoru. Kybernetické incidenty mohou vést k finančním ztrátám, neoprávněnému úniku dat, narušení plynulosti provozu informačních systémů nebo k poškození dobrého jména dotčených subjektů. Z uvedených důvodů je problematika kybernetických hrozeb považována za klíčovou oblast současné informační bezpečnosti, která vyžaduje systematickou prevenci a odpovídající bezpečnostní opatření.[16]

3.1 Pojem kybernetická hrozba

Pojem kybernetická hrozba označuje okolnost nebo faktor, který má potenciál negativně ovlivnit bezpečnost informačních systémů a digitálních sítí. Jedná se o situaci, při níž může dojít ke zneužití technických nebo organizačních slabin systému, což může mít za následek narušení ochrany dat, omezení dostupnosti služeb nebo poškození samotné infrastruktury. Kybernetické hrozby se mohou vyskytovat jak v důsledku cíleného a úmyslného jednání útočníků, tak i jako následek lidské chyby či technického selhání.

Podle Evropské agentury pro kybernetickou bezpečnost představují kybernetické hrozby široké spektrum rizik, mezi něž patří například šíření škodlivého softwaru, neoprávněné proniknutí do informačních systémů nebo zneužívání známých zranitelností softwaru a hardwaru. Závažnost těchto hrozeb se zvyšuje s rostoucím rozsahem digitalizace a vzájemného propojování informačních systémů, což klade vyšší nároky na zajištění kybernetické bezpečnosti.[17]

[16] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Kybernetická bezpečnost: hrozby a rizika. Brno: NÚKIB, 2023. Dostupné z: https://www.nukib.cz [cit. 2026-01-18]

[17] EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). Threat Landscape and Good Practice Guide. Heraklion: ENISA, 2016. Dostupné z: https://www.enisa.europa.eu. [cit. 2026-01-19].

3.2 Typy kybernetických hrozeb

V dnešní době jsou kybernetické hrozby jedním z nejkritičtějších problémů, kterým čelí informační společnost. Rozvoj ICT, rozšíření internetu a postupný přechod k digitalizaci znamenají, že jednotlivci i organizace jsou více závislí na informačních systémech. Tento fakt zároveň vytváří prostor pro vznik a rozvoj různých forem kybernetických útoků. Kybernetická hrozba může být považována za událost, aktivitu nebo okolnost, která je schopna ohrozit bezpečnost informací, zejména jejich důvěrnost, integritu a dostupnost.[18]

3.2.1 Malware

Malware nebo škodlivý software je rozšířený termín pro programy a kódy vyvinuté k narušení bezpečnosti informačních systémů. Takový software může ničit data, narušovat chování systému, získávat neoprávněný přístup k informacím nebo monitorovat uživatelské aktivity. Malware je jednou z nejběžnějších a nejnebezpečnějších kybernetických hrozeb, protože se neustále vyvíjí a přizpůsobuje novým technologiím a technikám.[19] Mezi základní typy malwaru patří počítačové viry, počítačoví červi, trojské koně, spyware a ransomware.

3.2.2 Phishing

Phishing je jedním z nejběžnějších kybernetických útoků využívajících sociální inženýrství. Phishing je kategorie online sociálního inženýrství, která se snaží oklamat vás, abyste dobrovolně poskytli své osobní údaje (zejména přihlašovací údaje, údaje o kreditní kartě atd.). Útoky obvykle využívají e-mailové zprávy, které se vydávají za e-mail od důvěryhodné a známé instituce, jako jsou banky, vládní instituce a podniky.[20] Phishingové útoky svou povahou využívají tlak, naléhavost nebo strach, aby přiměly své oběti jednat bez ohledu na možné následky. Phishingové útoky jsou dnes natolik sofistikované a cílené, že to významně zvyšuje jejich úspěšnost. Takové phishingové útoky mohou vést k odcizení identity, finančním ztrátám a ohrožení informačních systémů.[21]

[18] WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. 6th ed. Boston: Cengage Learning, 2018. ISBN 978-1-337-09812-6, s. 8-12.
[19] STALLINGS, William; BROWN, Lawrie. Computer Security: Principles and Practice. 4th ed. Boston: Pearson, 2018. ISBN 978-0-13-479410-5, s. 142-150.
[20] PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence; MARGULIES, Jonathan. Security in Computing. 5th ed. Boston: Pearson, 2015. ISBN 978-0-13-408504-3, s. 387-392.
[21] PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence; MARGULIES, Jonathan. Security in Computing. 5th ed. Boston: Pearson, 2015. ISBN 978-0-13-408504-3, s. 268-272.

3.2.3 Sociální inženýrství

Sociální inženýrství je technika útoku založená na manipulaci lidského chování spíše než na zneužívání technických zranitelností. Útočníci se snaží získat důvěru oběti, aby přesvědčili cíl k porušení bezpečnostních omezení, včetně prozrazení hesla nebo umožnění fyzického přístupu k zařízení.[22] Vishing, což jsou útoky prostřednictvím telefonu, a smishing, což jsou útoky prostřednictvím textových zpráv, jsou běžné techniky sociálního inženýrství. Sociální inženýrství je obzvláště škodlivé, protože zahrnuje prolomení nejslabšího článku v bezpečnostním řetězci – člověka. Účinnost těchto útoků je často způsobena nedostatkem povědomí o bezpečnostních hrozbách a absencí školení uživatelů.[23]

3.2.4 Hacking

Hacking lze zařadit mezi další významné formy počítačové kriminality, které se podobně jako malware či útoky založené na sociálním inženýrství zaměřují na narušení bezpečnosti informačních systémů. Obecně je hacking chápán jako neoprávněné proniknutí do systému jiným než standardním způsobem, tedy obejitím nebo prolomením jeho bezpečnostních mechanismů. V počátečních obdobích se tato činnost často pojila se snahou porozumět fungování systému, identifikovat jeho slabiny nebo získat uznání v rámci hackerské komunity, přičemž úmysl způsobit škodu nebýval vždy přítomen. Postupem času však dochází ke změně charakteru této činnosti a stále častěji se objevují případy, kdy je hacking motivován materiálním prospěchem. Z hlediska právní úpravy je samotný průnik do systému považován za trestný čin zejména tehdy, pokud dojde ke vzniku škody, jiné újmy nebo neoprávněného obohacení, přičemž výše trestu se odvíjí od závažnosti následků a okolností konkrétního jednání. Text rovněž poukazuje na existenci různých typů hackerů, od méně zkušených jedinců využívajících hotové nástroje až po vysoce kvalifikované osoby schopné sofistikovaných útoků. Zvláštní pozornost je věnována také skutečnosti, že významné bezpečnostní riziko nepředstavují pouze externí útočníci, ale i osoby s oprávněným přístupem k systémům, jejichž znalost prostředí a přístupových práv může vést k závažnějším dopadům než útoky z vnějšího prostředí.[24]

[22]WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. 6th ed. Boston: Cengage Learning, 2018. ISBN 978-1-337-09812-6, s. 255-260.
[23] PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence; MARGULIES, Jonathan. Security in Computing. 5th ed. Boston: Pearson, 2015. ISBN 978-0-13-408504-3, s. 372-378.
[24] MATĚJKA, Michal**.** *Počítačová kriminalita.* Praha: Computer Press, 2002. ISBN 80-7226-419-2, s. 53-56.

3.2.5 Útoky typu DoS a DDoS

Cílem útoků typu Denial of Service (DoS) a Distributed Denial of Service (DDoS) je narušit dostupnost informačních systémů a síťových služeb. Tyto útoky se snaží zaplavit cíl velkým množstvím požadavků, což způsobí zpomalení jeho výkonu nebo dokonce úplné vypnutí.[25] Při útocích DDoS se vytváří velké množství provozu z více kompromitovaných zařízení, která útočník ovládá pomocí takzvané botnetové sítě. Takové útoky mohou mít extrémně vážné následky a mohou být obzvláště škodlivé pro organizace, které nabízejí online služby. Tyto útoky mají přímé finanční dopady, stejně jako poškození značky a ztrátu důvěry zákazníků.[26]

3.2.6 Zneužití zranitelností a neoprávněný přístup

Neoprávněný přístup označuje situaci, kdy útočník získá přístup k informačnímu systému bez řádného povolení. Softwarové zranitelnosti, slabá hesla a nesprávné konfigurace systému obvykle vedou k neoprávněnému přístupu. Zranitelnosti mohou vzniknout během vývoje softwaru, jeho nasazení nebo provozu, a pokud nejsou včas řešeny, představují významná bezpečnostní rizika.[27] Jakmile útočník získá přístup k systému, může provádět různé škodlivé aktivity, včetně krádeže dat, modifikace dat nebo instalace dalšího škodlivého softwaru. Důsledky těchto typů útoků mohou ovlivnit dlouhodobou stabilitu a bezpečnost informačních systémů.[28]

3.2.7 Insider

Insider hrozby jsou specifickým typem kybernetických hrozeb, protože vznikají přímo z vnitřního prostředí organizace. To zahrnuje zaměstnance, bývalé zaměstnance nebo externí spolupracovníky, kteří mají legitimní přístup k informačním systémům. Insider hrozby mohou být úmyslné, například sabotáž nebo krádež dat, nebo neúmyslné, když zaměstnanec poruší bezpečnostní pravidla z nedbalosti. Protože útočník používá autorizovaný systém a obecně zná vnitřní strukturu, je tyto hrozby těžké odhalit. Proto je

[25] STALLINGS, William. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston: Addison-Wesley, 2020. ISBN 978-0-13-477280-6, s. 211-217.
[26] STALLINGS, William; BROWN, Lawrie. Computer Security: Principles and Practice. 4th ed. Boston: Pearson, 2018. ISBN 978-0-13-479410-5, s. 486-490.
[27] ANDRESS, Jason. The Basics of Information Security. 3rd ed. Waltham: Syngress, 2019. ISBN 978-0-12-812815-7, s. 61.
[28] KIZZA, Joseph M. Guide to Computer Network Security. 4th ed. Cham: Springer, 2017. ISBN 978-3-319-55605-5, s. 174.

důležité integrovat technické bezpečnostní přístupy s organizačními a personálními kontrolami.[29]

3.3 Kybernetické hrozby ohrožující mladistvé

Výše uvedené kybernetické hrozby nepředstavují riziko pouze pro dospělé uživatele, ale ve značné míře ohrožují také děti a mladistvé, kteří tvoří specifickou a zranitelnou skupinu uživatelů internetu. V důsledku častého využívání digitálních technologií, sociálních sítí nebo online her přicházejí mladiství do kontaktu s online prostředím již v raném věku, aniž by měli dostatečné zkušenosti k rozpoznání možných bezpečnostních rizik. Jejich schopnost používat moderní technologie se často rozvíjí rychleji než schopnost vyhodnocovat potenciální hrozby, jako jsou phishingové útoky, škodlivý software či manipulativní techniky sociálního inženýrství. Zároveň bývají v online prostředí důvěřivější vůči neznámým osobám, což zvyšuje pravděpodobnost, že se stanou obětí kybernetických útoků nebo podvodného jednání vedoucího ke zneužití osobních údajů či narušení soukromí.[30]

Mezi významná rizika, se kterými se mladiství v online prostředí setkávají, patří také kyberšikana.

3.3.1 Kyberšikana

Kyberšikana představuje specifickou formu agresivního chování realizovanou prostřednictvím digitálních technologií, která narušuje rovnováhu mezi agresorem a obětí. Charakter online prostředí umožňuje pachatelům jednat anonymně a bez přímé konfrontace, což může vést k intenzivnějším a obtížněji předvídatelným útokům než v případě tradiční šikany.

Za kyberšikanu lze považovat cílené a opakované jednání směřující k poškození psychické pohody nebo sociálního postavení oběti s využitím moderních komunikačních prostředků. Projevy tohoto jednání mohou zahrnovat různé formy psychického nátlaku, manipulace s osobními informacemi či veřejné znevažování. Specifika digitálního prostředí zároveň umožňují širší dosah útoků a jejich rychlé šíření mezi uživateli.

[29] CYBRELA s.r.o. Insider threat – definice a význam pojmu [online]. Praha: Cybrela, [cit. 2026-01-29]. Dostupné z WWW: https://cybrela.com/slovnik/insider-threat/
[30] EUROPEAN COMMISSION. *Better Internet for Kids* [online]. Brussels: European Commission, 2022 [cit. 2026-02-13]. Dostupné z WWW: https://better-internet-for-kids.europa.eu

Významným faktorem ovlivňujícím intenzitu kyberšikany je anonymita, která může u pachatelů snižovat vnímání odpovědnosti za vlastní jednání. Útoky se mohou odehrávat nepřetržitě a bez zjevných varovných signálů, což zvyšuje psychickou zátěž obětí. Důsledky kyberšikany se často projevují zejména v oblasti duševního zdraví, kdy oběť může situaci vnímat jako dlouhodobě neřešitelnou.[31]

[31] KOŽÍŠEK, M.; PÍSECKÝ, V. Bezpečně na internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3, s. 62-64.

4 Ochrana osobních údajů

Osobní údaje zahrnují veškeré informace, které se vztahují ke konkrétní fyzické osobě a umožňují její identifikaci, a to jak přímým, tak nepřímým způsobem. Subjektem údajů je tedy jednotlivec, jehož totožnost lze určit například prostřednictvím jména, identifikačního čísla nebo jiného specifického identifikátoru. Identifikace může vycházet také z charakteristik souvisejících s fyzickou či psychickou identitou, sociálním postavením, ekonomickou situací nebo kulturním prostředím dané osoby. Osobním údajem je proto jakákoli informace, která umožňuje určit konkrétního člověka.

Ochrana osobních údajů představuje významnou součást právní úpravy, jelikož úzce souvisí s ochranou soukromí jednotlivce. V praxi zahrnuje pravidla upravující způsoby shromažďování, uchovávání a dalšího zpracování osobních údajů. Subjekty, které s těmito údaji nakládají, jsou povinny zajistit jejich využívání pouze pro předem stanovené účely a v rozsahu nezbytném pro jejich naplnění. Současně musí přijmout opatření, která zabrání jejich zneužití, neoprávněnému přístupu nebo jinému zásahu do soukromí. [32] Nedostatečné zabezpečení osobních údajů může vést ke vzniku bezpečnostního incidentu, který může mít závažné právní i praktické důsledky.[33]

Zvláštní kategorii tvoří tzv. citlivé osobní údaje, které podléhají přísnějšímu režimu ochrany. Jedná se například o informace o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém přesvědčení či členství v odborových organizacích. Do této skupiny patří rovněž údaje o zdravotním stavu, sexuálním životě nebo biometrické a genetické informace. Vzhledem k jejich povaze je jejich zpracování zpravidla možné pouze za splnění zákonem stanovených podmínek a vyžaduje zvýšenou míru ochrany.[34]

4.1 Zpracování osobních údajů

Zpracování osobních údajů představuje souhrn činností souvisejících s nakládáním s informacemi, které umožňují identifikovat konkrétní fyzickou osobu. V současné digitální společnosti má tato oblast zásadní význam, jelikož s osobními údaji pracuje

[32] ŠTĚDROŇ, Bohumír a Miroslav LUDVÍK. Právo v informačních technologiích. Kralice na Hané: Computer Media, 2012. ISBN 978-80-86686-36-3, s. 13-14.
[33] NONNEMANN, F.; ČERVENÝ, V.; VÍTEK, D. Kybernetický bezpečnostní incident 3D: IT, právo a compliance. Praha: Wolters Kluwer, 2022. ISBN 978-80-7676-515-3, s. 155.
[34] ŠTĚDROŇ, Bohumír a Miroslav LUDVÍK. *Právo v informačních technologiích*. Kralice na Hané: Computer Media, 2012. ISBN 978-80-86686-36-3, s. 13-14.

široké spektrum subjektů napříč různými oblastmi společenského života. Každé zpracování musí být založeno na odpovídajícím právním titulu a současně respektovat základní principy ochrany osobních údajů, které vymezují pravidla jejich získávání, využívání a zabezpečení. Dodržování těchto zásad je nezbytné pro zajištění zákonného a odpovědného přístupu k ochraně soukromí jednotlivce.[35]

4.2 Zásady zpracování osobních údajů

Nakládání s osobními údaji je podmíněno dodržováním několika základních principů, které vymezují způsob jejich získávání, využívání a ochrany.

• Zákonnost, korektnost a transparentnost

Zpracování osobních údajů musí vycházet z právního důvodu a být prováděno otevřeným a srozumitelným způsobem vůči subjektu údajů. Správce je povinen jasně informovat o účelu zpracování i o způsobu nakládání s údaji.

• Účelové omezení

Osobní údaje mohou být shromažďovány pouze pro konkrétní, legitimní a předem stanovené účely. Jakékoli další využití nesmí být v rozporu s původním důvodem jejich zpracování.

• Minimalizace údajů

Rozsah zpracovávaných údajů má být omezen pouze na informace, které jsou nezbytné k naplnění stanoveného účelu.

• Přesnost

Osobní údaje musí být aktuální a správné. V případě zjištění nepřesností je nutné zajistit jejich opravu nebo aktualizaci.

• Omezení uložení

Údaje lze uchovávat pouze po dobu nezbytnou k dosažení účelu zpracování. Po jejím uplynutí by měly být bezpečně odstraněny nebo anonymizovány.

[35] USINESSINFO.CZ. Ochrana osobních údajů – zpracování osobních údajů [online]. Praha: CzechTrade, 2024 [cit. 2026-02-17]. Dostupné z WWW: https://www.businessinfo.cz/navody/ochrana-osobnich-udaju-ppbi/4/

• Integrita a důvěrnost

Zpracování osobních údajů musí být chráněno vhodnými technickými a organizačními opatřeními, která minimalizují riziko neoprávněného přístupu, ztráty nebo zneužití informací.[36]

Respektování uvedených zásad je pro správce důležité nejen z hlediska plnění právních povinností, ale také v souvislosti s odpovědným přístupem k ochraně soukromí jednotlivců.

4.3 Zpracování údajů zveřejněných na internetu

Veřejná dostupnost osobních údajů sama o sobě neznamená, že s nimi lze bez dalšího volně nakládat. I informace zveřejněné například v oficiálních registrech nebo dobrovolně sdílené na internetu podléhají pravidlům ochrany osobních údajů a jejich další využití musí být vždy opřeno o odpovídající právní titul. Při dalším zpracování je nutné respektovat účel, za kterým byly údaje zveřejněny, a dodržovat základní zásady jejich ochrany. V opačném případě může dojít k neoprávněnému zásahu do soukromí dotčené osoby.[37]

4.4 Legislativní ochrana osobních údajů

Ochrana osobních údajů v České republice je upravena především zákonem č. 110/2019 Sb., o zpracování osobních údajů. Tento právní předpis doplňuje obecné nařízení GDPR a stanovuje konkrétní pravidla pro nakládání s osobními údaji v rámci českého právního systému. Právní úprava vymezuje základní zásady zpracování osobních údajů, práva fyzických osob i povinnosti subjektů, které s těmito údaji pracují. Jejím hlavním cílem je zajistit ochranu soukromí jednotlivce a transparentní nakládání s osobními informacemi. Součástí institucionálního rámce je také Úřad pro ochranu osobních údajů, který plní funkci dozorového orgánu.[38]

[36] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Zásady zpracování osobních údajů [online]. Praha: Ministerstvo vnitra ČR, 2024 [cit. 2026-02-19]. Dostupné z WWW: https://mv.gov.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx

[37] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. Zásady zpracování osobních údajů [online]. Praha: Ministerstvo vnitra ČR, 2024 [cit. 2026-02-19]. Dostupné z WWW: https://mv.gov.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx

[38] ČESKO. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: Sbírka zákonů, Česká republika. 2019, částka 47.

Na úrovni Evropské unie je ochrana osobních údajů považována za významnou součást ochrany základních práv a svobod jednotlivce. V souvislosti s rozvojem digitálních technologií a rostoucí globalizací informačních toků vznikla potřeba vytvořit jednotný právní rámec, který by zajistil odpovídající úroveň ochrany ve všech členských státech a zároveň umožnil volný pohyb osobních údajů v rámci vnitřního trhu. Právní úprava proto usiluje o nalezení rovnováhy mezi ochranou soukromí jednotlivce a požadavky moderní informační společnosti.[39]

4.5 Rizika zneužití osobních údajů v online prostředí

4.5.1 Krádež identity

Krádež identity představuje závažný bezpečnostní i společenský problém, který spočívá v neoprávněném získání a následném zneužití digitální totožnosti jiné osoby. Pachatelé takto získávají přístup k různým online službám, zejména k e-mailovým účtům, profilům na sociálních sítích či dalším internetovým platformám. Po převzetí kontroly nad účtem se mohou za poškozenou osobu vydávat a využívat její identitu k podvodným aktivitám, získávání citlivých informací nebo poškození její pověsti.

Odcizená identita bývá často zneužívána například k rozesílání nevyžádaných zpráv, realizaci phishingových útoků nebo šíření škodlivého softwaru. Prostřednictvím kompromitovaných přístupových údajů mohou útočníci získat také neveřejné informace, například o fungování organizace nebo zabezpečení dalších systémů. Vzhledem k tomu, že změna přístupových údajů je v řadě případů podmíněna ověřením prostřednictvím e-mailové adresy, může převzetí kontroly nad jedním účtem vést k následnému přístupu i k dalším online službám.[40]

4.5.2 Zneužití fotografií a osobních informací

Zneužívání fotografií a osobních údajů představuje v digitálním prostředí významné riziko, které souvisí s intenzivním využíváním sociálních sítí, včetně platformy TikTok. Mladí uživatelé patří mezi nejaktivnější skupiny na těchto platformách a často sdílejí vizuální obsah nebo osobní informace, aniž by si plně uvědomovali možné

[39] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Základní příručka k ochraně údajů [online]. Praha: ÚOOÚ, [cit. 2026-02-20]. Dostupné z: https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaju
[40] INTERNETEM BEZPEČNĚ. Krádež identity [online]. 2024 [cit. 2026-02-21]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/

důsledky jejich dalšího šíření. Zveřejněním takového obsahu dochází ke snížení kontroly nad jeho dalším využitím, přičemž digitální materiály mohou být snadno kopírovány, upravovány nebo zneužity například k vytváření falešných profilů či k různým formám kyberšikany. [41]

Riziko zneužití se zvyšuje zejména v případech nadměrného sdílení soukromých informací nebo citlivých fotografií. Takový obsah může být využit nejen jednotlivci, ale i organizovanými skupinami například k manipulaci s identitou nebo jiným protiprávním aktivitám. V prostředí sociálních sítí, kde se obsah rychle šíří a jeho odstranění je obtížné, mohou mít tyto situace dlouhodobé dopady na osobní i sociální život mladých uživatelů.[42]

4.5.3 Únik dat

Únik dat, často označovaný také jako *data breach*, představuje situaci, kdy dojde k neoprávněnému přístupu k citlivým nebo chráněným informacím. Může se jednat například o osobní údaje, finanční informace, firemní dokumenty nebo zdravotní záznamy, které se dostanou do rukou nepovolaných osob. Tento problém patří mezi významná rizika v oblasti kybernetické bezpečnosti, protože jeho důsledky mohou zasáhnout jednotlivce, organizace i širší společnost. K únikům dat dochází z různých příčin, například v důsledku hackerských útoků, technických nedostatků v informačních systémech nebo chyb způsobených lidským faktorem. V souvislosti s rostoucí digitalizací se navíc tyto incidenty objevují stále častěji a bývají složitější, což může vést k závažným právním či finančním následkům. Únik dat se přitom může týkat jak menších organizací, tak velkých společností, protože cílem útoku se může stát prakticky jakýkoli subjekt.[43]

4.6 Ochrana osobních údajů u mladistvých

Ochrana osobních údajů nezletilých v digitálním prostředí představuje významnou oblast zejména z toho důvodu, že děti a dospívající často sdílejí různé informace bez dostatečného uvědomění si možných rizik. Publikování fotografií, osobních údajů nebo

[41] MAGDOŇOVÁ, Jana. „Všichni věděli, že je mi dvanáct.“ Děti ohrožuje na internetu sexting, intimní snímky se objeví i po letech [online]. iROZHLAS, 25. 5. 2022 [cit. 2026-02-21]. Dostupné z: https://www.irozhlas.cz/zivotni-styl/spolecnost/sexting-internet-kybersikana-kyberbezpecnost-bezpecnost-internet_2205250700_bko

[42] KRYTOLAND. Nebezpečí sharentingu: Jak sdílení fotek dětí může vést k jejich zneužívání na internetu [online]. 2024 [cit. 2026-02-21]. Dostupné z: https://www.krytoland.cz/nebezpeci-sharentingu-jak-sdileni-fotek-deti-muze-vest-k-jejich-zneuzivani-na-internetu

[43] VANĚK, Jiří. Co je to únik dat (Data Breach) a jak se mu bránit [online]. 2024 [cit. 2026-02-22]. Dostupné z: https://blog.jirivanek.eu/cs/co-je-to-unik-dat-data-breach-a-jak-se-mu-branit/

informací o každodenních aktivitách může zvyšovat pravděpodobnost jejich zneužití, například v souvislosti s kyberšikanou, podvodným jednáním či navazováním kontaktů s neznámými osobami. Sdílení citlivých dat tak může mít pro nezletilé závažné následky, a to především s ohledem na jejich vyšší míru zranitelnosti a omezenou schopnost předvídat rizika spojená s online prostředím.[44]

Zároveň je nutné zdůraznit, že ochrana osobních údajů nezletilých není pouze otázkou jejich individuální odpovědnosti, ale vyžaduje také aktivní zapojení rodičů, škol i dalších institucí. Preventivní opatření by měla směřovat k omezení sdílení citlivých informací, jako jsou například údaje o bydlišti, školní docházce nebo osobních zájmech, které mohou být následně zneužity k manipulaci či krádeži identity. V tomto kontextu je důležité podporovat informovanost a digitální gramotnost nezletilých, aby byli schopni bezpečně a odpovědně využívat online technologie.[45]

Problematika ochrany soukromí dětí je navíc reflektována i v právních předpisech, které kladou důraz na ochranu jejich důstojnosti a osobní integrity v digitálním prostoru. V odborné i veřejné debatě se proto objevují požadavky na vyšší odpovědnost provozovatelů digitálních platforem a na zavádění legislativních opatření, jejichž cílem je snížit rizika spojená s užíváním internetu nezletilými a posílit jejich bezpečí.[46]

Současně je třeba vnímat, že digitální prostředí přináší nejen nové možnosti komunikace a vzdělávání, ale také specifická rizika související s neoprávněným nakládáním s osobními údaji. Z tohoto důvodu je nezbytné rozvíjet preventivní strategie zaměřené na ochranu soukromí nezletilých a podporovat odpovědné chování všech subjektů, které se podílejí na jejich ochraně v online prostoru.[47]

[44] ČESKÁ TELEVIZE. Pozor na to, co sdílíte. Fotografie z internetu nezmizí [online]. 2025 [cit. 2026-02-23]. Dostupné z: https://ct24.ceskatelevize.cz/clanek/domaci/pozor-na-to-co-sdilite-fotografie-z-internetu-nezmizi-361169

[45] POLICIE ČESKÉ REPUBLIKY. Nebudujte svému dítěti digitální stopu [online]. 2025 [cit. 2026-02-23]. Dostupné z: https://policie.gov.cz/clanek/akce-a-projekty-nebudujte-svemu-diteti-digitalni-stopu.aspx

[46] ŠÍPOŠOVÁ, Veronika. Seriál specifické aspekty ochrany osobních údajů 4/5: Děti, internet a právo na ochranu osobních údajů [online]. 2020 [cit. 2026-02-23]. Dostupné z: https://www.epravo.cz/top/clanky/serial-specificke-aspekty-ochrany-osobnich-udaju-45-deti-internet-a-pravo-na-ochranu-osobnich-udaju-111248.html

[47] KUŽELOVÁ, Marie. Má pomoci ochránit děti na internetu. Nyní hrozí, že zákon neprojde Sněmovnou [online]. 2025 [cit. 2026-02-23]. Dostupné z: https://www.novinky.cz/clanek/domaci-ma-pomoci-ochranit-deti-na-internetu-nyni-hrozi-ze-zakon-neprojde-snemovnou-40527198

5 Sociální sítě a jejich vliv na uživatele

5.1 Charakteristika sociálních sítí

Sociální sítě představují digitální komunikační prostředí, které umožňuje vytváření a rozvoj vztahů mezi jednotlivci či skupinami sdílejícími společné zájmy nebo potřeby. V online prostoru fungují jako platformy podporující tvorbu uživatelských profilů, sdílení různých typů obsahu a vzájemnou interakci mezi uživateli. Tento vývoj vede k postupnému přesunu části sociálních aktivit z reálného prostředí do virtuálního prostoru, čímž se rozšiřují možnosti komunikace i spolupráce.[48]

Pro sociální sítě je typická aktivní role uživatelů, kteří nejsou pouze pasivními příjemci informací, ale zároveň se podílejí na jejich tvorbě a šíření. Takový interaktivní charakter přispívá k formování digitální identity jednotlivců a podporuje propojení lidí bez ohledu na geografickou vzdálenost. Sociální sítě tak vytvářejí prostor pro vznik online komunit a sdílení zkušeností, názorů i informací.

Z širšího pohledu lze sociální sítě zařadit do oblasti sociálních médií, která zahrnuje také další nástroje digitální komunikace, například blogy, diskusní platformy nebo služby zaměřené na multimediální obsah. Jednotlivé sociální sítě se liší svým zaměřením, funkcemi i cílovými skupinami uživatelů, což ovlivňuje způsob jejich využívání v současné společnosti.[49]

5.2 Historie sociálních sítí

Pojem sociální síť se v odborném prostředí začal objevovat již ve 20. století jako teoretický koncept popisující strukturu mezilidských vztahů. S postupným rozvojem informačních a komunikačních technologií získal nový význam a začal být spojován s online prostředím. Významným impulsem byl zejména rozvoj internetu a nástup principů Web 2.0, které umožnily aktivní zapojení uživatelů do tvorby a sdílení digitálního obsahu.

[48] PAVLÍČEK, Antonín; GALBA, Alexander; HORA, Michal. *Moderní informatika.* 2. rozšířené vydání. Praha: Professional Publishing, 2017. ISBN 978-80-906594-6-9, s. 104–106.
[49] KOPECKÝ, Kamil; KREJČÍ, Veronika. *Sociální sítě – úvod do problematiky.* Olomouc: Univerzita Palackého v Olomouci, 2023. ISBN 978-80-244-6369-8, s. 17.

Za počátky online sociálních interakcí lze považovat využívání elektronické pošty a dalších komunikačních nástrojů umožňujících kontakt na dálku. Postupně vznikaly první specializované platformy zaměřené na propojování uživatelů, mezi nimi například služba Classmates.com z 90. let 20. století. Tyto projekty položily základy dnešním sociálním sítím, které představují významný prostředek komunikace, sdílení informací i budování sociálních vztahů v digitálním prostoru.[50]

5.3 Druhy sociálních sítí

Sociální sítě je možné rozčlenit do šesti základních oblastí, přičemž s rozvojem nových funkcí dochází k jejich stále častějšímu vzájemnému prolínání. Jedná se o následující kategorie:

1. sdílení a sociální komunikace (Facebook, Instagram, X),
2. profesní a firemní prostředí,
3. platformy zaměřené na fotografický obsah (Snapchat, Pinterest, OnlyFans),
4. video platformy (TikTok, YouTube),
5. hudební služby (Soundcloud, Spotify),
6. filmové a hodnoticí platformy (Netflix, Disney+).

Facebook

Facebook patří mezi nejrozšířenější sociální sítě a jeho hlavní funkcí je umožnit uživatelům sdílení různých forem digitálního obsahu a vzájemnou komunikaci. Prostřednictvím individuálních uživatelských profilů mohou jednotlivci zveřejňovat vlastní příspěvky, reagovat na aktivitu ostatních a udržovat sociální vazby v online prostředí. Platforma současně nabízí nástroje pro nastavení úrovně soukromí, realizaci soukromé komunikace i zapojení do tematicky zaměřených skupin, čímž podporuje interakci mezi uživateli.[51]

Facebook byl původně vytvořen jako prostředek komunikace pro studenty Harvardovy univerzity, avšak postupně se rozšířil i mezi širší veřejnost.[52] Ačkoli přispívá k efektivnímu sdílení informací a usnadňuje mezilidskou komunikaci, jeho používání je spojeno

[50] SOCIALNISITE.ESTRANKY.CZ. Historie sociálních sítí [online]. [cit. 2026-02-20]. Dostupné z: https://socialnisite.estranky.cz/clanky/historie-socialnich-siti.html
[51] TRÉDEZ, Emmanuel. Sociální sítě - a to funguje jak?: všechno, co vás zajímá, když jste online. Praha, 2018. Malé a velké otázky. ISBN 978-80-256-2416-6, str. 32-33
[52] PEACOCK, Michael. Programujeme vlastní sociální síť v PHP 5. Brno: Computer Press, 2012. ISBN 978-80-251-3626-3, s. 20

také s určitými riziky, zejména v oblasti ochrany osobních údajů či výskytu kyberšikany.[53]

Instagram

Instagram je sociální síť zaměřená především na sdílení vizuálního obsahu, zejména fotografií a videí. Uživatelé zde komunikují prostřednictvím reakcí, komentářů, sdílení či soukromých zpráv a mohou sledovat obsah účtů podle svých zájmů. Platforma klade důraz na vizuální prezentaci profilu a využívání krátkodobých formátů, jako jsou příběhy nebo krátká videa.

Vedle osobního využití je Instagram významně využíván také v marketingu a propagaci produktů či služeb. Přestože umožňuje budování sociálních kontaktů a sdílení zkušeností, jeho používání je spojeno i s riziky, například v oblasti ochrany osobních údajů, výskytu falešných profilů nebo negativního vlivu na psychickou pohodu uživatelů.[54]

Snapchat

Na vizuální způsob komunikace typický pro Instagram navazuje také sociální aplikace Snapchat, která je populární především mezi mladšími uživateli. Platforma slouží ke sdílení fotografií a videí s omezenou dobou zobrazení a k rychlé komunikaci prostřednictvím textových, hlasových nebo video zpráv. Součástí aplikace jsou také krátkodobé příběhy a různé filtry či efekty, které umožňují upravovat sdílený obsah.

Pro Snapchat je charakteristická především dočasnost zveřejněných příspěvků a důraz na okamžitou interakci mezi uživateli. Aplikace nabízí i další funkce, například možnost zobrazování polohy nebo sdílení obsahu podle místa. Stejně jako u ostatních sociálních sítí je však její používání spojeno s otázkami ochrany soukromí a bezpečnosti uživatelů.

YouTube

YouTube patří mezi nejvyužívanější internetové platformy pro sdílení audiovizuálního obsahu. Uživatelé zde mohou sledovat, nahrávat a sdílet videa různých témat, od

[53] TRÉDEZ, Emmanuel. Sociální sítě - a to funguje jak?: všechno, co vás zajímá, když jste online. Praha, 2018. Malé a velké otázky. ISBN 978-80-256-2416-6, str. 32
[54] TRÉDEZ, Emmanuel. Sociální sítě - a to funguje jak?: všechno, co vás zajímá, když jste online. Praha, 2018. Malé a velké otázky. ISBN 978-80-256-2416-6, str. 33

zábavy a vzdělávání až po zpravodajství nebo živé přenosy. Po přihlášení se zobrazují doporučená videa podle předchozí aktivity uživatele, což usnadňuje vyhledávání obsahu.

Každý uživatel může spravovat vlastní kanál, zveřejňovat videa a komunikovat s ostatními prostřednictvím komentářů. Platforma podporuje také živé vysílání a krátká videa podobná jiným sociálním sítím. Přestože YouTube představuje významný nástroj pro sdílení informací i zábavu, jeho používání může být spojeno s negativními projevy, například s nevhodnými komentáři.[55]

5.4 Dopady využívání sociálních sítí na jedince

Komunikace mezi uživateli

Sociální sítě v současnosti představují důležitý nástroj mezilidské komunikace a umožňují navazování i udržování kontaktů bez ohledu na geografickou vzdálenost. Prostřednictvím těchto platforem mohou uživatelé jednoduše, rychle a zpravidla bez finančních nákladů komunikovat s rodinnými příslušníky, kolegy, spolužáky či například zdravotnickými pracovníky.[56]

Budování online komunity

Sociální sítě vytvářejí prostor pro vznik virtuálních komunit sdružujících uživatele s podobnými zájmy či hodnotami. Umožňují sdílení zkušeností, zapojení do diskusí a podporují pocit sounáležitosti i vzájemné spolupráce mezi členy.[57]

Závislost na sociálních sítích

Nadměrné využívání sociálních sítí může negativně ovlivnit životní styl, mezilidské vztahy i psychickou pohodu uživatelů. Rizikem je zejména sociální srovnávání a tlak na idealizovanou sebeprezentaci, který může vést k nespokojenosti a psychickým obtížím.[58]

[55] TRÉDEZ, Emmanuel. Sociální sítě - a to funguje jak?: všechno, co vás zajímá, když jste online. Praha, 2018. Malé a velké otázky. ISBN 978-80-256-2416-6, str. 46-47

[56] DOČEKAL, Daniel; MÜLLER, Jan; HARRIS, Anastázie a HEGER, Luboš. Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace. Flowee. Praha: Mladá fronta, 2019. ISBN 978-80-204-5145-3., str. 13-14

[57] LOSEKOOT, Michelle a VYHNÁNKOVÁ, Eliška. Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích. Žádná velká věda. V Brně: Jan Melvil, 2019. ISBN 978-80-7555-084-2., str. 31

[58] KREJČÍ SALÁTOVÁ, Renáta. POSPÍŠILOVÁ, Marie. *Facebooková (ne)závislost: identita, interakce a uživatelská kariéra na Facebooku.* První vydání. Praha: Univerzita Karlova, nakladatelství Karolinum, 2016. 136 stran. ISBN 978-80-246-3306-0., str. 80

Narušení soukromí uživatelů

Sdílení osobních údajů na sociálních sítích může vést k oslabení ochrany soukromí a zvýšenému riziku jejich zneužití, například v souvislosti s kyberšikanou či kyberstalkingem. Personalizované algoritmy navíc mohou omezovat kontakt s různorodými informacemi, což může negativně ovlivňovat schopnost kritického hodnocení obsahu.[59]

Obtěžování na sociálních sítích

Na sociálních sítích se mohou uživatelé setkat s nevhodným chováním, například s urážkami, nátlakem nebo šikanou. Tyto zkušenosti mohou negativně ovlivnit psychickou pohodu, sebevědomí i celkové duševní zdraví, zejména u mladších osob.[60]

Bezpečnostní rizika

Online prostředí sociálních sítí přináší riziko podvodů, šíření nepravdivých informací nebo škodlivého obsahu. Problematické mohou být i falešné profily či cílená reklama, která může ovlivňovat rozhodování uživatelů.[61]

Narušení spánku

Časté používání sociálních sítí může narušovat spánkový režim. Důsledkem může být únava, snížená schopnost soustředění a pokles studijní či pracovní výkonnosti.[62]

Dopady na zdraví

Nadměrné využívání sociálních sítí je spojeno také s určitými zdravotními komplikacemi. Dlouhodobé setrvávání u obrazovky může přispívat ke zhoršení zraku, zvýšenému riziku nadváhy či obezity a k problémům s pohybovým aparátem. Tyto obtíže často souvisejí s nedostatkem fyzické aktivity a sedavým způsobem trávení volného času.[63]

---

[59] KREJČÍ SALÁTOVÁ, Renáta. POSPÍŠILOVÁ, *Marie. Facebooková (ne)závislost: identita, interakce a uživatelská kariéra na Facebooku.* První vydání. Praha: Univerzita Karlova, nakladatelství Karolinum, 2016. 136 stran. ISBN 978-80-246-3306-0., str. 23

[60] KOPECKÝ, Kamil a KREJČÍ, Veronika. *Sociální sítě: úvod do problematiky*. Olomouc: Univerzita Palackého v Olomouci, 2023. ISBN 978-80-244-6369-8., str. 63

[61] VEJVODOVÁ, Jana a Miloš GREGOR. Nejlepší kniha o fake news!!!. Cpress, 2018. ISBN 978-80-264-1805-4, str. 142

[62] KOPECKÝ, Kamil a KREJČÍ, Veronika. *Sociální sítě: úvod do problematiky*. Olomouc: Univerzita Palackého v Olomouci, 2023. ISBN 978-80-244-6369-8., str. 69

[63] ARNKIL, Tom Erik. Dialogical meetings in social networks. Routledge, 2018, 236 p. ISBN 978-18-5575-410-2.

5.5 Zásady bezpečného používání sociálních sítí

Používání sociálních sítí je spojeno s různými bezpečnostními riziky, která mohou negativně ovlivnit soukromí i psychickou pohodu uživatelů. Dodržování základních zásad bezpečného chování v online prostředí může pomoci tato rizika omezit a přispět k ochraně osobních údajů.

1. Nesdílejte osobní údaje, jako je adresa, telefonní číslo nebo jiné citlivé informace.
2. Neposílejte ani nezveřejňujte intimní fotografie či obsah, který by mohl být zneužit.
3. Používejte různá a dostatečně silná hesla pro jednotlivé online služby.
4. Pečlivě si čtěte podmínky při registraci nebo potvrzování souhlasů.
5. Nepropojujte své účty na sociálních sítích s jinými službami bez zvážení rizik.
6. Nastavte si vhodnou úroveň soukromí a kontrolujte, kdo může vidět vaše příspěvky.
7. Rozlišujte přístupová práva mezi jednotlivými skupinami kontaktů.
8. Nereagujte na nevhodné nebo útočné zprávy a problematické uživatele blokujte.
9. Na osobní schůzky domluvené online choďte pouze po informování důvěryhodné osoby.
10. Zvažujte, jaký obsah zveřejňujete, protože může mít dlouhodobé následky.[64]

[64] KOHOUT, Roman; KARCHŇÁK, Radek. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, z. s., 2016. ISBN 978-80-260-9543-9, str. 41.

6 Charakteristika TikToku

TikTok je multimediální platforma, která umožňuje uživatelům vytvářet a sdílet amatérské videoklipy. Stala se extrémně populární a v současnosti je jednou z nejvíce stahovaných aplikací na světě. Původně byla platforma zaměřena hlavně na generaci Z – tedy na mladé lidi do 24 let, kteří se aktivně snaží získat svou „minutu slávy“ na internetu soutěžením o popularitu v krátkých videích. Dnes ale TikTok přitahuje nejen děti a teenagery, ale i lidi různého věku, protože platforma nabízí prostor pro kreativní sebevyjádření a umožňuje tvořivost. TikTok umožňuje natáčet, upravovat a publikovat krátká videa. Původně trvala videa pouze 15 sekund, ale později byl tento limit prodloužen na 60 sekund. Uživatelé mohou do svých videí přidávat různé filtry, hudbu, animace a speciální efekty, což činí obsah ještě kreativnějším a zajímavějším.

Vytváření videí na TikToku je velmi jednoduché, protože aplikace má vestavěný editor pro úpravu videí a také mnoho masek, filtrů a efektů pro vylepšení videí. Uživatelé mohou lajkovat a komentovat videa, která se jim líbí. Navíc mohou sledovat tiktokery — aktivní uživatele, jejichž obsah je jim sympatický. Vývojáři TikToku udělali aplikaci pohodlnou a jednoduchou pro použití na zařízeních s operačními systémy iOS a Android, což přispělo k popularitě této platformy mezi mobilními uživateli.[65]

6.1 Historie TikToku

V roce 2014 čínští podnikatelé Alex Zhu a Lu Yung vytvořili videoplatformu Musical.ly, která během několika let získala velkou popularitu mezi uživateli. To byl první krok k vytvoření TikToku, který se časem stal jednou z nejpopulárnějších aplikací na světě. [66] V září roku 2016 byla společností ByteDance pod vedením podnikatele Zhang Yiminga spuštěna aplikace Douyin, jejímž cílem bylo umožnit uživatelům snadnou tvorbu a sdílení krátkých videí zaměřených především na kreativitu a zábavu.[67]

[65] TikTok. TERMIN.IN.UA [online]. [cit. 2026-03-05]. Dostupné z: https://termin.in.ua/tiktok/#Novi_instrumenti_v_TikTok

[66] TikTok. TERMIN.IN.UA [online]. [cit. 2026-03-10]. Dostupné z: https://termin.in.ua/tiktok/#Novi_instrumenti_v_TikTok

[67] KOPECKÝ, Kamil a KREJČÍ, Veronika. Sociální sítě: úvod do problematiky [online]. Olomouc: Univerzita Palackého v Olomouci, 2023 [cit. 2026-03-10]. Dostupné z: https://e-bezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studenty/140-socialni-site-uvod-do-problematiky/file. ISBN 978-80-244-6370-4, str. 39

V listopadu 2017 byla platforma Musical.ly koupena mediální a technologickou společností ByteDance z Pekingu za 1 miliardu dolarů. V té době již měla ByteDance podobnou aplikaci – TikTok, který byl spuštěn v Číně v roce 2016. Obě platformy byly populární, ale podle Reuters každá dominovala v jiných částech světa: Musical.ly byla populární v Americe a Evropě s 100 miliony aktivních uživatelů měsíčně, zatímco TikTok dominoval v Asii s 500 miliony odběratelů. Rozhodnutí společnosti ByteDance sloučit dvě aplikace do jednoho produktu bylo krokem k zvýšení efektivity. Společnost uvedla, že TikTok lépe odráží širokou škálu obsahu, který přesahuje rámec hudby. Proto v srpnu TikTok pohltil Musical.ly. Všechny uživatelské profily a videa byly automaticky přesunuty na TikTok a aplikace dříve známá jako Musical.ly přestala existovat. Vzhledem k omezením internetu v Číně zůstává TikTok samostatnou aplikací pod názvem Douyin, která má více než 300 milionů aktivních uživatelů měsíčně.[68]

6.2 Uživatelé platformy TikTok a tvůrci obsahu na TikToku

Sociální síť TikTok zaznamenala v České republice výrazný nárůst popularity zejména mezi mladší generací uživatelů. Výsledky aktuálních výzkumů však ukazují, že přibližně 80 % uživatelské základny tvoří osoby starší 18 let. Počet aktivních uživatelů platformy v České republice dosahuje podle dostupných statistik přibližně 2,4 milionu měsíčně.[69] Nejpočetnější skupinu uživatelů představují osoby ve věku 18 až 24 let, přičemž v této kategorii převažují ženy. Z hlediska tematického zaměření obsahu patří mezi nejpopulárnější oblasti především hry a herní tvorba.[70]

Aplikace TikTok je oficiálně dostupná uživatelům od 13 let, přičemž některé funkce zůstávají omezené až do dosažení věku 16 nebo 18 let.[71] Podobně jako jiné sociální sítě, například Instagram, poskytuje TikTok vybraným uživatelům možnost získat širší veřejnou známost a vybudovat si vlastní publikum. Tvůrci obsahu, kteří na platformě aktivně působí a získávají větší počet sledujících, jsou běžně označováni jako tiktokeři.

[68] TikTok. TERMIN.IN.UA [online]. [cit. 2026-03-10]. Dostupné z: https://termin.in.ua/tiktok/#Novi_instrumenti_v_TikTok

[69] TikTok roste nejen u generace Z, zapojuje se i více značek. *Mediaguru.cz* [online]. 2023 [cit. 2026- 03-15]. Dostupné z: https://www.mediaguru.cz/clanky/2023/11/tiktok-roste-nejen-u-generace-z-zapojuje-se-i-vice-znacek/

[70] KLEMENT, Vítězslav. Tak takto to teď vypadá na českém TikToku… *LinkedIn* [online]. 2023 [cit. 2026-03-15]. Dostupné z:https://cz.linkedin.com/posts/vklement_tiktok-groupm-groupmnexus-activity-7023540897468272640-5Umz

[71] TikTok se v Česku blíží k 2,5 milionům, chystá další cílení. *Mediaguru.cz* [online] 2023 [cit. 2026-03-15]. Dostupné z: https://www.mediaguru.cz/clanky/2023/03/tiktok-se-v-cesku-blizi-k-2-5milionum-chysta-dalsi-cileni/

Mezi nejvýraznější osobnosti globální TikTok scény patří Khaby Lame, který má více než 160 milionů sledujících a proslavil se především svým charakteristickým humorem a výrazovou jednoduchostí.[72] V českém prostředí patří mezi nejúspěšnější tvůrce Ondy Mikula, jehož profil sleduje více než 38 milionů uživatelů. Jeho tvorba je zaměřena zejména na sdílení tipů a návodů pro zlepšení kvality videí na platformě. Vysokou popularitu si zároveň udržuje i známá tiktokerka Charli D'Amelio.[73]

Platforma TikTok umožňuje uživatelům finančně podporovat oblíbené tvůrce prostřednictvím tzv. virtuálních dárků. Tyto dárky lze aktivovat pomocí virtuální měny, kterou si uživatelé mohou zakoupit přímo v rámci aplikace. Výše odměny, kterou tvůrce obdrží, je závislá na typu a množství zaslaných dárků.[74]

6.3 Algoritmus TikToku

Sociální sítě využívají vlastní algoritmické mechanismy, jejichž primárním účelem je zobrazovat uživatelům takový obsah, který odpovídá jejich zájmům a zvyšuje pravděpodobnost jejich další aktivity na platformě.[75] Tyto systémy pracují s pokročilými technologickými nástroji, které analyzují chování uživatele a na základě získaných dat přizpůsobují strukturu zobrazovaného obsahu. Současně usilují o prodloužení času, který uživatel na dané platformě tráví.

Podobný princip funguje i na sociální síti TikTok, zejména prostřednictvím sekce označované jako „Pro tebe" (For You Page). Již při prvním použití aplikace si uživatel může zvolit oblasti, které ho zajímají, přičemž algoritmus následně vytváří počáteční podobu doporučovaného obsahu na hlavní stránce.

[72] CHEONG, Charissa; LLOYD, Andrew. Inside the rise of the top 25 most followed TikTok accounts of 2023. *Insider* [online]. 2023 [cit. 2026-03-15]. Dostupné z: https://www.businessinsider.com/top-25-most-followed-tiktok-creators-in-2023-ranked

[73] ŠNAJDROVÁ, Tereza. 10 nejsledovanějších českých tiktokerů a tiktokerek v roce 2022. *Refresher* [online]. 2022 [cit. 2026-03-15]. Dostupné z: https://refresher.cz/118023-10-nejsledovanejsich-ceskych-tiktokeru-a-tiktokerek-v-roce-2022

[74] TikTok zpoplatní část obsahu. *Mediaguru.cz* [online]. 2023 [cit. 2026-03-15]. Dostupné z: https://www.mediaguru.cz/clanky/2023/03/tiktok-zpoplatni-cast-obsahu/

[75] LOSEKOOT, Michelle a VYHNÁNKOVÁ, Eliška. *Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích.* Brno: Jan Melvil Publishing, 2019. ISBN 978-80-7555-084-2, str. 68.

Stránka For You Page představuje hlavní rozhraní aplikace, které se zobrazí po jejím spuštění. Nabízený obsah je individualizovaný na základě doporučovacího systému, který zohledňuje více faktorů. Mezi klíčové patří zejména:

- uživatelské interakce s obsahem (např. lajky, komentáře, sdílení či vlastní tvorbu),
- charakteristiky samotných videí (např. titulky, zvukové stopy nebo hashtagy),
- technická a jazyková nastavení aplikace a zařízení (např. lokalitu, jazyk či typ zařízení).

Algoritmus průběžně analyzuje uživatelské chování a na základě těchto poznatků upravuje strukturu zobrazovaného obsahu tak, aby byla co nejvíce personalizovaná. Výsledkem je skutečnost, že podoba stránky For You Page je pro každého uživatele odlišná a za určitých okolností se na ní může objevit i obsah vytvořený samotným uživatelem.[76] S rostoucí intenzitou využívání aplikace dochází k postupnému zpřesňování identifikace uživatelských preferencí a dalšímu přizpůsobování nabídky zobrazovaných videí.

6.4 Sdílení a zpracování osobních údajů na TikToku

Sociální síť TikTok při svém fungování shromažďuje a následně zpracovává široké spektrum osobních údajů svých uživatelů. Nejedná se pouze o informace poskytnuté při registraci, jako je jméno, věk či kontaktní údaje, ale také o data vznikající během samotného používání aplikace. Mezi ně patří například informace o aktivitě uživatele, sledovaném obsahu, interakcích s ostatními uživateli nebo technické údaje o zařízení a připojení k internetu. Tyto informace jsou využívány především za účelem zajištění funkčnosti služby, personalizace zobrazovaného obsahu a optimalizace reklamních sdělení.

Z pohledu kybernetické bezpečnosti však může být problematické především rozsáhlé množství shromažďovaných dat a způsob jejich dalšího využití. Platforma může osobní údaje sdílet s externími poskytovateli služeb či obchodními partnery, což může zvyšovat riziko jejich zneužití. Specifickou otázkou je rovněž uchovávání a přenos dat mezi jednotlivými státy, kdy nemusí být vždy zajištěna stejná úroveň ochrany soukromí. V tomto kontextu je důležité, aby si uživatelé byli vědomi toho, jaké informace o sobě sdílejí a jak mohou ovlivnit jejich digitální bezpečnost.[77]

[76] TikTok. #2023. Online. TikTok [online]. 2023 [cit. 2026-03-16]. Dostupné z: https://www.tiktok.com/tag/2023?lang=cs-CZ.
[77] TikTok. Privacy Policy (EEA). TikTok [online]. 2025 [cit. 2026-03-17]. Dostupné z: https://www.tiktok.com/legal/page/eea/privacy-policy/cs

6.5 Rizika spojená s ochranou osobních údajů uživatelů TikToku

Používání sociální sítě TikTok s sebou nese určitá rizika v oblasti ochrany osobních údajů, která mohou být výraznější zejména u mladších uživatelů, například studentů středních škol. Tito uživatelé často sdílejí obsah spontánně a bez dostatečného uvědomění si možných důsledků. Může tak docházet k nadměrnému zveřejňování osobních informací, které mohou být následně zneužity například k cílené manipulaci, kyberšikaně nebo jiným formám online útoků.

Dalším významným rizikem je nedostatečné zabezpečení uživatelského účtu, například používání slabých hesel nebo nevyužívání dostupných bezpečnostních funkcí. Problematická může být také nízká úroveň mediální a digitální gramotnosti, která vede k tomu, že mladí uživatelé často nerozlišují mezi veřejným a soukromým sdílením informací. V kontextu kybernetické bezpečnosti je proto důležité zdůraznit potřebu prevence, vzdělávání a informovanosti o možných hrozbách spojených s používáním sociálních sítí. Odpovědný přístup k ochraně osobních údajů a vhodné nastavení soukromí mohou významně snížit rizika spojená s používáním platformy TikTok.[78]

6.6 Digitální stopa a dlouhodobé dopady obsahu

Používání sociálních sítí, zejména platformy TikTok, je úzce spojeno se vznikem digitální stopy, která může mít dlouhodobé dopady na soukromí a bezpečnost uživatelů. Digitální stopa vzniká nejen zveřejňováním vlastního obsahu, jako jsou videa, komentáře nebo reakce, ale také prostřednictvím běžných online aktivit, například sledováním příspěvků či interakcemi s ostatními uživateli. Tyto informace mohou zůstat v digitálním prostředí dostupné po dlouhou dobu a být využívány například k personalizaci obsahu nebo cílení reklam. [79] V prostředí TikToku, kde dochází k rychlému šíření obsahu a jeho vysoké viditelnosti, může být digitální stopa výraznější než na jiných sociálních sítích.

Dlouhodobé dopady sdíleného obsahu mohou být obzvláště významné u mladších uživatelů, například studentů středních škol, kteří platformu často využívají k sebeprezentaci a komunikaci se svým sociálním okolím. Obsah publikovaný v období dospívání může být v budoucnu interpretován odlišně a může ovlivnit reputaci jednotlivce nebo

[78] TikTok. Privacy Policy (EEA). TikTok [online]. 2025 [cit. 2026-03-17]. Dostupné z: https://www.tiktok.com/legal/page/eea/privacy-policy/cs

[79] NETSAFE. Digital footprints [online]. Netsafe, 2025 [cit. 2026-03-18]. Dostupné z: https://netsafe.org.nz/children-and-young-people/digital-footprints

jeho studijní a pracovní příležitosti. Odborné zdroje upozorňují, že mladí lidé si často plně neuvědomují trvalost digitálních informací a rizika spojená s jejich sdílením, což může vést k neuváženému zveřejňování osobních údajů nebo citlivého obsahu.[80] Digitální gramotnost je proto důležité podporovat a informovanost o možných hrozbách, aby uživatelé dokázali lépe posoudit důsledky svého online chování a minimalizovat rizika spojená s používáním sociálních sítí, včetně TikToku.

[80] Digital Footprints and the Dangers of Just Being a Kid. *The Daily Free Press* [online]. 2017 [cit. 2026-03-18]. Dostupné z: https://dailyfreepress.com/04/07/17/212066/digital-footprints-and-the-dangers-of-just-being-a-kid-terms-and-conditions/

7 Praktická část

Praktická část této bakalářské práce je zaměřena na zjištění způsobu využívání sociální sítě TikTok mezi studenty střední školy TRIVIS v Praze a na analýzu rizik spojených s jejím používáním z hlediska kybernetické bezpečnosti a ochrany osobních údajů. Hlavním cílem výzkumu bylo zjistit, jak často studenti tuto sociální síť používají, jak mají nastavené zabezpečení svých uživatelských účtů a do jaké míry si uvědomují možná rizika související s používáním sociálních sítí v online prostředí. Výzkum se dále zaměřoval na zjištění zkušeností studentů s bezpečnostními hrozbami, jejich přístup k ochraně soukromí a informovanost o tom, že sociální síť TikTok shromažďuje a zpracovává osobní údaje uživatelů.

Ke sběru dat byla využita kvantitativní výzkumná metoda formou dotazníkového šetření. Dotazník byl vytvořen v online prostředí Microsoft Forms a obsahoval celkem 14 uzavřených otázek zaměřených na demografické údaje respondentů, frekvenci a způsob využívání sociální sítě TikTok, nastavení zabezpečení uživatelských účtů, zkušenosti s bezpečnostními incidenty a úroveň informovanosti o ochraně osobních údajů. Výzkumný soubor tvořili studenti střední školy TRIVIS v Praze.

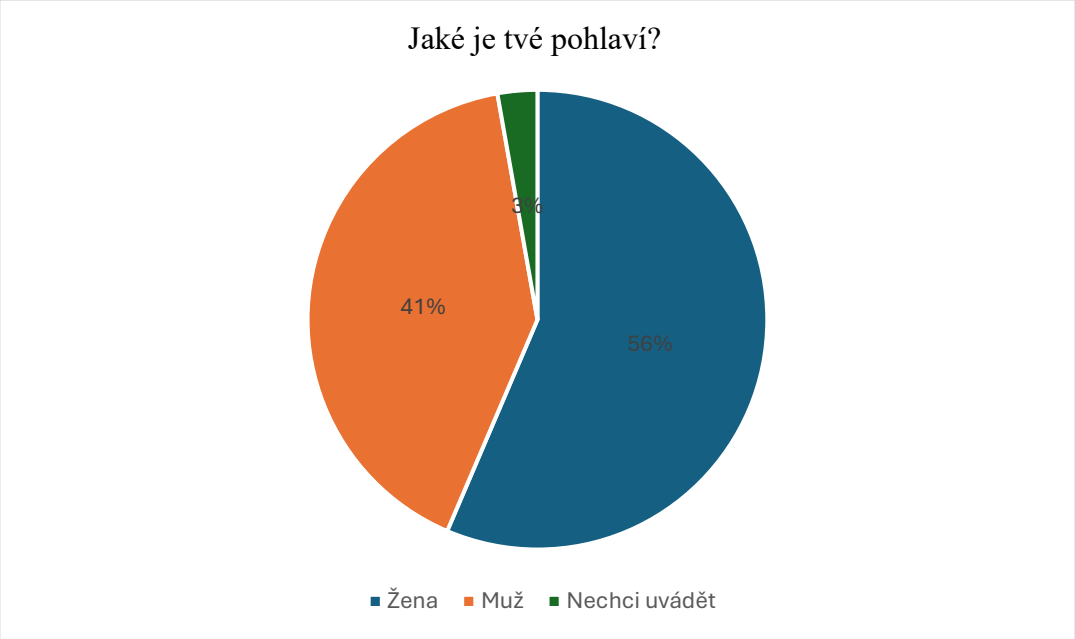
Dotazník byl distribuován prostřednictvím učitele působícího na uvedené střední škole, který jej studentům sdílel formou online odkazu. Sběr dat probíhal v období od 9. března do 10. března 2026 a výzkumu se zúčastnilo celkem 179 respondentů. Účast na výzkumu byla dobrovolná a respondenti byli před vyplněním dotazníku informováni o anonymitě šetření a o tom, že získaná data budou využita výhradně pro účely této bakalářské práce.

V dotazníku byla využita filtrační otázka č. 4 zaměřená na používání sociální sítě TikTok. Respondenti, kteří uvedli, že tuto sociální síť nepoužívají, byli automaticky přesměrováni na otázku č. 13, jelikož na následující otázky mohli odpovídat pouze respondenti, kteří TikTok aktivně využívají. Po zodpovězení této otázky pokračovalo v dotazníku celkem 158 respondentů. V otázce č. 13 odpovídal již celý soubor respondentů, tedy 179. Dotazník neobsahoval žádné identifikační ani citlivé osobní údaje, čímž bylo minimalizováno riziko zásahu do soukromí respondentů. Získaná data byla exportována z prostředí Microsoft Forms a následně zpracována pomocí základních statistických metod.

Výsledky výzkumu jsou prezentovány prostřednictvím absolutních a relativních četností a graficky znázorněny formou grafů.

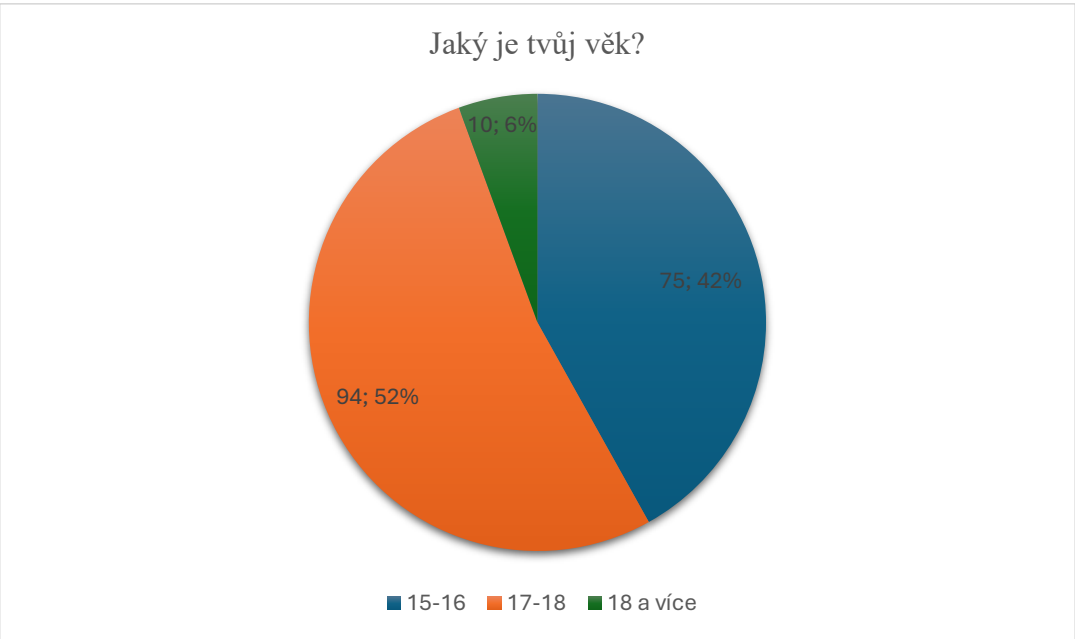
7.1 Vyhodnocení dotazníku

Graf 1: Jaké je tvé pohlaví?[81]



Z celkového počtu 179 respondentů uvedlo 101 respondentů (56 %) ženské pohlaví, 73 respondentů (41 %) mužské pohlaví a 5 respondentů (3 %) nechtělo své pohlaví uvést. Z výsledků vyplývá, že ve výzkumu převažovaly respondentky ženského pohlaví.

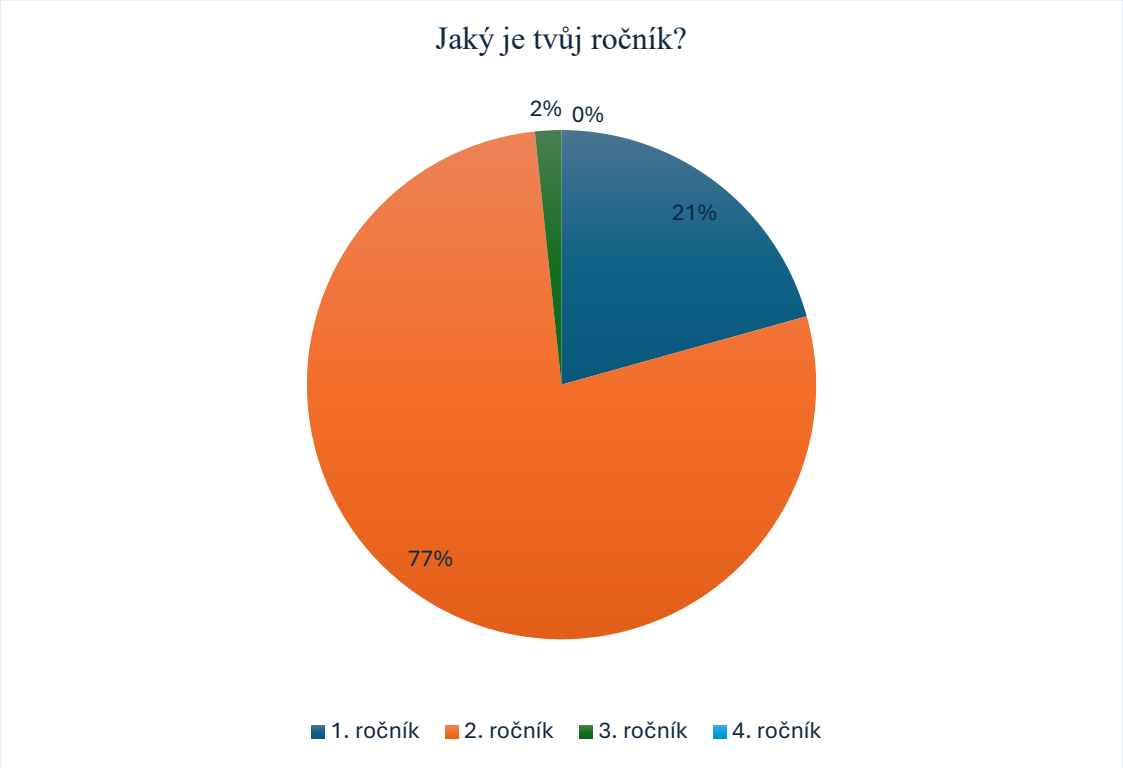
Graf 2: Jaký je tvůj věk?[82]



[81] Vlastní zpracování
[82] Vlastní zpracování

Největší skupinu respondentů tvořili studenti ve věku 17–18 let, celkem 94 respondentů (52 %). Ve věkové kategorii 15–16 let bylo zastoupeno 75 respondentů (42 %) a 10 respondentů (6 %) uvedlo věk 18 a více let. Výsledky ukazují, že výzkumný soubor tvoří převážně studenti ve věku odpovídajícím středoškolskému studiu.

Graf 3: Jaký je tvůj ročník?[83]

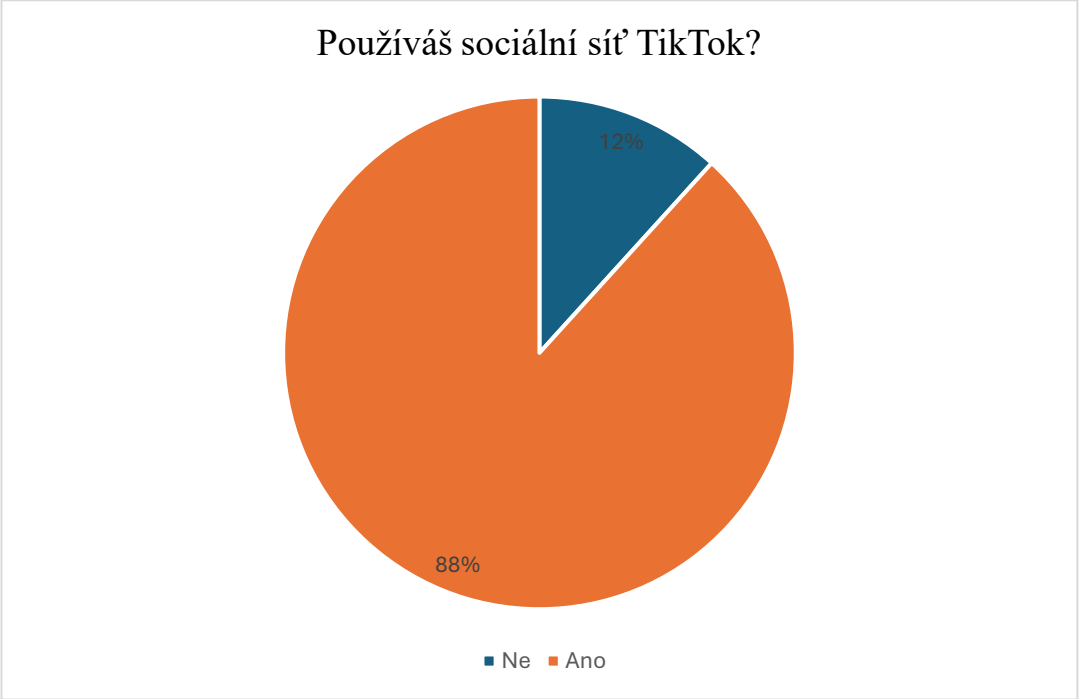


Z výsledků vyplývá, že 139 respondentů (77 %) studuje ve 2. ročníku, 37 respondentů (21 %) v 1. ročníku a 3 respondenti (2 %) ve 3. ročníku. Žádný z respondentů neuvedl 4. ročník. Výzkumný soubor je tedy tvořen převážně studenty nižších ročníků, což může souviset s věkovým složením školy a zároveň ovlivnit jejich zkušenosti s používáním sociálních sítí i úroveň povědomí o možných rizicích v online prostředí.

Tato skutečnost je důležitá při interpretaci dalších zjištění, jelikož mladší studenti mohou vykazovat odlišné návyky v oblasti digitální bezpečnosti, ochrany soukromí či vnímání online hrozeb ve srovnání se staršími ročníky.

[83] Vlastní zpracování

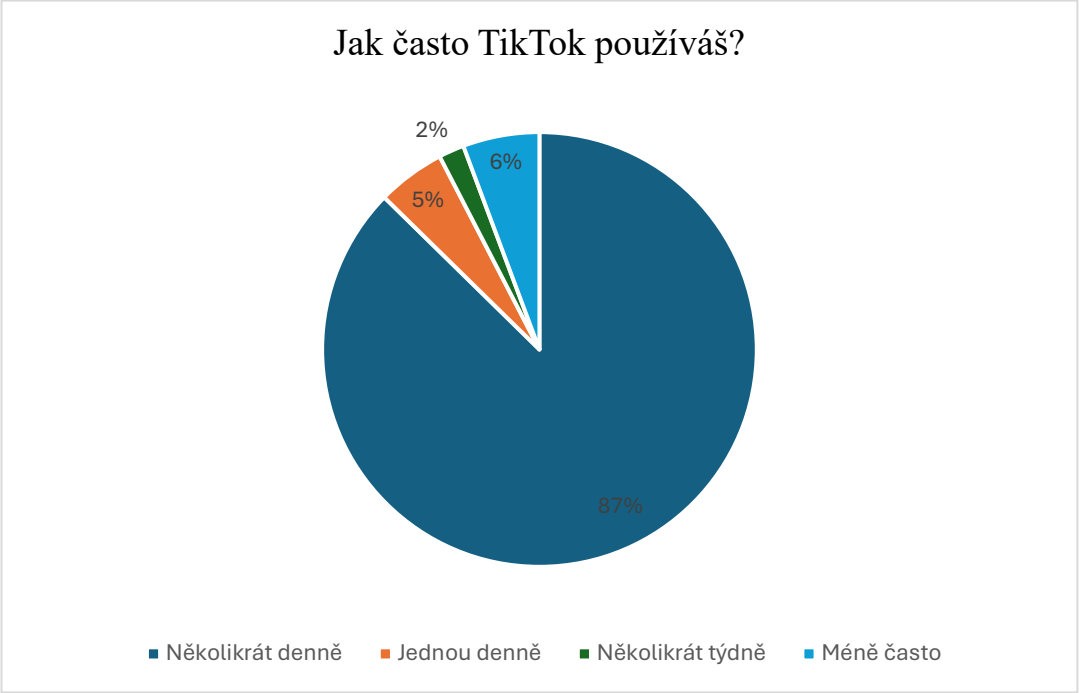
Graf 4: Používáš sociální síť TikTok?[84]



Součástí dotazníku byla filtrační položka zjišťující, zda respondenti využívají sociální síť TikTok. Celkem odpovědělo 179 respondentů, přičemž 158 z nich uvedlo, že TikTok používají (88 %), zatímco 21 respondentů uvedlo, že tuto sociální síť nevyužívají (12 %). Respondenti, kteří uvedli, že TikTok nepoužívají, byli v dotazníku automaticky přesměrováni na otázku č. 13, jelikož na následující otázky mohli odpovídat pouze respondenti, kteří tuto sociální síť aktivně využívají. Následující vyhodnocení proto vychází z odpovědí respondentů, kteří TikTok používají.

[84] Vlastní zpracování

Graf 5: Jak často TikTok Používáš?[85]



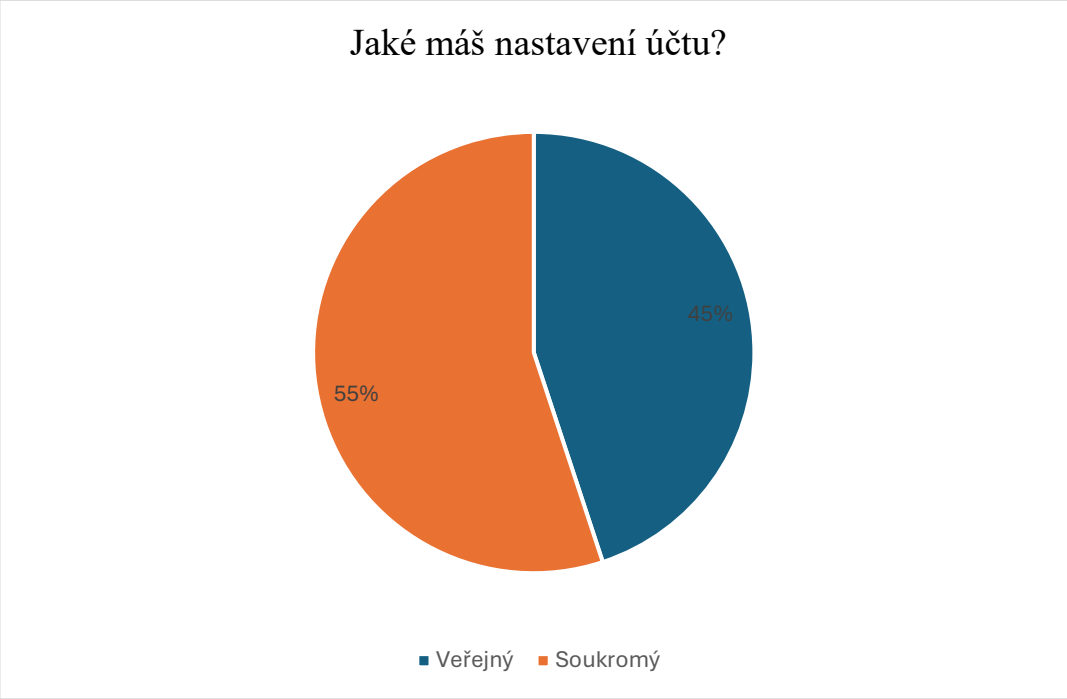
Frekvence využívání sociální sítě TikTok byla zjišťována u respondentů, kteří uvedli, že tuto platformu používají. Z celkového počtu 158 respondentů největší část uvedla, že TikTok využívá několikrát denně, konkrétně 138 respondentů (87 %).

Výrazně menší podíl respondentů uvedl, že TikTok používá méně často, a to 9 respondentů (6 %). Denní používání jednou za den deklarovalo 8 respondentů (5 %) a pouze 3 respondenti (2 %) uvedli, že platformu využívají několikrát týdně.

Z výsledků vyplývá, že TikTok představuje pro většinu respondentů běžnou součást každodenního života a je využíván velmi intenzivně. Nízký podíl méně častého používání naznačuje, že platforma má mezi studenty silné postavení a vysokou míru atraktivity.

[85] Vlastní zpracování

Graf 6: Jaké máš nastavení účtu?[86]

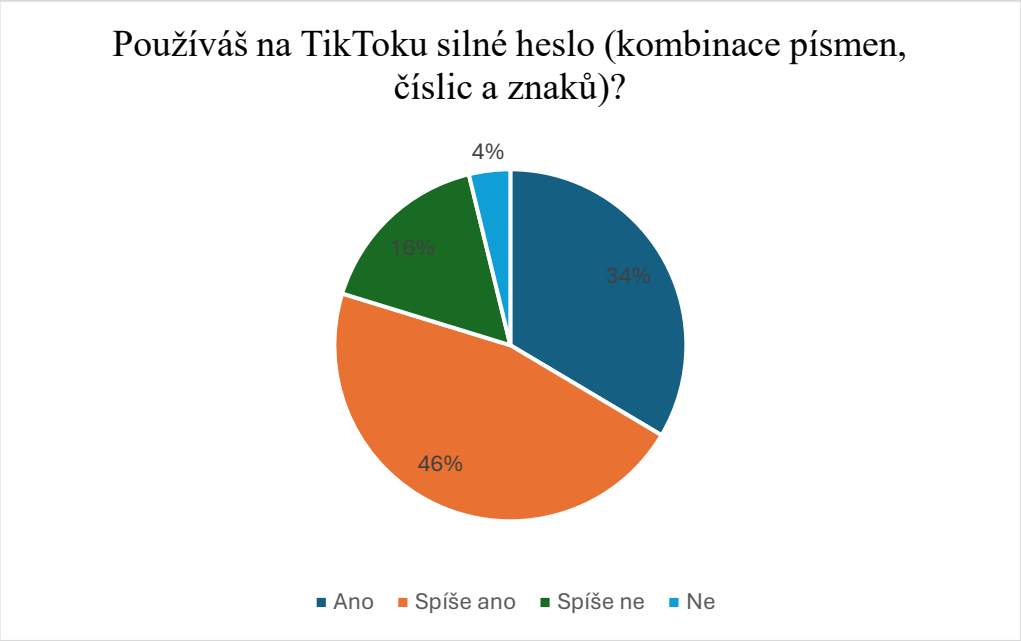


Otázka číslo 6 zjišťovala, jaké nastavení účtu na sociální síti TikTok respondenti využívají. Výsledky ukázaly, že 87 respondentů (55 %) má svůj účet nastavený jako soukromý, zatímco 71 respondentů (45 %) používá veřejné nastavení profilu. Převaha soukromých účtů naznačuje určitou míru uvědomění si významu ochrany soukromí a snahy o omezení přístupu cizích osob k publikovanému obsahu.

Současně je však podíl veřejných účtů stále poměrně vysoký, což může zvyšovat riziko nežádoucích kontaktů či zneužití sdílených informací. Výsledky tak poukazují na potřebu dalšího zvyšování informovanosti studentů o bezpečném nastavení soukromí a odpovědném chování v online prostředí.

[86] Vlastní zpracování

Graf 7: Používáš na TikToku silné heslo (kombinace písmen, číslic a znaků)?[87]

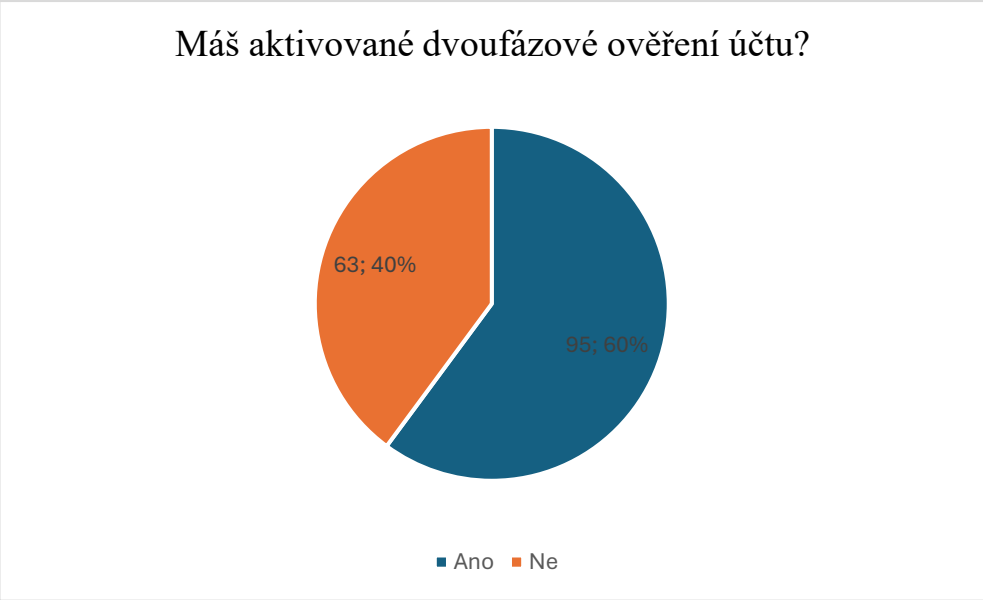


Respondenti měli na výběr ze čtyř možností odpovědi, které vyjadřovaly míru využívání silného hesla na sociální síti TikTok. Nejčastěji byla zvolena odpověď spíše ano, kterou uvedlo 73 respondentů (46 %). Jednoznačně kladnou odpověď ano zvolilo 53 studentů (34 %). Naopak možnost spíše ne označilo 26 respondentů (16 %) a pouze 6 respondentů uvedlo odpověď ne (4 %).

Z výsledků vyplývá, že většina studentů si význam silného hesla uvědomuje a alespoň částečně jej využívá. Přesto však část respondentů nepřistupuje k zabezpečení účtu dostatečně zodpovědně, což může zvyšovat riziko neoprávněného přístupu k jejich profilu. Zjištěná data tak poukazují na potřebu posilování povědomí o zásadách bezpečného chování v online prostředí, zejména v oblasti ochrany přihlašovacích údajů.

[87] Vlastní zpracování

Graf 8: Máš aktivované dvoufázové ověření účtu?[88]



Respondenti měli možnost vyjádřit se, zda mají na sociální síti TikTok aktivované dvoufázové ověření účtu, přičemž vybírali ze dvou variant odpovědi – ano nebo ne. Z výsledků vyplývá, že dvoufázové ověření má aktivováno 95 respondentů (60 %), zatímco 63 respondentů (40 %) uvedlo, že tuto formu zabezpečení nepoužívá. Lze tedy konstatovat, že většina dotazovaných využívá pokročilejší způsob ochrany svého účtu.

Získaná data naznačují, že část studentů si uvědomuje význam zabezpečení osobních údajů a snaží se aktivně chránit svůj profil před neoprávněným přístupem. Přesto je podíl respondentů bez aktivního dvoufázového ověření poměrně vysoký, což může zvyšovat riziko zneužití účtu nebo úniku citlivých informací. Výsledky proto poukazují na potřebu dalšího vzdělávání studentů v oblasti digitální bezpečnosti a důležitosti využívání dostupných ochranných nástrojů.

[88] Vlastní zpracování

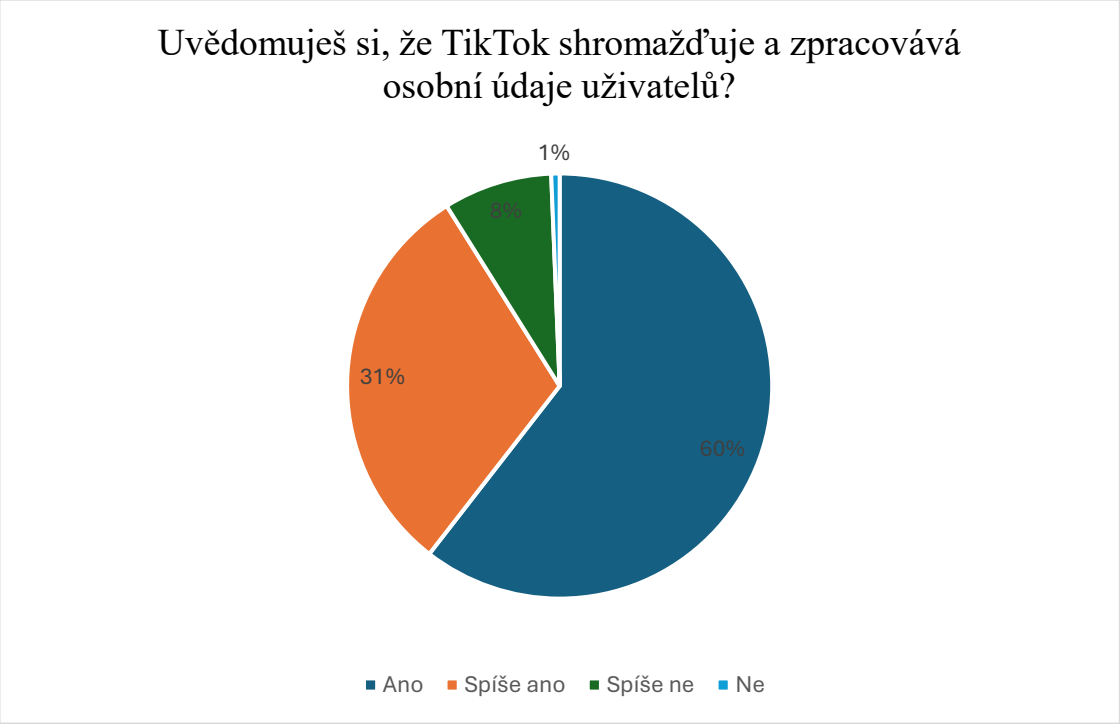
Graf 9: Setkal/a ses na TikToku s bezpečnostní hrozbou?[89]

Zjišťováno bylo, zda se respondenti na sociální síti TikTok již setkali s bezpečnostní hrozbou. Z výsledků vyplývá, že zkušenost s touto situací uvedlo 48 respondentů (30 %), zatímco většina, konkrétně 110 respondentů (70 %), se s žádným bezpečnostním rizikem nesetkala.

Výsledky naznačují, že přestože většina studentů nemá s bezpečnostními hrozbami na TikToku přímou zkušenost, nelze tuto problematiku podceňovat. Skutečnost, že se s rizikovou situací setkala téměř třetina respondentů, poukazuje na význam prevence a zvyšování povědomí o bezpečném chování v online prostředí.

[89] Vlastní zpracování

Graf 10: Uvědomuješ si, že TikTok shromažďuje a zpracovává osobní údaje uživatelů?[90]



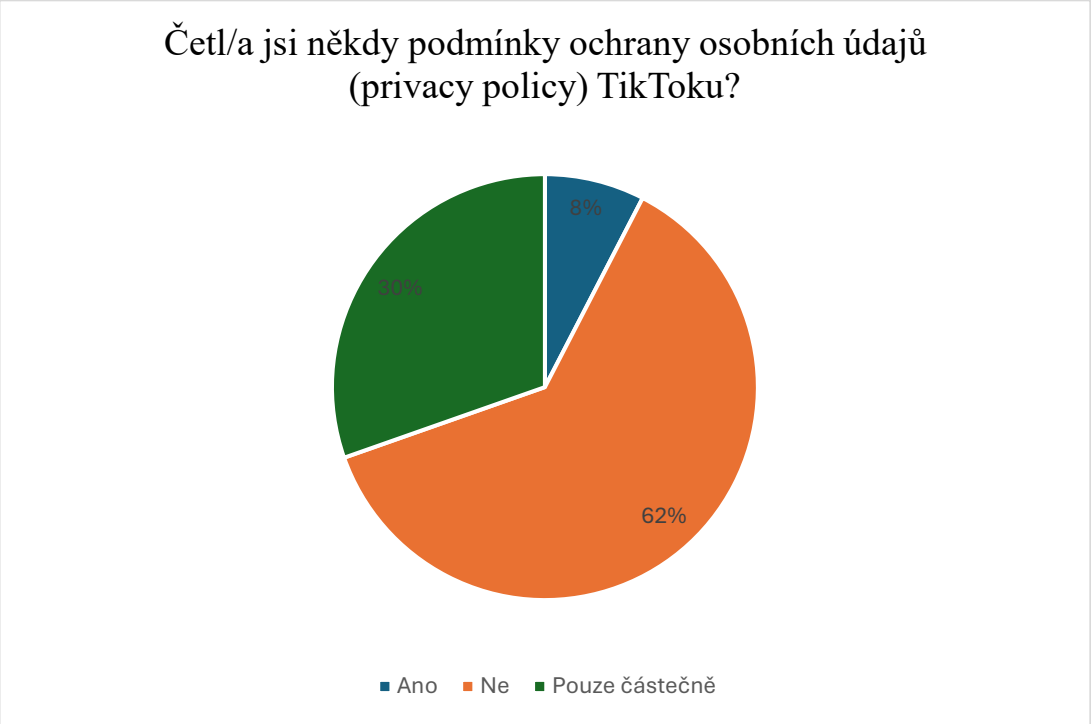
Zjišťováno bylo, zda si respondenti uvědomují, že sociální síť TikTok shromažďuje a zpracovává osobní údaje svých uživatelů. Respondenti měli možnost vybrat jednu ze čtyř odpovědí vyjadřujících míru jejich souhlasu či informovanosti o této skutečnosti. Největší podíl respondentů uvedl, že si této skutečnosti je vědom – celkem 95 respondentů (60 %) zvolilo odpověď „ano“ a dalších 49 respondentů (31 %) odpověď „spíše ano“. Naopak menší část respondentů vyjádřila nejistotu nebo nesouhlas, kdy 13 respondentů (8 %) uvedlo odpověď „spíše ne“ a pouze 1 respondent (1 %) odpověděl „ne“.

Výsledky naznačují, že většina studentů má základní povědomí o tom, že používání sociální sítě TikTok je spojeno se zpracováním osobních údajů, což může přispívat k jejich opatrnějšímu chování v online prostředí. Přesto se ukazuje, že část respondentů si rizika spojená se sdílením osobních dat plně neuvědomuje nebo jim nevěnuje dostatečnou pozornost. Tento fakt poukazuje na potřebu dalšího vzdělávání v oblasti digitální bezpečnosti, ochrany soukromí a informovaného používání sociálních sítí. Zvýšení povědomí o způsobech sběru a využívání osobních údajů může vést ke

[90] Vlastní zpracování

snížení rizik spojených s kybernetickými hrozbami a posílení bezpečného chování uživatelů v online prostoru.

Graf 11: Četl/a jsi někdy podmínky ochrany osobních údajů (privacy policy) TikToku?[91]



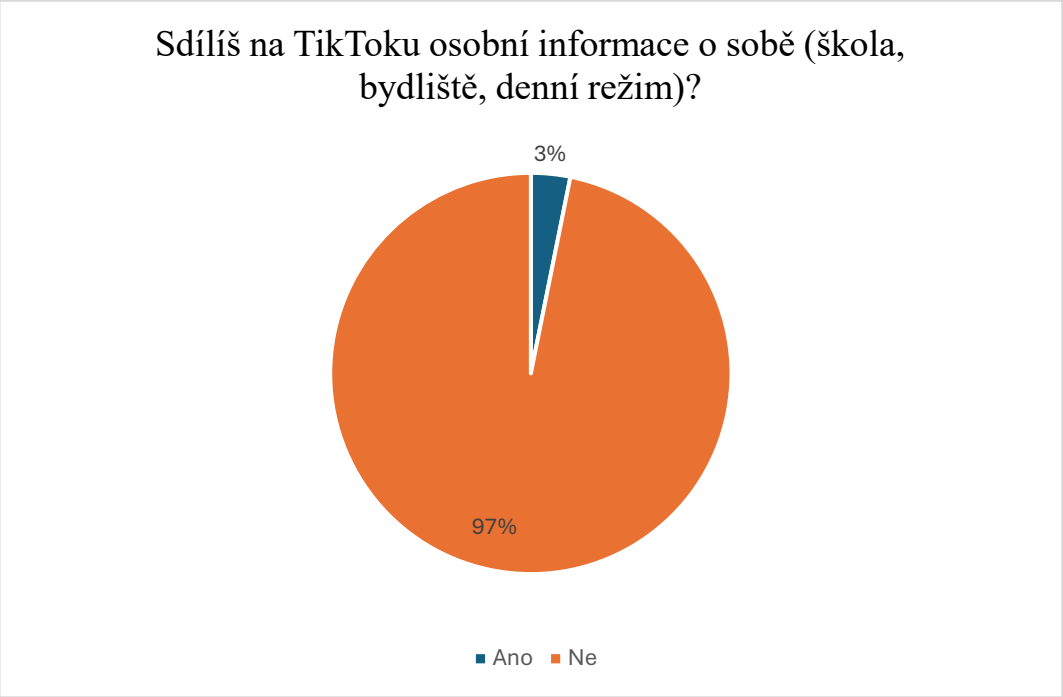
Respondenti se dále vyjadřovali k tomu, zda si někdy přečetli podmínky ochrany osobních údajů (privacy policy) sociální sítě TikTok. V této otázce měli možnost volby ze tří odpovědí, které zjišťovaly míru jejich seznámení s těmito podmínkami. Z odpovědí vyplynulo, že největší část studentů se s těmito podmínkami vůbec neseznámila – tuto možnost uvedlo 98 respondentů (62 %). Dalších 48 respondentů (30 %) uvedlo, že si podmínky přečetli pouze částečně, a pouze menší skupina, konkrétně 12 respondentů (8 %), deklarovala, že se s nimi seznámila v plném rozsahu.

Tyto výsledky naznačují, že ačkoli si studenti často uvědomují existenci zpracování osobních údajů na sociálních sítích, aktivní zájem o detailní informace o jejich ochraně není příliš vysoký. Nedostatečné seznámení s podmínkami může vést k nižší orientaci v tom, jakým způsobem jsou osobní data využívána a jaká rizika mohou být s jejich

[91] Vlastní zpracování

sdílením spojena. Z pohledu bezpečného chování v online prostředí se proto jeví jako důležité podporovat větší informovanost a motivovat uživatele k tomu, aby se s pravidly ochrany soukromí seznamovali důkladněji.

Graf 12: Sdílíš na TikToku osobní informace o sobě (škola, bydliště, denní režim)?[92]



Další otázka se zaměřovala na to, zda studenti na sociální síti TikTok sdílejí osobní informace o sobě, například údaje o škole, místě bydliště nebo svém denním režimu. Z výsledků vyplynulo, že naprostá většina respondentů tyto informace na této platformě neuvádí – tuto možnost zvolilo celkem 153 studentů (97 %). Pouze menší skupina, konkrétně 5 respondentů (3 %), uvedla, že některé osobní informace sdílí.

Výsledek naznačuje, že studenti jsou v oblasti zveřejňování osobních údajů na sociálních sítích spíše opatrní. Lze předpokládat, že si alespoň částečně uvědomují možná rizika spojená s nadměrným sdílením informací v online prostředí. Opatrnější přístup k publikování osobních údajů může přispívat k ochraně soukromí a snížení pravděpodobnosti jejich zneužití.

[92] Vlastní zpracování

Zároveň je však vhodné upozornit, že i malá část uživatelů, kteří osobní informace sdílejí, může být vystavena zvýšenému riziku například v podobě nevyžádaného kontaktu, zneužití údajů či jiných negativních jevů spojených s online komunikací. Proto je důležité nadále podporovat povědomí o bezpečném chování na sociálních sítích a zdůrazňovat význam ochrany soukromí v digitálním prostředí.

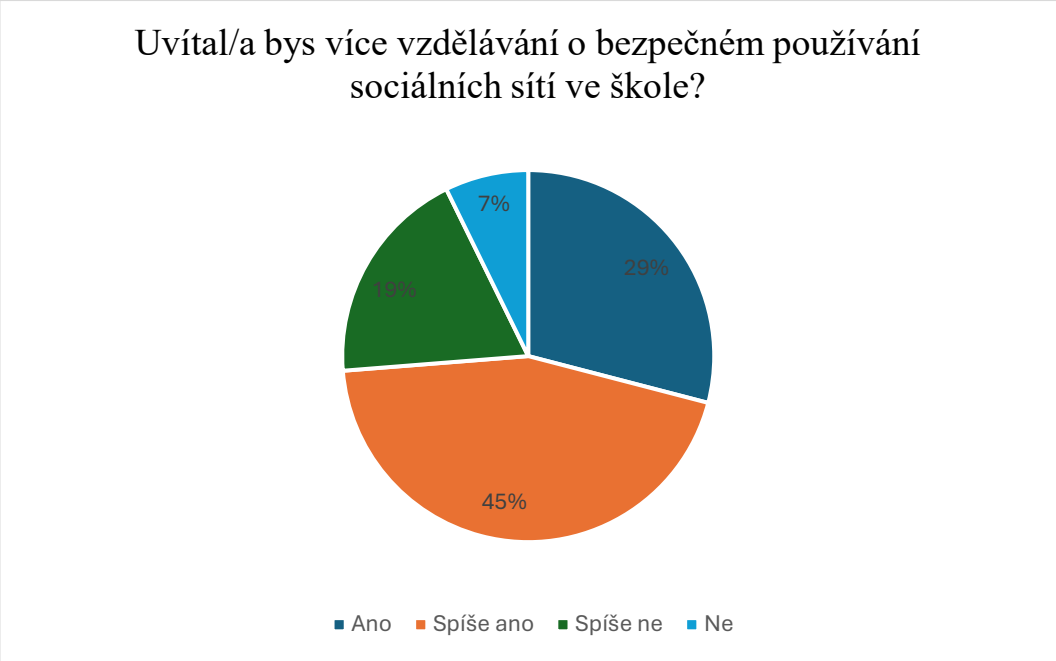
Graf 13: Považuješ TikTok za rizikovou platformu z hlediska kybernetické bezpečnosti?[93]

V této otázce se studenti vyjadřovali k tomu, zda považují sociální síť TikTok za rizikovou z hlediska kybernetické bezpečnosti. Na tuto položku již odpovídal plný počet respondentů, tedy celkem 179 studentů. Výsledky ukazují, že většina respondentů vnímá TikTok jako potenciálně rizikovou platformu – tuto možnost zvolilo 118 respondentů (66 %). Naproti tomu 61 respondentů (34 %) uvedlo, že tuto sociální síť za rizikovou nepovažují.

[93] Vlastní zpracování

Zjištěné výsledky poukazují na to, že mezi studenty převažuje spíše opatrnější postoj k používání této sociální sítě. Vnímání TikToku jako rizikového může souviset s obecně známými informacemi o ochraně soukromí, sdílení osobních údajů či možných kybernetických hrozbách, které jsou s online prostředím spojeny. Na druhou stranu část respondentů tato rizika nepovažuje za významná nebo si je nemusí plně uvědomovat, což může být ovlivněno jejich osobní zkušeností s používáním sociálních sítí nebo nižší mírou zájmu o problematiku digitální bezpečnosti. Celkově lze říci, že postoje studentů k této otázce nejsou zcela jednotné, avšak převládající názor naznačuje určitou míru uvědomění si možných rizik spojených s využíváním sociálních sítí v online prostředí.

Graf 14: Uvítal/a bys více vzdělávání o bezpečném používání sociálních sítí ve škole?[94]



Z odpovědí studentů vyplývá poměrně výrazný zájem o rozšíření informovanosti v oblasti bezpečného používání sociálních sítí. Největší část respondentů se přiklonila k možnosti „spíše ano“, kterou zvolilo 80 studentů (45 %). Jednoznačný souhlas s potřebou většího vzdělávání vyjádřilo dalších 52 respondentů (29 %). Naopak 34 studentů (19 %) uvedlo odpověď „spíše ne“ a pouze menší skupina, konkrétně 13 respondentů (7 %), uvedla, že by další vzdělávání v této oblasti neuvítala.

[94] Vlastní zpracování

Výsledky naznačují, že většina studentů si uvědomuje význam informací souvisejících s bezpečným chováním v online prostředí a vnímá potřebu prohloubení svých znalostí. Zájem o tuto problematiku může souviset s častým využíváním sociálních sítí v každodenním životě a s postupným uvědomováním si možných rizik, která jsou s jejich používáním spojena. Přesto je patrné, že část respondentů nepovažuje další rozšiřování znalostí za nezbytné, což může souviset s jejich subjektivním pocitem dostatečné informovanosti nebo nižší mírou zájmu o dané téma.

Celkově lze konstatovat, že otázka bezpečného používání sociálních sítí je mezi studenty vnímána jako relevantní a aktuální, přičemž většina z nich projevuje otevřenost k dalším informacím, které by mohly přispět k lepší orientaci v online prostředí a k uvědomělejšímu přístupu k ochraně osobních údajů.

7.2 Doporučení a opatření

Na základě výsledků dotazníkového šetření je možné formulovat několik konkrétních doporučení, která by mohla přispět ke zvýšení bezpečnosti studentů při používání sociální sítě TikTok. Výzkum ukázal, že studenti tuto platformu využívají velmi intenzivně, zároveň však ne vždy věnují dostatečnou pozornost ochraně svých osobních údajů a bezpečnostnímu nastavení účtu.

Za důležité opatření lze považovat především důslednější ochranu uživatelských účtů. Studenti by měli být vedeni k tomu, aby používali silná a unikátní hesla, která nebudou využívána i na jiných platformách. Současně je vhodné podporovat využívání dvoufázového ověření, které představuje účinný způsob, jak snížit riziko neoprávněného přístupu k účtu. Praktickým krokem může být také pravidelná kontrola bezpečnostních nastavení a aktualizace přihlašovacích údajů.

Další doporučení se týká sdílení osobních informací. Přestože většina studentů uvádí, že citlivé údaje na sociálních sítích nezveřejňuje, je vhodné nadále zdůrazňovat, že i zdánlivě běžné informace, jako je například místo pobytu, škola nebo denní režim, mohou být v určitých situacích zneužitelné. Studenti by proto měli být vedeni k větší obezřetnosti při zveřejňování obsahu a k uvědomění si možných důsledků svého online chování.

Výsledky výzkumu také naznačují, že část studentů se již setkala s různými formami rizikového nebo nevhodného jednání v online prostředí. V této souvislosti je vhodné podporovat schopnost rozpoznat potenciálně nebezpečné situace, například podezřelé zprávy, manipulativní komunikaci nebo pokusy o získání osobních údajů. Praktickým opatřením může být například seznamování studentů s typickými znaky podvodného jednání a s možnostmi, jak na takové situace reagovat.

Důležitou roli hraje rovněž informovanost o podmínkách ochrany osobních údajů a fungování samotné platformy. Z výsledků vyplynulo, že jen menší část respondentů se s těmito podmínkami seznamuje důkladně. Proto je vhodné motivovat uživatele k většímu zájmu o to, jakým způsobem jsou jejich data zpracovávána a jaká práva v této oblasti mají. Lepší orientace v těchto otázkách může vést k odpovědnějšímu přístupu k používání sociálních sítí.

V neposlední řadě je vhodné podporovat celkové zvyšování digitální gramotnosti a kritického přístupu k online obsahu. Studenti by měli být vedeni k tomu, aby dokázali vyhodnotit důvěryhodnost informací, které na sociálních sítích sledují, a aby si byli vědomi možných negativních dopadů nadměrného nebo neuváženého využívání těchto platforem.

Celkově lze konstatovat, že bezpečné používání sociálních sítí není pouze otázkou technických opatření, ale také odpovědného přístupu samotných uživatelů. Kombinace praktických bezpečnostních návyků, informovanosti a kritického myšlení může významně přispět k omezení rizik spojených s používáním sociálních sítí v každodenním životě studentů.

Závěr

Cílem této bakalářské práce bylo analyzovat způsoby využívání sociální sítě TikTok mezi studenty střední školy a identifikovat rizika spojená s ochranou osobních údajů a kybernetickou bezpečností. Na základě provedeného dotazníkového šetření lze konstatovat, že stanovené cíle byly naplněny. Výzkum poskytl přehled o frekvenci využívání této platformy, úrovni zabezpečení uživatelských účtů i o tom, jak studenti vnímají možná bezpečnostní rizika spojená s jejím používáním. Získaná data zároveň umožnila formulovat konkrétní doporučení směřující ke zvýšení informovanosti a bezpečného chování mladých uživatelů v online prostředí.

Z výsledků výzkumu vyplynulo, že sociální síť TikTok představuje pro většinu respondentů běžnou součást každodenního života a je využívána velmi intenzivně. Přestože si část studentů uvědomuje možná rizika související se sdílením osobních údajů či zabezpečením účtu, jejich přístup k ochraně soukromí není vždy dostatečně důsledný. Výzkum zároveň ukázal, že určité bezpečnostní nástroje, jako je například dvoufázové ověření nebo používání silných hesel, nejsou využívány všemi uživateli, což může zvyšovat jejich zranitelnost v digitálním prostředí.

Za významné zjištění lze považovat také skutečnost, že většina studentů vnímá TikTok jako potenciálně rizikovou platformu z hlediska kybernetické bezpečnosti, a zároveň projevuje zájem o větší informovanost v této oblasti. To naznačuje potřebu systematického vzdělávání zaměřeného na bezpečné používání sociálních sítí, které by mělo být součástí školního prostředí. Zvýšení povědomí o rizicích a možnostech jejich prevence může přispět k odpovědnějšímu chování mladých lidí v online prostoru a k lepší ochraně jejich osobních údajů.

Přínosem této práce je především zmapování aktuální situace mezi studenty vybrané střední školy a poukázání na oblasti, které vyžadují větší pozornost z hlediska digitální bezpečnosti. Získané poznatky mohou sloužit jako podklad pro další výzkum i pro tvorbu preventivních opatření a vzdělávacích aktivit. V kontextu současného digitálního vývoje je zřejmé, že schopnost bezpečně se pohybovat v online prostředí představuje důležitou součást digitální gramotnosti mladé generace.

Seznam použitých zdrojů

Literární zdroje

1. ANDRESS, J. *The Basics of Information Security.* 3rd ed. Waltham: Syngress, 2019, s. 274. ISBN 978-0-12-812815-7.
2. ARNKIL, Tom Erik. *Dialogical meetings in social networks. Routledge*, 2018, 236 p. ISBN 978-18- 5575-410 2.
3. DOČEKAL, D.; MÜLLER, J.; HARRIS, A.; HEGER, L. *Dítě v síti: manuál pro rodiče a učitele, kteří chtějí rozumět digitálnímu světu mladé generace.* Praha: Mladá fronta, 2019, s. 224. ISBN 978-80-204-5145-3.
4. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 284. ISBN 978-80-247-1561-2.
5. KIZZA, J. M. *Guide to Computer Network Security.* 4th ed. Cham: Springer, 2017, s. 545. ISBN 978-3-319-55605-5.
6. KOHOUT, R.; KARCHŇÁK, R. *Bezpečnost v online prostředí.* Karlovy Vary: Biblio Karlovy Vary, 2016, s. 41. ISBN 978-80-260-9543-9.
7. KOPECKÝ, K.; KREJČÍ, V. *Sociální sítě: úvod do problematiky.* Olomouc: Univerzita Palackého v Olomouci, 2023, s. 118. ISBN 978-80-244-6369-8.
8. KOŽÍŠEK, M.; PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online.* Praha: Grada, 2016, s. 176. ISBN 978-80-247-5595-3.
9. KREJČÍ SALÁTOVÁ, R.; POSPÍŠILOVÁ, M. *Facebooková (ne)závislost: identita, interakce a uživatelská kariéra na Facebooku.* Praha: Karolinum, 2016, s. 246. ISBN 978-80-246-3306-0.
10. LOSEKOOT, M.; VYHNÁNKOVÁ, E. *Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích.* Brno: Jan Melvil Publishing, 2019, s. 224. ISBN 978-80-7555-084-2.
11. MATĚJKA, M. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 176. ISBN 80-7226-419-2.
12. NONNEMANN, F.; ČERVENÝ, V.; VÍTEK, D. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance.* Praha: Wolters Kluwer, 2022, s. 232. ISBN 978-80-7676-515-3.
13. PAVLÍČEK, A.; GALBA, A.; HORA, M. *Moderní informatika.* 2. rozšířené vydání. Praha: Professional Publishing, 2017, s. 192. ISBN 978-80-906594-6-9.

14. PEACOCK, M. *Programujeme vlastní sociální síť v PHP 5.* Brno: Computer Press, 2012, s. 304. ISBN 978-80-251-3626-3.
15. PFLEEGER, C. P.; PFLEEGER, S. L.; MARGULIES, J. *Security in Computing.* 5th ed. Boston: Pearson, 2015, s. 888. ISBN 978-0-13-408504-3.
16. PORADA, V.; RAIS, K. a kol. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: Pocta Vladimíru Smejkalovi.* Brno: Akademické nakladatelství CERM, 2021, s. 246. ISBN 978-80-7623-065-0.
17. SMEJKAL, V. *Internet a § § §.* 2. aktualizované a rozšířené vydání. Praha: Grada, 2001, s. 188. ISBN 80-247-0058-1.
18. STALLINGS, W.; BROWN, L. *Computer Security: Principles and Practice.* 4th ed. Boston: Pearson, 2018, s. 840. ISBN 978-0-13-479410-5.
19. STALLINGS, W. *Effective Cybersecurity: A Guide to Using Best Practices and Standards.* Boston: Addison-Wesley, 2020, s. 320. ISBN 978-0-13-477280-6.
20. SVOBODOVÁ, M.; SCHEU, H.; GRINC, J. *Listina základních práv Evropské unie: deset let v praxi – hodnocení a výhled.* Praha: Auditorium, 2019, s. 192. ISBN 978-80-87284-89-1.
21. ŠTĚDROŇ, B.; LUDVÍK, M. *Právo v informačních technologiích.* Kralice na Hané: Computer Media, 2012, s. 176. ISBN 978-80-86686-36-3.
22. TRÉDEZ, E. *Sociální sítě – a to funguje jak?: všechno, co vás zajímá, když jste online.* Praha: Malé a velké otázky, 2018, s. 192. ISBN 978-80-256-2416-6.
23. VALUCH, J. *Kybernetické hrozby v kontextu mezinárodního práva a mezinárodní bezpečnosti.* Bratislava: Wolters Kluwer, 2019, s. 248. ISBN 978-80-8168-931-2.
24. VEJVODOVÁ, J.; GREGOR, M. *Nejlepší kniha o fake news!!!* Brno: CPress, 2018, s. 192. ISBN 978-80-264-1805-4.
25. WHITMAN, M. E.; MATTORD, H. J. *Principles of Information Security.* 6th ed. Boston: Cengage Learning, 2018, s. 528. ISBN 978-1-337-09812-6.

Elektronické zdroje

1. APTIEN. *What is Data Integrity?* Aptien Knowledge Base [online]. [cit. 11.01.2026]. Dostupné z WWW: https://aptien.com/cs/kb/articles/what-is-data-integrity
2. CYBRELA s.r.o. *Insider threat – definice a význam pojmu* [online]. Praha: Cybrela, [cit. 29.01.2026]. Dostupné z WWW: https://cybrela.com/slovnik/insider-threat/

3. ČESKÁ TELEVIZE. *Pozor na to, co sdílíte. Fotografie z internetu nezmizí* [online]. 2025 [cit. 23.02.2026]. Dostupné z WWW: https://ct24.ceskatelevize.cz/clanek/domaci/pozor-na-to-co-sdilite-fotografie-z-internetu-nezmizi-361169
4. *Digital Footprints and the Dangers of Just Being a Kid.* The Daily Free Press [online]. 2017 [cit. 18.03.2026]. Dostupné z WWW: https://dailyfreepress.com/04/07/17/212066/digital-footprints-and-the-dangers-of-just-being-a-kid-terms-and-conditions/
5. EUROPEAN COMMISSION. *Better Internet for Kids* [online]. Brussels: European Commission, 2022 [cit. 13.02.2026]. Dostupné z WWW: https://better-internet-for-kids.europa.eu
6. EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). *Threat Landscape and Good Practice Guide* [online]. Heraklion: ENISA, 2016 [cit. 19.01.2026]. Dostupné z WWW: https://www.enisa.europa.eu
7. CHEONG, C.; LLOYD, A. *Inside the rise of the top 25 most followed TikTok accounts of 2023.* Insider [online]. 2023 [cit. 15.03.2026]. Dostupné z WWW: https://www.businessinsider.com/top-25-most-followed-tiktok-creators-in-2023-ranked
8. INTERNETEM BEZPEČNĚ. *Krádež identity* [online]. 2024 [cit. 21.02.2026]. Dostupné z WWW: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/kradez-identity/
9. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* [online]. Geneva: International Organization for Standardization, 2022 [cit. 07.01.2026]. Dostupné z WWW: https://www.iso.org/standard/27001
10. KLEMENT, V. *Tak takto to teď vypadá na českém TikToku…* LinkedIn [online]. 2023 [cit. 15.03.2026]. Dostupné z WWW: https://cz.linkedin.com/posts/vklement_tiktok-groupm-groupmnexus-aktivityn7023540897468272640-5Umz
11. KOPECKÝ, K.; KREJČÍ, V. *Sociální sítě: úvod do problematiky* [online]. Olomouc: Univerzita Palackého v Olomouci, 2023 [cit. 10.03.2026]. Dostupné z WWW: https://e-bezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studenty/140-socialni-site-uvod-do-problematiky/file
12. KRYTOLAND. *Nebezpečí sharentingu: Jak sdílení fotek dětí může vést k jejich zneužívání na internetu* [online]. 2024 [cit. 21.02.2026]. Dostupné z WWW:

https://www.krytoland.cz/nebezpeci-sharentingu-jak-sdileni-fotek-deti-muze-vest-k-jejich-zneuzivani-na-internetu

13. KUŽELOVÁ, M. *Má pomoci ochránit děti na internetu. Nyní hrozí, že zákon neprojde Sněmovnou* [online]. 2025 [cit. 23.02.2026]. Dostupné z WWW: https://www.novinky.cz/clanek/domaci-ma-pomoci-ochranit-deti-na-internetu-nyni-hrozi-ze-zakon-neprojde-snemovnou-40527198
14. MAGDOŇOVÁ, J. „Všichni věděli, že je mi dvanáct.“ Děti ohrožuje na internetu sexting, intimní snímky se objeví i po letech [online]. iROZHLAS, 25. 5. 2022 [cit. 21.02.2026]. Dostupné z WWW: https://www.irozhlas.cz/zivotni-styl/spolecnost/sexting-internet-kybersikana-kyberbezpecnost-bezpecnost-internet_2205250700_bko
15. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY. *Zásady zpracování osobních údajů* [online]. Praha: Ministerstvo vnitra ČR, 2024 [cit. 19.02.2026]. Dostupné z WWW: https://mv.gov.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx
16. MINISTERSTVO ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. *Bezpečnostní strategie České republiky 2023* [online]. [cit. 04.01.2026]. Dostupné z WWW: https://mzv.gov.cz/file/5101086/Bezpecnostni_strategie_2023.pdf
17. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Kybernetická bezpečnost: hrozby a rizika* [online]. Brno: NÚKIB, 2023 [cit. 18.01.2026]. Dostupné z WWW: https://www.nukib.cz
18. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha: NÚKIB, datum publikování neuveden [cit. 09.01.2026]. Dostupné z WWW: https://nukib.gov.cz
19. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Vzdělávání* [online]. [cit. 02.01.2026]. Dostupné z WWW: https://nukib.gov.cz/cs/kyberneticka-bezpecnost/vzdelavani/
20. NETSAFE. *Digital footprints* [online]. Netsafe, 2025 [cit. 18.03.2026]. Dostupné z WWW: https://netsafe.org.nz/children-and-young-people/digital-footprint
21. O2 CZECH REPUBLIC a.s. *CIA triáda: důvěrnost, integrita a dostupnost* O2 CyberNews [online]. Praha: O2 Czech Republic a.s., datum publikování neuveden [cit. 12.01.2026]. Dostupné z WWW: https://o2cybernews.cz/slovnik/cia-triada

22. POLICIE ČESKÉ REPUBLIKY. *Nebudujte svému dítěti digitální stopu* [online]. 2025 [cit. 23.02.2026]. Dostupné z WWW: https://policie.gov.cz/clanek/akce-a-projekty-nebudujte-svemu-diteti-digitalni-stopu.aspx
23. SOCIALNISITE.ESTRANKY.CZ. *Historie sociálních sítí* [online]. [cit. 20.02.2026]. Dostupné z WWW: https://socialnisite.estranky.cz/clanky/historie-socialnich-siti.html
24. ŠÍPOŠOVÁ, V. *Seriál specifické aspekty ochrany osobních údajů 4/5: Děti, internet a právo na ochranu osobních údajů* [online]. 2020 [cit. 23.02.2026]. Dostupné z WWW: https://www.epravo.cz/top/clanky/serial-specificke-aspekty-ochrany-osobnich-udaju-45-deti-internet-a-pravo-na-ochranu-osobnich-udaju-111248.html
25. ŠNAJDROVÁ, T. *10 nejsledovanějších českých tiktokerů a tiktokerek v roce 2022* Refresher [online]. 2022 [cit. 15.03.2026]. Dostupné z WWW: https://refresher.cz/118023-10-nejsledovanejsich-ceskych-tiktokeru-a-tiktokerek-v-roce-2022
26. *TikTok roste nejen u generace Z, zapojuje se i více značek* Mediaguru.cz [online]. 2023 [cit. 15.03.2026]. Dostupné z WWW: https://www.mediaguru.cz/clanky/2023/11/tiktok-roste-nejen-u-generace-z-zapojuje-se-i-vice-znacek/
27. *TikTok se v Česku blíží k 2,5 milionům, chystá další cílení* Mediaguru.cz [online]. 2023 [cit. 15.03.2026]. Dostupné z WWW: https://www.mediaguru.cz/clanky/2023/03/tiktok-se-v-cesku-blizi-k-25-milionum-chysta-dalsi-cileni/
28. *TikTok zpoplatní část obsahu* Mediaguru.cz [online]. 2023 [cit. 15.03.2026]. Dostupné z WWW: https://www.mediaguru.cz/clanky/2023/03/tiktok-zpoplatni-cast-obsahu/
29. TIKTOK. *#2023* [online]. 2023 [cit. 16.03.2026]. Dostupné z WWW: https://www.tiktok.com/tag/2023?lang=cs-CZ
30. TIKTOK. *Privacy Policy (EEA)* [online]. 2025 [cit. 17.03.2026]. Dostupné z WWW: https://www.tiktok.com/legal/page/eea/privacy-policy/cs
31. TIKTOK. *TERMIN.IN.UA* [online]. [cit. 05.03.2026]. Dostupné z WWW: https://termin.in.ua/tiktok/#Novi_instrumenti_v_TikTok

32. ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. *Základní příručka k ochraně údajů* [online]. Praha: ÚOOÚ [cit. 20.02.2026]. Dostupné z WWW: https://uoou.gov.cz/verejnost/zakladni-prirucka-k-ochrane-udaj
33. USINESSINFO.CZ. *Ochrana osobních údajů – zpracování osobních údajů* [online]. Praha: CzechTrade, 2024 [cit. 17.02.2026]. Dostupné z WWW: https://www.businessinfo.cz/navody/ochrana-osobnich-udaju-ppbi/4/
34. VANĚK, J. *Co je to únik dat (Data Breach) a jak se mu bránit* [online]. 2024 [cit. 22.02.2026]. Dostupné z WWW: https://blog.jirivanek.eu/cs/co-je-to-unik-dat-data-breach-a-jak-se-mu-branit/

Legislativní dokumenty

1. ČESKO. *Zákon č. 110/2019 Sb., o zpracování osobních údajů.* In: *Sbírka zákonů České republiky.* 2019, částka 47, s. 1110–1132.
2. ČESKO. *Zákon č. 264/2025 Sb., o kybernetické bezpečnosti.* In: *Sbírka zákonů České republiky.* 2025.

Seznam zkratek

- Sb. - Sbírka zákonů
- ICT - Informační a komunikační technologie
- DoS - Denial of Service
- DDoS - Distributed Denial of Service
- GDPR - General Data Protection Regulation
- iOS - iPhone Operating System
- X - dříve Twitter

Seznam obrázků

Seznam grafů

Seznam příloh

Příloha č. 1 Dotazník

Dobrý den, jsem studentkou Vysoké školy evropských a regionálních studií v Českých Budějovicích. Jmenuji se Julija Didenko a ráda bych Vás požádala o vyplnění dotazníku, který je součástí mé bakalářské práce. Tato práce se zaměřuje na problematiku využívání sociální sítě TikTok a na bezpečnostní rizika spojená s jejím používáním. Cílem dotazníku je zjistit, jak často a jakým způsobem respondenti tuto sociální síť využívají, jaké mají povědomí o možných bezpečnostních hrozbách a jak přistupují k ochraně svého soukromí a osobních údajů v online prostředí.
Vaše odpovědi jsou zcela anonymní a budou použity pouze pro účely této bakalářské práce. Dotazník je dobrovolný a jeho vyplnění Vám zabere jen několik minut. Děkuji za váš čas a ochotu.

1.Jaké je tvé pohlaví?

- Žena
- Muž
- Nechci uvádět

2.Jaký je tvůj věk?

- 15-16
- 17-18
- 18 a více

3.Jaký je tvůj ročník?

- 1. ročník
- 2. ročník
- 3. ročník
- 4. ročník

4.Používáš sociální síť TikTok?

- Ano
- Ne

5.Jak často TikTok používáš?

- Několikrát denně
- Jednou denně
- Několikrát týdně
- Méně často

6. Jaké máš nastavení účtu?

- Veřejný
- Soukromý

7.Používáš na TikToku silné heslo (kombinace písmen, číslic a znaků)?

- Ano
- Spíše ano
- Spíše ne
- Ne

8.Máš aktivované dvoufázové ověření účtu?

- Ano
- Ne

9.Setkal/a ses na TikToku s bezpečnostní hrozbou?

- Ano
- Ne

10.Uvědomuješ si, že TikTok shromažďuje a zpracovává osobní údaje uživatelů?

- Spíše ano
- Spíše ne
- Ne

11.Četl/a jsi někdy podmínky ochrany osobních údajů (privacy policy) TikToku?

- Ano
- Ne
- Pouze částečně

12.Sdílíš na TikToku osobní informace o sobě (škola, bydliště, denní režim)?

- Ano
- Ne

13.Považuješ TikTok za rizikovou platformu z hlediska kybernetické bezpečnosti?

- Ano
- Ne

14.Uvítal/a bys více vzdělávání o bezpečném používání sociálních sítí ve škole?

- Ano
- Spíše ano
- Spíše ne
- Ne