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

BAKALÁŘSKÁ PRÁCE

POSTUP POLICIE ČESKÉ REPUBLIKY PŘI PROVĚŘOVÁNÍ OZNÁMENÍ O PODVODNÝCH E-SHOPECH

Autor práce: Daniel Šafránek, 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: Daniel Šafránek

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

Název bakalářské práce: Postup Policie České republiky při prověřování oznámení o podvodných e-shopech

Název bakalářské práce v anglickém jazyce: Procedure of the Police of the Czech Republic in Investigating Reports of Fraudulent E-shops

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): prosinec 2025

Cíl bakalářské práce:

Hlavním cílem práce je posoudit postup Policie České republiky při prověřování oznámení týkajících se podvodných e-shopů, a to se zaměřením na jednotlivé fáze policejního procesu od přijetí oznámení až po případné zahájení trestního řízení a vedení prověřování.

Vedlejším cílem práce je zhodnotit úroveň povědomí uživatelů internetu o bezpečném chování při nákupu na e-shopech, identifikovat rizikové faktory, které jsou veřejností často přehlíženy, a navrhnout opatření směřující k minimalizaci těchto rizik.

Student: Daniel Šafránek, DiS.	31.12.2025 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	5.1.2026 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	27.1.2026 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	27.1.2026 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	1.2.2026 *datum*	*podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval 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 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 a JUDr. Mgr. Milanu Kocíkovi Ph.D., MBA, LL.M. za připomínky a metodické vedení práce.

ABSTRAKT

ŠAFRÁNEK, D. Postup Police České republiky při prověřování o podvodných e-shopech. České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 76 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: kybernetická kriminalita, podvodné e-shopy, policejní orgán, trestní řízení, prevence

Bakalářská práce se zabývá problematikou podvodných e-shopů jako formy kybernetické kriminality a postupem policejního orgánu při prověřování oznámení této trestné činnosti. Cílem práce je popsat procesní postup od přijetí trestního oznámení až po rozhodnutí v rámci prověřování a poukázat na specifika těchto případů v online prostředí.

Práce vymezuje základní pojmy, charakterizuje formy kybernetické kriminality a přibližuje mechanismy fungování podvodných e-shopů. Dále se zaměřuje na jednotlivé úkony policejního orgánu při prověřování, včetně zajišťování důkazů a práce s poškozenými. Součástí je také analýza vybraných případů a zdůraznění významu prevence v oblasti bezpečného chování na internetu.

ABSTRACT

ŠAFRÁNEK, D. Procedure of the Police of the Czech Republic in Investigating Reports of Fraudulent E-shops. České Budějovice: The College European and Regiolan Studies, 2026. 76 pgs. Supervisor: RNDr. Růžena Ferebauerová

Keywords: cybercrime, fraudulent e-shops, Police of the Czech Republic, criminal proceedings, prevention

This bachelor's thesis addresses the issue of fraudulent e-shops as a form of cybercrime and the procedures of the Police of the Czech Republic when investigating reports of such criminal activity. The aim of the thesis is to describe the procedural steps from the receipt of a criminal complaint to the final decision within the investigation phase, while highlighting the specifics of these cases in the online environment.

The work defines fundamental concepts, characterizes various forms of cybercrime, and explains the operational mechanisms of fraudulent e-shops. Furthermore, it focuses on the individual actions taken by the Police of the Czech Republic during the investigation, including the securing of evidence and communication with victims. The thesis also includes an analysis of selected cases and emphasizes the importance of prevention in the context of safe online behavior.

Obsah

Úvod

Dynamický rozvoj informačních a komunikačních technologií v posledních dvou desetiletích zásadně proměnil podobu moderní společnosti. Internet přestal být pouhým zdrojem informací a stal se integrální součástí každodenního života, ovlivňující způsob, jakým komunikujeme, pracujeme a v neposlední řadě i jak nakupujeme. Rozmach e-commerce sektoru, který byl ještě více urychlen globální pandemií onemocnění COVID-19, přinesl spotřebitelům nesporné výhody v podobě pohodlí, širokého výběru a možnosti snadného srovnání cen. Souběžně s tímto pozitivním trendem se však do kybernetického prostoru přesunula i značná část kriminálních aktivit. Tradiční formy majetkové trestné činnosti jsou stále častěji nahrazovány sofistikovanými metodami v online prostředí, mezi nimiž zaujímají přední místo podvodné e-shopy.

Problematika podvodných e-shopů představuje pro současné orgány vynucující právo jednu z největších výzev. Pachatelé v tomto prostředí využívají anonymity internetu, nízkých nákladů na vytvoření vizuálně přesvědčivých stránek a často i přeshraničního charakteru sítě, což značně komplikuje jejich odhalování a následné usvědčování. Pro Policii České republiky to znamená nutnost neustálé adaptace procesních postupů, technického vybavení i odborných znalostí policistů. Efektivita postupu policie při prověřování oznámení o těchto podvodech je klíčová nejen pro ochranu majetku občanů, ale také pro zachování důvěry veřejnosti v právní systém. Bakalářská práce se zaměřuje na analýzu činnosti Policie České republiky v souvislosti s fenoménem podvodného prodeje zboží a služeb na internetu.

Hlavním tématem je procesní cesta, kterou musí každé podané oznámení urazit. Od momentu, kdy se poškozený dostaví na služebnu nebo podá elektronické oznámení, přes fázi vytěžování informací a zajišťování digitálních stop, až po rozhodnutí o zahájení úkonů trestního řízení podle trestního řádu.

Kromě represivní složky, tedy postupu policie, je však nezbytné nahlížet na problematiku i z pohledu prevence. Kriminalita v prostředí e-shopů totiž velmi často těží z nízké úrovně digitální gramotnosti a určité míry naivity nebo nepozornosti uživatelů. Ačkoliv jsou bezpečnostní varování a osvětové kampaně v médiích relativně časté, počet obětí podvodů neklesá, ba naopak. To naznačuje, že existuje propast mezi dostupnými informacemi o bezpečném nákupu a jejich reálnou aplikací v praxi. Proto se tato práce věnuje také analýze chování spotřebitelů a identifikaci rizikových faktorů, které vedou k úspěšnému dokončení podvodu ze strany pachatele.

Z hlediska metodologie bude práce vycházet z kombinace teoretických a praktických přístupů. V teoretické části bude provedena rešerše odborné literatury a relevantních právních předpisů, se kterými Policie České republiky při šetření těchto činů pracuje. Praktická část bude opřena o analýzu dostupných statistických dat o kybernetické kriminalitě a o kvantitativní šetření zaměřené na spotřebitelské chování. V neposlední řadě budou využity poznatky z kazuistik, které ilustrují typické postupy a obtíže v policejní praxi. Struktura práce je rozdělena do několika logických celků. První kapitoly definují základní pojmy. Následující část je věnována samotnému procesnímu postupu Policie České republiky. Závěrečné kapitoly se zaměřují na prevenci, vyhodnocení provedeného šetření a návrhy opatření pro minimalizaci rizik spojených s nákupy v podvodných e-shopech.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce je posoudit postup Policie České republiky při prověřování oznámení týkajících se podvodných e-shopů se zaměřením na jednotlivé fáze policejního postupu od přijetí trestního oznámení až po případné zahájení trestního stíhání a vedení prověřování podle příslušných ustanovení trestního řádu. Práce současně analyzuje specifika podvodných e-shopů jako jedné z forem kybernetické kriminality, charakterizuje jejich typické znaky a identifikuje problémy, se kterými se policejní orgány při jejich odhalování a dokazování setkávají. Vedlejším cílem práce je zhodnotit úroveň informovanosti uživatelů internetu o zásadách bezpečného nakupování prostřednictvím e-shopů, identifikovat nejčastější rizikové faktory vedoucí ke vzniku internetových podvodů a navrhnout preventivní opatření směřující ke snížení pravděpodobnosti jejich výskytu.

Pro naplnění stanovených cílů jsou v práci využity teoretické i empirické metody vědeckého poznání. V teoretické části je aplikována metoda analýzy odborné literatury, právních předpisů a dalších relevantních dokumentů zaměřených na problematiku kybernetické kriminality, podvodných e-shopů a postupu Policie České republiky při prověřování trestných činů. Praktická část práce vychází z dotazníkového šetření zaměřeného na zkušenosti a povědomí uživatelů internetu o bezpečném nakupování v online prostředí. Získaná data jsou statisticky vyhodnocena a doplněna o kazuistiky konkrétních případů internetových podvodů, jejichž prostřednictvím jsou analyzovány nejčastější způsoby páchání této trestné činnosti a postup policejních orgánů při jejím objasňování.

2 Vymezení základních pojmů

Pro snazší proniknutí do problematiky kybernetické kriminality je nejprve potřeba vymezit některé ze základních pojmů, které se k této oblasti trestné činnosti pojí. Jedná se o pojmy, jejichž pochopení a vymezení je ve vztahu k předmětu následujícího textu nezbytné. Zároveň se však nejedná o vyčerpávající výčet všech pojmů, jejichž definice lze nalézt například ve Výkladovém slovníku kybernetické bezpečnosti vydaném pod záštitou Národního bezpečnostního úřadu a Národního centra kybernetické bezpečnosti. Tento slovník je k dispozici jak v tištěné, tak v elektronické verzi.[1]

Vzhledem k širokému rozsahu a dynamickému vývoji informačních technologií text selektivně definuje ty fenomény, které mají přímý vztah k podvodnému jednání v prostředí e-shopů a k následnému procesnímu postupu Policie České republiky.[2]

2.1 Kybernetická trestná činnost (Cybercrime)

. Rozvoj informačních a komunikačních technologií významně ovlivnil fungování moderní společnosti a přinesl nové možnosti komunikace, sdílení informací i obchodování. Současně však vytvořil prostor pro vznik nových forem trestné činnosti, které využívají informační systémy, počítačové sítě a digitální technologie k páchání protiprávního jednání.

V odborné literatuře se lze setkat s různými označeními tohoto fenoménu, například informační kriminalita, elektronická kriminalita, počítačová kriminalita nebo kyberkriminalita. Přestože jsou tyto pojmy často používány jako synonyma, v současnosti je nejrozšířenějším označením pojem kybernetická kriminalita (cybercrime), který lépe vystihuje široké spektrum trestné činnosti páchané prostřednictvím informačních a komunikačních technologií nebo namířené proti nim.

Kybernetickou kriminalitou lze rozumět protiprávní jednání, při němž jsou informační a komunikační technologie využívány jako prostředek ke spáchání trestného činu, případně představují jeho cíl. Do této kategorie patří například neoprávněné přístupy

[1] JIRÁSEK, Petr. Cyber security glossary. Páté doplněné a upravené vydání. Centrum kybernetické bezpečnosti, z. ú., 2022. 352 s. ISBN 978-80-908388-4-0.
[2] Vlastní text

k počítačovým systémům, šíření škodlivého softwaru, phishingové útoky, internetové podvody nebo provozování podvodných e-shopů. [3]

S rostoucí digitalizací společnosti dochází k neustálému rozšiřování forem kybernetické kriminality a zvyšování její společenské nebezpečnosti. Pachatelé využívají anonymity internetového prostředí, přeshraniční povahy kyberprostoru a technické vyspělosti moderních komunikačních prostředků, což významně komplikuje jejich odhalování a dokazování. Právě podvodné e-shopy představují jednu z nejčastějších forem majetkové kriminality páchané v kyberprostoru, se kterou se orgány činné v trestním řízení v současnosti setkávají. [4]

2.2 Podvodný e-shop

Podvodný e-shop představuje specifickou formu kybernetické kriminality, při níž pachatel prostřednictvím internetového obchodu uvádí spotřebitele v omyl s cílem získat neoprávněný majetkový prospěch. Charakteristickým znakem podvodného e-shopu je skutečnost, že provozovatel nemá úmysl dodat nabízené zboží nebo službu, případně využívá internetový obchod k získání osobních nebo platebních údajů zákazníků.

Podvodné e-shopy bývají často vytvářeny tak, aby působily důvěryhodně a svým vzhledem připomínaly legitimní internetové obchody. Pachatelé využívají profesionálně zpracované webové stránky, kopírují obsah existujících e-shopů, uvádějí fiktivní kontaktní údaje nebo zneužívají identitu skutečných podnikatelských subjektů. Mezi typické znaky podvodných e-shopů patří výrazně nižší ceny oproti běžné tržní hodnotě zboží, požadavek platby předem, omezené kontaktní údaje, absence obchodních podmínek nebo nemožnost osobního odběru.

V současné době představují podvodné e-shopy jednu z nejčastějších forem internetových podvodů. Jejich odhalování je komplikováno anonymitou internetového prostředí, využíváním zahraničních serverů, krátkou dobou existence internetových stránek a častým přeshraničním prvkem trestné činnosti. Z pohledu trestního práva bývá

[3] KOLOUCH, Jan. Cybercrime [online]. CZ.NIC, z. s. p. o., 2016. Str. 31-32. ISBN 978-80-88168-16-4.
[4] ŠTĚDROŇ, B.; JAŠEK, R.; SVÍTEK, M. a kol. Umělá inteligence a právo. Plzeň: Aleš Čeněk, 2024. str. 54. ISBN 978-80-7380-947-8.

jednání provozovatelů podvodných e-shopů zpravidla kvalifikováno jako trestný čin podvodu podle § 209 zákona č. 40/2009 Sb., trestního zákoníku.[5]

Problematika podvodných e-shopů představuje významnou oblast zájmu Policie České republiky, neboť jejich provozování zpravidla naplňuje znaky majetkové trestné činnosti a vyžaduje specifické postupy při zajišťování digitálních stop a identifikaci pachatelů.[6]

2.3 Kybernetický prostor

Dle § 2 zákona o kybernetické bezpečnosti se kybernetickým prostorem rozumí „digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací“. Kybernetický prostor je tedy možné chápat jako prostředí zahrnující veškeré informační a komunikační technologie, jejichž prostřednictvím dochází k přenosu, ukládání a zpracování digitálních dat.

V současné době představuje kybernetický prostor nedílnou součást každodenního života, neboť umožňuje elektronickou komunikaci, poskytování online služeb i realizaci elektronického obchodování. Současně však vytváří prostor pro páchání různých forem kybernetické kriminality, mezi které patří například internetové podvody, phishingové útoky nebo provozování podvodných e-shopů. Právě podvodné e-shopy představují jednu z nejčastějších forem majetkové trestné činnosti páchané v kybernetickém prostoru. [7]

2.4 Poškozený

Poškozeným se dle § 43 zákona č. 141/1961 Sb., o trestním řízení soudním, rozumí osoba, které bylo trestným činem ublíženo na zdraví, způsobena majetková, nemajetková či jiná újma nebo na jejíž úkor se pachatel trestným činem obohatil.[8]

[5] KOLOUCH, Jan. CyberCrime. Brno: CZ.NIC, 2016. ISBN 978-80-88168-16-4.
[6] Vlastní text
[7] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Aleš Čeněk, 2019. str. 75. ISBN 978-80-7380-765-8.
[8] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů

Poškozený je jedním ze základních subjektů trestního řízení a jeho postavení je upraveno trestním řádem. V průběhu trestního řízení má poškozený řadu procesních práv, mezi která patří zejména právo podat trestní oznámení, navrhovat doplnění dokazování, nahlížet do spisu v rozsahu stanoveném zákonem nebo uplatnit nárok na náhradu škody či nemajetkové újmy způsobené trestným činem.

V souvislosti s podvodnými e-shopy je poškozeným zpravidla zákazník, který v důsledku podvodného jednání uhradil finanční prostředky za objednané zboží nebo službu, avšak sjednané plnění mu nebylo poskytnuto nebo bylo poskytnuto v rozporu s uzavřenou smlouvou. Právě poškozený je ve většině případů osobou, která podává trestní oznámení a poskytuje policejnímu orgánu informace a důkazní prostředky nezbytné pro prověřování oznámení.

2.5 Policejní orgán

Pojem policejní orgán je vymezen v § 12 zákona č. 141/1961 Sb., o trestním řízení soudním. Trestní řád řadí policejní orgán mezi orgány činné v trestním řízení, vedle soudu a státního zástupce. Policejním orgánem se rozumí útvary Policie České republiky, které jsou oprávněny provádět úkony trestního řízení v rozsahu stanoveném trestním řádem, případně další orgány.[9]

Postavení Policie České republiky upravuje zákon č. 273/2008 Sb., o Policii České republiky. Podle § 1 je Policie České republiky jednotným ozbrojeným bezpečnostním sborem. Podle § 2 tohoto zákona policie slouží veřejnosti a jejím základním úkolem je chránit bezpečnost osob a majetku, veřejný pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a vykonávat další úkoly svěřené jí právními předpisy.[10]

V trestním řízení plní policejní orgán nezastupitelnou úlohu zejména při přijímání trestních oznámení, prověřování skutečností nasvědčujících spáchání trestného činu, zajišťování důkazních prostředků a provádění dalších procesních úkonů podle trestního řádu. V případě oznámení týkajících se podvodných e-shopů policejní orgán zabezpečuje prvotní úkony trestního řízení, vyhodnocuje získané poznatky

[9] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
[10] ČESKO. Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů

a opatřuje důkazy potřebné pro posouzení, zda jsou splněny podmínky pro zahájení trestního řízení.

2.6 Trestní oznámení

Trestní oznámení představuje podání, kterým fyzická nebo právnická osoba upozorňuje orgány činné v trestním řízení na skutečnosti nasvědčující tomu, že byl spáchán trestný čin. Trestní oznámení může podat kdokoliv, kdo se o možném spáchání trestného činu dozví, a to bez ohledu na to, zda je sám poškozeným. Oznámení lze učinit písemně, ústně do protokolu, elektronicky nebo prostřednictvím datové schránky.

Po přijetí trestního oznámení je policejní orgán povinen posoudit uvedené skutečnosti a provést nezbytná opatření ke zjištění, zda jsou dány důvody pro zahájení úkonů trestního řízení. V případech podvodných e-shopů bývá trestní oznámení zpravidla podáváno poškozenými osobami, které uhradily finanční prostředky za objednané zboží, jež jim nebylo dodáno, případně zjistily, že se staly obětí internetového podvodu.[11]

2.7 Prověřování

Prověřování představuje první fázi přípravného řízení, která následuje po přijetí trestního oznámení nebo po zjištění skutečností nasvědčujících tomu, že byl spáchán trestný čin. Jeho účelem je ověřit důvodnost podezření ze spáchání trestného činu, zjistit základní skutkové okolnosti případu, opatřit potřebné podklady a rozhodnout o dalším procesním postupu.

V rámci prověřování policejní orgán vyhledává a zajišťuje důkazy, provádí potřebná šetření, vyslýchá osoby důležité pro trestní řízení a činí další úkony směřující k objasnění věci. Výsledkem prověřování může být zejména zahájení trestního stíhání konkrétní osoby, odložení věci nebo její odevzdání příslušnému orgánu. V případech podvodných e-shopů je součástí prověřování zejména zajišťování digitálních stop,

[11] JELÍNEK, Jiří a kol. Trestní právo procesní. 7. aktualizované a doplněné vydání. Praha: Leges, 2023. ISBN 978-80-7502-687-3

vyhodnocování elektronické komunikace, prověřování finančních toků a identifikace osob podílejících se na podvodném jednání.[12]

2.8 Elektronický důkaz

Elektronický důkaz představuje informaci nebo soubor informací uložených, zpracovávaných nebo přenášených v digitální podobě, které mohou sloužit jako důkazní prostředek v trestním řízení. Může se jednat například o e-mailovou komunikaci, údaje o bankovních transakcích, IP adresy, obsah webových stránek, data uložená v počítačových systémech nebo informace získané z mobilních zařízení.

V případě prověřování podvodných e-shopů mají elektronické důkazy zásadní význam pro identifikaci pachatele a prokazování jednotlivých skutkových okolností případu. Jejich zajištění a následné vyhodnocení představuje jednu z nejdůležitějších součástí činnosti policejního orgánu při odhalování kybernetické kriminality.[13]

[12] ŠÁMAL, Pavel a kol. Trestní řád. Komentář. II. díl. 8. vydání. Praha: C. H. Beck, 2025. ISBN 978-80-7400-998-3.
[13] KOLOUCH, Jan. CyberCrime. Brno: CZ.NIC, 2016. ISBN 978-80-88168-16-4.

3 Formy a projevy kybernetické kriminality

Kybernetická kriminalita představuje souhrn protiprávních jednání páchaných prostřednictvím informačních a komunikačních technologií nebo zaměřených proti informačním systémům a jejich uživatelům. S rozvojem digitálních technologií dochází k neustálému rozšiřování forem této trestné činnosti, přičemž pachatelé využívají stále sofistikovanější metody k dosažení svých cílů.

Významnou část kybernetické kriminality tvoří majetková trestná činnost, jejímž cílem je získání neoprávněného finančního prospěchu. Do této kategorie patří zejména podvody realizované prostřednictvím internetu, phishingové útoky, zneužívání elektronických platebních prostředků a provozování podvodných e-shopů.[14]

[14] DRAŠTÍK, Antonín a kol. Trestní zákoník. Komentář. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-790-4.

4 Poznání podvodného jednání

Rozpoznání podvodného jednání v prostředí elektronického obchodování představuje jeden ze základních předpokladů ochrany spotřebitelů před internetovými podvody. Podvodné e-shopy a falešné internetové nabídky často vykazují určité charakteristické znaky, jejichž identifikace může významně snížit riziko vzniku majetkové škody.

Jedním ze základních kroků při ověřování důvěryhodnosti internetového obchodníka je prověření dostupných informací o provozovateli. Doporučuje se ověřit obchodní jméno společnosti, kontaktní údaje, internetovou adresu a případné zkušenosti ostatních uživatelů. Důležitým zdrojem informací mohou být veřejné rejstříky, recenze zákazníků nebo databáze podnikatelských subjektů.

Významným indikátorem důvěryhodnosti je rovněž kvalita a úroveň zpracování internetových stránek. Podezření mohou vyvolávat zejména neúplné kontaktní údaje, absence identifikačních údajů podnikatele, jazykové chyby, nefunkční odkazy nebo využívání anonymních e-mailových adres. Zvýšenou pozornost je vhodné věnovat také internetovým stránkám registrovaným na neobvyklých zahraničních doménách, které mohou napodobovat vzhled legitimních obchodníků.

Za významný rizikový faktor je považován požadavek na platbu předem bez možnosti využití bezpečnějších platebních metod. Podvodné e-shopy často vyžadují úhradu celé kupní ceny před odesláním zboží, přičemž následně přestanou se zákazníkem komunikovat nebo objednané zboží vůbec nedodají. Zvýšená opatrnost je na místě zejména v případech, kdy jsou finanční prostředky požadovány na účet soukromé osoby nebo prostřednictvím obtížně dohledatelných platebních systémů.

Dalším typickým znakem podvodného jednání bývá nabídka zboží za cenu výrazně nižší, než je jeho obvyklá tržní hodnota. Pachatelé tímto způsobem vytvářejí dojem mimořádně výhodné nabídky a motivují potenciální zákazníky k rychlému rozhodnutí bez důkladného ověření důvěryhodnosti obchodníka.

Při využívání internetových služeb je rovněž nezbytné chránit osobní a platební údaje. Uživatelé by měli poskytovat pouze informace nezbytné pro realizaci nákupu

a vyvarovat se sdělování citlivých údajů prostřednictvím nedůvěryhodných internetových stránek nebo elektronické pošty. Zvýšenou obezřetnost je nutné zachovávat také vůči nevyžádaným obchodním sdělením a e-mailům obsahujícím odkazy na neznámé internetové stránky.

Identifikace uvedených znaků sice nezaručuje odhalení všech podvodných jednání, může však významně přispět ke snížení rizika, že se uživatel internetu stane obětí podvodu. Z pohledu prevence představuje informovanost a obezřetnost uživatelů jeden z nejúčinnějších nástrojů ochrany před podvodnými e-shopy.[15]

[15] Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech. Praha: Policejní akademie České republiky v Praze a kolektiv autorů, 2020. str. 149. ISBN 978-80-7251-505-9.

5 Pachatelé kybernetické kriminality

Pachateli kybernetické kriminality mohou být jednotlivci, organizované zločinecké skupiny, zaměstnanci organizací, teroristické skupiny i státní aktéři. Jednotlivé skupiny pachatelů se odlišují především motivací, použitými prostředky a cíli, kterých chtějí svou činností dosáhnout. Mezi nejčastější motivy patří finanční prospěch, získání citlivých informací, narušení činnosti informačních systémů, průmyslová špionáž nebo prosazování politických či ideologických zájmů.[16]

Významnou skupinu pachatelů představují organizované zločinecké skupiny. Ty využívají informační a komunikační technologie zejména k páchání majetkové trestné činnosti, praní výnosů z trestné činnosti, podvodům v elektronickém obchodování nebo neoprávněným finančním transakcím. Jejich činnost má často mezinárodní charakter, což významně komplikuje identifikaci pachatelů a následné trestní řízení.[17]

Další skupinu tvoří tzv. vnitřní pachatelé, tedy osoby disponující oprávněným přístupem k informačním systémům organizace. Nejčastěji se jedná o současné nebo bývalé zaměstnance, kteří mohou zneužít svá oprávnění k neoprávněnému přístupu k datům, jejich změně, odcizení nebo zveřejnění. Vzhledem k jejich znalosti interních procesů a bezpečnostních opatření bývá odhalování této formy kriminality zpravidla složitější.[18]

V souvislosti s podvodnými e-shopy, které jsou předmětem této bakalářské práce, jsou nejčastějšími pachateli jednotlivci nebo organizované skupiny motivované získáním neoprávněného majetkového prospěchu. Pachatelé využívají dostupných technologií k vytvoření věrohodně působících internetových obchodů, jejichž prostřednictvím uvádějí zákazníky v omyl a získávají od nich finanční prostředky bez úmyslu dodat objednané zboží nebo službu. Charakteristickým rysem těchto případů je anonymita internetového prostředí, přeshraniční působení pachatelů a obtížné zajišťování elektronických důkazů, což klade vysoké nároky na postup policejních orgánů při prověřování oznámení.

[16] KOLOUCH, Jan. CyberCrime. Brno: CZ.NIC, 2016. ISBN 978-80-88168-16-4.
[17] JELÍNEK, Jiří a kol. Trestní právo hmotné: obecná část, zvláštní část. 9. aktualizované vydání. Praha: Leges, 2025. ISBN 978-80-7502-799-3.
[18] KOLOUCH, Jan. CyberCrime. Brno: CZ.NIC, 2016. ISBN 978-80-88168-16-4.

6 Trestný čin podvodu

Trestný čin podvodu je upraven v § 209 zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších předpisů. Je systematicky zařazen do hlavy V zvláštní části trestního zákoníku mezi trestné činy proti majetku. Jeho účelem je ochrana majetkových práv fyzických a právnických osob před podvodným jednáním pachatele.

Dle § 209 odst. 1 trestního zákoníku se trestného činu podvodu dopustí ten, kdo sebe nebo jiného obohatí tím, že uvede jiného v omyl, využije jeho omylu nebo zamlčí podstatné skutečnosti a tím způsobí na cizím majetku škodu nikoli nepatrnou.

Podstata trestného činu podvodu spočívá v tom, že pachatel úmyslným jednáním vyvolá u poškozeného nesprávnou představu o skutečném stavu věci nebo využije již existujícího omylu. V důsledku tohoto omylu poškozený provede majetkovou dispozici, jejímž následkem vznikne škoda na jeho majetku a současně dojde k neoprávněnému obohacení pachatele nebo jiné osoby. Mezi podvodným jednáním pachatele, vznikem omylu, majetkovou dispozicí a vzniklou škodou musí existovat příčinná souvislost.

Objektem trestného činu podvodu je ochrana cizího majetku a majetkových práv. Objektivní stránku tvoří jednání pachatele spočívající v uvedení jiného v omyl, využití jeho omylu nebo zamlčení podstatných skutečností. Následkem tohoto jednání musí být vznik škody na cizím majetku alespoň ve výši škody nikoli nepatrné a současně neoprávněné obohacení pachatele nebo jiné osoby. Subjektem trestného činu může být každá trestně odpovědná fyzická osoba a subjektivní stránka vyžaduje úmyslné zavinění, neboť pachatel musí jednat s vědomím, že svým jednáním uvádí jinou osobu v omyl nebo jejího omylu využívá za účelem získání majetkového prospěchu.

Trestní zákoník rozlišuje základní a kvalifikované skutkové podstaty trestného činu podvodu. Přísnější trestní sazby jsou stanoveny zejména v případech, kdy pachatel způsobí větší škodu, značnou škodu nebo škodu velkého rozsahu, případně spáchá trestný čin jako člen organizované skupiny nebo za jiných okolností uvedených v § 209 odst. 2 až 6 trestního zákoníku.

Základní skutková podstata trestného činu představuje souhrn zákonem stanovených typových znaků trestného činu, jejichž naplnění je nezbytné pro vyvození trestní odpovědnosti pachatele za daný trestný čin. Tyto znaky jsou tradičně členěny

na objekt trestného činu, objektivní stránku, subjekt trestného činu a subjektivní stránku. Základní skutková podstata tak vyjadřuje základní, typovou podobu trestného činu a obsahuje minimální soubor znaků, které musí být v konkrétním případě naplněny, aby bylo možné určité jednání pod příslušné ustanovení trestního zákoníku podřadit.

Vedle základní skutkové podstaty trestní zákoník upravuje také kvalifikované skutkové podstaty. Kvalifikovaná skutková podstata obsahuje všechny znaky základní skutkové podstaty a současně další zákonem stanovené okolnosti, označované jako kvalifikační znaky. Tyto okolnosti zvyšují závažnost trestného činu, a odůvodňují proto použití vyšší trestní sazby. Kvalifikačním znakem může být například vyšší rozsah způsobené škody, zvláštní způsob spáchání trestného činu, postavení pachatele, opakované jednání nebo jiná okolnost, které zákon přikládá vyšší trestněprávní význam.

U trestného činu podvodu je základní skutková podstata upravena v § 209 odst. 1 trestního zákoníku. Její naplnění vyžaduje, aby pachatel sebe nebo jiného obohatil tím, že uvede jiného v omyl, využije jeho omylu nebo zamlčí podstatné skutečnosti, a tím způsobil na cizím majetku škodu nikoli nepatrnou. Pro posouzení, zda konkrétní jednání naplňuje znaky trestného činu podvodu, je proto nezbytné zabývat se jednotlivými obligatorními znaky jeho skutkové podstaty, tedy objektem, objektivní stránkou, subjektem a subjektivní stránkou.

Objektem trestného činu podvodu jsou majetkové vztahy, respektive zájem společnosti na ochraně cizího majetku před jednáním, při němž je majetková dispozice jiné osoby ovlivněna omylem. Ochrana se vztahuje na majetek fyzických i právnických osob. V případě podvodných e-shopů je zásahem do chráněného objektu typicky situace, kdy zákazník na základě nepravdivých nebo zamlčených informací provede platbu za zboží, které pachatel ve skutečnosti nemá v úmyslu dodat.

Objektivní stránka trestného činu podvodu spočívá v jednání pachatele, následku a příčinné souvislosti mezi nimi. Podvodné jednání může mít podle § 209 odst. 1 trestního zákoníku tři základní formy – uvedení jiného v omyl, využití omylu jiného nebo zamlčení podstatných skutečností. Uvedením v omyl pachatel aktivně vyvolává u jiné osoby nesprávnou představu o skutečnosti. Využitím omylu se rozumí situace, kdy pachatel sice omyl sám nevyvolal, avšak zjistí jeho existenci a vědomě jej využije ve svůj prospěch nebo ve prospěch jiné osoby. Zamlčení podstatných skutečností spočívá v

neposkytnutí takových informací, které jsou pro rozhodování poškozeného významné a jejichž znalost by mohla ovlivnit jeho majetkovou dispozici.

V důsledku omylu musí následovat majetková dispozice osoby jednající v omylu, která vede ke vzniku škody na cizím majetku a zároveň k obohacení pachatele nebo jiné osoby. Mezi podvodným jednáním, omylem, majetkovou dispozicí, škodou a obohacením musí existovat příčinná souvislost. V prostředí podvodných e-shopů může být typickým příkladem vytvoření zdánlivě důvěryhodné nabídky zboží, na jejímž základě zákazník odešle kupní cenu na účet pachatele, přestože pachatel již od počátku nemá v úmyslu objednané zboží dodat.

Subjektem trestného činu podvodu může být obecně každá fyzická osoba, která splňuje zákonné předpoklady trestní odpovědnosti. Jde tedy o trestný čin s obecným subjektem, neboť zákon u základní skutkové podstaty nevyžaduje žádné zvláštní postavení, vlastnost nebo způsobilost pachatele. V souvislosti s podvodnými e-shopy může být pachatelem například osoba, která podvodný internetový obchod vytvořila a provozuje, ale podle konkrétních okolností mohou přicházet v úvahu rovněž další osoby, které se na trestném jednání vědomě podílejí.

Subjektivní stránka trestného činu podvodu vyžaduje úmyslné zavinění. Pachatel si musí být vědom podvodné povahy svého jednání a musí chtít způsobem uvedeným v zákoně sebe nebo jiného obohatit, případně musí být alespoň s takovým následkem srozuměn. Právě prokázání úmyslu má zásadní význam při odlišování trestného činu podvodu od pouhého nesplnění občanskoprávního nebo obchodního závazku. Samotná skutečnost, že prodávající nedodá objednané zboží, ještě automaticky neznamená naplnění skutkové podstaty trestného činu podvodu. Z hlediska trestní odpovědnosti je podstatné zejména zjištění, zda pachatel již v době uzavírání obchodu, přijetí objednávky nebo převzetí finančních prostředků jednal s podvodným úmyslem a věděl, že sjednané plnění neposkytne.

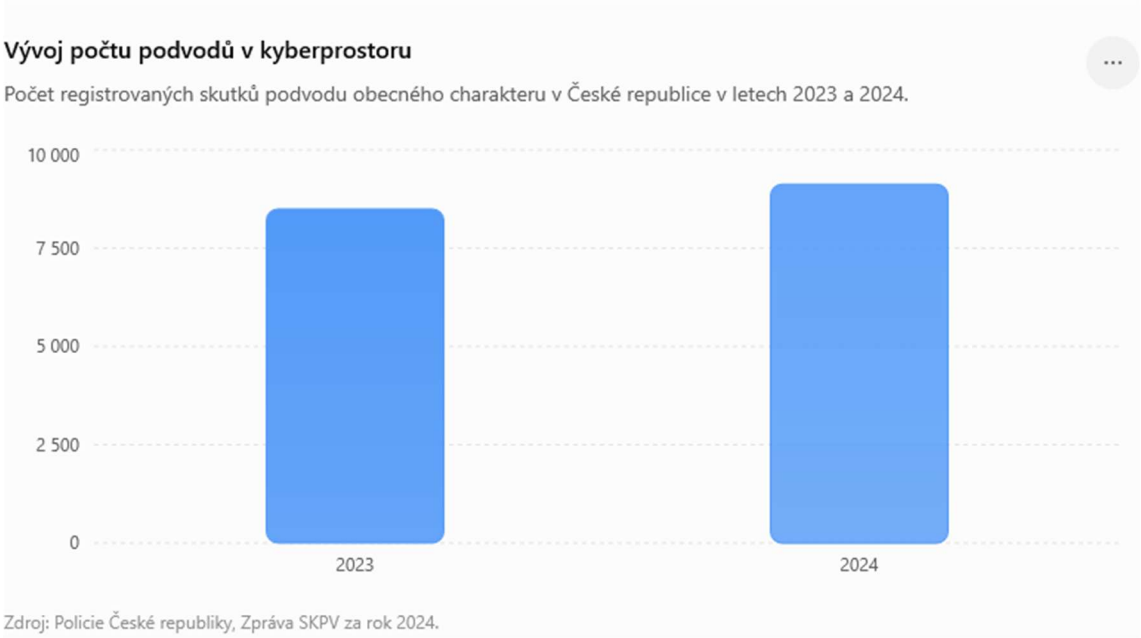
Na základní skutkovou podstatu trestného činu podvodu následně navazují jeho kvalifikované skutkové podstaty upravené v dalších odstavcích § 209 trestního zákoníku. Ty zohledňují okolnosti zvyšující závažnost jednání a stanovují pro ně přísnější trestní postih. Při prověřování podvodných e-shopů proto policejní orgán neposuzuje pouze to, zda byly naplněny znaky základní skutkové podstaty podvodu, ale rovněž zjišťuje okolnosti rozhodné pro případné použití kvalifikované skutkové

podstaty, zejména rozsah způsobené škody, počet poškozených, způsob provedení jednání a případné zapojení dalších osob. [19]

Pro potřeby orgánů činných v trestním řízení je nezbytné prokázat nejen vznik majetkové škody, ale také úmysl pachatele již v době uzavření smluvního vztahu. Rozhodující je především skutečnost, zda pachatel již při převzetí finančních prostředků věděl, že svůj závazek nesplní, nebo zda zákazníka úmyslně uvedl v omyl s cílem získat neoprávněný majetkový prospěch. Právě prokázání subjektivní stránky trestného činu bývá při prověřování podvodných e-shopů jedním z nejvýznamnějších úkolů policejního orgánu.

Vzhledem k rostoucímu počtu případů představují internetové podvody významnou výzvu pro orgány činné v trestním řízení, které musí při jejich objasňování pracovat se specifickými formami elektronických důkazů a digitálních stop.

[20] Graf č. 0: Vývoj počtu registrovaných podvodů obecného charakteru v kyberprostoru v letech 2023–2024.



[19] ŠÁMAL, Pavel a kol. Trestní zákoník. Komentář. 3. vydání. Praha: C. H. Beck
[20] Zdroj: vlastní zpracování podle Policie České republiky, Zpráva SKPV za rok 2024.

Specifika internetového prostředí, zejména anonymita pachatelů, využívání zahraničních serverů a obtížná identifikace skutečných provozovatelů internetových obchodů, kladou vysoké nároky na prověřování oznámení, zajišťování elektronických důkazů a mezinárodní spolupráci orgánů činných v trestním řízení. [21]

[21] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 111. ISBN 978-80-271-9074-4.

7 E-shopy

E-shop, označovaný také jako internetový nebo elektronický obchod, představuje softwarovou aplikaci a soubor vzájemně propojených webových stránek, jejichž prostřednictvím dochází k nabídce, objednávání, nákupu a prodeji zboží nebo služeb prostřednictvím sítě Internet. Z technického hlediska jde o informační systém, který umožňuje prezentaci nabízeného sortimentu, výběr zboží nebo služby, vytvoření objednávky, volbu způsobu dopravy a realizaci platby. Součástí e-shopu bývají rovněž databázové systémy, zákaznické účty, obchodní podmínky, kontaktní údaje provozovatele a další prvky nezbytné pro elektronické obchodování.

Z právního hlediska lze e-shop chápat jako prostředek umožňující uzavírání smluv distančním způsobem, tedy bez současné fyzické přítomnosti smluvních stran. Prostřednictvím internetového rozhraní dochází zpravidla k prezentaci nabídky zboží nebo služeb, odeslání objednávky zákazníkem a následnému vzniku smluvního vztahu mezi provozovatelem e-shopu a zákazníkem. Provozování e-shopu je proto spojeno s povinnostmi vyplývajícími zejména z občanského práva, právní úpravy ochrany spotřebitele, ochrany osobních údajů a dalších souvisejících právních předpisů.

Elektronické obchody patří v současnosti mezi nejrozšířenější formy elektronického obchodování. Spotřebitelům umožňují nakupovat zboží a služby bez nutnosti osobní návštěvy kamenné provozovny, přičemž celý obchodní proces může proběhnout prostřednictvím elektronických komunikačních prostředků.[22]

[22] ČESKÝ STATISTICKÝ ÚŘAD. Podniky a ICT – Slovník pojmů [online]. Praha: Český statistický úřad [cit. 2026-08-12]. Dostupné z: webových stránek Českého statistického úřadu.

8 Podvodné e-shopy

Podvodné e-shopy představují specifickou formu majetkové kybernetické kriminality, při níž pachatelé zneužívají prostředí elektronického obchodování k získání neoprávněného majetkového prospěchu. Jejich cílem bývá především vylákání finančních prostředků od zákazníků, případně získání osobních nebo platebních údajů využitelných k další trestné činnosti.

Na rozdíl od legitimních internetových obchodů jsou podvodné e-shopy provozovány bez úmyslu řádně plnit závazky vůči zákazníkům. Pachatelé zpravidla vytvářejí internetové stránky, které svým vzhledem a funkcionalitou napodobují běžné e-shopy. Nabízené zboží bývá často prezentováno za ceny výrazně nižší, než jsou ceny obvyklé na trhu, čímž dochází k nalákání potenciálních zákazníků.

Vznik podvodných e-shopů je usnadněn dostupností moderních technologií a komerčně dostupných řešení pro tvorbu internetových obchodů. Provozovatelé podvodných e-shopů využívají hotové šablony internetových stránek, kopírují obsah existujících obchodů nebo zneužívají identitu skutečných podnikatelských subjektů. Spotřebitelé tak mohou nabýt dojmu, že se jedná o důvěryhodného obchodníka.

Mezi typické znaky podvodných e-shopů patří zejména absence možnosti osobního odběru zboží, omezené kontaktní údaje, nedostatečná zákaznická podpora, požadavek platby předem a nejasné informace o provozovateli. Po přijetí finančních prostředků často dochází k ukončení komunikace se zákazníkem a objednané zboží není dodáno. V některých případech jsou internetové stránky po krátké době zcela odstraněny nebo nahrazeny jiným projektem.

Provozování podvodných e-shopů není doménou pouze jednotlivců. Na této trestné činnosti se často podílejí organizované skupiny působící na mezinárodní úrovni. Přeshraniční charakter internetového prostředí, využívání zahraničních serverů a anonymizačních technologií významně komplikují identifikaci pachatelů a následné trestní řízení.

Podvodné e-shopy představují významný problém nejen z pohledu ochrany spotřebitele, ale také z hlediska činnosti orgánů činných v trestním řízení. Jejich odhalování a prověřování vyžaduje odborné znalosti v oblasti informačních technologií,

elektronických důkazů a mezinárodní spolupráce při vyšetřování kybernetické kriminality. V následujících podkapitolách budou uvedeny konkrétní příklady podvodného jednání v prostředí internetového obchodování.[23]

8.1 Případ podvodného e-shopu s elektronikou

Kontext případu

Předmětem kazuistiky je případ podvodného jednání realizovaného prostřednictvím internetového obchodu zaměřeného na prodej spotřební elektroniky. Údaje umožňující identifikaci konkrétních osob a internetového obchodu nejsou s ohledem na účel této práce uváděny. Poškozeným byl zákazník, který internetové obchody využíval pravidelně a měl s nakupováním prostřednictvím internetu dlouhodobě pozitivní zkušenosti. Nešlo tedy o osobu, která by s prostředím elektronického obchodování neměla předchozí zkušenosti.

Při vyhledávání spotřební elektroniky poškozený narazil na internetový obchod nabízející mobilní telefony za cenu výrazně nižší, než byla jejich obvyklá tržní hodnota. Nižší cena byla provozovatelem vysvětlována tím, že nabízená zařízení pocházejí z doprodeje zahraničního mobilního operátora. Internetové stránky byly profesionálně zpracovány a svým vzhledem u poškozeného vzbuzovaly dojem legitimně fungujícího internetového obchodu.

Popis skutkového děje a jeho chronologie

Poškozený si prostřednictvím internetového obchodu objednal nabízenou elektroniku. Na základě pokynů provozovatele následně uhradil kupní cenu předem na uvedený bankovní účet a současně zaplatil službu expresního doručení. Provedením platby tak došlo k majetkové dispozici na straně poškozeného.

Po přijetí platby však objednané zboží nebylo v avizovaném termínu doručeno. Provozovatel internetového obchodu zpočátku s poškozeným nadále komunikoval a opakovaně mu sděloval nové termíny dodání. Ani v těchto termínech však ke splnění objednávky nedošlo. Po několika týdnech provozovatel přestal na komunikaci

[23] MINISTERSTVO PRŮMYSLU A OBCHODU ČR. Průvodce pro spotřebitele: Podvodný e-shop [online]. 24. 8. 2023 [cit. 12. 6. 2026].

poškozeného reagovat a následně se staly nedostupnými také samotné internetové stránky e-shopu. Poškozený proto pojal podezření, že se stal obětí podvodného jednání, a věc oznámil Policii České republiky.

Chronologicky lze mechanismus případu vyjádřit jako prezentace cenově atraktivní nabídky → vytvoření dojmu legitimního e-shopu → objednávka zboží → platba předem → opakované přísliby dodání → nedodání zboží → ukončení komunikace → znepřístupnění internetových stránek → oznámení věci Policii ČR.

Analýza a právní posouzení případu

Z trestněprávního hlediska je nutné posoudit jednání především ve vztahu ke skutkové podstatě trestného činu podvodu podle § 209 trestního zákoníku. Pro její naplnění je podstatné, zda pachatel sebe nebo jiného obohatil tím, že uvedl jiného v omyl, využil jeho omylu nebo zamlčel podstatné skutečnosti, a způsobil tak na cizím majetku zákonem požadovanou škodu.

Objektem trestného činu jsou v posuzovaném případě majetkové vztahy, konkrétně majetek poškozeného zákazníka. Předmětem útoku byly finanční prostředky, které poškozený převedl na bankovní účet uvedený provozovatelem internetového obchodu.

Z hlediska objektivní stránky lze podvodné jednání spatřovat zejména ve vytvoření nabídky, která u zákazníka vyvolávala přesvědčení, že uzavírá obchod s legitimním prodávajícím, jenž mu po zaplacení kupní ceny objednané zboží skutečně dodá. K vytvoření tohoto omylu přispívalo profesionální zpracování internetových stránek, atraktivní cenová nabídka a zdánlivě věrohodné vysvětlení původu levnějšího zboží. Na základě této představy poškozený provedl majetkovou dispozici spočívající v převodu finančních prostředků. Objednané zboží však nebylo dodáno a po určité době byla ukončena komunikace a internetové stránky přestaly být dostupné.

Pro trestněprávní posouzení je zásadní rovněž subjektivní stránka, tedy úmysl pachatele. Samotné nedodání objednaného zboží totiž automaticky neznamená spáchání trestného činu podvodu. Pro jeho kvalifikaci podle § 209 trestního zákoníku by bylo nutné prokázat, že pachatel již v době přijetí objednávky nebo platby věděl, že zboží nedodá, a jeho záměrem bylo finanční prostředky od zákazníka podvodně získat. Na takový úmysl mohou v konkrétním případě nepřímo poukazovat okolnosti, jako

je fiktivní či zkopírovaná nabídka, výrazně podhodnocená cena, požadavek platby předem, větší počet obdobně poškozených osob, následné přerušení komunikace nebo odstranění internetových stránek. Obecně jsou právě platba předem, nejasná identita provozovatele a následné ukončení komunikace typickými znaky popisovanými u podvodných e-shopů.

Výši škody by v konkrétním trestním řízení bylo nutné určit podle skutečně vynaložených finančních prostředků poškozeného. V podkladu použitém v této práci konkrétní částka uvedena není, a proto ji nelze bez dalšího doplnit. Stejně tak z dostupného popisu nelze definitivně konstatovat naplnění všech znaků trestného činu podle § 209, zejména zákonného znaku požadované výše škody a úmyslu pachatele. Tyto skutečnosti by musely být předmětem dokazování.

Z kriminalistického hlediska je případ charakteristický využitím prvků sociálního inženýrství. Pachatel pracuje především s důvěrou zákazníka. Výrazně nižší cena vytváří ekonomickou motivaci k rychlému nákupu, zatímco profesionální grafická úprava webu a zdánlivě logické vysvětlení nízké ceny snižují pochybnosti zákazníka. Významným prvkem je také pokračující komunikace po zaplacení, kdy opakované přísliby dodání mohou oddálit okamžik, kdy poškozený podvod rozpozná a obrátí se na banku nebo Policii ČR.

Z pohledu policejního prověřování by bylo významné zajistit zejména URL a obsah internetových stránek, potvrzení objednávky, elektronickou komunikaci, údaje o bankovním účtu příjemce, potvrzení o provedené platbě a případné snímky obrazovky e-shopu. Právě tyto elektronické stopy práce označuje za důležité pro další prověřování podvodných e-shopů.

Závěr

Popsaný případ ukazuje, že profesionální vzhled internetového obchodu sám o sobě není zárukou jeho důvěryhodnosti. Podstatným faktorem úspěchu podvodného jednání byla kombinace atraktivní ceny, věrohodného vysvětlení její výše, profesionální prezentace a požadavku na platbu předem. Případ současně dokládá, že obětí se může stát i zákazník, který má s internetovým nakupováním předchozí zkušenosti.

Z preventivního hlediska lze doporučit zejména ověření identity provozovatele e-shopu, porovnání ceny zboží s běžnou tržní cenou, kontrolu nezávislých recenzí, ověření

stáří a důvěryhodnosti internetové domény a zvýšenou obezřetnost v případech, kdy neznámý internetový obchod požaduje výhradně platbu předem. Pokud již k podvodnému jednání dojde, je důležité co nejrychleji uchovat dostupné elektronické důkazy a kontaktovat banku a Policii ČR. Vaše práce správně uvádí, že relevantními podklady mohou být zejména potvrzení o platbě, elektronická komunikace, objednávka, faktura a snímky obrazovky internetových stránek.[24]

[24] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 111-112. ISBN 978-80-271-9074-4.

9 Zásady bezpečného nakupování na internetu

Prevence představuje jeden ze základních prostředků ochrany spotřebitele před podvodnými e-shopy. Přestože nelze riziko podvodného jednání v internetovém prostředí zcela eliminovat, dodržování základních bezpečnostních zásad může významně snížit pravděpodobnost vzniku majetkové škody, zneužití osobních údajů nebo platebních prostředků. Za nejdůležitější lze považovat zejména následující zásady:

Ověření provozovatele internetového obchodu

Před uskutečněním nákupu je vhodné ověřit, kdo internetový obchod skutečně provozuje. E-shop by měl obsahovat základní identifikační a kontaktní údaje, zejména obchodní firmu nebo jméno podnikatele, sídlo, identifikační číslo a funkční kontaktní údaje. Samotné uvedení těchto informací však ještě nezaručuje důvěryhodnost obchodníka, neboť pachatel může zneužít údaje existujícího podnikatelského subjektu. Z tohoto důvodu je vhodné údaje porovnat s veřejně dostupnými registry a ověřit, zda skutečně odpovídají provozovateli daného internetového obchodu.

Kontrola internetové adresy a zabezpečení webových stránek

Pozornost je třeba věnovat samotné internetové adrese e-shopu. Pachatelé mohou vytvářet domény, které se pouze nepatrně liší od adres známých obchodníků, například změnou jednoho znaku nebo použitím jiné doménové koncovky. Uživatel by proto měl před zadáním osobních nebo platebních údajů zkontrolovat správnost internetové adresy. Zabezpečené připojení je důležitým technickým prvkem ochrany přenášených údajů, samo o sobě však není důkazem, že je konkrétní e-shop legitimní.

Posouzení ceny, nabídky a důvěryhodnosti e-shopu

Významným varovným signálem může být cena zboží, která je výrazně nižší než u ostatních prodejců. Podezření by měla vzbudit zejména kombinace mimořádně výhodné nabídky s časovým tlakem na rychlé uskutečnění nákupu. Před objednáním zboží je proto vhodné cenu porovnat s nabídkami jiných obchodníků a vyhledat zkušenosti předchozích zákazníků. Recenze je vhodné ověřovat z více nezávislých zdrojů, neboť hodnocení zveřejněná přímo na stránkách podvodného e-shopu mohou být smyšlená nebo manipulovaná.

Bezpečný způsob platby

Zvýšenou obezřetnost je vhodné zachovat v případě, kdy neznámý internetový obchod vyžaduje pouze platbu předem bankovním převodem a nenabízí alternativní způsob úhrady. Způsob platby je významný také z hlediska případné následné možnosti domáhat se vrácení finančních prostředků. Spotřebitel by měl před zaplacením zvážit nejen cenu zboží, ale také důvěryhodnost obchodníka a rizika spojená s konkrétní platební metodou.

Ochrana osobních a platebních údajů

Spotřebitel by měl internetovému obchodu poskytovat pouze takové osobní údaje, které jsou nezbytné pro uskutečnění objednávky. Zvýšenou pozornost je nutné věnovat zejména údajům o platební kartě a přihlašovacím údajům do internetového bankovnictví. Podezřelý požadavek na sdělení údajů, které nejsou pro uskutečnění nákupu potřebné, může být známkou snahy o jejich zneužití.

Postup při podezření na podvod

Pokud spotřebitel zjistí, že objednané a zaplacené zboží nebylo dodáno a provozovatel přestal komunikovat, měl by především uchovat dostupné důkazní materiály. Jedná se zejména o potvrzení objednávky, doklad o provedené platbě, elektronickou komunikaci, fakturu a snímky obrazovky internetového obchodu. V případě podezření na podvodné jednání je vhodné bez zbytečného odkladu kontaktovat banku a podle okolností podat trestní oznámení Policii České republiky. Význam rychlého zajištění elektronických stop spočívá mimo jiné v tom, že internetové stránky mohou být změněny nebo odstraněny a finanční prostředky mohou být následně převáděny mezi dalšími účty. Tuto potřebu ostatně podrobněji rozebíráte v části práce věnované policejnímu prověřování.

Dodržování uvedených zásad nemůže poskytnout absolutní ochranu před internetovým podvodem, může však podstatně snížit riziko jeho úspěšného dokonání. Z hlediska prevence je rozhodující zejména schopnost spotřebitele rozpoznat kombinaci několika varovných znaků a nepovažovat profesionální vzhled internetových stránek automaticky za důkaz důvěryhodnosti jejich provozovatele.[25]

[25] ČESKÁ OBCHODNÍ INSPEKCE. Rizikové internetové obchody [online]. [cit. 2026-07-12]. Dostupné z: Rizikové internetové obchody – ČOI

10 Podání a prověřování trestního oznámení

Trestní oznámení představuje oznámení o skutečnostech nasvědčujících tomu, že byl spáchán trestný čin. Podle § 158 odst. 2 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, jsou státní zástupce i policejní orgán povinni přijímat oznámení o skutečnostech nasvědčujících tomu, že byl spáchán trestný čin.

Trestní oznámení může podat každá fyzická nebo právnická osoba, která se dozví o skutečnostech nasvědčujících spáchání trestného činu. Oznamovatel není povinen právně posoudit jednání ani určit, o jaký trestný čin se jedná. Posouzení skutku a jeho právní kvalifikace náleží výhradně orgánům činným v trestním řízení.

Po přijetí trestního oznámení je policejní orgán povinen učinit potřebná šetření a opatření ke zjištění skutečností nasvědčujících tomu, zda byl spáchán trestný čin a postupovat v souladu s ustanoveními trestního řádu. Trestní oznámení lze podat písemně, ústně do protokolu nebo v elektronické podobě za podmínek stanovených právními předpisy. Oznámení lze učinit u kteréhokoli útvaru Policie České republiky nebo u státního zastupitelství.

V případech podvodných e-shopů představuje trestní oznámení zpravidla první procesní úkon, na jehož základě policejní orgán prověřuje skutečnosti nasvědčující tomu, že mohl být spáchán trestný čin podvodu podle § 209 trestního zákoníku.

10.1 Možnosti podání trestního oznámení

Trestní oznámení lze podat písemně, ústně do protokolu nebo elektronicky v souladu s ustanovením § 59 trestního řádu. Ústní oznámení se podává u kteréhokoli útvaru Policie České republiky nebo u státního zastupitelství, kde je o jeho obsahu sepsán protokol.[26]

[26] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 133-134. ISBN 978-80-271-9074-4.

Při přijetí trestního oznámení policejní orgán zjišťuje zejména okolnosti skutku, dobu a místo jeho spáchání, výši způsobené škody, osoby, které mohou poskytnout informace významné pro trestní řízení, a další skutečnosti důležité pro prověřování oznámení. Současně oznamovatele poučí o jeho právech a povinnostech vyplývajících z trestního řádu.

V případě podvodných e-shopů je vhodné k trestnímu oznámení přiložit dostupné důkazní prostředky, zejména potvrzení o provedené platbě, e-mailovou komunikaci s prodávajícím, snímky obrazovky internetových stránek, údaje o bankovním účtu příjemce platby, internetovou adresu (URL) e-shopu a další informace, které mohou napomoci objasnění věci.

10.2 Obsah trestního oznámení

Trestní řád nestanoví závazné náležitosti trestního oznámení. Pro účely efektivního prověřování je však vhodné, aby oznámení obsahovalo co nejúplnější informace o oznamovaném skutku.

Mezi základní údaje patří označení oznamovatele, popis skutkového děje, čas a místo jeho spáchání, označení osob, kterých se oznámení týká, dostupné důkazní prostředky a informace o vzniklé škodě. V případech internetové kriminality jsou významnými údaji rovněž internetové adresy (URL), e-mailové adresy, telefonní čísla, čísla bankovních účtů, uživatelské účty na internetových platformách nebo další elektronické identifikátory, které mohou přispět k identifikaci pachatele.

Čím přesnější a podrobnější informace jsou v trestním oznámení uvedeny, tím efektivněji může policejní orgán provést prvotní prověřování oznámených skutečností a zajistit potřebné důkazní prostředky.

10.3 Lhůty pro prověřování oznámení

Po přijetí trestního oznámení policejní orgán postupuje podle § 158 trestního řádu a prověřuje skutečnosti nasvědčující tomu, že byl spáchán trestný čin. Účelem prověřování je zjistit, zda jsou splněny podmínky pro zahájení trestního stíhání konkrétní

osoby nebo zda bude ve věci rozhodnuto jiným způsobem předpokládaným trestním řádem.

Podle § 159 odst. 1 trestního řádu policejní orgán ukončí prověřování zpravidla do dvou měsíců od zahájení úkonů trestního řízení. Ve skutkově nebo právně složitějších případech může být tato lhůta se souhlasem státního zástupce prodloužena.

Prověřování trestné činnosti páchané prostřednictvím internetu bývá zpravidla časově náročnější než u běžné majetkové kriminality. Důvodem je zejména potřeba zajišťování elektronických důkazů, vyžádání údajů od bankovních institucí, poskytovatelů internetových služeb, provozovatelů internetových platforem nebo zahraničních subjektů. V některých případech je nezbytná také mezinárodní policejní nebo justiční spolupráce, která může celkovou dobu prověřování prodloužit.[27]

[27] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 132. ISBN 978-80-271-9074-4.

11 Policie České republiky a kyberzločiny

Odhalování a vyšetřování trestné činnosti na internetu je dnes doslova každodenní prací Policie České republiky. V rámci organizační struktury jsou dnes vytvořena specializovaná pracoviště pro boj s internetovou kriminalitou na každém krajském ředitelství policie. Tato pracoviště poskytují ostatním složkám policie odborné znalosti při zajišťování důkazů ze sítě internet. Prudký rozvoj informačních technologií a s tím spojené přenesení části zločinů do virtuálního světa přinesly potřebu výše uvedená pracoviště rozšiřovat a prohlubovat jejich odborné znalosti. Není proto náhoda, že boj proti kyberkriminalitě se stal jednou z hlavních priorit Policie České republiky. Ovšem bez aktivní pomoci poskytovatelů služeb obsahu a připojení v rámci sítě internet bude tato snaha marná. Vzhledem k absenci centrální autority v rámci internetu leží pořizování důkazních materiálů o protiprávní činnosti pouze na straně poskytovatelů. Bez jejich součinnosti není možné důkazy pro trestní řízení často zadokumentovat.

Je jen na nás bychom například k nakupování na internetu využívali takové služby, které v rámci platných zákonů monitorují činnost svých uživatelů a v případě protiprávního jednání rychle a účinně poskytnou tyto informace pouze orgánům činným v trestním řízení na základě příslušných právních předpisů.[28]

11.1 Policie a justice – problém s odhalováním kyberkriminality

Kyberkriminalita, jako trestná činnost, je páchána s použitím velmi specifických technologických nástrojů a specializovaných znalostí. K jejímu odhalení a prokázání je tedy opět třeba velmi speciálních nástrojů, znalostí a postupů. A to je právě jeden z hlavních problémů policie a justice - nedostatek vysoce kvalifikovaných pracovníků, kteří by byli schopni zvládnout problematiku kyberkriminality nejenom po stránce technologické, ale i po stránce právní a policejní praxe. Mimo to, policie se musí vyrovnat i s tím, že klasické vyšetřovací metody selhávají. Je to zejména dáno odlišným charakterem stop v kyberprostoru, jejich trvanlivostí a použitelností v důkazním řízením. Zatímco stopy klasického trestného činu je možno zajistit ještě několik hodin nebo dnů po činu, v případě kyberkriminality je zajištění stop otázkou minut. Trestný čin se

[28] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. str. 135. ISBN 978-80-271-9074-4.

odehrává ve složitém technologickém prostředí, jehož stav se každou sekundou mění. Navíc, toto prostředí podléhá rychlému technologickému vývoji, a tak spektrum kybernetických trestných činů podléhá technologickým trendům, velmi rychle se rozvijí a modifikuje. Současná rychlost vyšetřovacího procesu neodpovídá technologickým trendům.

Obdobným problémem jako policie trpí i justice. Přestože je většina projevů kyberkriminality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Kromě běžných problémů nepomáhá jistě soudnímu řízení ani fakt, že soudci jsou specialisty na právo, nikoliv na informační technologie, takže v odborných případech musí využívat soudní znalce a spoléhat na ně. Nedostatek kvalifikovaného soudního personálu a soudců, kteří by byli schopni orientace ve složité struktuře kyberzločinu, nepřispívá ke kvalitě soudního řízení v případech, kdy je projednáván kybernetický trestný čin. Pomalost procesních postupů může vést i ke ztrátě důkazů, které bezprostředně po spáchání trestného činu existovaly, avšak dlouhé administrativní řízení neumožnilo jejich řádné zajištění.[29]

11.2 Oznamovací povinnost

Na závěr je třeba zmínit také skutečnost, že kdokoliv z nás se dozví o protiprávním jednání, je ze zákona povinen toto oznámit. Nesplnění této povinnosti ,je v některých případech postihováno jako trestný čin dle ustanovení § 368 trestního zákoníku. Skutkovou podstatu tohoto trestného činu naplní ten, kdo se hodnověrným způsobem dozví, že někdo jiný spáchal některý z taxativně vyjmenovaných trestných činů, a tuto skutečnost neoznámí policejnímu orgánu nebo státnímu zástupci. Za toto může provinilci hrozit trest odnětí svobody až ve výši tří let. Tato oznamovací povinnost platí také pro provozovatele různých internetových služeb.[30]

[29] JIROVSKÝ, Václav. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. str. 26-27. ISBN 978-80-247-1561-2.
[30] KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. 176 s. ISBN 978-80-271-9074-4.

11.3 Úloha policie a justice při postihování počítačové kriminality

Kybernalita jako trestná činnost je páchána s použitím velmi specifických technologických nástrojů a specializovaných znalostí. K jejímu odhalení a prokázání je tedy opět potřeba velmi speciálních nástrojů, znalostí a postupů. A to je právě jeden z hlavních problémů policie a justice- nedostatek vysoce kvalifikovaných pracovníků, kteří by byli schopni zvládnout problematiku kybernality nejen po stránce technologické, ale i po stránce právní a policejní praxe. Mimo to se policie musí vyrovnat i s tím, že klasické vyšetřovací metody selhávají. Je to zejména dáno odlišným charakterem stop v kyberprostoru, jejich trvanlivostí a použitelností v důkazním řízení. Přestože je většina projevů kybernality trestná, není vždy snadné takovou činnost odhalit, dokázat a pachatele odsoudit. Na začátku roku 2006 došlo ke změně struktury a vzniklo nové oddělení informační kriminality. Došlo k vytvoření specializovaných míst operativních detektivů na útvarech s republikovou působností a současně na jednotlivých krajských územních odborech Policie české republiky.[31]

- **Specializované útvary:** Na kyberkriminalitu se zaměřují specializované odbory v rámci obecné i hospodářské kriminality.
- **Vyšetřování a odhalování:** Policie vyšetřuje případy neoprávněného přístupu k počítačovým systémům (hacking), počítačové podvody (phishing, krádeže financí) a šíření škodlivého softwaru (ransomware).
- **Zajišťování důkazů:** Klíčovou činností je zajišťování digitálních stop a dat, často v mezinárodním měřítku.
- **Prevence:** Policie realizuje osvětové kampaně a preventivní projekty k minimalizaci rizik na sociálních sítích.[32]

[31] FEREBAUEROVÁ, R., PEKÁREK, O. Aplikovaná informatika. 1. vydání. České Budějovice: Vysoká škola evropských a regionálních studií, 2014, str. 139. ISBN 978-80-87472-74-3.

[32] POŽÁR, Josef. Specifické problémy boje s kybernetickou kriminalitou. Online. 2025. Dostupné z: https://mv.gov.cz/soubor/policejniakademie.aspx#:~:text=(Zdroj%20informac%C3%AD:%20resortn%C3%AD%20materi%C3%A1l%20%E2%80%9EAnal%C3%BDza%20aktu%C3%A1ln%C3%AD%20%C3%BArovn%C4%9B,kter%C3%A9%20se%20pod%C3%ADlej%C3%AD%20na%20vy%C5%A1et%C5%99ov%C3%A1n%C3%AD%20kybernetick%C3%A9%20kriminality.. [cit. 2026-03-24].

12 Mechanismy podvodných e-shopů

Pachatelé podvodných e-shopů využívají různé způsoby, jak přimět zákazníka k provedení platby nebo získat jeho osobní a platební údaje. Jedním z nejčastějších způsobů je vytvoření zdání důvěryhodného internetového obchodu. Pachatelé používají profesionální grafické zpracování webových stránek, zveřejňují obchodní podmínky, kontaktní údaje, loga platebních společností nebo informace o bezpečnosti plateb. Tyto prvky samy o sobě však nejsou zárukou důvěryhodnosti provozovatele.

Dalším mechanismem je propagace podvodných internetových obchodů prostřednictvím placené internetové reklamy, sociálních sítí nebo rozesílání odkazů prostřednictvím elektronické pošty či textových zpráv. V některých případech jsou zákazníci přesměrováni na podvodné stránky prostřednictvím phishingových kampaní nebo falešných reklamních sdělení.

Pachatelé mohou rovněž zneužívat identifikační údaje skutečně existujících podnikatelů. Použití názvu společnosti nebo identifikačního čísla osoby neznamená, že internetový obchod skutečně provozuje uvedený podnikatel. Proto je vhodné ověřit, zda kontaktní údaje zveřejněné na internetových stránkách odpovídají údajům uvedeným ve veřejných rejstřících.

Vedle získání finančních prostředků může být cílem pachatelů také neoprávněné získání osobních nebo platebních údajů zákazníků. Tyto údaje mohou být následně zneužity k dalším podvodným jednáním nebo neoprávněným platebním transakcím.

Charakteristickým znakem podvodných e-shopů bývá rovněž omezená nebo zcela nefunkční komunikace po provedení platby. Poškození často uvádějí, že provozovatel přestal reagovat na elektronickou komunikaci, telefonní čísla nejsou dostupná nebo byly internetové stránky po krátké době odstraněny.[33]

[33] Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů. Online. 2025. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/#:~:text=*%20Aktu%C3%A1ln%C3%AD%20informace.%20*%20Bezpe%C4%8Dnost%20v%C3%BDrobk%C5%AF. [cit. 2026-03-24].

12.1 Identifikační znaky podvodu

Přestože jsou podvodné e-shopy stále sofistikovanější, lze identifikovat určité skutečnosti, které mohou nasvědčovat podvodnému jednání.

Jedním z nejčastějších znaků je využívání internetových domén podobných doménám známých obchodníků. Pachatelé mohou využívat překlepy v názvu domény, odlišné doménové koncovky nebo jiné drobné změny, které mohou běžný uživatel snadno přehlédnout.

Dalším varovným znakem může být požadavek na úhradu celé kupní ceny předem bez možnosti využití jiného způsobu platby nebo osobního převzetí zboží. Zvýšenou obezřetnost je vhodné zachovat rovněž v případě mimořádně nízkých cen, které se výrazně odlišují od běžných cen na trhu.

Podezřelé mohou být také nedostatečné nebo neúplné identifikační údaje provozovatele, nefunkční kontaktní údaje, gramatické chyby na internetových stránkách nebo požadování osobních údajů, které nejsou nezbytné pro uzavření a splnění kupní smlouvy.

12.2 Možnosti nápravy a role finančních institucí

Pokud zákazník zjistí, že se stal obětí podvodného e-shopu, měl by bez zbytečného odkladu kontaktovat svou banku a informovat ji o uskutečněné transakci. V závislosti na způsobu provedené platby může banka posoudit možnost reklamace platební transakce nebo využití pravidel karetních asociací, je-li platba provedena platební kartou.

Současně je vhodné zachovat veškeré dostupné důkazní prostředky, zejména potvrzení o provedené platbě, elektronickou komunikaci s prodávajícím, objednávku, fakturu, snímky obrazovky internetových stránek a další dokumenty související s nákupem. Tyto podklady mohou být významné jak pro reklamační řízení u banky, tak pro následné trestní řízení.

Poškozený by měl následně podat trestní oznámení Policii České republiky, která posoudí, zda oznámené skutečnosti odůvodňují zahájení úkonů trestního řízení podle § 158 odst. 3 trestního řádu.[34]

[34] MINISTERSTVO PRŮMYSLU A OBCHODU. Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů [online]. Praha: Ministerstvo průmyslu a obchodu, Odbor živností a spotřebitelské legislativy, 13. ledna 2025 [cit. 2026-01-27]. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/

13 Postup policejního orgánu při prověřování trestné činnosti páchané prostřednictvím podvodných e-shopů

Prověřování oznámení o podvodných e-shopech představuje specifickou oblast činnosti Policie České republiky, při níž se prolínají obecné postupy trestního řízení se zvláštnostmi vyplývajícími z páchání trestné činnosti v kyberprostoru. Policejní orgán postupuje při prověřování v souladu se zákonem č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, přičemž současně využívá oprávnění vyplývající ze zákona č. 273/2008 Sb., o Policii České republiky.

Cílem prověřování je ověřit, zda oznámené skutečnosti odůvodňují závěr, že byl spáchán trestný čin, zjistit jeho pachatele, zajistit důkazní prostředky a vytvořit podklady pro rozhodnutí o dalším procesním postupu. V případech podvodných e-shopů je prověřování zpravidla složitější než u běžné majetkové trestné činnosti, neboť pachatelé využívají anonymitu internetového prostředí, zahraniční hostingové služby, účty vedené u různých bankovních institucí nebo prostředky elektronické komunikace umožňující ztížení jejich identifikace. Z tohoto důvodu je nezbytné zajistit elektronické důkazy bez zbytečného odkladu, protože jejich obsah může být v krátké době změněn nebo zcela odstraněn. [35]

13.1 Přijetí oznámení a zahájení úkonů trestního řízení

Prověřování podvodného e-shopu je nejčastěji zahájeno na základě trestního oznámení podaného poškozeným. Policejní orgán je podle § 158 odst. 2 trestního řádu povinen přijímat oznámení o skutečnostech nasvědčujících tomu, že byl spáchán trestný čin, a učinit potřebná opatření k prověření oznámených skutečností. Trestní oznámení může být podáno písemně, ústně do protokolu nebo elektronicky za podmínek stanovených právními předpisy.

Po přijetí trestního oznámení policejní orgán posuzuje, zda oznámené skutečnosti odůvodňují zahájení úkonů trestního řízení podle § 158 odst. 3 trestního řádu. Jsou-li zjištěny skutečnosti nasvědčující tomu, že byl spáchán trestný čin, sepíše policejní orgán

[35] Vlastní text

záznam o zahájení úkonů trestního řízení. Tento záznam obsahuje zejména popis skutku, pro který se úkony trestního řízení zahajují, předběžnou právní kvalifikaci a okolnosti odůvodňující zahájení prověřování. Opis záznamu policejní orgán zašle nejpozději do 48 hodin příslušnému státnímu zástupci, který vykonává dozor nad zachováváním zákonnosti v přípravném řízení.

V případech podvodných e-shopů je již při přijetí oznámení nezbytné věnovat zvýšenou pozornost zajištění základních elektronických stop. Policejní orgán od oznamovatele zjišťuje zejména internetovou adresu (URL) e-shopu, způsob navázání kontaktu s prodávajícím, identifikační údaje bankovního účtu, na který byla zaslána platba, čas uskutečnění objednávky a platby, způsob komunikace s prodávajícím a existenci dalších osob, které mohou poskytnout informace významné pro trestní řízení. Současně vyzve oznamovatele k předložení dostupných důkazních prostředků, mezi které zpravidla patří potvrzení o provedené platbě, e-mailová komunikace, textové zprávy, faktury, potvrzení objednávky nebo snímky obrazovky internetových stránek.

Včasné zajištění uvedených informací má zásadní význam pro další průběh prověřování. Internetové stránky mohou být během krátké doby odstraněny nebo změněny, bankovní prostředky mohou být převedeny na další účty a údaje uchovávané poskytovateli elektronických služeb podléhají zákonným retenčním dobám. Zajištění důkazních prostředků bezprostředně po oznámení proto významně zvyšuje pravděpodobnost objasnění trestné činnosti a identifikace pachatele.[36]

13.2 Prověřování podle § 158 trestního řádu

Prověřování představuje první fázi přípravného řízení po zahájení úkonů trestního řízení podle § 158 odst. 3 trestního řádu. Účelem této fáze je prověřit skutečnosti nasvědčující tomu, že byl spáchán trestný čin, opatřit potřebné podklady pro rozhodnutí policejního orgánu a zjistit, zda jsou splněny podmínky pro zahájení trestního stíhání konkrétní osoby. V rámci prověřování policejní orgán opatřuje potřebná vysvětlení, zajišťuje stopy trestného činu a provádí další úkony směřující k objasnění věci.[37]

[36] Vlastní text
[37] SMEJKAL, Vladimír. Kybernetická kriminalita. 2. vydání. Plzeň: Aleš Čeněk, 2018. str. 724 .ISBN 978-80-7380-720-7.

13.2.1 Zahájení úkonů trestního řízení (§ 158 odst. 3 tr. řádu)

Jakmile policejní orgán na základě trestního oznámení nebo vlastních poznatků získá podezření ze spáchání trestného činu, sepíše neprodleně Záznam o zahájení úkonů trestního řízení. Tento moment je oficiálním začátkem prověřování. Opis záznamu zasílá policejní orgán do 48 hodin státnímu zástupci a v záznamu jsou uvedeny okolnosti, pro které se řízení vede, a předpokládaná právní kvalifikace.[38]

13.2.2 Podání vysvětlení podle § 158 odst. 6 trestního řádu

V případech podvodných e-shopů bývá poškozený zpravidla hlavním zdrojem informací o průběhu skutku. Policejní orgán proto zjišťuje zejména způsob navázání kontaktu s internetovým obchodem, obsah objednávky, způsob úhrady kupní ceny, průběh komunikace s prodávajícím, identifikační údaje bankovního účtu, na který byla platba provedena, a další skutečnosti významné pro objasnění věci. Současně poškozený předkládá dokumenty a elektronické soubory, které mohou sloužit jako důkazní prostředky v dalším průběhu trestního řízení.

Osoba podávající vysvětlení musí být před jeho podáním poučena o svých právech a povinnostech v rozsahu stanoveném trestním řádem. O podaném vysvětlení policejní orgán pořizuje úřední záznam, který slouží jako podklad pro další postup v prověřování. Samotné podání vysvětlení však nelze zaměňovat s výslechem svědka nebo poškozeného prováděným až ve stadiu vyšetřování nebo v řízení před soudem.[39]

13.2.3 Opatřování podkladů a zajišťování důkazních prostředků

Po zahájení úkonů trestního řízení policejní orgán opatřuje podklady nezbytné pro posouzení, zda oznámené skutečnosti odůvodňují zahájení trestního stíhání konkrétní

[38] ÚZ Trestní předpisy. Sagit, 2024. str. 190 ISBN 978-80-7488-634-8.
[39] Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád). Online. Zákony pro lidi. 2026. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141. [cit. 2026-03-25].

osoby. Za tímto účelem využívá oprávnění stanovená trestním řádem a provádí jednotlivé úkony směřující ke zjištění skutkového stavu věci.

V případech podvodných e-shopů jsou důkazní prostředky převážně elektronického charakteru. Policejní orgán proto opatřuje zejména informace o uskutečněných platebních transakcích, údaje vztahující se k bankovním účtům, elektronickou komunikaci mezi poškozeným a provozovatelem e-shopu, obsah internetových stránek nebo údaje od poskytovatelů služeb elektronických komunikací. Při opatřování těchto údajů postupuje v souladu s ustanoveními trestního řádu upravujícími poskytování informací pro účely trestního řízení, zejména podle § 8 a následujících.

Součástí prověřování může být rovněž vyžádání údajů od peněžních ústavů, poskytovatelů platebních služeb nebo dalších subjektů, které disponují informacemi významnými pro trestní řízení. Tyto údaje mohou přispět k identifikaci osoby disponující bankovním účtem, objasnění pohybu finančních prostředků nebo ověření dalších skutečností důležitých pro trestní řízení.

Vedle opatřování podkladů policejní orgán zajišťuje důkazní prostředky, u nichž hrozí jejich ztráta, změna nebo zničení. V prostředí internetu má tento postup mimořádný význam, neboť obsah internetových stránek může být odstraněn během krátké doby, elektronická komunikace může být smazána a finanční prostředky mohou být převedeny na další účty nebo do zahraničí. Z tohoto důvodu je nezbytné provádět jednotlivé úkony bez zbytečného odkladu.

Vyžaduje-li to povaha věci, může policejní orgán postupovat podle ustanovení § 78 a násl. trestního řádu a zajistit věci důležité pro trestní řízení. V podmínkách kybernetické kriminality se může jednat například o výpočetní techniku, mobilní telefony nebo datová úložiště obsahující informace významné pro objasnění trestné činnosti. Jsou-li splněny zákonné podmínky, může policejní orgán podle § 79a trestního řádu rozhodnout také o zajištění peněžních prostředků na účtu u banky nebo jiné finanční instituce, je-li důvodná obava, že by jinak mohlo dojít ke zmaření nebo podstatnému ztížení účelu trestního řízení.

V případech vyžadujících odborné posouzení může policejní orgán vyžádat odborné vyjádření podle § 105 trestního řádu nebo přibrat znalce, jestliže objasnění skutečností důležitých pro trestní řízení vyžaduje odborné znalosti. V oblasti

kybernetické kriminality se může jednat zejména o analýzu digitálních dat, zajištěných datových nosičů nebo vyhodnocení elektronických stop.[40]

13.3 Specifika prověřování kybernetických podvodů

Prověřování trestné činnosti páchané prostřednictvím podvodných e-shopů se v řadě aspektů odlišuje od prověřování běžné majetkové kriminality. Specifika spočívají zejména v elektronické podobě většiny důkazních prostředků, anonymitě pachatelů, přeshraničním charakteru internetového prostředí a nutnosti rychlého zajištění digitálních stop.[41]

13.3.1 Zajišťování elektronických důkazů

V případech podvodných e-shopů tvoří podstatnou část důkazních prostředků elektronická data. Policejní orgán proto již od počátku prověřování usiluje o jejich zajištění, neboť jejich obsah může být změněn, odstraněn nebo znehodnocen. Mezi významné důkazní prostředky patří zejména elektronická komunikace mezi poškozeným a provozovatelem internetového obchodu, potvrzení o provedených platbách, údaje o bankovních účtech, obsah internetových stránek, elektronické objednávky, fotografie nabízeného zboží nebo další digitální dokumenty vztahující se k prověřovanému skutku.

Vedle podkladů předložených poškozeným opatřuje policejní orgán také informace od bank, poskytovatelů platebních služeb, poskytovatelů služeb elektronických komunikací nebo dalších subjektů, které disponují údaji významnými pro trestní řízení. Tyto informace mohou přispět zejména k identifikaci osob, zjištění pohybu finančních prostředků nebo objasnění způsobu komunikace mezi účastníky.[42]

[40] Zákon č. 141/1961 Sb. Zákon o trestním řízení soudním (trestní řád). Online. Zákony pro lidi. 2026. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141. [cit. 2026-03-25].
[41] Vlastní text
[42] Vlastní text

13.3.2 Přeshraniční charakter internetové kriminality

Charakteristickým znakem podvodných e-shopů je jejich častý přeshraniční prvek. Internetové stránky mohou být provozovány na serverech umístěných mimo území České republiky, provozovatel internetového obchodu může vystupovat pod nepravou identitou a finanční prostředky bývají převáděny prostřednictvím zahraničních bankovních účtů nebo platebních služeb. Tyto skutečnosti mohou ztěžovat zjištění totožnosti pachatele i opatřování důkazních prostředků.

Vyžaduje-li objasnění věci opatření důkazů nebo provedení procesních úkonů v zahraničí, postupují orgány činné v trestním řízení podle pravidel mezinárodní justiční spolupráce v trestních věcech. V závislosti na povaze případu může být využita rovněž mezinárodní policejní spolupráce, zejména prostřednictvím Europolu nebo Interpolu, jejímž cílem je usnadnit výměnu informací mezi příslušnými orgány jednotlivých států.[43]

13.3.3 Místní příslušnost policejního orgánu

Určení místní příslušnosti může být u trestné činnosti páchané prostřednictvím internetu složitější než u běžné majetkové kriminality. Jednotlivé dílčí části jednání mohou probíhat na různých místech, například v místě, kde se nachází poškozený, kde byla provedena platební transakce nebo kde se nachází zařízení využité pachatelem.

Místní příslušnost policejního orgánu se proto posuzuje podle obecných pravidel trestního řádu a konkrétních okolností každého případu. Samotná skutečnost, že internetové stránky nebo datové servery jsou umístěny mimo území České republiky, nevylučuje pravomoc orgánů činných v trestním řízení postupovat podle českého právního řádu, jsou-li splněny podmínky stanovené trestním zákoníkem a trestním řádem.[44]

[43] Vlastní text
[44] Vlastní text

13.4 Dozor státního zástupce nad prověřováním

Nedílnou součástí přípravného řízení je dozor státního zástupce nad zachováváním zákonnosti. Podle § 174 trestního řádu vykonává státní zástupce dozor nad postupem policejního orgánu již od zahájení úkonů trestního řízení až do skončení přípravného řízení. Účelem dozoru je zajistit, aby byly jednotlivé procesní úkony prováděny v souladu se zákonem, aby byl skutkový stav zjištěn v rozsahu nezbytném pro rozhodnutí a aby byla respektována práva osob zúčastněných na trestním řízení.

Policejní orgán je povinen státního zástupce průběžně informovat o významných skutečnostech zjištěných v průběhu prověřování a řídit se jeho závaznými pokyny. Státní zástupce je oprávněn ukládat policejnímu orgánu provedení jednotlivých úkonů, požadovat doplnění prověřování nebo přezkoumávat zákonnost a odůvodněnost jeho rozhodnutí. Současně vykonává dohled nad dodržováním zákonných lhůt a nad tím, aby byly zajištěny všechny důkazní prostředky potřebné pro řádné objasnění věci.

V případech podvodných e-shopů může státní zástupce uložit policejnímu orgánu doplnění prověřování zejména tehdy, pokud je třeba opatřit další důkazní prostředky, vyžádat informace od bankovních institucí nebo poskytovatelů služeb elektronických komunikací, případně využít nástrojů mezinárodní justiční spolupráce. Jeho role je významná zejména ve složitějších případech s přeshraničním prvkem, kdy je nezbytné koordinovat postup jednotlivých orgánů činných v trestním řízení.

Dozor státního zástupce představuje významnou záruku zákonnosti přípravného řízení. Přispívá nejen k ochraně práv osob dotčených trestním řízením, ale současně zajišťuje, aby rozhodnutí policejního orgánu o zahájení trestního stíhání nebo o jiném způsobu skončení prověřování vycházelo z dostatečně zjištěného skutkového stavu.[45]

13.5 Rozhodnutí policejního orgánu po skončení prověřování

Po provedení všech potřebných úkonů v rámci prověřování policejní orgán vyhodnotí zjištěné skutečnosti a rozhodne o dalším procesním postupu. Rozhodnutí vychází z výsledků prověřování, opatřených důkazních prostředků a právního posouzení věci. Trestní řád stanoví několik způsobů, jimiž může být prověřování ukončeno.

[45] Vlastní text

Nejčastěji se jedná o zahájení trestního stíhání, odložení věci nebo její odevzdání jinému příslušnému orgánu.[46]

Zahájení trestního stíhání

Dospěje-li policejní orgán na základě výsledků prověřování k závěru, že zjištěné skutečnosti dostatečně odůvodňují závěr, že skutek spáchala určitá osoba, zahájí podle § 160 odst. 1 trestního řádu trestní stíhání vydáním usnesení o zahájení trestního stíhání. Toto rozhodnutí představuje významný procesní okamžik, kterým končí fáze prověřování a přípravné řízení přechází do stadia vyšetřování.

Usnesení o zahájení trestního stíhání musí obsahovat přesné vymezení skutku, jeho právní kvalifikaci a označení osoby, proti níž se trestní stíhání vede. Od tohoto okamžiku získává osoba procesní postavení obviněného a vznikají jí práva a povinnosti stanovené trestním řádem. Následné dokazování již probíhá v rámci vyšetřování, jehož cílem je objasnit všechny okolnosti významné pro rozhodnutí ve věci.

Odložení věci

Nejsou-li po provedeném prověřování splněny podmínky pro zahájení trestního stíhání, může policejní orgán rozhodnout o odložení věci podle § 159a trestního řádu. K tomuto postupu dochází pouze v případech stanovených zákonem, například pokud nejde o podezření ze spáchání trestného činu nebo není důvod zahájit trestní stíhání.

Rozhodnutí o odložení věci musí vycházet z dostatečně provedeného prověřování a z objektivního posouzení všech zjištěných skutečností. Policejní orgán je povinen své rozhodnutí řádně odůvodnit a seznámit s ním osoby, kterým toto právo přiznává trestní řád. Nad zákonností tohoto postupu vykonává dozor státní zástupce.

Odevzdání věci jinému orgánu

V průběhu prověřování může policejní orgán dospět k závěru, že projednání zjištěného jednání nenáleží orgánům činným v trestním řízení, ale jinému příslušnému orgánu. V takovém případě věc odevzdá orgánu příslušnému k jejímu projednání podle zvláštních právních předpisů.

[46] Vlastní text

Odevzdání věci jinému orgánu přichází v úvahu zejména tehdy, pokud provedeným prověřováním nebyly zjištěny skutečnosti odůvodňující závěr, že byl spáchán trestný čin, avšak zjištěné jednání může zakládat odpovědnost podle jiného právního předpisu. Policejní orgán současně předá příslušnému orgánu podklady opatřené v průběhu prověřování, které mohou být významné pro další řízení.[47]

[47] ÚZ Trestní předpisy. Sagit, 2024. str. 193. ISBN 978-80-7488-634-8.

14 Případové kazuistiky

14.1 Případ číslo 1

NP (neznámý pachatel) z profilového účtu pod jménem T. R. reagovala dne 15. 04. 2024 na inzerát na sociální síti Facebook na prodejní aplikaci Marketplace, kde poškozená M. O. prodávala dětské jízdní kolo za částku 5.000,-Kč, kdy projevila zájem o zakoupení dětského jízdního kola. Dne 15. 04. 2024 po vzájemné komunikaci se společně domluvili na přepravě zboží kurýrem DPD včetně zaplacení zboží předem na účet. NP následně poslal odkaz (http://dpdcz.info371.com/*), kde si poškozená po kliknutí na uvedený odkaz měla vybrat svoji banku Česká spořitelna a přihlásit se na údajný web DPD. Zde vyplnila své údaje k přihlášení do svého internetového bankovnictví, kam následně měla dostat peníze za prodané jízdní kolo. Poté dostala potvrzení Smart klíčem, které potvrdila. Následně zkontrolovala svůj účet a zjistila, že došlo k provedení dvou transakcí přes Transfergo a to ve výši 2 x 9.990,-Kč. Celkem byla poškozené způsobena škoda ve výši 19.980,-Kč.

Ve věci byly dne 15. 04. 2024 podle ust. § 158 odstavce 3 trestního řádu zahájeny úkony trestního řízení pro přečin Podvod podle ust. § 209 odst. 1 trestního zákoníku a zločin Neoprávněné opatření, padělání a pozměnění platebního prostředku podle ust. § 234 odst. 1, 3 trestního zákoníku.

S poškozenou byl následně sepsán protokol o podání vysvětlení podle ust. § 158 odst. 6 trestního řádu, kde uvedla veškeré jí známé skutečnosti a odpověděla na dotazy podané policejním orgánem. Uvedla tedy veškeré jména osob, kontakty, přezdívky a názvy profilů, ze kterých s ní podezřelá osoba komunikovala. Dále podrobně uvedla kdy ke komunikaci a přeposlání finančních prostředků z jejího účtu došlo. Policejnímu orgánu poskytla písemné a elektronické podklady důležité k trestnímu řízení, jako jsou screenshoty komunikace a další. Byl s ní sepsán souhlas s poskytnutím bankovních informací, kdy díky tomuto může policejní orgán požadovat po bance poškozené výpisy z jejího bankovního účtu, aby se zjistilo, kam byly finanční prostředky převedeny a také konkrétní dny a časy, kdy k převodu došlo.

Ve smyslu ust. § 8 odst. 1 zákona číslo 141/1961 Sb., trestního řádu bylo policejním orgánem požádáno o zaslání podkladů pro trestní řízení. Konkrétně bylo požadováno od bankovní společnosti Česka spořitelna, a.s. o zaslání identifikace bankovního účtu číslo 2307****93/0800 (číslo, datum založení, dispoziční práva, příp. další skutečnosti) a o výpis z bankovního účtu číslo 2307****93/0800 s uvedením, kdy byly zaúčtovány dvě platby ve výši 9.990,-Kč zadané dne 15. 04. 2024 a veškeré detaily plateb (IP logy autorizace a připojení k účtu, atd.).

Policejním orgánem byly následně vyhodnoceny informace, které obdržel od České spořitelny, jakožto bankovního ústavu, u které má poškozená zřízený svůj bankovní účet č. 2307****93/0800, který jí byl dne 15. 04. 2024 napaden dosud neznámým pachatelem. V odpovědi od bankovního ústavu se nachází výpis z uvedeného bankovního účtu, výpis IP logů a detaily obou zájmových transakcí. Z doručené odpovědi bylo zjištěno, že výše uvedená je jediným majitelem a disponentem uvedeného bankovního účtu. Z detailů obou zájmových plateb bylo zjištěno, že tyto byly provedeny dne 15. 04. 2024 v 9:57 hod. a 10:01 hodin pokaždé v částce 9.990,- Kč a to přes platební portál TransferGo. Obě platby byly zadány z IP adresy 2a03:***:420:a7:e850:****:7c7e:4178 a z mobilního zařízení Mozilla/5.0 (iPhone OS 15_8_2). Dále z výpisu IP logů k uvedenému bankovnímu účtu bylo zjištěno, že dne 15. 04. 2024 v době od 09:45 - 10:01 hod. se na účet někdo opakovaně připojil z IP adresy 4a03:***:410:a7:e850:****:7c7e:5984 a celkem osmkrát se pokoušel odeslat platbu ve výši 9.990,-Kč. Dle výpisu z uvedeného bankovního účtu, byla platba schválena pouze dvakrát. Uvedená IP adresa je shodná i s IP adresou, ze které se NP přihlašoval k účtu vedeném u společnosti TransferGo.

Dále policejní orgán obdržel na zaslanou žádost od společnosti TransferGo odpověď, kde byly uvedeny údaje k účtu, přes který prošly finanční prostředky poškozené. Z této odpovědi bylo zjištěno následující: jméno a příjmení majitele účtu: S.D, nar. 03.**.19**, bydliště: M****, 5** 01 L***č, telefonní číslo: +420733***948, e-mail: di***@gmail.com a IP adresy: 62.221.71.***, 4a03:***:410:a7:e850:****:7c7e:5984. Následně byla vyžádána lustrace těchto údajů Oddělením analytiky a kybernetické kriminality, SKPV, ÚO Rychnov nad Kněžnou.

Jelikož bylo šetřením policejního orgánu zjištěno, že se jedná o sériově páchanou trestnou činnost, byl spisový materiál na základě věcné příslušnosti dle PPP (pokynu policejního prezidenta) číslo 103/2013 postoupen ke společnému řízení na Obvodní oddělení Policie Frýdek Místek, kde bylo pokračováno v šetření výše uvedené trestného činu a jeho pachatele.

Vyhodnocení případu

Tento případ představuje typický příklad podvodu využívajícího sociální inženýrství, kdy pachatel zneužil důvěry poškozené prostřednictvím falešného odkazu vydávajícího se za služby společnosti DPD. Z hlediska postupu policejního orgánu bylo rozhodující bezprostřední zahájení úkonů trestního řízení a rychlé zajištění elektronických důkazních prostředků, zejména IP logů, údajů od bankovní instituce a společnosti TransferGo. Kazuistika současně ukazuje význam spolupráce policejních útvarů při odhalování sériově páchané trestné činnosti, neboť propojení jednotlivých případů umožnilo jejich společné prověřování. Případ potvrzuje, že rychlost opatřování digitálních stop má zásadní význam pro úspěšné objasnění obdobné trestné činnosti.

14.2 Případ číslo 2

Dne 15. 11. 2023 osobně na Obvodním oddělení Policie České republiky v Hostinném oznámil pan M. J. že si dne 5. 11. 2023 na internetovém portálu www.heureka.cz vyhledal a objednal sadu zimních pneumatik NOKIAN za částku 15.515.-Kč, kterou předem odeslal ze svého bankovního účtu číslo 31468****/0300 na bankovní účet 166774****/2700 společnosti PNEU a TRANS s.r.o. Do dnešního dne mu nebyly objednané pneumatiky doručeny, poškozený nemá vráceny peníze zpět a firma je nekontaktní.

Oznamovatel, pan M. J. byl řádně poučen podle zákona číslo 45/2013 Sb., o obětech trestných a poté sním byl sepsán Úřední záznam o podání vysvětlení podle ust.. § 158 odst. 6 tr. řádu, kde uvedl veškeré skutečnosti týkající se jeho případu. Na základě přijatého oznámení a předložených dokladů policejní orgán vyhodnotil, že se jedná o podezření ze spáchání přečinu Podvodu podle ust. § 209 tr. zákoníku. Byl sepsán Záznam o zahájení úkonů trestního řízení, čímž byla oficiálně zahájena fáze prověřování. Následně byl policejním orgánem podle ust. § 78 odst. 1 tr. řádu vyzván, aby vydal veškeré potřebné soubory a dokumenty týkající se podvodného jednání. Vydal

tedy fakturu, která mu byla doručena při zaplacení objednaného zboží, dále výpis ze svého bankovního účtu a veškerou emailovou komunikaci s podezřelým.

Policejní orgán prověřil společnost PNEU a TRANS s.r.o. v obchodním rejstříku. Zjistil, že se jedná o tzv. „prázdnou schránku“ s nastrčeným jednatelem (bílý kůň), na kterou bylo v poslední době podáno více obdobných oznámení po celé České republice. Dále bylo provedeno šetření k bankovnímu účtu podle ust. § 8 odst. 2 tr. řádu policejní orgán zaslal přes Státního zástupce Okresního státního zastupitelství vyžádání bance k identifikaci majitele účtu a výpisu transakcí. Z výpisu vyplynulo, že finanční částka 15.515,-Kč byla ihned po připsání přeposlána na jiný účet nebo vybrána z bankomatu. Policejním orgánem bylo tedy požádáno provozovatele portálu Heureka.cz a registrátora domény o sdělení IP adres, ze kterých byl e-shop spravován a ze kterých byla vedena komunikace se zákazníky. Lustrací v systému ETŘ bylo zjištěno, že pod stejným číslem účtu a názvem firmy figuruje dalších 45 poškozených z celé České republiky. Celková škoda tedy přesáhla hranici 500.000,-Kč, čímž došlo k překvalifikaci na Podvod se značnou škodou podle ust. § 209 odst. 4 písm. d) tr. zákoníku.

Díky analýze IP adres a kamerových záznamů z výběrů z bankomatů byl ztotožněn podezřelý pan A. B., který v inkriminované době ovládal bankovní účty i webové rozhraní e-shopu. Na základě příkazu soudu byla u podezřelého provedena domovní prohlídka, při které byl zajištěn notebook, mobilní telefony a SIM karty použité při páchání trestné činnosti. Zajištěná technika byla předána k analýze, která potvrdila přítomnost přístupových údajů k e-shopu a komunikaci s poškozenými.

Jakmile byly shromážděny dostatečné důkazy (výpisy z účtů, IP adresy, data z domovní prohlídky), policejní orgán vydal Usnesení o zahájení trestního stíhání proti panu A. B., jako obviněnému. Policejní orgán předal spis státnímu zástupci s návrhem na podání obžaloby. Okresní soud uznal pana A. B. vinným. Byl mu uložen úhrnný trest odnětí svobody v trvání 3 let s podmíněným odkladem na zkušební dobu 5 let a povinnost nahradit škodu všem poškozeným, včetně pana M. J. ve výši 15.515,-Kč.

Vyhodnocení případu

Druhá kazuistika dokumentuje případ fiktivního internetového obchodu, jehož prostřednictvím bylo poškozeno větší množství osob. Z provedeného prověřování vyplývá význam včasného zajištění údajů od bankovních institucí, provozovatele internetového portálu a registrátora domény. Současně případ ukazuje význam analytické

činnosti policejního orgánu, která umožnila propojit jednotlivá oznámení vedená na různých útvarech Policie České republiky. K objasnění skutku významně přispělo propojení digitálních důkazů s dalšími procesními úkony, zejména domovní prohlídkou a následnou analýzou zajištěných elektronických zařízení.

14.3 Případ číslo 3

Dne 15. 01. 2025 se dostavil na Obvodní oddělení Policie České republiky v Kostelci nad Orlicí poškozený, pan J. M., bytem v přilehlé obci. Službu konajícímu policistovi uvedl, že se stal obětí podvodu na inzertním portálu Bazoš.cz.

Pan Jaroslav popsal, že si týden předtím vyhlédl inzerát na zánovní mobilní telefon iPhone 15 Pro za lákavou, nikoliv však nereálnou cenu 16.500,-Kč. S prodejcem komunikoval prostřednictvím e-mailu a aplikace WhatsApp. Po dohodě zaslal celou částku na bankovní účet prodejce, který přislíbil odeslání balíku přes Zásilkovnu. Předchozího dne si poškozený balík vyzvedl v boxu v Kostelci nad Orlicí. Po otevření krabice doma zjistil, že namísto telefonu obsahuje jeden kilogram krystalového cukru v originálním papírovém obalu, aby váha zásilky odpovídala předpokládanému obsahu.

Policista vyhodnotil, že popsané jednání naplňuje znaky skutkové podstaty trestného činu Podvodu podle ust. § 209 trestního zákoníku. Ihned po přijetí oznámení sepsal s poškozeným Úřední záznam o podání vysvětlení podle ust. § 158 odst. 6 tr. řádu. Poškozený policii předal veškerou dokumentaci:

- Vytištěnou e-mailovou komunikaci.
- Screenshoty z aplikace WhatsApp s telefonním číslem pachatele.
- Potvrzení o bankovním převodu (číslo účtu příjemce).
- Podací štítek ze Zásilkovny.
- Samotný „obsah“ zásilky (cukr) i s obalovým materiálem pro případné zajištění daktyloskopických stop či DNA.

Následně byl sepsán Záznam o zahájení úkonů trestního řízení podle ust. § 158 odst. 3 tr. řádu, čímž byla oficiálně zahájena fáze prověřování. Policejní orgán provedl „lustraci“ všech dostupných atributů. Tento proces zahrnoval zejména lustraci bankovního účtu podle ust. § 8 odst. 2 tr. řádu na bankovní ústav za účelem zjištění

majitele účtu a historie transakcí (zasílá Státní zástupce). Dále lustraci telefonního čísla, tedy zjištění registrovaného uživatele u mobilního operátora (často jde o anonymní předplacenou kartu), prověření IP adres, tedy vyžádání dat od provozovatele inzertního portálu o tom, z jaké IP adresy byl inzerát vložen. Vzhledem k tomu, že se jednalo o trestnou činnost páchanou v kyberprostoru, byl spisový materiál a zjištěné atributy (číslo účtu, e-mail, telefon) postoupeny k analýze na Službu kriminální policie a vyšetřování – analytické pracoviště.

Analytici SKPV provedli kontrolu v systémech (například v databázi informací o trestné činnosti páchané na internetu). Zjistili, že stejné číslo účtu figuruje v dalších sedmi případech napříč celou Českou republikou (například v Ostravě, Praze a Plzni), kde bylo rovněž zasíláno znehodnocené zboží (cukr, rýže, staré časopisy). Dalším šetřením bylo zjištěno, že bankovní účet je veden na jméno tzv. „bílého koně“ – osoby bez domova, která účet založila za úplatu a k platební kartě nemá přístup. Výběry z bankomatu byly prováděny osobou v roušce a kapuci v místech mimo dosah kvalitních kamerových systémů. IP adresy pachatele vedly přes zahraniční VPN servery, což znemožnilo přímou identifikaci koncového zařízení.

Přes intenzivní snahu policejního orgánu a analytickou podporu SKPV (Služba kriminální policie a vyšetřování) se nepodařilo ustanovit konkrétní osobu, která se za fiktivním prodejcem skrývala. „Bílý kůň“ nebyl schopen, nebo ochoten identifikovat osobu, která jej k založení účtu najala a digitální stopa skončila u anonymizačních nástrojů.

Vzhledem k tomu, že byly vyčerpány všechny dostupné operativní i procesní možnosti a nepodařilo se zjistit skutečnosti opravňující zahájit trestní stíhání proti konkrétní osobě, rozhodl policejní orgán o tom, že ne 10. 03. 2025 bude věc podle ust. § 159a odst. 5 tr. řádu odložena, neboť se nepodařilo zjistit pachatele. Poškozenému bylo doručeno Usnesení o odložení věci a byl telefonicky kontaktován, kdy mu vysvětleno, že pokud v budoucnu vyjdou najevo nové skutečnosti (například dopadení pachatele při jiné trestné činnosti, kde se přizná k těmto útokům), bude v prověřování neprodleně pokračováno.

Vyhodnocení případu

Třetí případ dokládá situaci, kdy ani rozsáhlé prověřování nevede ke zjištění pachatele. Přestože policejní orgán provedl všechny dostupné procesní úkony, využil analytickou podporu a opatřil potřebné informace od bankovních institucí i dalších

subjektů, nepodařilo se ustanovit konkrétní osobu odpovědnou za spáchání trestného činu. Kazuistika poukazuje na limity vyšetřování internetové kriminality, zejména při využívání anonymizačních prostředků, zahraničních serverů a osob vystupujících jako tzv. bílí koně.

14.4 Komparace kazuistik a doporučení pro policejní praxi

Analýza předložených kazuistik ukazuje, že podvodné e-shopy mají přes rozdílný způsob provedení řadu společných znaků. Ve všech případech byly rozhodujícími důkazními prostředky elektronická komunikace, údaje o bankovních transakcích a informace získané od poskytovatelů internetových služeb. Současně se potvrdilo, že rychlost prověřování významně ovlivňuje možnost zajištění digitálních stop a následné objasnění trestné činnosti.

Z provedené analýzy lze formulovat několik doporučení pro policejní praxi:

- bezodkladně zahájit úkony trestního řízení po přijetí oznámení,
- co nejdříve zajistit elektronické důkazní prostředky, zejména bankovní údaje, IP logy a elektronickou komunikaci,
- využívat analytickou podporu specializovaných útvarů Policie České republiky při prověřování sériově páchané trestné činnosti,
- v případech s mezinárodním prvkem neprodleně využít dostupné nástroje mezinárodní justiční a policejní spolupráce,
- průběžně informovat poškozené o procesním postupu a významu předkládání elektronických důkazů.

Provedená komparace současně potvrzuje, že úspěšnost prověřování podvodných e-shopů je významně ovlivněna rychlostí prvotních úkonů policejního orgánu, kvalitou zajištěných digitálních stop a efektivní spoluprací s bankovními institucemi, poskytovateli elektronických komunikací a specializovanými útvary Policie České republiky.

15 Výsledky dotazníkového šetření

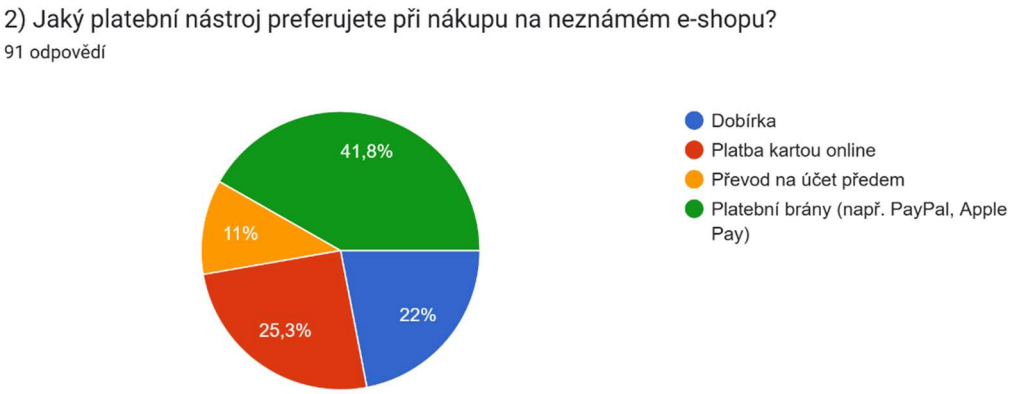
V této části jsou vyhodnocena data získaná prostřednictvím dotazníkového šetření. Výsledky jsou kvantitativně zpracovány a interpretovány s ohledem na formulované cíle. Dotazníkového šetření se účastnilo celkem 93 respondentů, kteří odpověděli na připravené otázky v dotazníkovém formátu.

Otázka č. 1 - Jak často nakupujete na e-shopech?

[48] Graf č. 1

Nejvíce respondentů nakupuje na e-shopech několikrát do měsíce (34,4 %), následuje druhá nejčastější odpověď, několikrát týdně (28 %), jednou do měsíce (22,6 %), jednou týdně (12,9 %) a vůbec na e-shopech nenakupuje minimální počet respondentů.

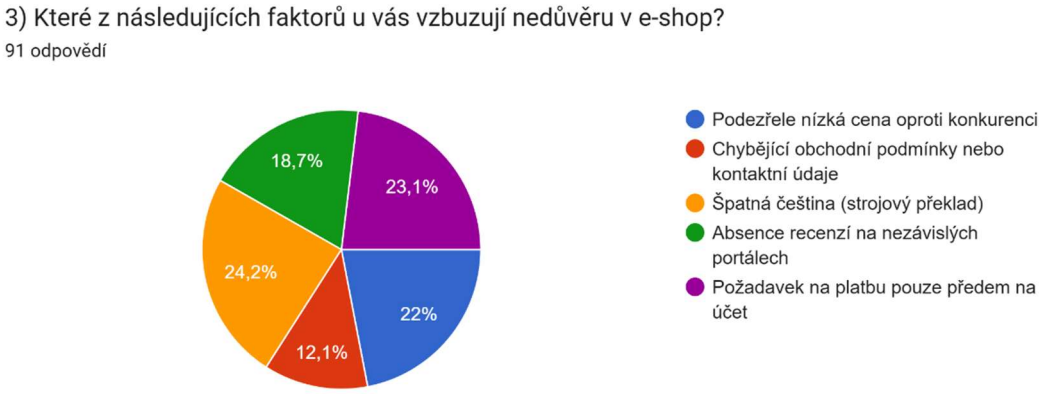
Otázka č. 2 – Jaký platební nástroj preferujete při nákupu na neznámém e-shopu?



[48] Google Forms

[49] Graf č. 2

Nejvíce respondentů preferuje na e-shopech platbu přes tzv. platební brány, například PayPal, Apple Pay atd., (41,8 %), druhý nečastější způsob je platba kartou online (25,3 %), třetí nejčastější způsob je platba na tzv. dobírku (22 %) a poslední způsob je převod na účet předem (11 %).



Otázka č. 3 – Které z následujících faktorů u vás vzbuzují nedůvěru v e-shop?
[50] Graf č. 3

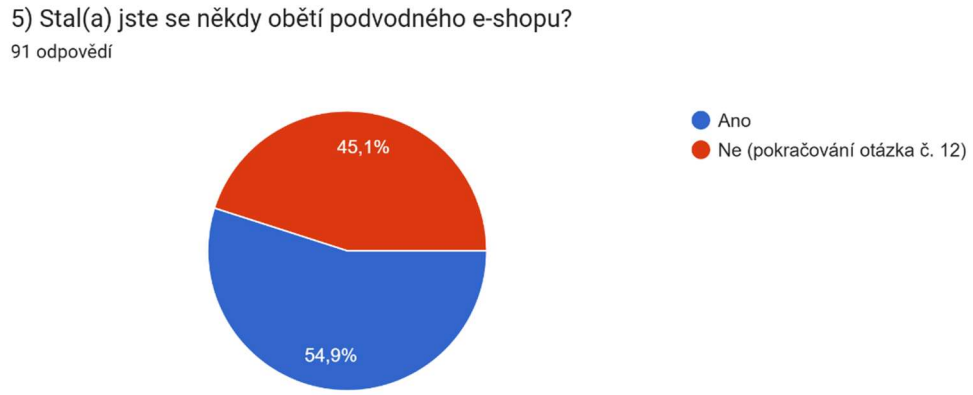
U oslovených respondentů vzbuzuje nejvíce nedůvěru faktor, pokud je e-shop tzv. strojově přeložen, tedy špatná gramatika apod. (24,2 %), druhý nejčastější faktor je požadavek na platbu předem na účet (23,1 %), třetím nejčastějším faktorem je podezřele nízká cena oproti konkurenci (22 %), dalším faktorem vzbuzujícím podezření je absence recenzí na nezávislých portálech (18,7 %) a posledním faktorem je chybějící obchodní podmínky, nebo kontaktní údaje na e-shopu (12,1 %).

[49] Google Forms
[50] Google Forms

Otázka č. 4 – Prověřujete si e-shop před nákupem na stránkách ČOI (seznam rizikových e-shopů) nebo policie?

[51] Graf č. 4

Graf číslo 4 odpovídá na otázku, zda si oslovení respondenti prověřují e-shop na stránkách České obchodní inspekce. Nejčastější odpovědí bylo Nikdy (51,8 %), druhou nejčastější odpovědí bylo Výjimečně (24,2 %), třetí odpověď byla Vždy (15,4 %) a poslední odpověď, Skoro vždy (8,8 %).



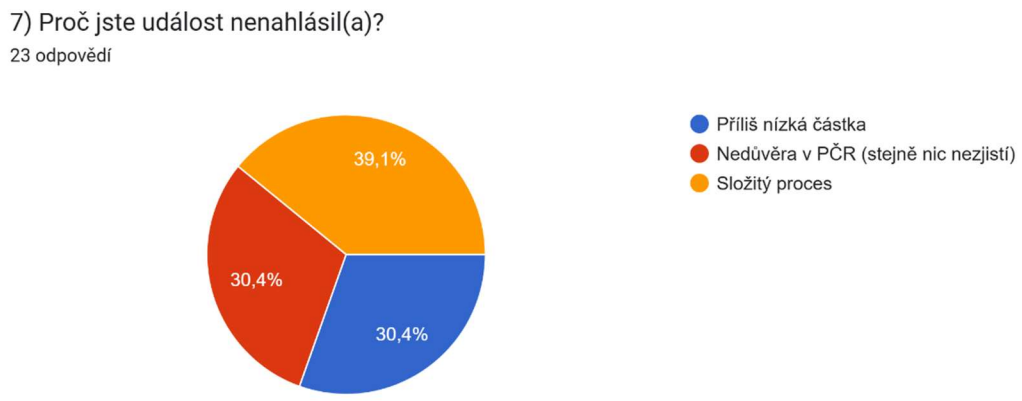
Otázka č. 5 – Stal(a) jste se někdy obětí podvodného e-shopu?

[52] Graf č. 5

Na otázku číslo 5 odpovědělo celkem 91 respondentů. Otázkou bylo, zda se respondent stal někdy obětí podvodného e-shopu. Ano odpovědělo 54,4 % respondentů a Ne odpovědělo 45,1 % respondentů.

[51] Google Forms
[52] Google Forms

Otázka č. 6 – Nahlásil(a) jste tuto skutečnost Policii České republiky?



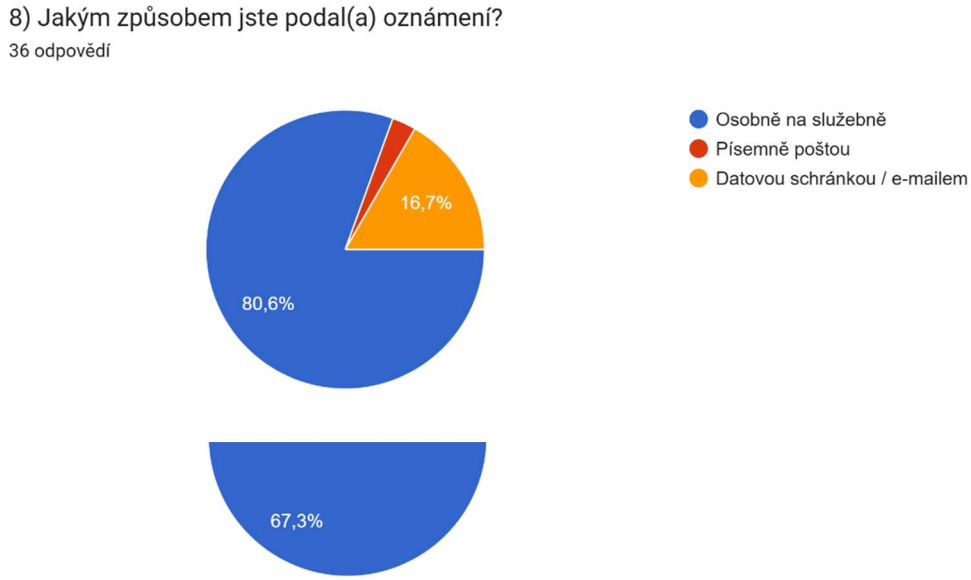
[53] Graf č. 6

Graf číslo 6 znázorňuje odpověď na otázku, zda respondent nahlásil skutečnost, že se stal poškozeným na Policii České republiky. Ano odpovědělo 67,3 % respondentů. Ne odpovědělo v součtu 32,7 % respondentů.

Otázka č. 7 – Proč jste událost nenahlásil(a)?

[54] Graf č. 7

Na otázku, proč nebyla událost nahlášena na Policii České republiky odpovědělo



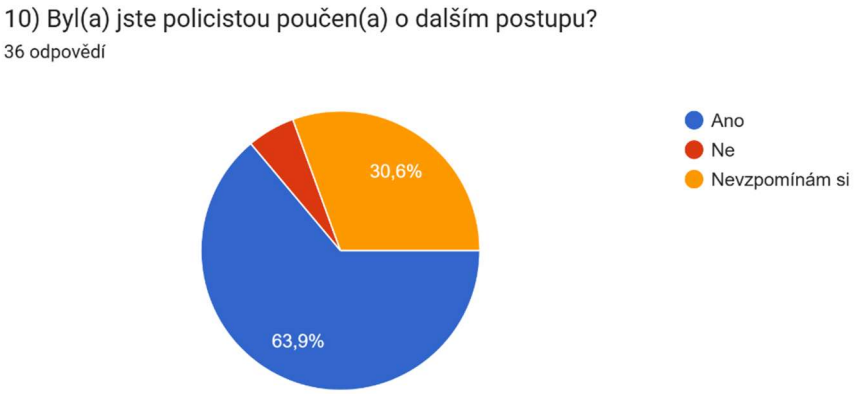
39,1 % respondentů, že z důvodu složitého procesu. Shodně 30,4 % respondentů odpovědělo, že z důvodu nedůvěry v Policii a z důvodu příliš nízké částky, o kterou přišli.

Otázka č. 8 – Jakým způsobem jste podal(a) oznámení?

[55] Graf č. 8

[53] Google Forms
[54] Google Forms
[55] Google Forms

Graf číslo 8 odpovídá na otázku, jakým způsobem bylo podáno oznámení o protiprávním jednání na Policii České republiky. Největší procento, tedy 80,6 % respondentů odpovědělo, že osobně na služebně Policie České republiky. Dále 16,7 % respondentů odpovědělo, že podání poslali datovou schránkou a minimální množství respondentů odpovědělo, že oznámení podali písmě poštou.



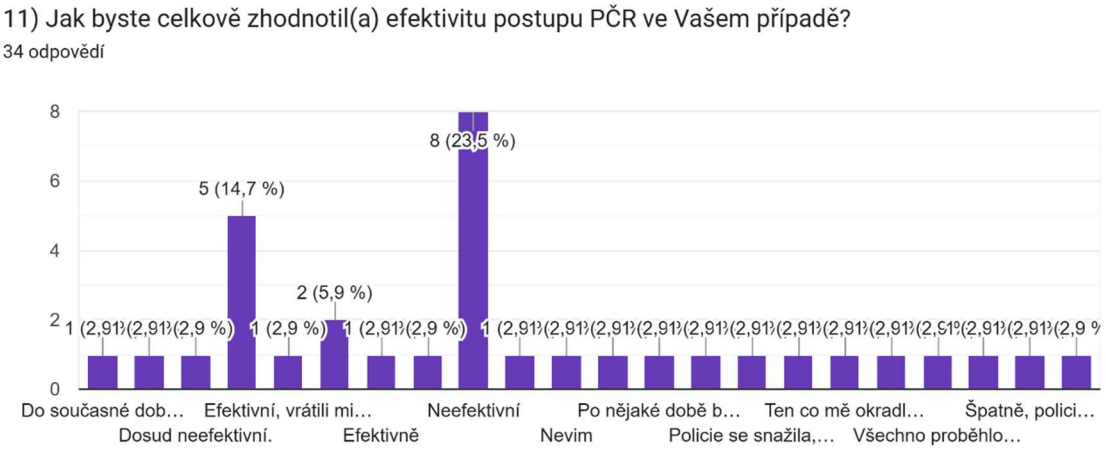
Otázka č. 9 – Byly ve Vašem případě zahájeny úkony trestního řízení?
[56] Graf č. 9

Graf číslo 9 odpovídá na otázku, zda byly v konkrétním případě dotazovaných respondentů zahájeny úkony trestního řízení. 63,2 % respondentů uvedlo, že ne, jelikož se jednalo o jednání v rovině přestupku a 36,8 % dotazovaných odpovědělo, že ano, jelikož se jednalo o trestný čin.

Otázka č. 10 – Byl(a) jste policistou poučen(a) o dalším postupu?
[57] Graf č. 10

[56] Google Forms
[57] Google Forms

Graf číslo 10 odpovídá na otázku, zda byl respondent poučen o dalším postupu



v rámci šetření případu Policií, kdy 63,9 % respondentů odpovědělo, že ano. Dalších 30,6 % respondentů odpovědělo, že si již nevzpomíná a minimální množství dotazovaných odpovědělo na otázku, že ne.

Otázka č. 11 – Jak byste celkově zhodnotil(a) efektivitu postupu Policie České republiky ve Vašem případě?
[58] Graf č. 11

Na otázku, jak by celkově dotazovaný respondent zhodnotil efektivitu postupu Policie České republiky, odpovědělo nejvíce dotazovaných, celkem 23,5 %, že postup byl neefektivní. Dalších 14,7 % respondentů odpovědělo, že postup byl efektivní, jelikož se jim vrátily finanční prostředky, o které přišli. Další odpovědi se pohybovaly okolo 3 %.

[58] Google Forms

Závěr

Cílem bakalářské práce bylo analyzovat postup policejního orgánu při prověřování trestné činnosti páchané prostřednictvím podvodných e-shopů, popsat jednotlivé procesní postupy podle trestního řádu a poukázat na specifika této formy kybernetické kriminality. Současně bylo cílem zhodnotit vybrané případy z policejní praxe a formulovat poznatky využitelné při prověřování obdobné trestné činnosti.

Teoretická část vymezila problematiku podvodných e-shopů, jejich charakteristické znaky a právní rámec postihu. Pozornost byla věnována zejména trestnému činu podvodu podle § 209 trestního zákoníku a procesnímu postupu policejního orgánu od přijetí trestního oznámení přes zahájení úkonů trestního řízení až po skončení prověřování. Významnou součást představovala rovněž problematika elektronických důkazů a digitálních stop, které mají při objasňování trestné činnosti páchané v internetovém prostředí zásadní význam.

Praktická část byla založena na analýze tří případových kazuistik vycházejících z policejní praxe. Jejich porovnání ukázalo, že možnosti objasnění internetových podvodů významně ovlivňuje zejména rychlost prvotních úkonů a včasné zajištění dostupných elektronických stop. Ve zkoumaných případech hrály důležitou roli zejména údaje o bankovních transakcích, elektronická komunikace, IP adresy a další informace získané od poskytovatelů elektronických služeb. Prověřování naopak komplikovalo využívání zahraničních služeb, anonymizačních prostředků nebo účtů vedených na jiné osoby. Zpracované případy tak poukázaly na význam spolupráce policejního orgánu s bankovními institucemi, poskytovateli služeb a specializovanými útvary Policie České republiky.

Z provedené analýzy vyplývá, že již při přijetí trestního oznámení je nezbytné věnovat zvýšenou pozornost zajištění informací, které mohou mít pouze dočasný charakter. Významné je rovněž vzájemné propojování jednotlivých oznámení a využívání analytické podpory, která může vést k odhalení sériově páchané trestné činnosti. Vedle represivního postupu má důležitou úlohu také prevence zaměřená na informovanost spotřebitelů a schopnost rozpoznat základní znaky rizikového internetového obchodu.

Přínos bakalářské práce spočívá především v propojení teoretických východisek trestního práva a trestního řízení s konkrétními poznatky z policejní praxe. Zpracované kazuistiky ukázaly praktické možnosti i limity prověřování této trestné činnosti a potvrdily význam rychlého zajištění elektronických důkazů, analytické činnosti a spolupráce s dalšími subjekty. S ohledem na pokračující rozvoj elektronického obchodování lze předpokládat, že podvodná jednání v internetovém prostředí budou i nadále představovat významnou výzvu pro orgány činné v trestním řízení a budou klást stále vyšší nároky na jejich odbornou a technologickou připravenost.

Seznam použitých zdrojů

Literární zdroje

1. DRAŠTÍK, Antonín a FREMR, Robert. Trestní zákoník: komentář. 1. díl. Praha: Wolters Kluwer, 2015. 1568 s. ISBN 978-80-7478-790-4.
2. DRAŠTÍK, Antonín a kol. Trestní zákoník. Komentář. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-790-4.
3. FEREBAUEROVÁ, R., PEKÁREK, O. Aplikovaná informatika. 1. vydání. České Budějovice: Vysoká škola evropských a regionálních studií, 2014. 151 s. ISBN 978-80-87472-74-3.
4. JELÍNEK, Jiří a kol. *Trestní právo procesní*. 7. aktualizované a doplněné vydání. Praha: Leges, 2023, s. 254. ISBN 978-80-7502-687-3.
5. JELÍNEK, Jiří a kol. Trestní právo procesní. 7. aktualizované a doplněné vydání. Praha: Leges, 2023, s. 427. ISBN 978-80-7502-687-3
6. JIRÁSEK, Petr. Cyber security glossary. Páté doplněné a upravené vydání. Centrum kybernetické bezpečnosti, z. ú., 2022. 352 s. ISBN 978-80-908388-4-0.
7. JIROVSKÝ, Václav. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. 288 s. ISBN 978-80-247-1561-2.
8. KOLOUCH, Jan. Cybercrime [online]. CZ.NIC, z. s. p. o., 2016. 511 s. ISBN 978-80-88168-16-4.
9. KOLOUCH, Jan. CyberCrime. Brno: CZ.NIC, 2016, s. 241. ISBN 978-80-88168-16-4.
10. KOŽÍŠEK, Martin a PÍSECKÝ, Václav. Bezpečně na internetu. Praha: Grada Publishing, 2016. 117-119 s., 132-135 s., 176 s. ISBN 978-80-271-9074-4.
11. Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech. Praha: Policejní akademie České republiky v Praze a kolektiv autorů, 2020. 214 s. ISBN 978-80-7251-505-9.
12. PORADA, Viktor a RAK, Roman. Kriminalita související s informačními a komunikačními technologiemi a identifikace osob na základě projevu lokomoce člověka. Druckvo, spol., 2007. 262 s. ISBN 978-80-254-0797-4.
13. SMEJKAL, V. Kybernetická kriminalita. 2. vydání. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

14. SMEJKAL, Vladimír. Kybernetická kriminalita. Třetí rozšířené a aktualizované vydání. Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.
15. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Aleš Čeněk, 2019. 378 s. ISBN 978-80-7380-765-8.
16. ŠÁMAL, Pavel a kol. Trestní řád. Komentář. II. díl. 8. vydání. Praha: C. H. Beck, 2025. 314 s. ISBN 978-80-7400-998-3.
17. ŠÁMAL, Pavel a kol. Trestní zákoník. Komentář. Praha: C. H. Beck. ISBN 978-80-7400-893-1.
18. ŠTĚDROŇ, B. JAŠEK, R.; SVÍTEK, M. a kol. Umělá inteligence a právo. Plzeň: Aleš Čeněk, 2024. 233 s. ISBN 978-80-7380-947-8.
19. VANTUCH, Pavel. Trestní zákoník s komentářem. ANAG, 2011. 1356 s. ISBN 978-80-7263-677-8.
20. ÚZ Trestní předpisy. Sagit, 2024. 511 s. ISBN 978-80-7488-634-8.

Elektronické zdroje

1. Jednotlivé druhy kyberkriminality. Online. Policie ČR. 2024. Dostupné z: https://policie.gov.cz/clanek/jednotlive-druhy-kyberkriminality.aspx. [cit. 2026-01-15].
2. Kybernetická kriminalita - fenomén dneška. Online. PRÁVNÍ PROSTOR. 2015. Dostupné z: https://www.pravniprostor.cz/clanky/ostatni-pravo/kyberneticka-kriminalita-fenomendneska. [cit. 2026-04-09].
3. MINISTERSTVO PRŮMYSLU A OBCHODU. *Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů* [online]. Praha: Ministerstvo průmyslu a obchodu, Odbor živností a spotřebitelské legislativy, 13. ledna 2025 [cit. 2026-01-27]. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--ktere-kopiruji-weby-znamych-obchodu--289453/
4. Kyberneticka_kriminalita.pdf. POKORNÝ, Pavel. Kyberkriminalita [online]. Zlín, 2016. Diplomová práce
5. KORMOŠOVÁ, I. Podvody na internetu [online].[cit. 2026-04-11]. Dostupné z WWW: https://www.policie.cz/clanek/podvody-na-e-shopech.aspx.
6. Českem se šíří odkazy na podvodné e-shopy, které kopírují weby známých obchodů. Online. 2025. Dostupné z: https://mpo.gov.cz/cz/ochrana-spotrebitele/aktualni-informace/ceskem-se-siri-odkazy-na-podvodne-e-shopy--

ktere-kopiruji-weby-znamych-obchodu--289453/#:~:text=*%20Aktu%C3%A1ln%C3%AD%20informace.%20*%20Bezpe%C4%8Dnost%20v%C3%BDrobk%C5%AF. [cit. 2026-03-24].

7. POŽÁR, Josef. Specifické problémy boje s kybernetickou kriminalitou. Online. 2025. Dostupné z: https://mv.gov.cz/soubor/policejni akademie.aspx#:~:text=(Zdroj%20informac%C3%AD:%20resortn%C3%AD%20materi%C3%A1l%20%E2%80%9EAnal%C3%BDza%20aktu%C3%A1ln%C3%AD%20%C3%BArovn%C4%9B,kter%C3%A9%20se%20pod%C3%ADlej%C3%AD%20na%20vy%C5%A1et%C5%99ov%C3%A1n%C3%AD%20kybernetick%C3%A9%20kriminality.. [cit. 2026-03-24].
8. Phishing. Online. Www.eset.com/cz/phishing. 2025. Dostupné z: https://www.eset.com/cz/phishing/#:~:text=Phishing%20je%20typ%20kybernetick%C3%A9ho%20%C3%BAtoku,nebo%20prod%C3%A1vaj%C3%AD%20na%20%C4%8Dern%C3%A9m%20trhu.. [cit. 2026-03-25].
9. Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV. Online. 2026 Policie ČR. 2026. Dostupné z: https://policie.gov.cz/clanek/narodni-centrala-proti-terorismu-extremismu-a-kyberneticke-kriminalite.aspx. [cit. 2026-03-25].
10. Vishing a spoofing. Online. Policejní prezidium ČR. 2021. Dostupné z: https://policie.gov.cz/clanek/vishing-a-spoofing.aspx. [cit. 2026-03-25].
11. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40.
12. ČESKO. Zákon č. 370/2017 Sb., o platebním styku. In: Zákony pro lidi.cz [online]. [cit. 2026-03-25]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370.
13. ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, § 12.
14. ČESKO. Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, § 1 a § 2.
15. ČESKÝ STATISTICKÝ ÚŘAD. Podniky a ICT – Slovník pojmů [online]. Praha: Český statistický úřad [cit. 2026-08-12]. Dostupné z: webových stránek Českého statistického úřadu.
16. MINISTERSTVO PRŮMYSLU A OBCHODU ČR. Průvodce pro spotřebitele: Podvodný e-shop [online]. 24. 8. 2023 [cit. 12. 6. 2026].

17. ČESKÁ OBCHODNÍ INSPEKCE. Rizikové internetové obchody [online]. [cit. 2026-08-12]. Dostupné z: Rizikové internetové obchody – ČOI

Seznam zkratek

ČOI -	Česká obchodní inspekce
DPD -	Dynamic Parcel Distribution
DPH -	daň z přidané hodnoty
ETŘ -	Evidence trestního řízení
IP adresa -	Internet Protocol (internetový protokol)
NP -	neznámý pachatel
NÚKIB -	Národní úřad pro kybernetickou a informační bezpečnost
PČR -	Policie České republiky
PPP -	Pokyn policejního prezidenta
SKPV -	Služba kriminální policie a vyšetřování
SIM karty -	Subscriber Identity Module (účastnická identifikační karta)
TČ -	trestný čin
Tr. řádu -	Trestního řádu
Tr. zák. -	Trestního zákoníku
TZ -	Trestní zákoník
URL adresa -	Uniform Resource Locator (v češtině jednotný lokátor zdrojů)
ÚO -	územní odbor
ZKB -	Zákon o kybernetické bezpečnosti

Seznam tabulek a grafů

Seznam příloh

PŘÍLOHY

Příloha – dotazník

Cílem mého výzkumu je zmapovat, jak se my, uživatelé internetu, chováme při online nákupech, a především zjistit, jaké jsou reálné zkušenosti s postupem policie v případech, kdy k podvodu dojde. Vaše odpovědi mi pomohou identifikovat slabá místa v prevenci i v následném procesu prověřování trestné činnosti.

Odkaz naleznete zde:

https://docs.google.com/forms/d/e/1FAIpQLSfUkHtZ2P26931FAEXZq_2U5rWh9SfR4HqRE0ronfaSRluYfQ/viewform?usp=dialog

Předem vám děkuji za vaši ochotu a čas. Velmi si vážím vaší pomoci při tvorbě mé závěrečné práce

1) Jak často nakupujete na e-shopech?

- Několikrát týdně
- Jednou týdně
- Několikrát měsíčně
- Jednou měsíčně
- Vůbec

2) Jaký platební nástroj preferujete při nákupu na neznámém e-shopu?

- Dobírka
- Platba kartou online
- Převod na účet předem
- Platební brány (např. PayPal, Apple Pay)

3) Které z následujících faktorů u vás vzbuzují nedůvěru v e-shop?

- Podezřele nízká cena oproti konkurenci
- Chybějící obchodní podmínky nebo kontaktní údaje
- Špatná čeština (strojový překlad)
- Absence recenzí na nezávislých portálech

- Požadavek na platbu pouze předem na účet

4) Prověřujete si e-shop před nákupem na stránkách ČOI (seznam rizikových e-shopů) nebo policie?

- Vždy
- Skoro vždy
- Výjimečně
- Nikdy

5) Stal(a) jste se někdy obětí podvodného e-shopu?

- Ano
- Ne (pokračování otázka č. 12)

6) Nahlásil(a) jste tuto skutečnost Policii ČR?

- Ano (otázka č. 8)
- Ne (otázka č. 7, poté 12)

7) Proč jste událost nenahlásil(a)?

- Příliš nízká částka
- Písemně poštou
- Datovou schránkou / e-mailem

9) Byly ve Vašem případě zahájeny úkony trestního řízení?

- Jednalo se o trestný čin (škoda nad 10.000,-Kč, popřípadě jiné okolnosti)
- Jednalo se o přestupek (škoda do 10.000,-Kč)

10) Byl(a) jste policistou poučen(a) o dalším postupu?

- Ano
- Ne
- Nevzpomínám si

11) Jak byste celkově zhodnotil(a) efektivitu postupu PČR ve Vašem případě?

- Otevřená otázka