A U S P I C I A

Recenzovaný vědecký časopis pro oblast společenských a humanitních věd

Reviewed Scholarly Journal Dealing with Social Sciences

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ
ČESKÉ BUDĚJOVICE
VYSOKÁ ŠKOLA TECHNICKÁ A EKONOMICKÁ – ÚSTAV PODNIKOVÉ STRATEGIE
ČESKÉ BUDĚJOVICE
Ročník XXII, číslo 1

2025

AUSPICIA
Recenzovaný vědecký časopis pro otázky společenských a humanitních věd.
Založen v roce 2004. Vydáván Vysokou školou evropských a regionálních studií, České Budějovice, Česká republika a Vysokou školou technickou a ekonomickou, České Budějovice, Česká republika.

Rada pro výzkum, vývoj a inovace jako odborný a poradní orgán vlády ČR zařadila recenzovaný vědecký časopis Auspicia pro rok 2015 mezi recenzované neimpaktované časopisy, které uvedla v oborech Národního referenčního rámce excelence (NRRE).

V roce 2016 byl recenzovaný vědecký časopis Auspicia zařazen do mezinárodní databáze ERIH PLUS a od roku 2024 do online knihovny pro střední a východní Evropu – CEEOL.

AUSPICIA
A peer-reviewed scholarly journal for questions of the social sciences and humanities.
Founded in 2004. Published by The College of European and Regional Studies, České Budějovice, Czech Republic and The Institute of Technology and Business, České Budějovice, Czech Republic.

The Research, Development and Innovation Council, as a professional and consultative body of the Government of the Czech Republic, indexed Auspicia – a peer-reviewed scholarly journal on a list of peer-reviewed non-impacted journals in 2015, being published in the fields of the National Reference Framework of Excellence.

In 2016 Auspicia – a peer-reviewed scholarly journal was indexed in the international database ERIH PLUS and since 2024, it has been indexed in the Central and Eastern Europe Online Library – CEEOL.

Adresa redakce: Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 1632/5b, 370 01 České Budějovice, tel.: 00420 386 116 839, https://auspicia.cz. Vychází dvakrát ročně v elektronické verzi (od roku 2019). **Září 2025**. Časopis je financován VŠERS a VŠTE. **ISSN 2464-7217 (Online)**. **DOI: 10.36682/a_2025_1**.

Editorial Office Address: Vysoká škola evropských a regionálních studií, z. ú., Žižkova tř. 1632/5b, 370 01 České Budějovice, tel.: 00420 386 116 839, https://auspicia.cz. It has been published twice a year electronically (since 2019). **September 2025**. This journal is financed by The College of European and Regional Studies and The Institute of Technology and Business. **ISSN 2464-7217 (Online)**. **DOI: 10.36682/a_2025_1.**

EDIČNÍ RADA VŠERS · EDITORIAL BOARD OF VŠERS

Předseda ediční rady · Chairman of the Editorial Board

doc. Ing. Jiří **DUŠEK**, Ph.D.

Interní členové · Internal Members

doc. JUDr. PhDr. Jiří **BÍLÝ**, CSc.; RNDr. Růžena **FEREBAUEROVÁ**; PhDr. Jan **GREGOR**, Ph.D.; doc. Ing. Marie **HESKOVÁ**, CSc.; PhDr. Štěpán **KAVAN**, Ph.D.; Mgr. Josef **KŘÍHA**, PhD.; doc. PhDr. Miroslav **SAPÍK**, Ph.D.; doc. Ing. Ladislav **SKOŘEPA**, Ph.D.; doc. Ing. Jaroslav **SLEPECKÝ**, PhD, MBA.; doc. JUDr. Roman **SVATOŠ**, Ph.D.

Externí členové · External Members

Ing. Jiří **ALINA**, Ph.D. *(Jihočeská univerzita, České Budějovice,* **ČR***)*; doc. PhDr. PaedDr. Silvia **BARNOVÁ**, PhD., MBA (Vysoká škola *DTI*, **Slovensko**); prof. Berislav **BOLFEK**, Ph.D. (*Zadarská univerzita, Zadar*, **Chorvatsko**); doc. dr. sc. Jurica **BOSNA** (*Zadarská univerzita, Zadar*, **Chorvatsko)**; doc. Ing. Jozefína **DROTÁROVÁ**, PhD., MBA (*Vysoká škola bezpečnostného manažérstva v Košiciach*, **Slovensko**); doc. MUDr. Lenka **HODAČOVÁ**, Ph.D. *(Univerzita Karlova, Hradec Králové,* **ČR***)*; doc. Ing. Petra **PÁRTLOVÁ**, Ph.D. (*Vysoká škola technická a ekonomická v Českých Budějovicích*, **ČR**); prof. PhDr. Miroslava **SZARKOVÁ**, CSc. *(Ekonomická univerzita, Bratislava,* **Slovensko***)*; doc. Ing. Jarmila **STRAKOVÁ**, Ph.D. *(Vysoká škola technická a ekonomická v Českých Budějovicích,* **ČR***)*

REDAKCE ČASOPISU AUSPICIA · EDITORIAL OFFICE OF JOURNAL AUSPICIA

Předseda redakční rady · Chairman of the Editorial Board

doc. Ing. Jiří **DUŠEK**, Ph.D. *(Vysoká škola evropských a regionálních studií, České Budějovice,* ***ČR****)*

Místopředseda redakční rady · Vice-chairman of the Editorial Board

doc. et doc. PaedDr. Mgr. Zdeněk **CAHA**, Ph.D., MBA, MSc. *(Vysoká škola technická a ekonomická v Českých Budějovicích,* ***ČR****)*

Šéfredaktor · Editor-in-Chief

doc. PhDr. Miroslav **SAPÍK**, Ph.D.

Výkonný redaktor · Managing Editor

doc. PhDr. Miroslav **SAPÍK**, Ph.D.

Technická redaktorka · Technical Editor

RNDr. Růžena **FEREBAUEROVÁ**

Redaktoři anglických textů · English Language Editors

Centrum jazykových služeb Vysoké školy technické a ekonomické

ČLENOVÉ MEZINÁRODNÍ REDAKČNÍ RADY (25) · MEMBERS OF THE INTERNATIONAL EDITORIAL BOARD (25)

OBSAH

CONTENTS

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2025_1_1

THE PRESENT AND THE FUTURE HELICOPTER EMERGENCY MEDICAL SERVICE

Současnost a budoucnost letecké záchranné služby

Pavel BÖHM – Tomáš HACAPERKA

Kladno, Czech Republic

ABSTRAKT: Letecká záchranná služba za posledních 30 let prošla významnými změnami od své koncepce, organizace, kompetencí, přes výběrová řízení až po financování. V současné době je oficiálně schválena koncepce od roku 2028, která sebou nese další významné změny, které budou mít dopady na personální zajištění letecké záchranné služby a její financování. Retrospektivní analýzou byly zkoumány možnosti minimalizace nákladů na provoz letecké záchranné služby. Za pomoci komparace získaných dat mezi Českou republikou a Spolkovou republikou Německo byl vytvořen možný rámcový model fungování letecké záchranné služby. Výsledná komparace údajů ukazuje na vyšší přístrojovou vybavenost německé letecké záchranné služby. Personální vybavenost posádek letecké záchranné služby v Německu a České republice je na stejné úrovni. Zcela absentují mezinárodní smlouvy o vzájemné pomoci a zásahu letecké záchranné služby na území druhého státu pouze na příkaz zdravotnického operačního střediska. Model pokrytí území ukazuje, že území, kde od roku 2028 vznikne nová letecká základna (pokrytí Karlovarského kraje) je již nyní pokryto leteckou záchranou službou ze Spolkové republiky Německo.

*Klíčová slova***:** letecká záchranná služba – zdravotnická záchranná služba – mezinárodní spolupráce – právní rámec

ABSTRACT: The Helicopter Emergency Medical Service has undergone significant changes over the last 30 years, both in its concept, organisation, competences, selection procedures and funding. The concept from 2028 onwards is now officially approved, bringing with it significant changes that will have implications for the staffing of the Helicopter Emergency Medical Service and its funding. A retrospective analysis has been conducted to examine the possibilities of reducing the costs of operating the air ambulance service. By comparing the data obtained between the Czech Republic and the Federal Republic of Germany, a possible framework model for the operation of the Helicopter Emergency Medical Service was created. The resulting data comparison shows a higher instrumental equipment of the German air ambulance service. The staffing of Helicopter Emergency Medical Service crews in Germany and the Czech Republic is at the same level. International agreements on mutual assistance and Helicopter Emergency Medical Service intervention on the territory of the other state only on the order of the medical operations centre are completely absent. The territorial coverage model shows that the territory where the new air base will be established from 2028 (coverage of the Karlovy Vary Region) is already covered by the Helicopter Emergency Medical Service from the Federal Republic of Germany.

Key words: Helicopter Emergency Medical Service – Emergency Medical Service – international cooperation – legal Framework

1. Úvod

Letecká záchranná služba (LZS) je dnes v České republice nedílnou součástí přednemocniční neodkladné péče. Potýká se však za posledních 30 let s několika zásadními problémy. Jedná se o změny v celkové koncepci, ve výběrových řízení, ve financování a další.

První let k záchraně lidského života proběhl 27. 4. 1956 jako sekundární transport pacienta z Terezína do Ústřední vojenské nemocnice v Praze. Následně se uskutečnilo ještě mnoho podobných transportů, většinou se jednalo o příslušníky lidové armády. Stejně jako v SRN, tak i v ČSSR se zkoušely různé projekty se zapojením vrtulníků v souvislosti se záchranou osob, zejména ve Vysokých Tatrách nebo při povodních; nejednalo se však o trvalé základny a primární vzlety. První snahy o založení LZS v ČSSR, které měly blízko k současnému modelu vznikly v roce 1977. Zlom však nastal až v roce 1985 po kongresu LZS Air-med v Curychu. Následně byl vytvořen tým specialistů, kteří měli za úkol vytvořit systém LZS na celém území ČSSR. Do týmu byli přizváni zástupci Státní letové inspekce, ministerstva zdravotnictví a horské služby. První stanice LZS vznikla k 1. 4. 1987 v Praze pod volacím znakem Kryštof 1. Poslední stanoviště vzniklo v roce 1992 v Liberci a z původního záměru 12 stanovišť jich nakonec vzniklo do roku 1992 dokonce 16 (Havrlant a Staněk, 2010).

Po rozpadu ČSFR v roce 1992 přešla správa LZS pod Ministerstvo zdravotnictví, které garantuje kvalitu, činnost a rozvoj. (Krutský 1998) V České republice (ČR) je v provozu aktuálně 10 základen LZS, jedná se o jednu z nejhustějších sítí na světě (Vilášek, 2023).

Na šesti základnách je provoz 24/7, ostatní základny fungují v režimu od východu do západu slunce. Akční rádius LZS v ČR je zpravidla 70 km a dolet maximálně do 20 minut. Při zásazích v odlehlejších částech kraje, které nedisponují vlastní LZS (Karlovarský, Zlínský a Pardubický kraj), se tento rádius prodlužuje. Aktuální provozovatelé jsou čtyři: Letecká služba Policie ČR (zdravotnická posádka ZZS hl. města Prahy a ZZS Středočeského kraje), LZS Armády ČR – Letecká záchranná služba Armády České republiky, DSA – Delta systém air (zdravotnickou část posádky zajišťuje vždy zdravotnická záchranná služba daného kraje), ATE – Air Transport Europe (zdravotnickou část posádky zajišťuje vždy zdravotnická záchranná služba daného kraje), (Peterová, 2021).

V ČR existují tři základní kategorie letů – primární lety (tvoří většinu vzletů), sekundární (mezi nemocniční transporty) a technické vzlety (provádí hasič–lezec, vyškolený

člen HS, záchranáři LZS AČR pouze tzv. level 1). Sedm základen provádí technické vzlety za pomoci podvěsu nebo palubního jeřábu (Kryštof 5, Kryštof 7, Kryštof 9). Vrtulníky provozované historicky v ČSSR a později v ČR: Mil Mi-2, PZL W-3 A Sokół, MBB Bo 105, PZL Kania, Bell 412HP, BK 117, EC 135 T2 (Fojtík, 2007; Peterová, 2021).

V roce 2024 v ČR fungují 4 základny, kde je možné pacientovi podat plnou krev (Hradec Králové, Ostrava, Plzeň – Líně, Olomouc). Okolní země v Evropě podávají převážně pouze oddělené krevní elementy (erytrocyty s krevní plazmou), plná krev však obsahuje všechny krevní elementy ochuzené pouze o lymfocyty. Používá se krev skupiny 0 s Rh negativním faktorem. Ve světě se plná krev podává v USA, Norsku, Dánsku a Velké Británii (Modrá hvězda života, 2022; Yazer et al., 2022).

Provoz a financování LZS jsou v ČR zajišťovány primárně Ministerstvem zdravotnictví ČR (MZD). Celkový provoz všech 10 stanovišť stojí přes cca půl miliardy Kč ročně. Soukromým provozovatelům je zaplaceno především poskytnutí vrtulníku a platba za letovou hodinu je minimální. (Štěpanyová, 2020) Opakem je LZS PČR a AČR, kdy MZD hradí především letovou hodinu a ostatní náklady hradí Ministerstvo vnitra, Ministerstvo obrany a Ministerstvo zemědělství. Zdravotní pojišťovna pacienta však proplácí pouze zdravotní výkony a spotřebovaný materiál během zásahu, ale nikoliv kompletní zásah LZS (letový čas, posádka, provozní náklady), což je rozdílné oproti SRN (Franěk, 2019).

2. Metodika

Sběr dat v oblasti klíčových prvků, které mají dopad nebo potenciální dopad na bezpečnost státu, infrastruktury, život a zdraví obyvatelstva a další zájmy (např. finanční) bývá složitý, data jsou obtížně dostupná a neexistují adekvátní měřítka pro porovnávání mezi státy. Pro přístup k informacích byly vybrány retrospektivní analýzy veřejně dostupných dokumentů, které lze nezávisle ověřit.

Pro šetření v oblasti vybavení a personálního zabezpečení byly vybrány základny, jenž spadají do oblasti nových změn od roku 2028, kdy bude platit nová doktrína letecké záchranné služby pro Českou republiku. V České republice to byly letecké základny v Hradci králové a v Plzni-Líních. V Německu byly vybrány základny Weiden a Zwickau, tedy potenciální letecké základny, ze kterých by mohl být veden zásah v České republice. Základny byly osobně navštíveny a byla provedena analýza vybavení ve smyslu obecného určení tak, aby nebyly narušeny chráněné zájmy daných subjektů. V rámci vybavení byly sledovány např. kritéria – typ přístroje, množství přístrojů/vybavení, tržní cena vybavení (bez započtení udržitelnosti přístroje), uživatelská přívětivost (subjektivní hodnocení) a použitelnost přístroje při letu.

V rámci experimentu dosahu letecké skupiny ze Spolkové republiky Německo a České republiky byla použita aplikace *RadiusMaps*, kde podkladová data vycházela z prováděcí vyhlášky a nařízení (tj. vzdálenost dosahu LZS dle maximálních možností až 80 km), (Oster, 2008).

Nevýhodou zvoleného tématu je absence výzkumu či odborných publikací směřujících k porovnání systémů LZS (HEMS) a použití adekvátního kriteriálního hodnocení.

3. Výsledky a diskuze

Příspěvek je zaměřen na porovnání systémů LZS, jejich řízení a funkce, vybavení, letovou techniku a rámcové finanční náklady. Podklady byly získány analýzou veřejně dostupných materiálů.

3.1 Operační řízení letecké záchranné služby ve Spolkové republice Německo a v České republice

V případě vzniku události vyžadující vyslání zdravotnické záchranné služby (ZZS) se volající spojí prostřednictvím evropského jednotného nouzového čísla 112. Následně je spojen s operačním centrem. V SRN existují v dnešní době dvě základní operační centra, a to operační centrum Spolkové policie na čísle 110 a integrované operační centrum pro hasičský záchranný systém (HZS) a ZZS na čísle 112. Operátoři na lince integrovaného záchranného střediska mají kvalifikaci tzv. Notfallsanitäter (zdravotnický záchranář). Operátor následně zpracuje veškeré informace do aplikace Rescuetrack a ta operátorovi ihned nabídne dostupná řešení konkrétní situace pro všechny složky IZS. Pomocí aplikace může zároveň operátor operačního střediska poslat posádce LZS tzv. „předvýzvu“ se souřadnicemi místa události. Posádka tak může připravit vrtulník ke vzletu a čekat tak na potvrzení vzletu na místo události (dle studie má tato metoda úsporu až 90 sekund). Dále je možné upozornit posádku prostřednictvím centrálního alarmu na základně, faxu s informacemi o zásahu, telefonním alarmem a pagerem. V aplikaci Rescuetrack pak posádka na zásahovém tabletu nebo v navigačním systému vrtulníku vidí přesné místo zásahu, další vyslané složky IZS a dostupnost místa. Vrtulníky jsou dostupné pro noční akce po celém území SRN (Biege, 1994; adac, 2024). U typu vrtulníků ITH je zřízeno středisko KITH (Koordinationszentrale für Intensivtransporthubschrauber), které se nachází v každé spolkové zemi samostatně.

V ČR fungují čtyři základní tísňová čísla. Stejně jako v SRN jednotné evropské nouzové číslo 112 a dále národní čísla (PČR 158, HZS 150 a ZZS 155). Operátor zdravotnického operačního střediska vždy zpracuje informace od volajícího a zvolí vhodnou výjezdovou

skupinu, kterou vyšle na místo. Pokud jsou splněna kritéria pro vyslání LZS, pošle ZOS výzvu posádce LZS prostřednictvím centrálního alarmu na základně, „faxu“ s informacemi o zásahu, telefonním alarmem a pagerem. Konkrétní informace o pacientovi, místě zásahu či dalších složkách IZS jsou za letu podávány přímo posádce prostřednictvím radiokomunikace. Stejně jako v SRN, tak i v ČR má operátor ZOS možnost poslat posádkám LZS tzv. „předvýzvu“. Pokud operátor vyhodnotí, že se jedná o život ohrožující stav může ihned po zjištění orientačního místa události vyslat jak pozemní výjezdové skupiny, tak i letové posádky na místo události a v průběhu cesty/letu jim doplní konkrétní informace. Každá LZS spadá pod konkrétní ZOS. Pokud příslušné ZOS, např. v Karlovarském kraji nemá vlastní LZS, pošle žádost např. ZOS ZZS Plzeňského kraje, které disponuje LZS. V případě, že je LZS volná, operační středisko ji vyšle do sousedního kraje. Posádka se pak pomocí radiové komunikace spojí s konkrétním ZOS a dostane informace. V nočních hodinách jsou základny, které mohou mít režim 24/7, v případě potřeby, nasazovány v rámci celého území ČR (Šín et al., 2024; Franěk, 2023).

3.2 Přístrojové a technické vybavení vybraných základen

V tabulce 1 je porovnáno přístrojové a materiální vybavení jednotlivých společností. Data byla získána při prohlídce základen. Červeně vyznačené vybavení je to, které kvalitativně převyšuje nad ostatními, tedy je výhodnější pro provoz LZS. U nezabarvených řádků není možné konstatovat, který z přístrojů je kvalitativně výhodnější.

Největší odlišnosti byly zjištěny při porovnávání jednotlivých typů provozovaných vrtulníků. V ČR je, s výjimkou jednoho stanoviště (LZS AČR, PZL W-3 A Sokół), provozován výhradně vrtulník EC 135. V SRN je provozován rovněž model EC 135, nebo jeho modernější verze H 135 a větší model H 145, případně pak ještě H 155. Provozovatelé LZS v SRN téměř každý rok obnovují vrtulníkový park, ČR v tomto ohledu poměrně dost zaostává a nejmladší vrtulník, který je aktuálně provozován, byl vyroben v roce 2010. Na toto zjištění reagoval Franěk (2023) ve svém příspěvku: „*20 let Écéček v letecké záchrance ČR“*. Současné vrtulníky EC 135 v ČR se blíží průměrně k 20 letům v provozu, což sice neznamená nutně jejich maximální dobu životnosti, ale po roce 2028 bude v rámci udržitelnosti nutná jejich obměna.

Tabulka 1: *Vybrané přístrojové vybavení (zdroj: vlastní)*

LZS	LZS DSA Hradec Králové	LZS AČR Plzeň-Líně	LZS DRF Luftrettung Weiden	LZS ADAC Luftrettung Zwickau
Monitor	Lifepak 15 (možnost přenosu dat)	Zoll X Series (možnost přenosu dat)	Corpuls 3 (možnost přenosu dat a zaznamenání 22svodového EKG)	Corpuls C3 touch (možnost přenosu dat a zaznamenání 22svodového EKG)
Odsávačka	Laerdal LCSU 4	Weinmann accuvac Pro	Weinmann accuvac Rescue	Boscarol
Ventilátor	Oxylog 3000 plus (plus transportní ventilátor)/ZOLL	Oxylog 3000 plus (plus transportní ventilátor)	Hamilton-T1 (plus transportní ventilátor)	Hamilton-T1 (plus transportní ventilátor)
Přístroj pro zevní srdeční masáž	LUCAS 3	LUCAS 2	Corpuls CPR*	Corpuls CPR*
Tablet pro zdravotnickou dokumentaci	Panasonic Toughbook G2 (s klávesnicí)	iPad air M1 (mobilní tiskárna brother)	medDV NIDApad (s technologií RFID karet)	medDV NIDApad (s technologií RFID karet)
Ultrazvukový přístroj	SonoSite P21	GE Vscan Extend	GE Vscan Extend	GE Vscan Extend
Analyzátor krevních plynů	-	-	Siemens EPOC	Siemens EPOC
Lineární dávkovač	2x Braun Compact S	2x Braun Compact S	4 – 8x Braun Space	4 – 8x Braun Space/compact
Video laryngoskop	Karl Storz C-MAC (měnitelné lžíce pro opakované použití)	McGRATH MAC (měnitelné lžíce jednorázové)	Karl Storz C-MAC (měnitelné lžíce pro opakované použití)	Karl Storz C-MAC (měnitelné lžíce pro opakované použití)
Nosítka	Aerolite – bez podvozku	Medirol Sanero – s podvozkem	Stryker hydraulické – s podvozkem/ Bucher s podvozkem	Bucher bez podvozku

**Oproti přístroji LUCAS se dá CORPULS CPR aplikovat i během letu.*

Limity pro vzlet jsou rovněž totožné a vrtulníky v obou zemích startují zpravidla do 3 minut, v nočních hodinách pak většinou do 10 min, kromě LZS AČR, kde jsou tyto limity striktní. SRN má při přepočtu na km² a počet obyvatel hustší síť než ČR, když však vezmeme

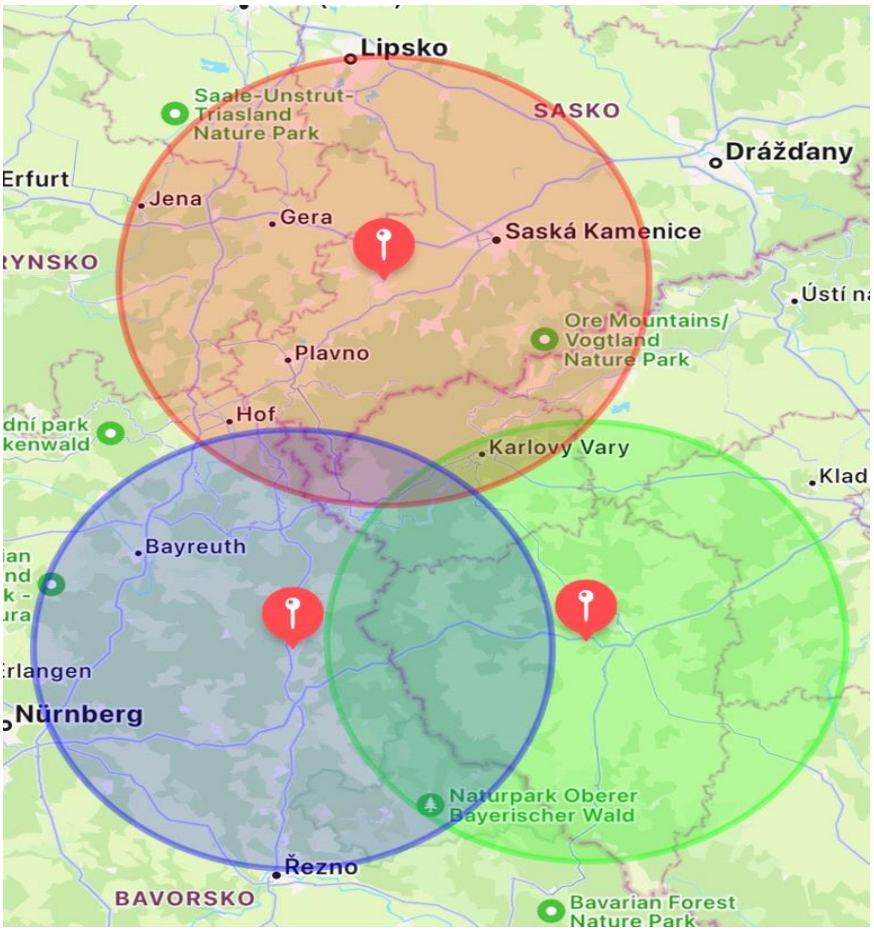
základny pro noční lety a technické zásahy a přepočteme opět na počet obyvatel, vychází pokrytí ČR znatelně lépe než SRN. Základny v SRN jsou projektovány tak, aby dostupnost LZS byla do 15 minut, to znamená, že rádius jedné základny je přibližně 60 km, v ČR je počítáno s rádiem 70 km a dostupností do 20 min. na 95,9 % našeho území. V SRN má stanoviště LZS v průměru téměř dvakrát více vzletů ročně než stanoviště LZS v ČR. Příčinou je, že operační střediska v SRN vysílají posádky LZS k více událostem z důvodu vyšší kvalifikace oproti pozemním posádkám. Posádka LZS tak často zaléčí pacienta na místě, a pokud to zdravotní stav pacienta nevyžaduje, odlétá zpět na základnu. Tento postup by se dal přirovnat k práci rande-vous systému v tuzemsku, leč je obsluhován posádkou LZS (zákon 374/2011, Sb.; cca, 2024).

Stěžejním doporučením pro praxi a efektivitu využití LZS je rozvoj přeshraniční spolupráce mezi ČR a SRN. SRN významně spolupracuje např. s Rakouskem a Švýcarskem, ale i dalšími zeměmi v rámci přeshraniční spolupráce LZS. Díky tomu jsou tyto země schopny efektivně pokrývat i odlehlejší regiony na svých hranicích. Pokud by byla v platnosti dohoda o přeshraniční spolupráci LZS mezi ČR a SRN, došlo by definitivně k pokrytí celé části často diskutovaného Karlovarského kraje, a to základnami ve Weidenu, Zwickau a Plzni – Líních. (viz Obrázek 1) V rámci pozemních posádek ZZS je v platnosti dohoda o spolupráci mezi ČR a SRN, ta se však netýká posádek LZS.

V současné době došlo na vládní úrovni k rozhodnutí o vytvoření 11. základny LZS, a to v Karlovarském kraji od roku 2028. Pokud bychom se zaměřili na možné pokrytí LZS z Německa, došlo by prakticky k téměř úplnému pokrytí území Karlovarského kraje (viz Obrázek 1). V případě platnosti přeshraniční spolupráce mezi ČR a SRN, kdy rádius činí 70 km ze základen Zwickau, Weiden a Plzeň by byl zachován požadovaný doletový čas.

Odborné exkurze probíhaly na vrtulníkových základnách v SRN a v České republice, které disponují vrtulníky EC/H 135, EC/H 145, EC 135 a PZL W-3 A Sokół. Porovnání jednotlivých typů je problematické, protože PZL W-3 A Sokół a EC 135 se již nevyrábí a jejich náhradní díly jsou výrazně dražší, tzn. dlouhodobý provoz je neudržitelný a další porovnávání tak nejsou relevantní.

Obrázek 1: *Pokrytí Karlovarského kraje, pokud by* byla *v platnosti přeshraniční spolupráce mezi ČR a SRN, rádius činí 70 km ze základen Zwickau, Weiden a Plzeň*



Zdroj: vlastní; vytvořeno za pomocí Aplikace RadiusMaps.

V otázce modernizace nebo nákupu nových strojů z uživatelského pohledu vychází pozitivně model vrtulníku H 145, je výkonnější a má vyšší stabilitu ve vzduchu. Tyto vlastnosti jsou důležité při technických typech zásahů. Další výhodou je velikost vnitřních prostor. Vrtulníky pro technické zásahy vyžadují daleko více místa pro uložení vybavení (lezecké postroje, speciální transportní vak/síť pro pacienta, horolezecké a lavinové sety), zároveň je možné transportovat i mnohem těžší pacienty, a to i přes 200 kg.

Zdravotnické vybavení je srovnatelné. SRN má však kompatibilnější přístroje napříč LZS i ZZS oproti ČR. Největší rozdíl ve vybavení je patrný ve zdravotnických zástavbách vrtulníků. Společnosti v SRN mají vlastní koncept zástavby, který vyvinuly společně se soukromou firmou, která je dodává a montuje. Provozovatelé v ČR používají zahraniční dodavatele zástaveb. Jednotlivé přístrojové vybavení je porovnáno v rámci tabulky č. 1, kdy jsou vidět kvalitativní výhody v přístrojích pro mechanickou kardiopulmonální resuscitaci. Corpuls CPR používaný německou LZS je možné aplikovat i během letu oproti přístroji

LUCAS. Další rozdíly se vyskytují v zásahových tabletech. V ČR se používají tablety pouze s programy pro záchranné služby, kdežto v SRN používají speciální tablety vyvinuté přímo pro záchranné služby (NIDApad), které disponují kompatibilitou se zdravotnickými přístroji a přímým propisováním dat i čtečkou karet pojištěnce atd.

ČR je oproti SRN mnohem dále v poskytování transfuzí plné krve (v současné době na 4 stanovištích). SRN poskytuje pouze transfuzi krevní plazmy a červených krvinek na 3 stanovištích.

Analýza dokumentů ukázala, že složení posádek je v obou zemích totožné (kapitán, případně kopilot, lékař, NLZP), to platí i při technických zásazích, kdy je k zásahu přibrán lezec HZS, pokud je nutné transportovat pacienta pomocí lanových technik. (Peřan, 2019) Jedinou výjimkou je LZS AČR, kde výše vyjmenované členy posádky doplňuje ještě palubní technik. Vzdělání lékařů a NLZP je srovnatelné, a to včetně požadavků na délku jejich praxe.

Další doporučení pro ČR v rámci rozvoje LZS může být v budoucnu strategické umisťování základen LZS přímo v areálech fakultních/krajských nemocnic, což by vedlo ke snížení provozních nákladů v rámci eliminace přeletů z nemocnic zpět na vzdálené základny, nebo alespoň ve všech fakultních a krajských nemocnicích vybudovat přístup z heliportu přímo do nemocnice bez nutnosti převozu pacientů ze vzdálenějších míst v okolí nemocnic.

Vypisování budoucích tenderů po vzoru SRN na provozovatele stanovišť LZS by mělo za cíl motivovat soukromé provozovatele k pravidelným obměnám vrtulníkových parků. Vhodná by byla plošná unifikace vrtulníkové flotily v rámci ČR na jeden konkrétní model, popřípadě na modely od jednoho výrobce, což vy vedlo ke snížení cen nákladů na rozvoj i provoz, i na výcvik pozemního personálu a posádek. V ČR rovněž absentuje právní zakotvení v rámci přistávání vrtulníků soukromých provozovatelů LZS v terénu; dle zákona smí v terénu přistávat pouze vrtulníky AČR nebo PČR, vrtulníky soukromých provozovatelů v terénu přistávají rovněž, však de iure nelegálně.

3.3 Limity práce

Slabou stránkou analýzy a komparace jednotlivých vzletů (primární či sekundární) k mimořádné události LZS v SNR a ČR není možné adekvátně porovnat. Organizace zajišťující LZS v Německu přesné statistiky nezveřejňují, tak jako je tomu v ČR, a to z důvodu konkurenčního prostředí. Interní data z německé strany byla poskytnuta k nahlédnutí, ale pod podmínkou mlčenlivosti a nelze je použít jako relevantní zdroj; s touto skutečností souvisí kalkulace nákladů a efektivity, může být tedy stanoven pouze obecný rámec, kolik reálně se pohybují jednotlivé vzlety. V Německu je provoz hrazen částečně z příspěvků, ale i ze subvencí

a darů, které si zajišťuj jednotlivý provozovatelé; oproti tomu v ČR se počítá paušální částka, se kterou se operuje po dané časové období.

Závěr

Příspěvek je zaměřen na rámcové vymezení současného stavu letecké záchranné služby a její udržitelnost. Pro porovnání byly vybrány letecké základny z Plzeňského kraje a příhraniční základny ze Spolkové republiky Německo. Jedná se o shrnutí dvou systémů, používaného vybavení, složení a nároků na posádku a zhodnocení modelů provozovaných vrtulníků.

Na základě provedené analýzy můžeme konstatovat, že letová flotila České republiky, ať státu nebo soukromých provozovatelů, je do budoucna neudržitelná a je nutná významná modernizace. Zdravotnické vybavení LZS je v obou státech na téměř shodné úrovni, mírně převyšují kvalitativní hodnoty u německé LZS. Zcela shodné jsou pak požadavky na personál a jeho vzdělání.

Významný rozdíl je ve vytíženosti LZS. ČR má oproti SRN znatelně větší síť základen provádějící noční a technické lety, i přes to každá jedna základna LZS v SRN uskuteční za den téměř dvakrát více vzletů.

Zásadní bude změna LZS po roce 2028, která byla schválena v srpnu 2024. Avizuje stažení poskytovatelů v podobě Armády ČR a Policie ČR a vytvoření nové LZS v Karlovarském kraji. Podle námi provedeného experimentu, by byl Karlovarský kraj, v případě existence smluv mezinárodní spolupráce pro LZS, více pokryt LZS než jiné příhraniční části republiky (toto pokrytí by zajišťovaly základny Zwickau a Weiden) a vytvoření nové základny LZS v tomto kraji by tedy bylo nadbytečné. V současné chvíli však chybí řádné podklady pro konečnou finanční analýzu.

LITERATURA A POUŽITÉ INFORMAČNÍ ZDROJE

Monografie

1. BIEGE, B. (1994). *Luftrettung Geschichte, Technik, Organisation*. 1. Stumpf & Kossendey. ISBN 978-3-9231-2451-0.

2. FANĚK, O. (2023). *Operační řízení přednemocniční neodkladné péče*. Praha, MUDr. Ondřej Franěk, ISBN 978-80-908057-4-3.

3. FOJTÍK, Jakub. (2007). *Policejní vrtulníky*. Praha, Naše vojsko, ISBN 978-80-206-0870-3.

4. OSTER, R. (2008). *Luftrettung von Roland Oster*. 1. Stuttgart, Stuttgart, Motorbuch Verlag, ISBN 978-3-6130-2846-3.

5. PEŘAN, D. (2019). *Hems crew training manual: course manual*. Praha, Education and Training Centre, Prague Emergency Medical Services, ISBN 978-80-907428-2-6.
6. ŠÍN, R. – ŠŤOURAČ, P. et al. (2024) *Urgentní medicína*. Praha, Galén, ISBN 978-80-7492-706-5.
7. VILÁŠEK, J. – FIALA, M. – VONDRÁŠEK, D. (2023). *Integrovaný záchranný systém ČR na počátku 21. století. 2.* Praha, Karolinum, ISBN 978-80-246-2477-8.

Články v časopisech

1. HAVRLANT, P. – STANĚK, J. (2010). Historie a současnost letecké záchranné služby [online]. Praha, *Zdravotnický deník*. Dostupné z: http://www.zdn.cz/clanek/sestra/historiea - soucasnost-letecke-zachranne-sluzby-453256.
2. YAZER, M. – BECKETT, A. – CORLEY, J. et al. (2022). Tips, tricks, and thoughts on the future of prehospital blood transfusions. Online. *Transfusion*. 2022, roč. 62, č. S1. ISSN 0041-1132. DOI: https://doi.org/10.1111/trf.16955.

Internetové stránky

1. ADAC LUFTRETTUNG. *ADAC Luftrettung*. (2024). Online. Dostupné z: https://luftrettung.adac.de.
2. CAA. (2024) ÚŘAD PRO CIVILNÍ LETECTVÍ ČESKÉ REPUBLIKY. *Úřad pro civilní letectví*. Online. 2024. Dostupné z: https://www.caa.cz.
3. FRANĚK, O. (2023). 20 let Écéček v letecké záchrance ČR. Online. *ZACHRANNASLUZBA.CZ*. 2023, roč. 2023, č. 1, s. 1. Dostupné z: https://zachrannasluzba.cz/predstaveni-prvniho-ec-135-v-cr-dsa-16-1-2003/.
4. KRUTSKÝ, J. (1998). *Optimalizace letecké záchranné služby České republiky* [online]. Dostupné z: "http://www.apra.ipvz.cz/download.asp?docid=85"d.asp?docid=85.
5. NOVINKA V PÉČI: PODÁVÁNÍ PLNÉ KRVE PACIENTŮM PŘI ZÁSAZÍCH OSTRAVSKÉHO Modrá hvězda života. (2022). VRTULNÍKU LZS. Online. *Modrá hvězda života*. 2022. Dostupné z: https://modrahvezdazivota.cz/2022/08/10/novinka-v-peci-podavani-plne-krve-pacientum-pri-zasazich-ostravskeho-vrtulniku-lzs/.
6. ŠTĚPANYOVÁ, G. (2020) *Provoz letecké záchranné služby od roku 2021 bude o miliardu levnější*. Online. 2020. Dostupné také z: https://mzd.gov.cz/tiskove-centrum-mz/provoz-letecke-zachranne-sluzby-od-roku-2021-bude-o-miliardu-levnejsi/.

7. PETEROVÁ, B. (2021) *Leteckou záchrannou službu čeká v roce 2021 řada změn*. Online. 2021. Dostupné z: https://mzd.gov.cz/tiskove-centrum-mz/leteckou-zachrannou-sluzbu-ceka-v-roce-2021-rada-zmen/.
8. USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 24. července 2024 č. 511 k zabezpečení letecké záchranné služby po roce 2028. (2024). Dostupné z: https://www.odok.gov.cz/portal/zvlady/usneseni/2024/511/.
9. Zákon o zdravotnické záchranné službě. (2011). Zákon. Dostupné z: 374/2011 Sb., 1. 1. 2024, aktuální znění, informativní znění systému e-Sbírka (e-sbirka.cz).

Příspěvek byl zpracován v rámci Studentské grantové soutěže ČVUT SGS24/071/OHK5/1T/17.

ADDRESS & ©

PhDr. Pavel BÖHM, Ph.D., MSc., MBA
Katedra zdravotnických oborů a ochrany obyvatelstva
Fakulta biomedicínského inženýrství
České vysoké učení technické v Praze
Sportovců 2311, 272 01 Kladno
Czech Republic
Pavel.bohm@fbmi.cvut.cz
ORCID: 0000-0002-7239-4120

Bc. Tomáš HACAPERKA
Fakultní nemocnice v Motole
V Úvalu 84, 150 06 Praha 5
Czech Republic
tomas.hacaperka@fnmotol.cz
ORCID: 0009-0002-7172-7250

DOI: 10.36682/a_2025_1_2

DISINFORMATION AS A TOOL OF HYBRID ACTION: SECURITY, POLITICAL AND STRATEGIC CHALLENGES FOR THE EUROPEAN UNION

Dezinformácie ako nástroj hybridného pôsobenia: Bezpečnostné, politické a strategické výzvy pre Európsku úniu

Roman Bartolomej BOROVSKÝ

Liptovský Mikuláš, Slovak Republic

ABSTRACT: The article analyses disinformation as a key tool of hybrid warfare in the current deteriorating security situation and an environment marked by strategic uncertainty and instability, where the confrontation between democratic and authoritarian regimes is intensifying. In this context, disinformation has ceased to be merely a marginal phenomenon; instead, it has become a systematic tool for undermining democratic institutions, polarizing society, and eroding public trust. In this context, the European Union faces a growing need to safeguard the information space through coordinated measures at both domestic and international levels. The article draws on qualitative and comparative analyses of political strategies and documents, identifying the main weaknesses of current approaches and proposes strategic priorities, including the establishment of a legally binding framework, the strengthening of media literacy, the enhancement of technological capacities, and the promotion of global norm-setting. The article concludes by emphasizing that a successful response to disinformation requires not only technical solutions but, more importantly, educated, resilient, and critically minded citizens as the cornerstone of democratic society.

Key words: Disinformation – security threat – measures – cooperation – challenges

ABSTRAKT: Článok analyzuje dezinformácie ako kľúčový nástroj hybridného pôsobenia v súčasnej zhoršujúcej sa bezpečnostnej situácii a prostredí strategickej neistoty a nestability, v ktorom sa zintenzívňuje konfrontácia medzi demokratickými a autoritárskymi režimami. Dezinformácie prestali byť v tejto súvislosti len náhodným sprievodným javom, ale sa stali systematickým nástrojom na oslabovanie demokratických inštitúcií, polarizáciu spoločnosti a narušanie verejnej dôvery. Európska únia v tomto kontexte čelí rastúcej potrebe efektívnej ochrany informačného priestoru prostredníctvom koordinovaných opatrení na vnútornom aj medzinárodnom fóre. Článok sa opiera o kvalitatívnu a komparatívnu analýzu politických stratégií a dokumentov, pričom identifikuje hlavné slabiny aktuálnych prístupov a navrhuje strategické priority vrátane právne záväzného rámca, posilnenia mediálnej gramotnosti, technologickej kapacity a globálnej normotvorby. Autor v závere zdôrazňuje, že úspešný boj proti dezinformáciám si vyžaduje nielen technické riešenia, ale najmä vzdelaných, odolných a kriticky mysliacich občanov ako základ demokratickej spoločnosti.

Kľúčové slová: Dezinformácie – bezpečnostná hrozba – opatrenia – spolupráca – výzva

INTRODUCTION

The current global security environment, both worldwide and within individual regions is highly volatile, unstable, and tense. This is due to the unresolved or inadequately addressed nature of many global problems facing humanity, the intensifying competition among great powers, rivalry, the struggle for influence and resources, and the resulting international and internal conflicts, as well as attempts to revise the currently valid international order. Under the influence of these circumstances, a geopolitical transformation is gradually taking place, bringing serious negative consequences for democratic countries. Liberal democratic societies – especially in Europe – have recently been exposed to intensive hybrid influence from various state and non-state actors pursuing their own goals. They use various methods, techniques, and tools that go beyond the framework of conventional open military confrontation. Disinformation represents one such tool of hybrid warfare (Dušek, Kavan, 2024; Ivančík, 2025).

Disinformation is therefore no longer just some random by-product occurring in contemporary liberal society. On the contrary, in recent years, it has become a very systematically and deliberately used tool for influencing and manipulating citizens, aimed at destabilizing democratic societies, undermining public trust in democratic rules, principles, and institutions, and disrupting social cohesion (Dušek, Kavan, 2024; Ivančík, Nečas, 2022; Ivančík, 2024, Hajdúková, 2024). The dissemination of various disinformation, conspiracy theories, hoaxes, and fake news – primarily through social media and its platforms – has proven to be a cost-effective, difficult-to-attribute, and highly effective tool of hybrid influence (Pamment, 2020; Ivančík et al., 2024; Dušek, Kavan, 2024). From this perspective, disinformation constitutes a non-military asymmetric security threat, primarily directed against open, liberal, democratic countries (Flore et al., 2019; Ivančík, 2025, Ružbacká, 2024; Ivančík, 2024).

METHODOLOGY AND OBJECTIVE

From a methodological perspective, the article is based on content, qualitative, and comparative analyses of relevant sources, particularly scientific and specialized literature, works by domestic and foreign authors, official documents, research reports, as well as political and security strategies, concepts, and initiatives. In addition, an analytical-synthetic method is employed, emphasizing the logical connections between actors, activities, and responses within the fight against disinformation and its adverse consequences.

The objective of this article is to analyse disinformation as an asymmetric security threat to the EU in the current period of deteriorating security conditions in Europe and globally. Particular attention is devoted to the relationship between the political, security, economic, and other strategic goals of various actors, disinformation activities, external interference and influence, and the responses of the European Union (as a grouping of democratic states) expressed through adopted political, security, legislative, and other measures.

RESULTS AND DISCUSSION

In the current era of deepening contradictions and rivalry between democratic and authoritarian states, information operations and the manipulation of public discourse are gaining increasing importance. Within the framework of hybrid warfare, the spread of disinformation is one of the most effective tools for shaping the information space. The aim is to weaken the resilience of target societies, primarily democratic ones disrupt their functioning, undermine democratic processes and their foundational pillars, challenge the credibility of democratic institutions, and destabilise political systems without the use of military force (Pamment, 2020; Ivančík, Nečas, 2022).

Liberal democratic societies are inherently open, pluralistic, and grounded in trust—whether in institutions, media, science, or public participation. However, these very values, which constitute the foundations of liberal democracy, also become a source of vulnerability in the context of disinformation campaigns. Unlike authoritarian regimes, which exercise highly centralized control over the information space and restrict their citizens' access to a plurality of opinions, democratic societies uphold freedom of expression, privacy protection, and openness of information flows. Hybrid actors exploit these very features to pursue their own goals (Bridgman, 2025).

One of the vulnerabilities of democratic systems lies in their high degree of exposure to external interference. European elections, referendums, and other political processes are repeatedly targeted by information operations and manipulation efforts. These are designed both to reduce citizen participation in elections and to increase support for extremist and Eurosceptic actors. In the period preceding parliamentary elections in EU member states or elections to the European Parliament, numerous instances of foreign interference have been recorded, including the dissemination of various false narratives concerning migration, religion, sexual minorities, or the erosion of member states' sovereignty (EEAS, 2024b).

The information presented suggests that the vulnerability of liberal democratic societies is multi-layered, combining political openness, social polarization, technological imbalance,

and legislative inertia. Consequently, democratic states in today's information society are compelled to pursue common, comprehensive, systemic, and adaptive solutions that can both reflect the specifics of individual states while simultaneously establishing a common framework for resilience not only at the EU level but across the broader democratic world (Nieminen, 2024).

INTERNATIONAL COOPERATION IN THE FIGHT AGAINST DISINFORMATION

Given the growing intensity and complexity of disinformation campaigns, the European Union acknowledges that effective protection of democratic discourse and information sovereignty cannot be ensured solely at the level of individual states or institutions. Disinformation transcends geographical, linguistic, and institutional boundaries, representing a challenge that requires a broad and internationally coordinated response. In this context, EU cooperation with partners such as NATO, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), and the G7 group has been significantly strengthened. These actors play a crucial role in strategic communication, analysis, and enhancing resilience against hybrid threats.

In joint declarations from 2016, 2018, and 2023, NATO and the EU acknowledged the need for greater synergy in building resilience against hybrid attacks, including the spread of disinformation, public opinion manipulation, cyber operations, and psychological influence. In 2022, the updated Joint Declaration on EU-NATO Cooperation was signed, explicitly emphasizing the importance of shared situational awareness, early warning, and coordinated responses to information-related threats. This collaboration further extends to the exchange of analytical capabilities, exercises, and joint scenarios for countering hybrid campaigns (EPRS, 2023).

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), based in Helsinki, holds a unique position in the fight against disinformation. It serves as a platform for the exchange of knowledge, strategies, and recommendations among the EU, NATO, and their member states. The Hybrid CoE focuses on analysing hybrid techniques, methods, and tools, including disinformation operations, while also organizing education and training activities, and formulating recommendations for both political and expert audiences. The Centre also publishes specialized outputs such as Strategic Analyses, Research Reports, and Working Papers, which contribute to a deeper understanding of information influence and manipulation tools (Hybrid CoE, 2025).

The G7 Rapid Response Mechanism (G7 RRM), established in 2018 in response to foreign interference in democratic processes, also plays a significant role. The G7 RRM facilitates the coordinated exchange of threat information, the joint analysis of disinformation campaigns, and the development of strategic responses among G7 member states. The EU participates in this platform as a partner and collaborates on establishing norms and standards for protecting democratic institutions from disinformation (GoC, 2024).

Another crucial platform in the fight against disinformation is transatlantic cooperation between the EU and the USA, primarily promoted through the EU-US Trade and Technology Council. Within this council, a working group was established to combat foreign information manipulation, enhance platform transparency, and exchange knowledge on legislative measures in the fight against disinformation. The goal of this cooperation is to prevent cross-border influence by authoritarian regimes and safeguard the integrity of democratic processes in both regions (Ignatidou, 2024).

At the multilateral level, the United Nations also plays a vital role. On 22 September 2024, at the Summit of the Future in New York, the UN adopted the Global Digital Compact (GDC). This document was accepted as part of a broader document titled the Pact for the Future. With this adoption, the GDC became the official UN framework for global digital cooperation and artificial intelligence governance, aiming to foster an inclusive, open, sustainable, equitable, secure, and protected digital future for all. The GDC also outlines principles related to combating harmful content and protecting online discourse (UN, 2024). The EU actively participated in this process, thereby strengthening its position as a global norm-setter in the digital sphere.

These forms of international cooperation demonstrate that the fight against disinformation can no longer be viewed as an isolated national problem but rather a component of a broader geopolitical struggle for truth, trust, and information sovereignty. The aforementioned European, transatlantic, and global initiatives clearly show that the fight against disinformation inherently possesses an international dimension. To achieve success through these (and other) efforts and initiatives, it is necessary not only to share technical and analytical capacities but also to ensure the alignment o values among partners (Monsees, 2021).

IDENTIFICATION OF CRITICAL WEAKNESSES AND STRATEGIC PRIORITIES

Despite significant progress made by the European Union in combating disinformation, several critical weaknesses persist, limiting the effectiveness and consistency of adopted measures. One of the most significant is the fragmentation of approaches among member states.

Differences in political will, legislative preparedness, and available capacities create disparities in individual countries' ability to respond to information threats, thereby weakening the Union's collective resilience.

Another key weakness is the insufficient integration of educational, research, and civic initiatives into national security and strategic frameworks. Media and digital literacy often remain marginalized or are addressed on an ad hoc project basis without systemic embedding, which hinders the long-term sustainability of results. Furthermore, the technological sector – especially global platforms and artificial intelligence developers – continues to lack clear accountability obligations for content, generating an asymmetry between their influence and the regulatory reach of public institutions (Söderlund et al., 2024).

A persistent challenge is also the limited interoperability and data exchange among European institutions, member states, and partners. The absence of standardized procedures for collecting, categorizing, and analysing data on disinformation campaigns impedes the development of a robust and adaptive early warning ecosystem. Similarly, an effective methodology for evaluating the effectiveness of adopted measures is lacking, complicating evidence-based revision and improvement (EP, 2025).

For these reasons, it is crucial to identify and advance several strategic priorities. First and foremost, a truly unified European framework for combating disinformation needs to be established. This framework should be legally binding, institutionally embedded, and compatible with fundamental rights and freedoms. Furthermore, it is essential to strengthen analytical and detection capabilities, including artificial intelligence and digital forensics, while ensuring transparency and public oversight.

The third pillar of a strategic response should be the development of an integrated policy for media literacy and education. This policy should be systematically implemented from preschool age through lifelong learning and professional development. The fourth priority is the institutionalization of cooperation with civil society and academia, which provides the necessary expert background, contextualization, and legitimacy for these measures.

Finally, the EU should strengthen its role in establishing international standards and norms, not only within the UN, G7, and transatlantic cooperation but also in relation to technological corporations operating in the global digital space. Without the active involvement of these actors, genuine protection of the information space as a public good cannot be achieved (Bjola, Pamment, 2018; Flore et al., 2019; Nieminen, 2024; Söderlund et al., 2024; Dušek, 2024; Kavan, 2024; Ivančík, 2025).

CONCLUSION

In the coming years, disinformation is highly likely to become an even more sophisticated and harder-to-detect non-military asymmetric security threat for all democratic societies, particularly in Europe. The advent of artificial text and image generators, the development of multimodal models, micro-targeting using big data, as well as the globalization of digital platforms will contribute to a more complex environment where it will be increasingly difficult to distinguish truth from manipulation, and authentic from artificially created content. Simultaneously, it can be expected that geopolitical actors—both state and non-state—will increasingly utilize information operations as part of hybrid warfare, including interfering in elections, influence over foreign policy decisions, and the erosion of public trust in democratic institutions.

Therefore, it will be crucial for the EU and its member states to become strategically foresightful, technologically competent, and normatively consistent actors in the field of information security. The future of the fight against disinformation will require the integration of security, technological, and societal policies, investment in interdisciplinary research, the development of institutional capacities at both strategic and local levels, and, above all, the preservation of public trust as the most valuable asset of any democratic system.

The EU must prioritize transparency, democratic accountability, and inclusion in the creation of digital regulations, so as not to become a technological protectorate of large platforms or authoritarian powers. The goal must not be to control discourse, but to protect its integrity in an environment where truth is not imposed by force, but verified through dialogue, evidence, and societal reflection. In the long run, the most effective defence against disinformation is certainly not legal frameworks or technology, but primarily an educated, critically thinking, and resilient citizen who understands how media functions, recognizes the risks of manipulation, and can independently evaluate information. It is precisely upon such foundations that a resilient, democratic, and value-driven European Union of the 21st century needs to be built.

LITERATURE AND INFORMATION SOURCES USED

1. BJOLA, C., PAMMENT, J. (2018). The EU's struggle with countering disinformation: policy frameworks and external communication coordination. In *Journal of European Integration*, 2018, Vol. 40, No. 5, pp. 527543. ISSN 0703-6337. [online]. [cit. 2025-05-23]. Available at: <https://doi.org/10.1080/07036337.2018.1465411>.

2. DUŠEK, J. – KAVAN, Š. (2024). Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia,* 2024, Vol. 21, No. 1, pp. 7-25. [online]. [cit. 2025-05-20]. ISSN 2464-7217. DOI: 10.36682/a_2024_1_1.
3. DUŠEK, J. (2024). Česká dezinformační scéna: Vývoj a hlavní aktéři. In *Dušek, J. a kol.: Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v ére umělé inteligence a digitálních technologií.* České Budějovice: Vysoká škola evropských a regionálních studií, 2024, pp. 26-38. ISBN 978-80-7556-143-5.
4. EP. (2025). Working Document on Protecting European Democracy and our Values. In *European Parliament – Special Committee on the European Democracy Shield*, 2025. [online]. [cit. 2025-05-23]. Available at: <https://www.europarl.europa.eu/doceo/document/EUDS-DT-771957_EN.pdf>.
5. EPRS. (2023). The third EU-NATO joint declaration. In *European Parliamentary Research Service*, 2023. [online]. [cit. 2025-05-21]. Available at: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739333/EPRS_ATA(2023)739333_EN.pdf>.
6. FLORE, M. – BALAHUR, A. – PODAVINI, A. – VERILE, M. (2019). *Understanding Citizens' Vulnerabilities to Disinformation and Data-Driven Propaganda*. Luxembourg: Publications Office of the European Union, 2019. 94 p. ISBN 978-92-76-03320-2. [online]. [cit. 2025-05-20]. Available at: <https://doi.10.2760/919835>.
7. GoC. (2024). G7 Rapid Response Mechanism. In *Government of Canada*, 2024. [online]. [cit. 2025-05-21]. Available at: <https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html>.
8. HAJDÚKOVÁ, T. (2024). Zdroje informácií alebo dezinformácií. In *Auspicia*, 2024, Vol. 21, No. 1, pp. 37-49. ISSN 2464-7217. [online]. [cit. 2025-05-20]. DOI: 10.36682/a_2024_1_3
9. Hybrid CoE. (2025). Publications. In *Centre of Excellence for Countering Hybrid Threats*, 2025. [online]. [cit. 2025-05-21]. Available at: <https://www.hybridcoe.fi/all-publications/>.
10. IGNATIDOU, S. (2024). EU–US Cooperation on Tackling Disinformation. In *Chatham House – The Royal Institute of International Affairs*, 2024. [online]. [cit. 2025-05-21]. Available at: <https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf>.

11. IVANČÍK, R. (2024). Dezinformácie ako bezpečnostná hrozba šírená na internete. In *Auspicia*, 2024, Vol. 21, No. 1, pp. 26-36. ISSN 2464-7217. [online]. [cit. 2025-05-20]. DOI: 10.36682/a_2024_1_2
12. IVANČÍK, R. (2025). *Dezinformácie. Teoretické východiská ich skúmania*. Praha: Leges, 2025. 188 s. ISBN 978-80-7502-769-6.
13. IVANČÍK, R. – NEČAS, P. – ILAŠČÍKOVÁ, L. (2024). Attention as a Commodity in the World of Disinformation and Social Media. In *Entrepreneurship and Sustainability Issues*, 2024, Vol. 12, no. 2, p. 176-192. ISSN 2345-0282. [online]. [cit. 2025-05-20]. Available at: <https://doi.org/10.9770/k7393698996>.
14. KAVAN, Š. (2024). Dezinformace a bezpečnost v podmínkách České republiky a Evropské unie. In *Dušek, J. a kol.: Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v éře umělé inteligence a digitálních technologií.* České Budějovice: Vysoká škola evropských a regionálních studií, 2024, pp. 39-63. ISBN 978-80-7556-143-5.
15. MONSEES, L. (2021). Information disorder, fake news and the future of democracy. In *Globalizations*, 2021, Vol. 20, No. 1, pp. 123-140. ISSN 1474-774X. [online]. [cit. 2025-05-20]. Available at: <https://doi.org/10.1080/14747731.2021.1927470>.
16. NIEMINEN, H. (2024). Why Does Disinformation Spread in Liberal Democracies? The Relationship between Disinformation, Inequality, and the Media. In *Journal of the European Institute for Communication and Culture*, 2024, Vol. 31, No. 1, pp. 123-140. ISSN 1854-8377. [online]. [cit. 2025-05-20]. Available at: <https://doi.org/10.1080/13183222.2024.2311019>.
17. PAMMENT, J. (2020). The EU's Role in Fighting Disinformation: Taking Back the Initiative. In *Carnegie Europe*, 2020. [online]. [cit. 2025-05-20]. Available at: <https://carnegieeurope.eu/2020/06/22/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82124>.
18. RUŽBACKÁ, M. (2024). Dezinformácie ako hrozba pre spoločnosť a snahy o ich elimináciu. In *Auspicia*, 2024, Vol. 21, No. 1, pp. 50-58. ISSN 2464-7217. [online]. [cit. 2025-05-20]. DOI: 10.36682/a_2024_1_4
19. SÖDERLUND, K. – ENGSTRÖM, E. – HARESAMUDRAM, K. – LARSSON, S. – STRIMLING, P. (2024). Regulating high-reach AI: On transparency directions in the Digital Services Act. In *Internet Policy Review*, 2024, Vol. 13, č. 1. [online]. [cit. 2025-05-23]. Available at: <https://policyreview.info/articles/analysis/regulating-high-reach-ai>.
20. UN. (2024). Global Digital Compact. In *United Nations*, 2024. [online]. [cit. 2025-05-22]. Available at: <https://www.un.org/digital-emerging-technologies/global-digital-compact>.

ADDRESS & ©

JUDr. PhDr. Roman Bartolomej BOROVSKÝ
Akadémia ozbrojených síl generála M. R. Štefánika
Demänová 393
031 01 Liptovský Mikuláš
Slovenská republika
roman.borovsky@aos.sk

BEZPEČNOST • SAFETY

DOI: 10.36682/a_2025_1_3

DIGITAL TRACES AND DISINFORMATION IDENTIFICATION

Digitálne stopy a identifikácia dezinformácií

Branislav BELICA

Bratislava, Slovak Republic

ABSTRACT: The article examines the role of digital traces in identifying and countering the spread of disinformation in digital environments. In the context of increasing hybrid threats, digital traces serve as a crucial tool for analysing and regulating the dissemination of manipulative content. The study explores how digital traces help determine the origin of disinformation, distribution mechanisms, and the actors involved in disinformation campaigns. It underscores the pivotal role of social media and online platforms in spreading false information, exacerbating political polarization, and undermining trust in institutions. By analysing metadata, IP addresses, and domain registrations, analysts can uncover networks of propaganda websites linked to geopolitical interests. The study further addresses challenges posed by anonymization technologies and AI-generated content, which complicate detection processes. Combating disinformation requires a combination of digital forensics, fact-checking, and AI-driven data analysis. The conclusion emphasizes the necessity of interdisciplinary collaboration among security experts, data analysts, and representatives of the academic community to strengthen information security and safeguard society against manipulative narratives.

Key words: Security – hybrid threat – disinformation – digital traces

ABSTRAKT: Článok sa zaoberá úlohou digitálnych stôp v identifikácii a potláčaní šírenia dezinformácií v digitálnom priestore. V kontexte narastajúceho vplyvu hybridných hrozieb predstavujú digitálne stopy významný nástroj na analýzu a reguláciu šírenia manipulatívneho obsahu. Práca skúma, ako digitálne stopy umožňujú určovať pôvod dezinformácií, mechanizmy ich distribúcie a identifikovať aktérov zapojených do dezinformačných kampaní. Zdôrazňuje tiež, že sociálne siete a online platformy zohrávajú kľúčovú úlohu pri šírení nepravdivých informácií, čím prispievajú k politickej polarizácii a oslabeniu dôvery v inštitúcie. Prostredníctvom analýzy metadát, IP adries a registrácie domén môžu analytici odhaliť siete propagandistických webových stránok napojených na geopolitické záujmy. Článok sa taktiež venuje výzvam spojeným s anonymizačnými technológiami a obsahom generovaným umelou inteligenciou, ktoré komplikujú detekčné procesy. Na boj proti dezinformáciám je preto nevyhnutné využívať kombináciu forenzného skúmania digitálnych stôp, fact-checkingu a analýzy dát podporovanej umelou inteligenciou. V závere sa zdôrazňuje potreba interdisciplinárnej spolupráce medzi bezpečnostnými expertmi, dátovými analytikmi a zástupcami akademickej obce s cieľom posilniť informačnú bezpečnosť a chrániť spoločnosť pred manipulatívnymi naratívmi.

Kľúčové slová: Bezpečnosť – hybridná hrozba – dezinformácie – digitálne stopy

INTRODUCTION

In a digitally connected world, the dissemination of information occurs at an unprecedented speed and scale. Modern technologies, particularly the vast possibilities offered by online communication, have facilitated the massive sharing and spread of various types of content. However, these technologies have also created an environment susceptible to misuse. In recent years, there has been a significant increase in the spread of fake news, hoaxes, propaganda, and, most notably, disinformation, which has had a profoundly negative impact on contemporary society (Kavan, 2024; Hajdúková, 2024a; Dušek, 2024). Social networks and the internet have become the primary distribution channels for disinformation, which enable anonymous and rapid dissemination at minimal costs and with little direct accountability (Dušek – Kavan, 2024; Ivančík, 2024; Ružbacká, 2024).

Social and political polarization, combined with the anonymity of the online environment, creates conditions that allow for the effective manipulation of public opinion. Disinformation campaigns erode trust in state institutions, destabilize democratic processes, and exploit fundamental rights, such as freedom of speech, to undermine the very system that guarantees them. The consequences of disinformation vary widely, ranging from election interference and economic disruption to threats to public health and security. Like other countries, the Slovak Republic faces these challenges and is actively seeking ways to effectively combat the harmful effects of disinformation (Ivančík, 2025).

A key step in countering disinformation is the analysis of the actors that are responsible for its dissemination and understanding of their underlying motivations. Since disinformation spreaders can range from individuals to organized groups pursuing political or economic objectives, there is no universal strategy for their elimination. Therefore, it is crucial to develop mechanisms for identifying and monitoring disinformation campaigns (Zachar Kuchtová, 2024).

A promising approach in this field is the analysis of digital traces, which examines the information that internet users leave behind during their online activities. Digital traces can provide essential insights into the origins of disinformation, its distribution channels, and the mechanisms by which it spreads among the population. Traditional fact-checking methods often struggle to keep up with the speed at which disinformation spreads, highlighting the need for technologies such as artificial intelligence and machine learning to analyse large volumes of data. These methods can help identify behavioural patterns, pinpoint the sources of false information, and more effectively counter its dissemination.

Digital traces enable the identification of the creators of false information, the recognition of its disseminators, and the monitoring of its impact. Their analysis is essential for an effective defence against disinformation threats and the formulation of countermeasures. In the future, digital traces analysis is expected to play an increasingly important role in ensuring information integrity and protecting society from the adverse effects of disinformation.

METHODOLOGY AND OBJECTIVE

The aim of this study is to examine the role of digital traces in the process of identifying and analysing the spread of disinformation. It focuses on methods of tracking digital traces, their application in determining the origins of disinformation campaigns, and the challenges associated with their detection. Special attention is also given to anonymization technologies and artificial intelligence, which complicate the identification of manipulation sources in the digital space.

The study employs an analytical approach based on a review of available scientific literature and expert articles and incorporating case study comparisons and forensic analysis of digital traces. The research focuses on various forms of data traces that can be used to identify disinformation disseminators, while also considering the legal framework and technological challenges that affect their practical effectiveness. The insights gained may contribute to improving methodologies for monitoring digital traces and provide recommendations for implementing regulatory and security measures.

An essential aspect of this research is the examination of the dynamics of disinformation dissemination in the online environment and the potential for detecting it through the analysis of digital traces. In this context, the study explores the use of machine learning techniques and advanced algorithms for identifying disinformation patterns. Additionally, the research addresses ethical and legal issues related to the monitoring of digital traces, thereby opening a discussion on the balance between privacy protection and the need to safeguard information integrity.

RESULTS AND DISCUSSION

The research findings confirm that digital traces play a crucial role in identifying and mapping the spread of disinformation; however, their effectiveness is constrained by various factors. Analysis of IP addresses and metadata enables the tracking of disinformation distribution channels, yet the widespread use of anonymization tools significantly complicates the precise attribution of sources. Forensic analysis of digital traces suggests that many

disinformation websites are registered in jurisdiction with minimal regulatory oversight, making their monitoring and prosecution more challenging.

With the ongoing advancement and increasing use of artificial intelligence, the challenge posed by mass-produced manipulative content is also becoming more pronounced. Traditional fact-checking methods struggle to keep pace with the rapid generation of disinformation through advanced language models and deepfake technologies, highlighting the need for the development of novel detection and content analysis methods. The study indicates that combining traditional analytical tools with artificial intelligence and machine learning can substantially enhance the effectiveness of identifying disinformation campaigns.

Beyond technological barriers, legal constraints also pose challenges, as the protection of user privacy can create an imbalance between personal data protection and the need for effective digital space monitoring. Legislative frameworks vary across countries, providing different levels of protection and regulation, which complicates international cooperation in addressing the spread of disinformation.

Effective protection against disinformation therefore requires not only advanced analytical tools but also coordinated collaboration among security experts, data analysts, and representatives of the academic community. The research demonstrates that digital traces represent a vital tool for identifying disinformation operations, but their effectiveness depends on the ability to quickly respond to the evolving strategies of manipulative content disseminators. Moving forward, greater attention should be directed toward the development of regulatory frameworks that enable effective digital footprint monitoring while maintaining the principles of privacy protection and freedom of expression.

POSSIBILITIES FOR IDENTIFYING DISINFORMATION IN THE DIGITAL SPACE

To effectively identify disinformation, it is essential to understand its characteristic features. Only then can the process of locating, securing, and analysing digital footprints proceed efficiently. In this context, the European Parliament has therefore developed a guide titled “How to Spot Fake News” to enhance efforts against disinformation. According to this guide, approximately 85% of Europeans perceive "fake news" as a problem in their country, while 83% consider it a threat to democracy in general (Bentzen, 2019). These figures underscore the importance of disinformation identification, which occurs in multiple phases and steps.

The first step involves verifying content by assessing factual accuracy, potential bias, and any one-sided presentation in an article. Credible media outlets that adhere to ethical codes

ensure balanced reporting and provide space for various perspectives, whereas subjective opinions are typically confined to blogs and commentary. Fact-checking is conducted professionally by so-called fact-checkers, who are often journalists or members of various non-governmental organizations (Benham, 2019).

The second step involves verifying the source of the information. A key aspect is determining whether the source is a well-established and reputable media outlet. Most established media oranizations, whether in Slovakia, the Czech Republic, or elsewhere in the world, are publicly recognized and trusted. However, the internet also hosts various platforms with unclear origins, ownership, or funding. Such sources pose potential risks, particularly if their domains are registered abroad and their actual operators cannot be traced. Media outlets with questionable transparency and objectivity require a high degree of scrutiny. Consequently, analysts focus primarily on unfamiliar or obscure sources when identifying disinformation (Mintal et al., 2021).

Another crucial step in assessing information credibility is verifying both the author and the source of the content. Many disinformation websites do not disclose author names and instead cite foreign sources, obscure figures, or even fictional individuals and organizations. Conversely, an author may be publicly known but associated with the disinformation ecosystem, systematically spreading manipulative content. This often involves so-called commercial disinformers, whose primary goal is to disseminate misleading information for personal gain. A common tactic is also the exploitation of a well-known personality's name, where the individual has no actual connection to the content, but their credibility is leveraged to enhance the perceived legitimacy of false materials (Chudíková, Vojtek, 2020).

An important component of verification is the analysis of images and videos, which may be manipulated or presented out of context. Tools such as Google Lens, which allows users to trace the source of an image (Maurya, Kumar, Alimohammadi, 2023), or the InVID module, which helps detect edits and manipulations in multimedia content (Teyssou et al., 2017), can support this process. A common example includes the use of stock photos or images from past events that are presented as recent and linked to different circumstances. For instance, images of mass protests may be falsely labelled as demonstrations in another country or timeframe, creating a misleading impression of the situation (Ivančík, 2025).

A critical step in detecting disinformation is carefully evaluating its content. Most hoaxes and manipulative messages are designed to provoke an emotional response from the reader, thereby encouraging further dissemination. Sensational headlines that elicit fear, outrage, or other strong emotions are commonly used. A typical tactic of disinformation actors

is to create a false sense of urgency, often employing phrases such as "the truth has finally come out, share it before it is deleted". People who share such content may experience a sense of exclusivity, believing they have "uncovered hidden truths", and in doing so, unknowingly becoming part of the disinformation cycle (Martel et al., 2020).

One of the key warning signs is an overly dramatic or sensationalized story that appears too extraordinary to be true. A reliable method to verify such content is to check whether reputable media outlets are covering the topic. If an event is genuinely significant, credible sources that adhere to journalistic ethical standards will report on it. However, disinformation actors often deliberately undermine trust in established media, promoting the narrative that only they provide the "real" information. This approach helps them build a loyal base of followers who not only regularly consume their content but may also financially support them (Jost et al., 2019).

Many disinformation platforms, besides relying on undisclosed funding sources, receive financial contributions from regular readers while presenting themselves as independent media funded solely by their subscribers. This form of self-promotion aims to enhance perceived credibility while minimizing operational costs. Some websites even publish data on collected financial contributions, though the reported amounts may be inaccurate. A portion of these funds may originate directly from individuals or organizations that covertly manage these media outlets, thereby creating a misleading impression of widespread public support (Papadogiannakis et al., 2022).

The final step toward effectively detecting disinformation is continuous education in media literacy and critical thinking. Following credible websites and organizations dedicated to combating disinformation helps identify manipulative techniques and enhances the ability to distinguish between reliable and misleading information. In today’s digital landscape, developing critical content evaluation skills is essential to resist emotionally charged and one-sided claims that lack proper verification (Bentzen, 2019).

The European Digital Media Observatory (EDMO) also provides guidance for identifying disinformation. This EU-funded initiative functions as an independent platform bringing together fact-checkers, researchers, and other stakeholders engaged in countering disinformation (EC, 2024). Through its research, EDMO experts have outlined five fundamental steps that assist in recognizing disinformation and strengthening individual resilience against misleading narratives.

The first and most crucial step is the cultivation of critical thinking and emotional self-regulation. Disinformation is often crafted to provoke strong emotional reactions, which can

undermine rational judgment. Impulsive responses are a key factor contributing to the uncontrolled spread of hoaxes across the internet.

Another important step is verifying whether the same information has been reported by other sources. This principle aligns with recommendations from various credible sources, reinforcing its significance. Reliable news is typically covered by multiple reputable media outlets, whereas disinformation often originates from questionable or anonymous sources.

The third step involves using advanced search tools to verify images and videos. Visual content is frequently taken out of context or deliberately altered to mislead the public. Tools such as Google Lens or InVID can help determine whether an image has been manipulated or misrepresented by identifying its original source.

The fourth step emphasizes caution regarding sensationalism. Disinformation often relies on sensational headlines and implausible claims, adhering to a simple rule: if something appears too good or too bad to be true, it probably is not. Sensationalism and conspiracy narratives are designed to appeal to emotions and encourage people to accept information uncritically.

The fifth and final recommendation from EDMO is the use of fact-checking platforms to verify suspicious claims. If a person doubts the truthfulness of a certain piece of information, there is a high likelihood that fact-checking websites have already addressed it. Well-known platforms such as DW Fact Check, EUvsDisinfo, AFP Fact Check, and others provide detailed analyses and debunk misleading claims.

These guidelines establish a fundamental theoretical framework for identifying disinformation, focusing not only on detection but also on preventing its further spread. The outlined strategies can be applied not only in the user environment but also in analytical work (Casey, 2022).

IDENTIFICATION OF DISINFORMATION THROUGH DIGITAL TRACES

Digital traces emerge with every interaction in the online space, whether it involves sharing posts, creating fake accounts, or utilizing bots for automated content dissemination. Analysing these traces enables analysts and forensic experts to effectively map networks of disinformation actors and identify behavioural patterns. Various methods are employed to detect disinformation through digital traces, allowing for the tracking of its origin and the mechanisms used to spread false information:

IP address and metadata analysis – By examining IP addresses and associated metadata, it is possible to determine the geographical origin of disinformation and the connections

between individual accounts. This method helps identify coordinated campaigns and locate key distribution hubs of disinformation.

Web domain analysis – Information on domain registration and hosting services can reveal connections between websites that disseminate disinformation. Tracking data about domain owners and server operators can uncover the sources of false information.

Social media analysis – Monitoring interactions on social networks allows for the detection of disinformation dissemination patterns. Automated bots and fake accounts often rely on repetitive phrases and distribute content in a coordinated manner.

Detection and analysis of malicious content – Identifying suspicious links, harmful files, and phishing campaigns is crucial for uncovering disinformation strategies (Bokolo, Liu, 2024).

In practice, digital traces have been successfully utilized to identify multiple disinformation campaigns:

Russian interference in the 2016 U.S. elections – Digital analyses revealed that hundreds of fake social media accounts disseminated misleading information aimed at influencing voters.

Spread of conspiracy theories during the COVID-19 pandemic – Researchers traced digital footprints associated with false medical recommendations and identified the main sources of disinformation.

Manipulation of public opinion in Europe – Tracking IP addresses and domain registrations led to the discovery of propaganda website networks linked to various geopolitical interests (Mintál, 2021; Mirga, 2023).

While digital traces provide essential tools for identifying disinformation, several challenges complicate this process. A major issue is the use of anonymization technologies such as VPNs, Tor, and encrypted communication, which significantly hinder the tracking of disinformation actors. Another factor is automation and artificial intelligence. Advanced AI models can generate highly sophisticated fake news, making detection increasingly challenging. However, artificial intelligence is also an essential tool for identifying harmful content, fake accounts, and manipulation on social media. Technologies such as natural language processing and deep learning enable automated analysis of large volumes of data.

At the same time, generative AI-based tools can rapidly and efficiently produce original content based on user input. A particularly serious risk today is deepfake technology, which produces highly convincing but entirely fabricated or manipulated audiovisual content. Over time, distinguishing between reality and fiction is becoming increasingly difficult, particularly due to the advancement of machine learning mechanisms.

Finally, legal and ethical constraints represent another challenge. The collection, preservation, and analysis of digital traces must be conducted in compliance with personal data protection rules and applicable legal frameworks.

CONCLUSION

The use of digital traces in identifying disinformation constitutes a key element of modern information security and the fight against manipulation in the digital space. Digital traces have become an integral part of the online environment, and their application in detecting and analysing disinformation plays a crucial role in safeguarding the informational integrity of society.

In recent years, the spread of disinformation has emerged as a major challenge not only for state institutions but also for academia, technology companies, and independent research centres. Digital technologies facilitate the rapid dissemination of manipulative content, making its detection and elimination increasingly complex. In this context, the analysis of digital traces is gaining importance, providing opportunities to trace the sources of disinformation, map its dissemination, and assess its impact on the public.

The identification of disinformation through digital traces requires a multidisciplinary approach that combines various methods and techniques from cybersecurity, data analysis, media literacy, and the legal aspects of digital content regulation. Leveraging digital traces in the analysis of disinformation campaigns allows for a more effective and efficient response to disinformation threats while minimizing their impact on society.

Digital traces enable not only the detection of disinformation but also its attribution to specific actors. Although anonymization technologies and encrypted communication channels complicate the process of tracking disinformation sources, advanced analytical tools and artificial intelligence offer new opportunities for regulating its dissemination. In the future, it will be necessary to continuously refine methods for analysing digital traces to effectively uncover organized disinformation networks and their originators.

A significant factor in addressing the problem of disinformation is the legislative regulation of the digital space. Implementing stricter rules for online platforms, greater transparency in the funding and management of digital media, and accountability for parties involved in spreading false content can contribute to mitigating the negative consequences of disinformation campaigns. Collaboration among technology companies, academia, and government institutions will be essential for developing effective tools to counter disinformation.

Although digital traces serve as an effective means of tracking disinformation activities, it is crucial to ensure the protection of personal data and compliance with legal restrictions in their analysis. Balancing security measures with the safeguarding of privacy rights remains one of the primary challenges of the modern digital era.

In conclusion, digital traces play a significant role in the analysis and detection of disinformation in the online environment. The growing demand for protecting the digital space from the spread of manipulative content can be met through continuous technological advancements and the strengthening of interdisciplinary cooperation among security experts, data analysts, and representatives of academia.

LITERATURE AND INFORMATION SOURCES USED

1. BENHAM, J. (2019). Best practices for journalistic balance: Gatekeeping, imbalance and the Fake news. In *Journalism Practice.* [online]. [cit. 2025-02-21]. Available at: <https://www.researchgate.net/publication/335587904_Best_Practices_for_Journalistic_Balance_Gatekeeping_Imbalance_and_the_Fake_News_Era>.
2. BENTZEN, N. (2019). Ako odhaliť falošnú správu. [online]. [cit. 2025-02-19] Available at: <https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_SK.pdf>.
3. BOKOLO, B. G. – LIU, Q. (2024). Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. In *Electronics 2024*. [online]. [cit. 2025-02-27] Available at: <https://www.mdpi.com/2079-9292/13/9/1671>.
4. CASEY, K. (2022). Five fact-checking tips from disinformation experts. In *Horizon – The EU Research & Innovation Magazine,* 2022. [online]. [cit. 2025-02-25]. Available at: <https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine/five-fact-checking-tips-disinformation-experts>.
5. CHUDÍKOVÁ, A. – VOJTEK, D. (2020). Dezinformačné weby a ich vplyv na vnímanie reality. In *Otázky žurnalistiky.* [online]. [cit. 2025-02-22]. Available at: <https://fphil.uniba.sk/fileadmin/fif/katedry_pracoviska/kzur/Otazky_zurnalistiky/Archiv/vsetky_cele_cisla/OZ_1-2_2020.pdf>.
6. DUŠEK, J. (2024). Česká dezinformační scéna: Vývoj a hlavní aktéři. In *Dušek, J. a kol.: Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v ére umělé inteligence a digitálních technologií.* České Budějovice: Vysoká škola evropských a regionálních studií, 2024. s. 26-38. ISBN 978-80-7556-143-5.

7. DUŠEK, J. – KAVAN, Š. (2024). Dezinformace jako součást hybridních hrozeb – česko-slovenský pohled. In *Auspicia,* 2024, roč. 21, č. 1, s. 7-25. ISSN 2464-7217. DOI: 10.36682/a_2024_1_1.
8. EC. (2024). European Digital Media Observatory (EDMO). In *European Commission.* [online]. [cit. 2025-02-20]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>.
9. HAJDÚKOVÁ, T. (2024). Informačné vplyvy a informačné operácie z pohľadu recipientov bezpečnostnej praxe. In *Dušek, J. a kol.: Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v ére umělé inteligence a digitálních technologií.* České Budějovice: Vysoká škola evropských a regionálnych studií, 2024. s. 64-89. ISBN 978-80-7556-143-5.
10. IVANČÍK, R. (2024). Dezinformácie ako bezpečnostná hrozba šírená na internete. In *Auspicia,* 2024, roč. 21, č. 1, s. 26-36. ISSN 2464-7217. DOI: 10.36682/a_2024_1_2.
11. IVANČÍK, R. (2025). *Dezinformácie*. Teoretické východiská ich skúmania. Praha: Leges, 2025. 188 s. ISBN 978-80-7502-769-6.
12. JOST, J. T. – TUCKER, M. C. – POPESCU, V. A. (2019). Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. [online]. [cit. 2025-02-23]. Available at: <https://misinforeview.hks.harvard.edu/article/misinformation-in-action-fake-news-exposure-is-linked-to-lower-trust-in-media-higher-trust-in-government-when-your-side-is-in-power/>.
13. KAVAN, Š. (2024). Dezinformace a bezpečnost v podmínkách České republiky a Evropské unie. In *Dušek, J. a kol.: Dezinformace ve střední Evropě: vývoj, právní rámce a bezpečnostní dopady v ére umělé inteligence a digitálních technologií.* České Budějovice: Vysoká škola evropských a regionálnych studií, 2024. s. 39-63. ISBN 978-80-7556-143-5.
14. MARTEL, C. – PENNYCOOK, G. – RAND, D. G. (2020). Reliance on emotion promotes belief in fake news. In *Cognitive Research: Principles and Implications.* [online]. [cit. 2025-02-23]. Available at: <https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-020-00252-3>.
15. MAURYA, A. – KUMAR, A. – ALIMOHAMMADI, D. (2023). Application of Google Lens to Promote Information Services beyond the Traditional Techniques. In *Qualitative and Quantitative Methods in Libraries* [online]. [cit. 2025-02-23]. Available at:

<https://www.researchgate.net/publication/369659184_Application_of_Google_Lens_to_Promote_Information_Services_beyond_the_Traditional_Techniques>

16. MINTÁL, J. M. – KALMAN, M. – FABIÁN, K. (2021). *Hide and Seek in Slovakia: Utilizing Tracking Code Data to Uncover Untrustworthy Website Networks*. [online] [cit. 2025-02-22]. Available at: <https://arxiv.org/pdf/2109.01527>.
17. MIRGA, T. (2023). Šírenie dezinformácií a organizované ovplyvňovanie verejnej mienky: trolie farmy ako nástroj sociálnej a politickej manipulácie. In *ITlib. Informačné technológie a knižnice.* [online]. [cit. 2025-02-27] s. 42-55. Available at: <https://itlib.cvtisr.sk/clanky/sirenie-dezinformacii-a-organizovane-ovplyvnovanie-verejnej-mienky-trolie-farmy-ako-nastroj-socialnej-a-politickej-manipulacie/>.
18. PAPADOGIANNAKIS, E. – PAPADOPOULOS, P. – MARKATOS, E. P. – KOURTELLIS, N. (2022). *Who Funds Misinformation? A Systematic Analysis of the Ad-related Profit Routines of Fake News Sites*. [online]. [cit. 2025-02-24]. Available at: <https://arxiv.org/abs/2202.05079>.
19. RUŽBACKÁ, M. (2024). Dezinformácie ako hrozba pre spoločnosť a snahy o ich elimináciu. In *Auspicia,* 2024, roč. 21, č. 1, s. 50-58. ISSN 2464-7217. DOI: 10.36682/a_2024_1_4.
20. TEYSSOU, D. – LEUNG, J.-M. – APOSTOLIDIS, E. – APOSTOLIDIS, K. – APADOPOULOS, S. – ZAMPOGLOU, M. – PAPADOPOULOU, O. – MEZARIS, V. (2017). *The InVID Plug-in: Web Video Verification on the Browser*. [online]. [cit. 2025-02-23]. Available at: < https://dl.acm.org/doi/10.1145/3132384.3132387 >.
21. ZACHAR KUCHTOVÁ, M. (2024). Bezpečnostné riziká šírenia dezinformácií na internete prostredníctvom nástrojov umelej inteligencie. In *Auspicia,* 2024, roč. 21, č. 1, s. 72-83. ISSN 2464-7217. DOI: 10.36682/a_2024_1_6.

ADDRESS & ©

JUDr. Branislav BELICA
Akadémia Policajného zboru
Sklabinská 1
817 35 Bratislava
Slovenská republika
branislav.belica@akademiapz.sk

DOI: 10.36682/a_2025_1_4

CYBERCRIME AS A EUROPEAN CRIME

Počítačová kriminalita ako európsky zločin

Jaroslav KLÁTIK – Milada RAĎAŠOVÁ – Miroslav FELCAN

Banská Bystrica, Slovak Republic, České Budějovice, Czech Republic

ABSTRACT: The article addresses the issue of cybercrime, which is a topic of constant relevance and growing importance in today's age of information technology. Cybercrime encompasses both unlawful acts directed against computer systems and those committed through their use. The article outlines the primary aspects of cybercrime, provides an overview of its regulation at the level of the Council of Europe and the European Union. It takes a closer look at the sanctioning of natural and legal persons and compares the Slovak criminal legislation on cybercrimes with the corresponding regulatory framework at the level of the European Union.

Key words: Cybercrime – Non-cash instruments – Sanctions

ABSTRAKT: Článek se věnuje problematice počítačové kriminality, která je v dnešní době informačních technologií neustále aktuálním a důležitým tématem. Počítačová kriminalita zahrnuje jak protiprávní jednání směřující proti počítači, tak protiprávní jednání spáchané s použitím počítače. Článek odpovídá na otázku, jaké jsou hlavní aspekty počítačové kriminality, poskytuje přehled regulace počítačové kriminality na úrovni Rady Evropy a Evropské unie. Podrobněji se zabývá sankcionováním fyzických a právnických osob a porovnává slovenskou trestněprávní regulaci počítačové kriminality s trestněprávní regulací na úrovni Evropské unie.

Klíčová slova: Kyberkriminalita – nepeněžní prostředky – sankce

INTRODUCTION

At the end of the second decade of the 21st century, the defining features of the current era can undoubtedly be seen in strong cultural, economic and commercial globalization, the constant modernization of technology, and the increasing availability and speed of the transfer of information. Smartphones, electronic payment terminals, tablets and computers have become an everyday part of our lives; we spend considerable time on social networks and make full use of information technology in our daily activities. However, communication, work, payments, and other applications have also become a means that can be misused to harm individuals or

groups. For this reason, it was natural for legislators to respond to these developments by addressing serious offences through the legal definition of specific criminal acts.

The origins of cybercrime can be traced back to the 1960s and 1970s. Given the rapid development of information technology, it is natural that opportunities for committing harmful anti-social activity were significantly fewer in the past than they are today. At present, it is not unusual that the high level of development of computers, the Internet and other information technologies has made it more efficient and easier to commit non-cybercrime offences, while one of the problems in the investigation of such offences is the very anonymity of the perpetrators.

The negative phenomenon of cybercrime has become a society-wide problem, which has been tackled not only by national legislators, but also by institutions within the European Union, the Council of Europe, and, on a nearly global scale, the United Nations. The choice of this topic reflects the fact that cybercrime is an extremely serious and highly topical issue at national, European and international levels, which must be dealt with adequately. Finally, it should be emphasized that this is an interdisciplinary problem, involving experts from the fields of law, public administration, technology, business, finance and other areas.

This article relies on standardized search processes, utilizing the analysis and synthesis of available literature in a systematic, transparent, and reproducible manner.

In terms of structure, the article consists of successive parts entitled Primary Aspects of Cybercrime and its International Dimension, Regulation of Cybercrime at the level of the Council of Europe, a follow-up section entitled The Regulation of Cybercrime within the European Union, and finally a fourth section entitled Comparison of the Slovak Criminal Regulation of Cybercrime with the criminal regulation of cybercrime under Directive (EU) 2019/713 of the European Parliament and of the Council on Combating Fraud and Counterfeiting of Non-Cash Means of Payment.

The article raises questions in the introduction within the given issue and provides answers to them within the scope of the article.

Which primary cybercrime terminology can be considered the most relevant and accurate? What are the main historical aspects of cybercrime? What obligations related to the European Union form the basis of the Slovak Republic´s national criminal law on cybercrime? What are the penalties for cybercrime-related offences?

PRIMARY ASPECTS OF CYBERCRIME AND ITS INTERNATIONAL DIMENSION

According to the professional literature (Požár, 2015), the term computer crime refers to a group of crimes directed against computers, as well as a group of crimes that are committed by means of a computer. In general, these crimes can be defined as offences against the integrity, availability or confidentiality of computer systems. They also include crimes involving the use of information or telecommunications technology. A common definition of cybercrime describes it as the sum of all activities that lead to unauthorized access, manipulation, deletion or misuse of data in the form of so-called defrauding.

According to Kováč (Kováč, 2011), the term cybercrime encompasses the full spectrum of crimes that involve the use of computers, the Internet and other new technologies.

According to Musil (Musil, 2000), the term cybercrime refers to three basic groups of offences. The first group includes crimes in which the computer itself is the target. The second group comprises crimes in which the computer is used as a tool to commit the offence. The third group consists of crimes in which the computer serves only as a kind of ancillary or occasional means for carrying out criminal activity. The second concept, namely Internet crime, can be further illustrated through the expert opinion of Lošonczi and Meszároš (Lošonczi, Meszároš, 2016). According to these authors, Internet crime is a narrower term within the broader concept of cybercrime, referring to criminal activity in which the Internet connection itself can serve as a tool, a target, or a location for the commission of the offence. The authors further explain that such crimes encompass a wide range of unlawful activities, including theft, extortion, fraud, sexual offences, or other illegal acts. Internet crimes can be divided into offences targeting computer networks or devices and offences that are facilitated by computer networks or devices (Horváthová, 2005).

Another primary concept that we will pay attention to in the context of the primary conceptualization of cybercrime is the concept of "information and communication technologies". Pursuant to the provisions of Section 2 (1) of Act No. 95/2019 Coll. on Information Technologies in Public Administration and on Amendments and Additions to Certain Acts (hereinafter referred to as the "Act on Information Technologies in Public Administration"), the legislator defines the term information technology as a means or procedure, the purpose of which is to process data or information in electronic form. In this provision, information technology is classified as encompassing the information system itself, as well as infrastructure, information activities and electronic services. According to the expert opinion of Horváth, the term information and communication technologies includes both the term information technologies, comprising the hardware and software components of

computers, telephones, scanners, cameras and other devices enabling electronic access, electronic search, insertion, organization, and presentation of information, and communication technologies, which consists ofcommunication equipment through which information can be transmitted and the devices that make this information accessible. .

Another primary concept in the field of cybercrime in the form of an information system can be defined under the provision of Section 5 (l) of Act No. 18/2018 Coll. on the Protection of Personal Data and on Amendments and Additions to Certain Acts, according to which an "information system" is any ordered set of personal data of a centralized or decentralized nature, made available according to predetermined criteria.

Another key term in the field of cybercrime is the term "cyber security". This term is defined under the provision of Section 3 (g) of Act No. 69/2018 Coll. on Cyber Security and Amendments to Certain Acts, according to which cyber security denotes a state in which not only networks but also information systems are able, with a certain level of reliability, to withstand any interference in the form of an action that would pose a threat to the stored, transmitted or processed data in terms of their availability, confidentiality, authenticity or integrity.

The last term selected from the primary conceptual area of cybercrime is the term "cyberspace". Following the above-mentioned essential distinction between cyber and information security, incorporating the term cyberspace will also help to clarify the terminological boundaries of information security itself, which is not limited to information technology and computer networks (Marshall, Saulawa, 2015). It shall be noted that cybercrime is characterized by a high variability in the ways in which the relevant offence can be committed. Furthermore, due to the gradual development of information technologies, we are witnessing a continuous proliferation of new socially dangerous acts. These may involve not only the commission of previously regulated offences by new methods, but may also represent qualitatively new types of unlawful acts, the definition of which may not yet be specifically included in Act No. 300/2005 Coll., the Criminal Act. Consequently, the continuous qualitative and quantitative development can be considered as one of the characteristic features of computer crimes. Among the specific features of cybercrime is also its global reach, extending from the home (Brvnišťan, 2018).

In terms of cybercrime involving the Internet or other networks, it is also international in nature, with legal implications in the form of jurisdictional challenges and the need for cross-border cooperation (Pande, 2017). Other specific features of cybercrime are the possibility of decentralization, frequent anonymity, remote interaction, the potential to manipulate devices

and data at low cost. Additional characteristics are the sophistication of attacks, the possibility of automating criminal process, the ease of multiplying the harmful effect of initially small actions, the aggregation of profits through the theft of tiny decimal amounts from transactions, extensive access to information, continuous innovativeness and the limited possibilities for protection (Oops, 2010).

COUNCIL OF EUROPE REGULATION OF CYBERCRIME

As the Council of Europe is an international organization of European states, which is larger than the European Union in terms of its 46 member states, compared to the EU´s 27 member states (following the planned exit of the United Kingdom), we have decided to address the issue of cybercrime as a European-level crime, starting with the primary legislation of the Council of Europe.

The Council of Europe's primary international legislation in the field of cybercrime is undoubtedly the Council of Europe Convention on Cybercrime (Budapest Convention). Despite the fact that the Slovak Republic has been a member of the Council of Europe since 1993 and the Budapest Convention on Cybercrime was opened for signature as early as 2001, it was only ratified by the Slovak Republic in 2007, with the Convention coming into force for the Slovak Republic on 1 May 2008. Given that the Convention on Cybercrime enshrines extensive legal aspects of cybercrime in the European area, we have decided to focus on the issue of the General Principles of International Cooperation.

The general principles of international cooperation in the Convention on Cybercrime are regulated through Chapter III entitled International Cooperation, Section 1, General Principles on International Cooperation, Titles 1 to 4. The principle of the necessity of adopting a set of indispensable legislative and other measures is expressed in Article 25, Section 2 of the Convention on Cybercrime.

The principle of sending a request for legal aid by means of rapid communication is established in Article 25, Section 3 of the Convention. Subsequently, in the framework of the provisions of Article 25, Sections 4 and 5 of the Convention, the Contracting Parties address the conditions of legal assistance, which derive from the requested party, from existing legal assistance treaties, as well as the principle of conditioning legal assistance on the existence of mutual criminality. This requirement is considered fulfilled even if the legal system of the requested party classifies, designates and characterizes the unlawful conduct differently from that of the requesting party. Finally, under the provisions of Article 26, Sections 1 and 2 of the Convention, the Contracting Parties discuss the provision of spontaneous assistance during

investigations, as well as the principle of conditioning the use of such information on, for example, confidentiality of the information or other requirements. As mentioned above, the Convention on Cybercrime entered into force for the Slovak Republic on 1 May 2008 and all obligations imposed by the Convention in the framework of criminal law have been duly transposed and incorporated into the national legal order of the Slovak Republic.

The offence of falsification of computer data is enshrined in Article 7 of the Convention, under which the Contracting Parties are obliged to take legislative and other measures to criminalize the intentional and unauthorized insertion, alteration, deletion of computer data or prevention of access to such data. Notably the provision allows individual Contracting Parties to condition the criminality of these unlawful acts on the presence of fraudulent or dishonest intent. The acts of intentional and unauthorized insertion, alteration, deletion, or prevention of access to computer data are embedded in the Slovak legal system through several provisions: namely, § 247a of the Criminal Code, concerning unauthorized interference with a computer system; § 247b, concerning unauthorized interference with computer data; and § 247c, which implements Article 7 of the Convention on Cybercrime.

The offence of computer fraud is addressed in the provisions of Article 8 (a) and (b) of the Convention on Cybercrime, in which the Contracting Parties outline the obligation of individual Contracting Parties to adopt adequate legislative or other measures establishing as a criminal offence the intentional causing of property damage to another person through the insertion, alteration, deletion of computer data, or by preventing access to such data, as well as actual interference with a computer system. Computer fraud is characterized by a fraudulent or dishonest intent to obtain a pecuniary advantage. Furthermore, the Contracting Parties, through Articles 10, Sections 1 and 2, agreed that all Contracting Parties are obliged to take the necessary legislative or other measures to ensure that the conduct of intentional offences involving the infringement of both copyright and related rights by means of a computer system are addressed and incorporated into national law.

Within the above provision, it is significant that the Contracting Parties do not explicitly enumerate the infringements in the wording of the Convention that fall under the offences of infringement of copyright and related rights. Instead, they refer to the Berne Convention for the Protection of Literary and Artistic Works, the Agreements on Trade-Related Aspects of Intellectual Property Rights and the World Intellectual Property Organization treaties relating to copyright and trade-related aspects of intellectual property rights, and the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations. For example, the criminal aspects of copyright and related rights infringement

offences referred to in Article 10 of the Convention on Cybercrime, referred to above, are addressed in Article 61 of the Agreement on Trade-Related Aspects of Intellectual L 336/214 Rights, according to which Members are required to provide minimum national legal measures to establish criminal proceedings and penalties for the intentional counterfeiting of trademarks and copyright infringement in the commercial sphere. It is clear from the foregoing that the minimum legal standard of criminal protection under the Agreement in question is defined only in general terms.

REGULATING CYBERCRIME IN THE EUROPEAN UNION

The institutional protection of cyberspace and the fight against cybercrime within the European Union represents a structured network of interconnected relationships, encompassing cooperation both among the main institutions of the Union and with smaller or less prominent bodies. Among the numerous institutions, organizations and agencies, particular attention is given to the primary roles of the European Commission, the European Council, the European Network and Information Security Agency (ENISA) and the primary role of the European Cybercrime Centre (EC3). Regarding the question "What is the role of the European Commission in the fight against cybercrime?" Mogherini and Kunasek argue that the European Union fulfils its role in cybersecurity by focusing on three main objectives, which are the proactive mainstreaming key cybersecurity issues into the European Union's various policies, enhancing cybersecurity capabilities and cooperation so as to ensure its full development evenly within each Member State, and striving to position the EU among the world's most advanced actors in terms of technological, administrative, personnel, and information preparedness. In addition to the above-mentioned tasks, it is clear that the European Commission, as the European Union's highest executive institution, performs its role in the field of cybersecurity by proposing European Union legislative acts to the European Parliament and the Council of the European Union, as well as by providing assistance to individual Member States in implementing the relevant legislation, and by managing and allocating financial resources to promote innovative solutions for the protection of cyberspace.

The European Commission, with its supervisory powers, together with the European Court of Justice, ensures compliance with European legislation and, alongside the European External Action Service, represents the views of the European Union externally on these issues (Megherini, Kunasek, 2018). In addition to the most important legislative documents in the field of cybercrime regulation within the European Union, namely Directive (EU) 2013/40 of the European Parliament and of the Council on attacks against information systems and

Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment, reference may also be made to Directive (EU) 2016/1148 on measures to ensure a high common level of network and information systems security in the Union, Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (which repealed Directive 1999/93/EC), as well as Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on the cybersecurity certification of information and communication technologies, repealing Regulation (EU) No. 526/2013, commonly known as the Cybersecurity Act.

The primary role of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, which repealed Directive 1999/93/EC, is defined in Article 1, letters (a) to (c). According to these provisions, the main objective of the Regulation is to ensure the functioning of the EU internal market (Article 1 (2) (a) to (e) of Directive (EU) 2016/1148 on measures to ensure a high common level of security of network and information systems across the Union), with a particular focus on the issue of an adequate level of security not only for trust services, but also for the issue of an adequate level of security of the means used for electronic identification. To achieve this objective, the Regulation sets out the conditions for the recognition of electronic identification means for natural and legal persons, the rules for trust services, such as electronic transactions, and the legal framework for electronic signatures, electronic time stamps and electronic seals, electronic documents, etc.

Furthermore, particular attention should be paid to the primary role of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cyber Security) and on the certification of cybersecurity of information and communication technologies, repealing Regulation (EU) No. 526/2013, which, As mentioned above, this act is also referred to as the Cybersecurity Act, and which, together with Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud, counterfeiting and forgery of non-cash means of payment, represents one of the most recent legislative efforts of the European Union in the field of cybersecurity. Pursuant to the provisions of Article 1, Section 1 a) and b) of the Regulation (EU) 2019/881 of the European Parliament and of the Council, its main task, as in the case of the above-mentioned legislative documents, is to ensure the proper functioning of the internal market. In addition, the European Union, through this Regulation, aims to achieve a high level of cybersecurity, resilience and trust (Article 1 Section 1 a) and b) of Regulation (EU) No. 2019/881 of the European Parliament and of the Council on ENISA

(the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification, repealing Regulation (EU) No. 526/2013). The tasks in question are to be ensured through the establishment of objectives and tasks, as well as specific organizational aspects relating to the European Union Agency for Cybersecurity, and through the establishment of a framework for the implementation of European systems relating to cybersecurity certification (Article 1, a) to c) of the Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC).

When considering the choice of one of the primary European legislations regulating the issue of cybercrime for the purposes of comparison with Slovak legislation, we took into account the fact that, in the case of older European legislation, although equally important, directives have already been in force long enough to allow for their proper transposition into the national legislation of individual Member States. By contrast, regulations, which are directly applicable according to Article 288 of the Treaty on the Functioning of the European Union, do not require such a transposition period. The adoption by the EU Member States of the necessary legislative and other measures to criminalize unlawful access to information systems is laid down in the provisions of Article 3 of Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems (as well as Article 20 of Directive (EU) No. 2019/713 of the European Parliament and of the Council on combating fraud, counterfeiting and alteration of non-cash means of payment). These provisions oblige Member States to take appropriate measures to ensure that the intentional and unlawful act of gaining access either to the whole information system or only in part, is punishable when such access is achieved by breaching a security measure. This obligation applies in particular where the circumstances cannot be considered minor (Article 3 of the Directive (EU) No. 2013/40 of the European Parliament and of the Council on attacks against information systems, replacing Council Framework Decision 2005/222/JHA).

Since, according to Article 16 of the Directive on attacks against information systems, the Directive of 12 August 2013 was to be transposed within a two-year period, i.e., by 4 September 2015, it is natural that the relevant obligation to criminalize unlawful access to information systems is fulfilled by the provisions of Section 247(1) to (3) of the Criminal Code,. According to these provisions, the basic offence of unauthorized access to a computer system consists in overcoming a security measure and thereby gaining access to either the entire computer system or only to part of it. In particular, under the provisions of Article 4 of Directive (EU) 2013/40 of the European Parliament and of the Council on attacks against information

systems, Member States were required, by 4 September 2015, to adopt the necessary legislative and other measures to ensure that the intentional act of seriously hindering the proper functioning of an information system, as well as the actual act of ensuring the interruption of the proper functioning of an information system, is legislated and sanctioned as a criminal offence, whereby the actual obstruction or interruption of the functioning of the information system may be carried out by means of the insertion or transmission of data, or by damaging, deleting, altering, deteriorating, suppressing, as well as preventing access to computer data without proper authorization, in cases that cannot be classified as minor.

SANCTIONING OF NATURAL AND LEGAL PERSONS

Cyber theft is linked to the financial opportunities that arise from internet use. Cyber theft also encompasses digital piracy, which is seen as the most common form of cyber theft among young adults. In fact, digital or software piracy is frequently used as a standard indicator of cybercrime in criminological research (Onwuadiamu, 2025).

The obligation of individual Member States to adopt adequate legislative measures ensuring that the offences defined in Articles 3 to 8 of the Directive are punishable by penalties of a proportionate, effective and dissuasive nature is laid down in the provisions of Article 9 (1) to (6), Article 8 (2) of Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and forgery, replacing Council Framework Decision 2001/413/JHA. In Articles 2 to 5, the European legislator sets out the minimum upper limits of criminal penalties for the commission of computer-related offences involving non-cash means of payment as basic offence, while Article 6 addresses the minimum upper limits of criminal penalties for certain qualifying offences. The European legislator envisages three categories of minimum custodial sentences for the aforementioned computer-related offences concerning non-cash means of payment within the scope of basic offences.

In the first category, Article 9, Section 3 of the Directive requires that the offences referred to in Article 4 c) and d), as well as those in Article 5 c) and d), must be punishable by a custodial sentence with a minimum upper limit of at least one year.

Consequently, the European legislator, in Article 9(2) and, where applicable, Article 9(5), lays down the obligation to adopt adequate legislative measures to ensure that the offences referred to in Article 3, Article 4(a) and (b), Article 5(a) and (b) and Article 7 of the Directive are punishable under the national law of the Member States by custodial sentences, with a minimum upper limit of two years. Regarding the question of which provision and for which

offences the Directive on combating fraud, counterfeiting and alteration of non-cash means of payment establishes a minimum upper penalty of three years' imprisonment, the answer is Article 9(4). In this provision, the European legislator sets the three-year custodial penalty for the offences referred to in Article 6 of the Directive in question (Article 9, Sections 2 and 5 of Directive (EU) 2019/713 of the European Parliament and of the Council on combating fraud, counterfeiting and alteration of non-cash means of payment, replacing Council Framework Decision 2001/413/JHA).

COMPARISON OF SLOVAK CRIMINAL LEGISLATION ON COMPUTER CRIMES WITH THE CRIMINAL LEGISLATION ON COMPUTER CRIMES UNDER DIRECTIVE (EU) 2019/713 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON COMBATING FRAUD, COUNTERFEITING AND FORGERY OF NON-CASH MEANS OF PAYMENT

In the light of European Union regulations, the European legislator does not provide for a transposition period into the national law of the individual Member States, as is the case with directives. Instead, regulations are directly applicable twenty days after their publication in the Official Journal of the European Union. Nevertheless, despite the prohibition on transposition, Member States may adopt legislation to implement certain provisions of a regulation. For this reason, we have also excluded from the selection of European legislation for the purpose of comparison some of the most important European Union regulations (Walliman, 2011), such as Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, repealing Directive 1999/93/EC, as well as the new Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cyber Security) (Porta, Keating, 2008) and on the certification of cybersecurity of information and communication technologies, repealing Regulation (EU) No. 526/2013, despite the fact that some of its provisions have only been in force since 28 June 2021 (Bhattacherjee, 2012).

Consequently, when comparing the provisions of Articles 4 (criminal offences related to the fraudulent use of tangible non-cash payment instruments) and 5 (criminal offences related to the fraudulent use of intangible non-cash payment instruments) of the Directive in question, concerning the obligation of the EU Member States to adopt adequate legislative measures to ensure that these offences related to the fraudulent use of both tangible and intangible non-cash payment instruments is enshrined in national legislation as a criminal offence, we find in the Slovak criminal law, as in the case of Article 3 mentioned above, the possibility of subsuming

the facts of the provisions in question under Section 219 of the Criminal Code, which defines the criminal act of unauthorized production and use of a means of payment.

However, as in Article 3 (fraudulent use of non-cash payment instruments), there is an incomplete interpretation of non-cash payment instruments, the concept of which is not formally recognized in the Criminal Code, but in relation to which the Slovak legislator refers in the above-mentioned provision of Article 219, Section 1) as means of payment, electronic money and payment and telephone cards, or as another object capable of performing such a function. It follows from the above that, although the Slovak criminal law does not distinguish between tangible and intangible non-cash means of payment, and does not formally recognize the concept of non-cash means of payment as such, it does recognize the concept of means of payment, under which all their subdivisions may be included. Therefore, theft, fraudulent forgery, counterfeiting, imitation, unlawful possession, unlawful appropriation, imitation and unlawful acquisition or circulation of a tangible non-cash means of payment, as well as unlawful acquisition, fraudulent imitation, counterfeiting and forgery, as well as the unlawful acquisition, possession and unlawful putting into circulation of an intangible non-cash means of payment, can also be subsumed under the relevant provision of Section 219 of the Criminal Code. However, in the case of Article 5 a) (criminal offences related to the fraudulent use of intangible non-cash payment instruments), which requires Member States to ensure that the conduct referred to therein is punishable when committed intentionally, it is necessary to pay particular attention to the European legislator's reference to Articles 3 (unlawful access to information systems) and 6 (unlawful data collection) of the Directive on attacks against information systems.

Since, in the light of the obligations of Member States to take measures ensuring that the conduct referred to in Articles 4, 5 and 6 of the Directive on combating fraud, counterfeiting and alteration of non-cash means of payment is punishable when committed intentionally, the provision of Article 219 of the Criminal Code is largely in line with these obligations, we considered it relevant to assess its compatibility also with the requirements of Article 7 (instruments used to commit offences) of the Directive, which concerns the instruments used to commit the offences set out in Articles 4 a) and b), 5 a) and b) and 6 of the Directive. We found that the provision of Article 219, Section 2 of the Criminal Code, which also provides for a penalty of up to three years' imprisonment for the offence in question, also meets the requirement for imposing penalties in Article 9 (penalties for individuals), Section 5 of the Directive, according to which the upper limit of imprisonment in this case should be at least two years, and therefore appears to be sufficient.

CONCLUSION

Using scientific research methods, the article provides answers to the questions raised. In the light of digitalization and smart technologies, we can observe not only the positive aspects of this modern era, but increasingly there is a need to address the negative phenomena associated with it. Computer crime, as one such negative phenomena, has become a society-wide problem, and the need to address it has arisen not only at the national level, but also at the level of the EU Member States as well as at the level of UN Member States.

The term cybercrime has been defined by the professional community under different definitions, but the essential characteristics remain the same. In general terms, cybercrime can be understood as the full spectrum of crimes involving the use of computers, the Internet and, nowadays, rapidly evolving new technologies.

LITERATURE AND INFORMATION SOURCES USED

1. BENEDEKOVÁ, D. (2016). Právna úprava počítačovej kriminality. In Bhattacherjee, A. 2012. *Social science research: Principles, methods and practices*. Tampa: University of South Florida, 2012. 159 s. ISBN 978-1475146127.

2. GREGUŠ, L. (2013). Obete kybernetickej kriminality (Niektoré trestnoprávne aspekty obetí kriminality prostredia informačných sietí). In *Obete kriminality*. Bratislava: Paneurópska vysoká škola, 2013. s. 54–68. ISBN 978-80-8153-015-9.

3. HENNYEYOVA, K. – GERHÁTOVÁ, G. (2016). Bezpečnostné aspekty spracovania informácií. In *International scientific days 2016*. Nitra: SPU, 2016. s. 77-84. ISBN 978-80-552-1505-1.

4. HORVÁTHOVÁ, Z. (2005). Využitie informačných a komunikačných technológií vo vzdelávaní. In Jandová R. a kol. *Příprava učitelů a aktuální proměny v základním vzdělávání*. České Budějovice: Jihočeská univerzita v Českých Budějovicích, 2005. s. 84–86. ISBN 80-7040-789-1.

5. IONITA, G. I. – BURDA, S. D. (2009). International and regional organizations with attributes and preoccupations in preventing and fighting against cybercrime and their main accomplishments. In *Journal of information systems & operations management*. 2009, roč. 5, č. 2, s. 1-10. ISSN 1843-4711.

6. LOŠONCZI, P. – MESÁROŠ, M. (2016). Východiská pre bezpečnosť detí v prostredí internetu. Ostrowiec: College of Business and Entrepreneurship. In *Acta Scientifica Academiae Ostroviensis.* 2016, roč. 7, č. 1. s. 163–173. ISSN 2300-1739.

7. MADRIAZA, P. a kol. (2018). *6th International Report on Crime Prevention and Community Safety: Preventing Cybercrime*. Montreal: International Centre for the Prevention of Crime, 2018. 165 s. ISBN 978-2-924939-01-7.

8. MARKOVÁ, V. (2018). Súčasný stav a východiská počítačovej kriminality v právním poriadku Slovenskej republiky. In *Aktuálne výzvy prevencie počítačovej kriminality*. Bratislava: Akadémia Policajného zboru v Bratislave, 2018. s. 106-126. ISBN 978-80-8054-774-5.

9. MARSHALL, J. B. – SAULAWA, M. A. (2015). *CYBER-ATTACKS: THE LEGAL RESPONSE*. Baijnath: Universal Multidisciplinary Research Institute. 2015, roč. 1, č. 2, s. 1–18. ISSN 2394-2622.

10. MOGHERINI, F. – KUNASEK, F. (2018). *Handbook on Cybersecurity The Common Security and Defence Policy of the European Union*. Vienna: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. 264 s. ISBN 978-92-95201-10-1.

11. MUSIL, S. (2000). *Počítačová kriminalita*. Praha: Institut pro kriminologii a sociální prevenci, 2000. 299 s. ISBN 80-86008-80-0.

12. NGO, F. T. – PATERNOSTER, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. Sarasota: University of South Florida Sarasota-Manatee. In: *International Journal of Cyber Criminology*. 2011, roč. 5, č. 1, s. 773-793. ISSN 0974-2891.

13. ONWUADIAMU, G. Cybercrime in criminology, A systematic review of criminological theories, methods and concepts. In: *Journal of Economic* Criminology 8 2025. ISSN 2949-7914.

14. PANDE, J. (2017). *Introduction to Cyber Security*. Haldwani: Uttarakhand Open University. 2017. 152 s. ISBN: 978-93-84813-96-3.

15. PORTA, D. D. – KEATING, M. (2008). *Approaches and Methodologies in the Social Sciences*. Cambridge: Cambridge University press, 2008. 383 s. ISBN 978-0-521-88322-1.

16. POŽÁR, J. (2015). Vybrané trendy kybernetické kriminality. In *Acta Informatica Pragensia*. 2015, roč. 4, č. 3, s. 336–348. ISSN 1805-4951.

17. SHARMA, Y. a kol. (2015). *Cyber Crimes*. Kota: Vardhaman Mahaveer Open University. 2015. 278 s. ISBN-978-81-8496-579-7.

18. WALLIMAN, N. (2011). *Research methods the basics*. Abingdon: Routledge, 2011. 205 s. ISBN 978-0-415-48994-2.

Legislation

1. *Act No. 18/2018* Coll. on the protection of personal data and on amending and supplementing certain acts.

2. *Act No. 45/2011* Coll. on Critical Infrastructure.

3. *Act No. 69/2018* Coll. on Cyber Security and amending certain Acts.

4. *Act No. 300/2005* Coll., the Criminal Act.

5. *Act No. 583/2008* Coll. on the Prevention of Crime and Other Anti-Social Activities and on Amendments and Additions to Certain Acts.

6. *Act No. 91/2016* Coll. on Criminal Liability of Legal Persons and on Amendments and Additions to Certain Acts.

7. *Act No. 95/2019* Coll. on Information Technologies in Public Administration and on Amendments and Additions to Certain Acts.

8. *Directive (EU) 2013/40* of the European Parliament and of the Council on attacks against information systems, replacing Council Framework Decision 2005/222/JHA.

9. *Directive (EU) 2016/1148* on measures to ensure a high common level of network and information systems security in the Union.

10. *Directive (EU) 2019/713* of the European Parliament and of the Council on combating fraud, counterfeiting and forgery of non-cash means of payment.

11. *Regulation (EU) 2019/881* of the European Parliament and of the Council on ENISA (European Union Agency for CyberSecurity) and on the certification of cybersecurity of information and communication technologies and repealing Regulation (EU) No. 526/2013 (CybersecurityAct).

12. *Regulation (EU) No. 910/2014* of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

13. Report from the Commission to the European Parliament and the Council on the assessment of theextent to which Member States have taken the measures necessary to couly with *Directive 2013/40/EU* on attacks against informatic systems replacing Council Framework Decision 2005/222/JHA.

14. *Slovak Republic Cyber Security Concept 2015-2020*.

15. *United Nations Manual on the Prevention and Control of Cybercrime*.

ADDRESS & ©

prof. JUDr. Jaroslav KLÁTIK, PhD.
Katedra trestného práva, kriminológie, kriminalistiky a forenzných disciplín
Právnická fakulta UMB v Banskej Bystrici
Univerzita Mateja Bela v Banskej Bystrici
Komenského 20
974 01 Banská Bystrica
jaroslav.klatik@umb.sk

JUDr. Milada RAĎAŠOVÁ
Katedra trestného práva, kriminológie, kriminalistiky a forenzných disciplín
Právnická fakulta UMB v Banskej Bystrici
Univerzita Mateja Bela v Banskej Bystrici
Komenského 20
974 01 Banská Bystrica
milada.radas@gmail.com

doc. JUDr. Miroslav FELCAN, PhD., LL.M., DSc., dr. h. c.
Katedra právních oborů a bezpečnostních studií
Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 1632/5b,
370 01 České Budějovice
Czech Republic
felcan@vsers.cz

VEŘEJNÁ SPRÁVA, ŘÍZENÍ • PUBLIC ADMINISTRATION, MANAGEMENT

DOI: 10.36682/a_2025_1_5

EFFICIENCY OF ADMINISTRATIVE PROCEEDINGS IN THE FIELD OF OFFENSES IN SLOVAKIA

Katarína LIPTÁKOVÁ – Katarína DROCÁROVÁ

Banská Bystrica, Slovak Republic

ABSTRACT: Offenses represent unlawful actions and undesirable antisocial behavior. The issue of efficiency in administrative proceedings regarding offences has come to the forefront in Slovakia due to an amendment to the Criminal Code, effective as of 6 August 2024. The efficiency of administrative proceedings is influenced by various factors, primarily the quality of offence investigation, the professional competence of state employees, and staff number. This study quantitatively and qualitatively examines these factors using data from two district offices in the years 2021–2023. The results confirm the validity and justification of our assumptions.

Key words: administrative proceedings – offenses – efficiency

ABSTRAKT: Přestupky představují protiprávní jednání a nežádoucí protispolečenské chování. Otázka efektivity správního řízení o přestupcích se na Slovensku dostala do popředí v důsledku novely trestního zákoníku účinné od 6. srpna 2024. Efektivitu správního řízení ovlivňují různé faktory, především kvalita vyšetřování přestupků, odborná způsobilost státních zaměstnanců a počet zaměstnanců. Tato studie tyto faktory kvantitativně i kvalitativně ověřuje na základě údajů ze dvou okresních úřadů v letech 2021-2023. Výsledky potvrzují platnost a oprávněnost našich předpokladů.

Klíčová slova: správní řízení – přestupky – účinnost

INTRODUCTION

If unlawful conduct results in property damage of up to €700, it is classified as an offence under the amended Criminal Code. This change has led to an increase in the number of cases and a higher workload for employees. Such a workload can only be managed under appropriate conditions that support the efficiency of administrative proceedings. These

influencing factors are quantitatively and qualitatively analysed in selected district offices in Slovakia during the observed period.

Administrative proceedings are defined as a process governed by procedural administrative law, involving administrative authorities, participants, and other entities in issuing, reviewing, and enforcing administrative decisions. These decisions concern the rights, legally protected interests, and obligations of individuals and legal entities (Kollár, 1999). It is a process through which public administration tasks are carried out. Disputed issues that arise between individual subjects are resolved in the proceedings, as well as issues that are of broader societal interest. To a certain extent, this process ensures a balance between individual, group, and societal interests (Kiovská, 1993). Administrative proceedings are time-intensive, culminating in a binding decision enforceable by the state. They are governed by Act No. 71/1967 Coll. on Administrative Proceedings, which regulates all essential procedural institutes. State authorities act in accordance with this Act, supplemented by specific legislation governing distinct areas of public administration, under the principle of subsidiarity[1].

Offence proceedings, as a critical instrument of the state, serve to impose sanctions on individuals engaging in unlawful antisocial conduct. Managed by administrative authorities, effective proceedings fulfil not only punitive but also preventive and educational functions. Substantive and procedural provisions governing offences are dispersed across various legal regulations, with the primary framework provided by Act No. 372/1990 Coll. on Offences.

General administrative departments of district offices in Slovakia manage offence-related agenda as part of their core duties, adhering to both the Offences Act and, subsidiarily, the Administrative Proceedings Act. By contrast, other specialized departments handle offence proceedings as part of their specific state administration tasks (Operational Guidelines for District Offices, 2021).

To analyze the factors influencing the efficiency of administrative or offence proceedings, it is first necessary to define the concept of efficiency. In general terms, efficiency refers to achieving the highest possible level of output with the least possible input. Effectiveness, by contrast, is understood as a measure of success in relation to achieving a specific goal (Vrabko, 2013). The traditional definition of efficiency is associated with output per man-hour, yield from raw materials, and similar benchmarks. For anyone operating in a competitive marketplace, such calculations remain essential and constant; however, when

[1] In matters governed by special legislation, proceedings are conducted primarily in accordance with those laws, and only were such legislation does not provide regulation are the relevant provisions of Act No. 162/2015 Coll., the Administrative Procedure Code.

confined to these immediate measures, they are no longer sufficient (Coy, 1970). Measures of economic efficiency are usually defined as productive efficiency or the private, pecuniary unit costs of production. These measures differ significantly from the concept of Pareto optimality, which remains the only theoretical definition of economic efficiency (Lang, 1980). An economy can be both efficient and sustainable, but efficiency alone does not guarantee sustainability (Bishop, 1993). With regard to the analysis of economic efficiency, there is currently no literature review addressing theoretical or methodological developments (Camanho – Silva – Piran - Lacerda, 2024).

In public administration, efficiency entails fulfilling tasks to the required standard, within the desired scope and quality, relative to the available material and human resources. Within administrative proceedings, efficiency considerations include timeliness, legality, and compliance with procedural rules (Kurilovská – Krásna, 2021). Speed can be regarded as a fundamental determinant and evaluation criterion of efficiency (Mihálik – Filip, 2022).

Drawing on previous practical experience, we have identified three key factors that most significantly influence the efficiency of administrative proceedings. The quality of offence investigation conducted by district departments of the Police Force of the Slovak Republic impacts efficiency. The professional competence of civil servants plays a decisive role in ensuring the effectiveness of offence-related processes. Furthermore, the number of civil servants assigned to the offence agenda is closely connected with the overall - efficiency of administrative proceedings.

METHODOLOGY AND OBJECTIVE

Using quantitative methods (based on selected indicators) and qualitative methods (drawing on interviews with heads of relevant departments), the research examines the impact of selected factors on the efficiency of administrative proceedings in the area of offences within district offices in Slovakia during the years 2021–2023, which is the objective of the research. The results of the quantitative research are presented in a summary table containing 16 monitored indicators.

This study examines two district offices (Senec and Pezinok), which are comparable in terms of their internal structure, number of departments, and the scope of their responsibilities. Information sources comprised internal documents; the collected data had to be adjusted, recalculated, and adapted to permit further analysis.

The study employed comparative and synthetic methods, mathematical techniques, and logical procedures such as analysis, induction, and deduction. Description was applied in the

theoretical part, complemented by explanatory reasoning to draw implications and derive conclusions from the findings.

RESULTS AND DISCUSSION

The clarification phase, as the initial step in the process of resolving administrative offences, is carried out by the police authorities. Experienced department heads have confirmed that this process does not meet the required standards. Police officers often fail to ascertain all essential facts, do not secure necessary documentary evidence, and inadequately guide interviewed individuals to focus on the matter at hand or address key issues. They may not identify all individuals present at the incident or verify the presence of potential witnesses.

To evaluate the quality of offence investigation, three indicators were monitored: the absolute and relative number of files returned for further clarification[2], the number of oral hearings conducted by the respective departments, and the number of decisions issued as penalty orders for offences. It is assumed that an increase in the number of well-clarified offences will lead to a higher number of penalty orders issued. Issuing such orders is less time-consuming and involves fewer procedural steps, which significantly enhances the efficiency of administrative proceedings.

It is assumed that higher professional competence among state employees results in higher quality administrative proceedings, ensuring greater efficiency. Professional competence is primarily influenced by the level of education completed. Offence proceedings are considered a form of criminal procedure, and participants are often represented by lawyers, rendering the process complex. In practice, this complexity is underestimated, and the agenda is sometimes managed by employees who lack expertise, procedural knowledge, and a general understanding of legal regulations. For this reason, based on our opinion and long-term practical experience, legal education appears to be indispensable. To assess this hypothesis, interviews were conducted with experienced heads of the respective departments at the examined district offices, as they are best positioned to assess the matter. These department heads interact daily with employees, assign offence files for processing, and approve written outputs, including final decisions. They observe employees' professional skills and ability to apply legal provisions in

[2] If police authorities forward an offence file to an administrative authority for further proceedings and decision-making in cases where the investigation has been insufficiently conducted, the administrative authority has two options. It may return the file to the police with a request to conduct the investigation in accordance with Section 58 of Act No. 372/1990 Coll. on Offences in order to secure essential facts that were not obtained or were completely overlooked. Alternatively, the administrative authority may address the deficiencies by holding an oral hearing on the offense, summoning all parties to the proceedings and witnesses to establish the facts necessary to clarify the case and issue a decision. Both approaches cause delays in the proceedings and increase complexity, thereby slowing and hindering the overall decision-making process.

practice. Both the head of the Senec office and the head of the Pezinok office agreed that higher education significantly reduces the duration of training and adaptation for employees. This process lasts at least one year, with employees holding legal qualifications adapting to the offence agenda more quickly, whereas those with education in other fields require assistance and guidance even after a year.

The impact of professional competence on the efficiency of administrative proceedings was quantitatively assessed by comparing the total annual number of completed offence files with the number of employees holding legal qualifications in the departments. Data comparison between districts revealed that, during the study period, the offence agenda in Senec was managed by at least one state employee with legal qualifications, allowing nearly all submitted offence files to be processed within the calendar year when the department was fully staffed. In contrast, no employees with legal qualifications managed the offence agenda in Pezinok during the study period, leading to a declining number of processed offence files and a lower percentage of completed cases relative to the total number of files.

For the third hypothesis, the following relationship was assumed: if a department is fully staffed[3], offence files are processed continuously, and only a minimal number carry over into the next calendar year as unprocessed. The head of the Senec department stated that the department consistently maintained four state employee positions, remaining fully staffed from 2021 to 2023. This ensured an average annual completion rate of 98% of offence files, with minimal unprocessed cases carried over annually. Conversely, the Pezinok department experienced suboptimal staffing from 2021 to 2023, with only two positions allocated to offence proceedings. One employee was always in a probationary period, and a high staff turnover was observed. The relationship between the total number of annually completed offence files and the number of staffed positions was examined, determining the average number of files handled per employee. Additionally, the number of unprocessed files carried out to the following year was compared based on staffing levels. The proportion of unprocessed cases was calculated by subtracting the percentage of completed files from the total annual number of offence files.

In Senec, one employee processed an average of 120 files annually, while in Pezinok, the average was 129 files[4] per employee. However, Senec consistently maintained 100%

[3] It is necessary to highlight the uneven number of state employee positions for managing offence-related matters in the respective departments across Slovak district offices, given the size of districts in terms of population. When comparing these numbers, no clear rationale or criteria can be identified that would explain how these positions were allocated in the past.

[4] The difference in the average number of cases processed per state employee per year between the two departments appears to be relatively small. However, it is important to note that in Senec, due to long-term full staffing, more oral hearings are conducted, and more cases are returned to the police for further clarification compared with

staffing (four employees), corresponding to an average annual completion rate of 98% of all offence files and a minimal, stable number of unprocessed cases. In contrast, Pezinok had an average staffing rate of only 52.8% annually, resulting in a declining average completion rate of 65.4% of offence files and an increasing number of unprocessed cases, rising from 26% to 45% over the observed period.

Table 1: Monitored indicators in years 2021-2023

	DISTRICT OFFICE SENEC				DISTRICT OFFICE PEZINOK			
Year	**2021**	**2022**	**2023**	**Average**	**2021**	**2022**	**2023**	**Average**
Total number of files	519	483	478	**493**	214	215	191	**207**
Number of cases returned for further clarification	130	120	130	**126**	29	40	31	**33**
Number of oral hearings	89	107	90	**95**	15	16	10	**14**
Share of oral hearings from total cases	17%	22%	19%	**19%**	7%	7%	5%	**6.5%**
Share of returned cases from total cases	25%	25%	27%	**26%**	14%	19%	16%	**16%**
Number of issued orders	168	105	92	**122**	78	75	29	**61**
Share of issued orders from total cases	32%	22%	19%	**24%**	36%	35%	15%	**29%**
Number of insufficiently clarified cases	(130+89) 219	(120+107) 227	(130+90) 220	**(127+95) 222**	(29+15) 44	(40+16) 56	(31+10) 41	**(33+14) 47**
Share of insufficiently clarified cases from total cases	42%	47%	46%	**45%**	21%	26%	21%	**23%**
Number of cases finalized with legal effect	509	473	468	**483**	158	145	105	**136**
Share of cases finalized with legal effect	98%	98%	98%	**98%**	74%	67%	55%	**65%**
Average number of offenders per case	4	4	4	**4**	1.25	1	0.92	**1.06**
Number of cases handled per state employee	127	118	117	**120**	126	145	115	**129**

Pezinok. In Senec, one employee works more efficiently and performs a higher number of actions per case. His workload is more complex, diverse, and complicated; in addition to issuing decisions he also conducts a higher number of hearings, which involves additional tasks. When returning a case for further clarification, he must prepare requests with specifically detailed instructions to address the identified deficiencies.

Number of unfinished cases	10	10	10	**10**	56	70	86	**71**
Percentage of unfinished cases from total cases	2%	2%	2%	**2%**	26%	33%	45%	**35%**
Staffing levels in the department	100%	100%	100%	**100%**	63%	50%	46%	**53%**

Source: Data obtained from internal records of selected district offices. Own calculations.

We have shown that the quality of offence investigations, the professional competence of state employees, and the number of staff all influence the efficiency of administrative proceedings in the selected district offices in Slovakia.

CONCLUSION

The fundamental condition for effectively resolving offences is to structure the entire process so that high-quality materials for decision-making are ensured. The clarification process, the quality of offence investigations significantly influence the subsequent decision-making process of administrative authorities. The higher the quality, the faster the decision-making process, requiring fewer actions. When this condition is combined with stable staffing in general internal administration departments by professionally competent state employees, an optimal situation is achieved. Our research has both qualitatively and quantitatively justified the necessity of higher education in the field of law. It has confirmed a correlation between the number of employees in administrative offence departments and the quality and speed of case resolution. During the period under review, the department with full staffing achieved a higher number of actions of better quality.

The factors verified in the conditions of district offices in Slovakia appear to be the most significant when assessing efficiency. We emphasize the importance of properly configuring all these factors simultaneously. Only then can the efficiency of administrative proceedings be guaranteed.

This topic is highly relevant. Compared to criminal offences, administrative offences are often underestimated and do not receive the attention they deserve. Given the anticipated increase in their number in the future, there is a need to identify additional factors influencing the efficiency of administrative proceedings, which presents a subject for further research in this area.

REFERENCES AND INFORMATION SOURCES USED

1. BISHOP, R. C. (1993). Economic Efficiency, Sustainability, and Biodiversity. *Ambio*. 22, 2-3. pp. 69-73.
2. CAMANHO, A. S. – SILVA, M. C. – PIRAN, F. S. – LACERDA, D. P. (2024). A literature review of economic efficiency assessments using Data Envelopment Analysis. *European Journal of Operational Research*. 315, 1. pp. 1-18.
3. COY, MC. (1970). Social versus (?) economic efficiency. *Chemical and Engineering News*. 48, 39. pp. 5-10.
4. KIOVSKÁ M. (1993). *Procesy vo verejnej správe.* Košice: Univerzita P. J. Šafárika. 161 p. ISBN 80-7079-254-8.
5. KOLLÁR J. (1999). *Základné pramene správneho práva.* Banská Bystrica: Univerzita Mateja Bela. 230 p. ISBN 80-8055-304-1.
6. KURILOVSKÁ, L. – KRÁSNÁ, P. (2021). *Efektívnosť prípravného konania- výzvy a perspektívy*. Bratislava: Akadémia Policajného zboru. 227 p. ISBN 978-80-8054-926-8.
7. LANG, M. G. (1980). Economic Efficiency and Policy Comparisons. *American Journal of Agriculture Economics*. 62, 4. pp. 772-777.
8. MIHÁLIK, S. – FILIP, V. (2022). Hodnotenie efektívnosti prípravného konania s ohľadom na jeho vybrané inštitúty. In: *Efektívnosť prípravného konania- súčasný stav a výzvy pro futuro*. Bratislava: Wolters Kluwer SR, 420 p. ISBN 978-80-571-0546-6.
9. Operational Guidelines for District Offices, Internal Sources
10. VRABKO M. a kol. (2013). *Správne právo procesné*. Bratislava: C. H. Beck. 304 p.. ISBN 978-80-89603-13-8.
11. *Act No. 71/1967* Coll. on Administrative Proceedings.
12. *Act No. 372/1990* Coll. on Offenses.
13. *Act No. 162/2015* Coll. on Administrative Procedure Code.

ADDRESS & ©

doc. Ing. Katarína LIPTÁKOVÁ, PhD.
Department of Political Science
Faculty of Political Science and International Relations
Matej Bel University
Kuzmányho 1, 974 01 Banská Bystrica
Slovak Republic
katarina.liptakova@umb.sk
ORCID iD - 0000 0002 6711 1405

JUDr. Katarína DROCÁROVÁ, PhD.
Slovak Republic
drocarova@lignus.sk
ORCID iD - 0009 0007 2153 4166

VEŘEJNÁ SPRÁVA, ŘÍZENÍ • PUBLIC ADMINISTRATION, MANAGEMENT

DOI: 10.36682/a_2025_1_6

ANALYSIS OF IMPACTS OF A SELECTED ELECTORAL SYSTEM REFORM PROPOSAL IN THE SLOVAK REPUBLIC

Analýza dopadov vybraného návrhu reformy volebného systému v podmienkach SR

Natália KOVÁČOVÁ – Roman ŠIMÁČEK

Sládkovičovo, Slovak Republic

ABSTRACT: Electoral reforms are often the subject of political debate, as their implementation can significantly affect political entities, voter behaviour, as well as the representativeness of political processes. The current political scene in Slovakia is marked by intense debates over possible changes to the electoral system, highlighting the need to make democracy and political processes more effective. The aim of the article is to analytically examine the proposal for modifying the electoral quorum, promoted by the Prime Minister of the Slovak Republic following the parliamentary elections in 2023. The article also assesses the potential political and systemic consequences of implementing this reform for the stability and functioning of the Slovak political system.

Key words: electoral system – proportional electoral system – electoral quorum – deformation index

ABSTRAKT: Volebné reformy sú často predmetom politických diskusií, keďže ich implementácia môže významne ovplyvniť politické subjekty, voličské správanie a v neposlednom rade reprezentatívnosť politických procesov. Súčasné politické prostredie je na Slovensku poznačené intenzívnymi debatami o možných zmenách volebného systému, ktoré zdôraznili potrebu zefektívnenia demokracie a politických procesov. Cieľom príspevku je analyticky preskúmať návrh modifikácie volebného kvóra, ktorý po parlamentných voľbách v roku 2023 presadzoval predseda vlády SR. Príspevok zároveň hodnotí možné politické a systémové dôsledky implementácie tejto reformy na stabilitu a fungovanie slovenského politického systému.

Kľúčové slová: volebný systém – pomerný volebný systém – volebné kvórum – index deformácie

INTRODUCTION

The electoral system represents a complex institutional framework that determines the mechanisms by which voter preferences are translated into the form of mandate distribution in legislative bodies. Its function goes beyond the framework of formal election administration, as it fundamentally affects the dynamics of party competition, mechanisms of political representation, the stability of executive structures, the efficiency of governance, etc. According to G. Sartori, "the electoral system is a mechanism that converts voters' votes into political results, thereby affecting the functioning of the entire political system" (Sartori, 2001, p. 45). Within the theory of democracy, electoral engineering performs not only a regulatory, but also a normative role, as the choice of a specific model reflects preferred democratic principles. From the perspective of system analysis, electoral design represents a key determinant that shapes the structure of the party system, patterns of political competition and the degree of coherence of parliamentary arithmetic. The electoral system cannot, therefore, be understood as an isolated technical variable, but as a fundamental institutional element of the state that significantly shapes the character and functioning of a democratic regime. The optimization of electoral mechanisms thus requires not only a descriptive analysis of their functioning in a specific context, but also a thorough reflection of their long-term consequences for the quality of political representation and the legitimacy of governance.

Electoral reforms and changes to the electoral system in Slovakia represent a significant area of interest in domestic political science literature. A key work in this field is the monograph by P. Spáč, *Direct and Representative Democracy in Slovakia: Electoral Reforms and Referendums after 1989*, which provides a comprehensive analysis of the development of electoral mechanisms in the context of the transformation of the Slovak political system after 1989 (Spáč, 2010). Discussions on electoral reform at the parliamentary level often focus on the issues of the number and size of constituencies, the electoral threshold, or preferential voting. The professional discourse in this area has been enriched by publications, research, and public contributions of several authors, including G. Mesežnikov, who analyses the Slovak political system and electoral processes in his works, as well as T. Koziak, G. Szekély, J. Bardovič, M. Beblavý, M. Martinkovič, and M. Klus, who analyze and evaluate the effects and nature of proposed changes to electoral systems.

METHODOLOGY AND OBJECTIVE

The aim of the paper is to analyse the impacts of a selected electoral system reform in the Slovak Republic, which came to the fore after the parliamentary elections in 2023. The paper focuses on identifying political entities that would benefit from the proposed change, as well as those that would be disadvantaged by the reform. Special attention is paid to the frequently discussed proposal by the Prime Minister of the Slovak Republic to increase the electoral quorum for political parties to enter parliament to 7%. Based on a model example and simulated calculations, using the results of the last early parliamentary elections, we examine the possible political consequences of the proposed change in the paper. For the sake of accuracy, it should be emphasized that the above calculations are only illustrative, as electoral dynamics are conditioned by various factors and strategic considerations that cannot be predicted with certainty. Nevertheless, the results and numerical indicators provide a clearer understanding of the potential impacts of the reform. In this context, the purpose of the content dimension of the paper is to answer the research question: "What impact would a change in the proposed electoral rules (increasing the quorum) have on the distribution of political forces within the Slovak political spectrum?"

To achieve the goal of the paper, we primarily employed the method of analysis and synthesis of knowledge, which enabled a detailed examination of the electoral reform proposal. The comparative method was used to formulate conclusions regarding the potential impact of the analysed proposal, such as the impact on the distribution of political forces, while the starting point was the current state, compared with model results. To support the conclusions, we applied mathematical calculations that simulated the effect of the proposed change based on data from the 2023 early parliamentary elections.

RESULTS AND DISCUSSION

Optimizing the efficiency rate when amending electoral legislation is a complex process, the inherent complexity of which lies in the fact that even with an identical distribution of votes among political entities, the application of different electoral systems can generate markedly different outcomes. Comparative analysis of electoral models applied in other countries can serve as a source of inspiration, but their direct adoption does not guarantee effectiveness in a different political, institutional and social context. When proposing changes to the electoral system, it is necessary to consider historical determinants of political development, regional disparities, demographic structure, the degree of ethnic and cultural heterogeneity, and the specifics of the party system of a given country, which fundamentally

shape the functioning of electoral mechanisms (Kováčová, N.-Prášil, 2023). Modification of the electoral system is not only a technical adjustment, but also an intervention in the foundations of the political system. It requires thorough expert discussion and broad political consensus.

The most recent legislative electoral regulation is Constitutional Act No. 24/2023, which amends and supplements the Constitution of the Slovak Republic No. 460/1992 Coll., as amended. The amendment constitutionally enshrines the system of proportional representation and establishes that the territory of the Slovak Republic constitutes one electoral district for elections to the National Council of the Slovak Republic (Domin, 2024). From a legal and political perspective, the amendment did not constitute a fundamental change to the previous status quo, but rather formally confirmed the existing legislative framework. At the end of 2024, a proposal to modify the electoral system was also presented by R. Fico (Smer-SD), who, in addition to increasing the electoral deposit from the current €17,000 to €500,000, proposes raising the threshold required for political parties to enter parliament from the current 5% to 7% (Linhart, 2024).

The proposal to increase the electoral quorum should be understood in light of two constitutional norms. The first constitutional norm has been present in the Constitution of the Slovak Republic since its founding and is Art. 31: "The legal regulation of all political rights and freedoms and its interpretation and application must enable and protect the free competition of political forces in a democratic society" (Constitution of the Slovak Republic, 1992). This provision safeguards the free political competition of party forces in Slovakia. The above-mentioned aspect carries an important psychological effect. If the entry threshold for political parties is set too high (which can be considered, for example, at 7%), this can have a demotivating effect on voters, who are influenced in their decision-making not only by the parties' programmatic starting points, but also by their realistic chances of success. If a preferred party in public opinion polls consistently fail to reach the threshold for a long time, voters may tend to vote strategically, i.e., supporting an alternative party with a higher likelihood of winning mandates. This can weaken genuine competition, favour established political entities over new and smaller parties and thus reduce political diversity within representative bodies. The second constitutional norm was included in the Constitution of the Slovak Republic in 2023 in connection with early elections. One of the advantages of a proportional representation system is that it has a smaller number of forfeited votes, in comparison with a majoritarian system. However, imposing an excessively high entry threshold would undermine this principle, blurring the distinction between proportional and majoritarian systems. The

Constitution of the Slovak Republic clearly established that parliamentary elections are held on the basis of a proportional electoral system, and therefore it is essential to preserve its basic characteristics, which include a fair distribution of mandates and proportionality in relation to voter preferences. Setting the electoral threshold too high could artificially concentrate political power in the hands of a smaller number of entities, thereby reducing the plurality of the political environment and weakening its openness to new political actors.

Increasing the electoral threshold to 7% could significantly reduce the number of political entities represented in parliament and move the proportional system closer to the characteristics of a majoritarian model. Majoritarian electoral systems traditionally promote a two-party structure (bipartisanship) and limit fragmentation of the political spectrum, which simplifies the decision-making process for voters, but at the same time may marginalize smaller and alternative political movements. On the contrary, proportional systems are characterized by greater inclusivity and support for pluralistic political perspectives. This aspect often leads to fragmentation of the party system and necessitates coalition governance, which can affect voters´ trust in the stability of the political system, particularly if there are frequent intra-coalition disputes or ineffective governance. Consequently, altering the electoral system can thus affect not only political representation but also voters´ long-term attitudes towards democratic institutions.

Table 1 presents a model composition of the parliament under a 7% electoral threshold, based on the results of the 2023 parliamentary elections.

Table 1: Model example - Composition of the National Assembly of the Slovak Republic with a 7% electoral threshold for political parties to enter parliament

Political parties	**Number of valid votes**	**Percentage share**	**Votes/republic number (r.n)**	**Number of mandates in relation to the r.n.**	**Allocated mandates based on the remaining votes**	**Final number of mandates**
Smer-SD	680 017	22.94%	53.658	53		53
PS	533 136	17.96%	42.068	42		42
Hlas-SD	436 415	14.70%	34.436	34		34
0ĽaNO a priatelia	264 137	8.89%	20.842	20	+1	21
Together	1914705		**r.n. 12680**	**149**		**150**
KDH (outside parliament)		*6.82%*				
SaS (outside parliament)		*6.32%*				
SNS (outside parliament)		*5.62%*				
***Number of lost votes* 35.4%**						

Source: (Statistical Office of the Slovak Republic 2023; Own calculation).

The above calculations indicate that increasing the electoral threshold from 5% to 7% would lead to a significant reduction in the number of parliamentary entities, leaving only four political parties represented in the National Council of the Slovak Republic. Compared to the current situation, political parties such as KDH, SaS and SNS would lose parliamentary representation under this model, while the dominant political parties of the two main blocs would strengthen their position in the National Council of the Slovak Republic. The number of forfeited votes would exceed 35% in this scenario, which would represent the highest value in history since the establishment of an independent Slovak Republic. At the same time, it is necessary to consider possible change in voting behaviour, as voters could be more inclided to vote strategically. Therefore, the above figures should be seen as illustrative, reflecting the expected impact of increasing the electoral threshold on the party system. To assess the degree of proportionality between the electoral system and political parties, the distortion index, which measures the discrepancy between election results and allocated mandates (Spáč, 2010). If a political party receives fewer parliamentary mandates relative to its electoral votes, it is considered under-represented in the system. On the contrary, if it receives more mandates than its actual voter support, it is over-represented. The naturalness of representation is the difference between the percentage of votes received by a party out of the total number of valid votes cast in the elections and the percentage of mandates received by this party out of the total number of mandates in parliament. The most natural representation occurs when this difference is equal to zero. The greater the absolute value of the difference, the less natural the representation. The average naturalness of representation is calculated as the arithmetic mean of the naturalness of representation of all parties that have met the specified quorum (Kerekes, 2012). The distortion index and the value of naturalness of representation are illustrated in Table 2. The results of these indicators give us a clearer picture of how a change in the electoral threshold would affect the political representation of individual parties and the fairness of the electoral process.

Table 2: Distortion index and naturalness of representation – model example at a 7% quorum for political parties to enter parliament

Political parties	Actual percentage of mandates (A)	Percentage share of votes (B)	Number of mandates with respect to r.n.	Allocated mandates based on the remaining votes	Final number of mandates	Index of deformation (C) (A/B= C)	The value of the naturalness of the representation (C) (A-B=C)
Smer-SD	35.33%	22.94	53		53	1.54	12.39
PS	28%	17.96	42		42	1.55	10.04
Hlas-SD	22.66%	14.70	34		34	1.54	7.96
0Ľ'aNO a priatelia	14%	8.89	20	+1	21	1.57	5.11
						average 1.55	**average 8.88**

Source: (processed and converted by the author).

The data in the table shows that the distortion index for no political party fell below the value of 1, which indicates that an electoral system configured in this way would not under-represent political parties and, ultimately, they would occupy more seats than their actual voter support. The distortion index of all parties that would gain parliamentary representation is almost identical. For this reason, it can be concluded that such electoral system in Slovakia would neither favour nor disadvantage any party. On the other hand, a higher electoral quorum would not only lead to a greater percentage of wasted votes but also to a higher numerical value of the naturalness of representation, which means that the composition of parliament would not reflect the real will of the voters to a greater extent and would stimulate the strategic behaviour of voters.

In summary, it can be concluded that an increase in the electoral threshold would lead to a narrowing of the representation of political opinions in parliament, which could weaken democratic processes. This step would lead to the restriction of democratic competition and reinforce the dominant position of larger political entities. Such an amendment to the electoral rules would reduce the opportunities for smaller and new political parties and, at the same time, weaken the plurality of the political spectrum. The resulting reduction in political diversity could also be seen as a step towards authoritarian tendencies, resulting in the facilitation of governance by dominant political parties at the expense of smaller ones.

In this context, attention should be paid to a proposal that the KDH political party has been promoting for a long time, namely to increase the number of electoral districts to eight, aligning them with the self-governing regions. In comparison with other V4 countries, Slovakia is the only country that has a single electoral district, which is a so-called legacy of Mečiarism.

Several parties have previously promoted proposals to modify electoral districts, but so far, these proposals have not gained sufficient political support for implementation.

We conclude that changing the electoral system to increase the number of electoral districts would also require a change in the behaviour of political parties, forcing them to adapt their strategies to standard political practices. In such a scenario, the aspect of the dominance of one prominent personality would diminish. The current single-district system is advantageous for parties that have a small membership base and rely on one leader. The current system also leads to a degree of parliamentary anonymity, as individualsare represented by politicians who are elected largely based on their position on the party list rather than through voter preferences in specific areas. The creation of multiple districts would, by its very nature, contribute to bringing politics closer to voters and increase political engagement at the regional level, as political parties would be compelled to strengthen their regional structures at the same time. A single constituency distorts party competition and encourages the transformation of political parties into centralised organisations led by a narrow group of individuals with a minimal degree of legitimacy.

The introduction of a model of eight electoral districts, aligned with the borders of the self-governing regions, would not represent a fundamental change to the technical framework of the electoral system, as the proportional electoral system and the electoral quorum for the entry of political parties into parliament would remain in place. The methodology for distributing mandates would continue to follow the Hagenbach-Bischoff quota and would be governed by the regional (originally republican) number within the districts. However, a significant change would be the increased number of candidate lists, corresponding to the number of self-governing regions. This would narrow the selection of candidates and thereby strengthen the weight of preferential votes.

Expert discussions have also considered allowing voters to cast four preferential votes for individual candidates. Voters would not select four candidates from the entire pool of 150 deputies, but only from candidates standing within their own district of permanent residence. The number of deputies allocated to individual districts would be determined based on the size of the district and the number of its inhabitants. Under this new model, the dominance of the Bratislava region in parliament would be reduced, promoting a more balanced regional representation.

According to the KDH proposal, the number of mandates in individual constituencies (regions) should be limited to a maximum of 25, which would ultimately lead to an increase in the total number of deputies in parliament compared to the current system. In smaller

constituencies, the party proposes introducing a limit of two preferential votes per candidate list. However, the KDH party is open to discussion regarding the criteria that would determine the number of mandates in individual regions, taking into account factors such as the size of the constituency, the number of inhabitants, regional differences and demographic structures, in order to ensure an even and fair representation of voters in the electoral process (Slovensko by mohlo.., 2024).

The question of whether this proposal would favour any political party, and which party could significantly benefit from it, is addressed through a simulated model example in Table 3. The calculations in the table illustrate how the introduction of the proposed model would affect the distribution of mandates among individual political entities, compared with the actual results of the 2023 parliamentary elections.

Table 3: Model example of eight electoral districts - Comparison of the number of mandates of political parties with the current situation

Political parties	**Number of mandates**	
	1 district	**8 districts**
SMER-SD	42	46
PS	32	34
HLAS	27	28
OĽANO A PRIATELIA, KÚ A ZA ĽUDÍ	16	16
KDH	12	9
SAS	11	10
SNS	10	7

Source: (processed and converted by the author).

The conclusions presented in the table are based on a quantitative analysis of the election results. First, we aggregated the votes of all political entities that met the legally established conditions for entering parliament within individual electoral districts (regions). We then divided the total number of valid votes by the number of mandates assigned to the given region. The distribution of mandates was derived from the number of inhabitants of individual regions. The resulting value represents an analogue of the so-called "republic number", which in this model can be referred to as the "regional number". Subsequently, the number of valid votes cast for individual political parties and coalitions was divided by this regional number, thereby yeilding the final number of mandates according to the proportional calculation method.

Based on the quantitative indicators presented in the table, it can be concluded that the eight-district model would not alter the overall distribution of political forces across the party spectrum and none of the political parties would significantly benefit from it compared to the current system. However, its primary consequence would be to balance the personal

representation of regional deputies in parliament and strengthen the connection between voters and their elected representatives.

CONCLUSION

A change in the electoral system can have significant consequences for voter behaviour, trust in the electoral process, and the stability of the political system. Any major reform of the electoral system raises uncertainty, especially in an environment where voters have long been accustomed to a specific electoral model. For this reason, it is essential that any modification of the electoral system be underpinned by thorough expert analysis.

The proposals that are currently emerging reflect various political interests and an effort to adapt elections to contemporary challenges, as well as to prevailing social and political conditions. In this paper, we analysed a selected proposal for reforming the electoral system for elections to the National Assembly of the Slovak Republic, which came to the fore after the early parliamentary elections of 2023. We examined its potential impact on political representation, while trying to clarify what changes the implementation of the reform would bring. Based on the analysis and simulated calculations, we have shown that increasing the electoral threshold for political parties to enter the National Council of the Slovak Republic to 7% would lead to a narrower political spectrum. A higher threshold would represent a more substantial obstacle for smaller political parties in securing parliamentary representation, which would strengthen the position of dominant parties such as Smer-SD, PS, or Hlas-SD. Limiting access for new or smaller parties to the legislative process would also reduce competition within the party system and could negatively affect the quality of democratic competition, which is essential for the stability and representativeness of parliamentary democracy. Although reducing fragmentation within the party system could contribute to more efficient functioning of the government, at the same time the increase in the number of forfeited votes would weaken the representativeness of the election results. Consequently, the parliamentary composition would reflect the actual preferences of voters to a lesser extent, as confirmed by the above calculation of the naturalness of representation.

Finally, we discussed the proposal to increase the number of electoral districts from one to eight, as long advocated by the KDH party. From the perspective of electoral preferences and voter behaviour, it can be assumed that increasing the number of districts would likely enhance the representation of regional interests in parliament. Voters would be more inclined to support candidates from their own region rather than nationally prominent personalities, which would contribute to a greater representation of local political actors. In smaller districts,

the importance of individual candidacy would become more important, and personal campaigns would play a key role in mobilizing voters. The model would also motivate candidates to engage more intensively at the regional level, which would strengthen their ties with voters and increase the level of political participation. At the same time, preferential votes could be strengthened, which would heighten voters´ perception that their vote has a real impact on the final composition of parliament. In a broader context, the introduction of multiple constituencies could therefore stimulate public interest in political events and lead to higher voter turnout.

LITERATURE AND INFORMATION SOURCES

1. DOMIN, M. (2024). Constitutional Protection of the Electoral System: The Slovak Republic in a Comparative Perspective. In *Právny obzor*, 107, 2024, No. 4, pp. 408 – 427. Available online: <https://doi.org/10.31577/pravnyobzor.2024.4.04 >.

2. KEREKEŠ, D. (2012). Failure of Slovak Democracy or Elections to the National Council of the Slovak Republic. In OLOŠTIAK, M. – CHOVANEC, M. (ed.) *8th Student Scientific Conference. Proceedings of the Full Papers*. [online] [cited 02-06-2025] Prešov: Prešov University in Prešov. ISBN 978-80-555-0770-5. with 729-737. Available online: <https://www.pulib.sk/web/kniznica/elpub/dokument/Olostiak4/subor/Kerekes.pdf>

3. KOVÁČOVÁ, N. – PRÁŠIL, F. (2023). Paradoxes of preferential voting and possibilities of strengthening the vote in the conditions of the Slovak Republic. In *Political Sciences*. Vol. 26, no. 1, pp. 136-155. ISSN 1335 – 2741. Available online: https://doi.org/10.24040/politickevedy.2023.26.1.136-155.

4. LINHART, M. (2024). *Fico proposes a change in the electoral system, but what does the Constitution say? Fewer parties will not improve politics*, *Bujňák assesses*. [online]. [cit. 04-05-2025] Available online: <https://www.ta3.com/clanok/966995/fico-navrhuje-zmenu-volebneho-systemu-ale-co-hovori-ustava-menej-stran-politiku-nezlepsi-hodnoti-bujnak>

5. SARTORI, G. (2001). *Comparative Constitutional Engineering: An Inquiry into Structures, Incentives and Outcomes*. New York: NYU Press, 2001. 374 p. ISBN: 9780814794904.

6. SPÁČ, P. (2010). *Direct and Representative Democracy in Slovakia. Election Reforms and Referendums after 1989*. Brno, Center for the Study of Democracy and Culture, 2010, p. 278. ISBN: 978-80-7325-238-0.

7. STATISTICAL OFFICE OF THE SR (2023). Available online: https://slovak.statistics.sk/

Slovensko by mohlo mať viac volebných obvodov, zhodli sa Majerský a Šutaj Eštok. (2024) [online]. [cit. 25-08-2025] Available online: https://spravy.pravda.sk/domace/clanok/714731-slovensko-by-mohlo-mat-viac-volebnych-obvodov-zhodli-sa-majersky-a-sutaj-estok/.

8. CONSTITUTION OF THE SR. Collection of Laws No. 460/1992.

ADDRESS & ©

doc. PhDr. Natália KOVÁČOVÁ, PhD.
Fakulta verejnej politiky a verejnej správy
Vysoká škola Danubius,
Fučíkova 269, 92521 Sládkovičovo,
Slovak Republic
natalia.kovacova@vsdanubius.sk

JUDr. Mgr. Roman ŠIMÁČEK
Fakulta verejnej politiky a verejnej správy
Vysoká škola Danubius,
Fučíkova 269, 92521 Sládkovičovo,
Slovak Republic
roman.simacek@seznam.cz

RECENZNÍ ŘÍZENÍ PRO Č. 1/2025

Jednotliví oponenti (6) recenzovali 1–2 články. Redakce od nich obdržela na každý příspěvek 1–2 posudky, celkem 10 posudků.

doc. JUDr. PhDr. Jiří **BÍLÝ**, CSc.	Katedra právních oborů a bezpečnostních studií, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
Mgr. et Mgr. Radek **FABIAN**	Katedra právních oborů a bezpečnostních studií, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
Dr. h. c. doc. JUDr. Miroslav **FELCAN**, PhD., LL.M., DSc.	Katedra právních oborů a bezpečnostních studií, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**
plk. Ing. Tomáš **HORVÁT**, Ph.D.	Ředitel územního odboru Příbram, rada HZS Středočeského kraje, **ČR**
doc. Ing. Radoslav **IVANČÍK**, PhD. et PhD., MBA	Katedra filozofie a politológie, FF UKF v Nitre, Nitra, **SR**
doc. PhDr. Miroslav **SAPÍK**, PhD.	Katedra managementu veřejné správy, Vysoká škola evropských a regionálních studií z. ú., České Budějovice, **ČR**

POČET OBDRŽENÝCH VĚDECKÝCH ČLÁNKŮ:	7
POČET RECENZOVANÝCH VĚDECKÝCH ČLÁNKŮ:	6
POČET OBDRŽENÝCH RECENZNÍCH POSUDKŮ:	10
POČET PUBLIKOVANÝCH VĚDECKÝCH ČLÁNKŮ:	6

VARIA

How to Prepare Leaders for SMART Cities: UCM in Trnava Concludes the Jean Monnet Module LEADER

Doc. PhDr. Andrea Čajková, PhD., Faculty of Social Sciences UCM in Trnava, andrea.cajkova@ucm.sk

The Faculty of Social Sciences at the University of Ss. Cyril and Methodius in Trnava has successfully completed the Jean Monnet Module LEADER. The project set out to prepare future political leaders and professionals for the challenges of the twenty-first century, with a particular focus on SMART Cities and the changing role of public governance. Along the way, it not only enriched the curriculum but also created a space for genuine dialogue between academics, students, and practitioners.

Students as Leaders in the Making

The project's main ambition was to bridge the distance between theory and practice. Today's students, if they are to become tomorrow's decision-makers, must combine solid academic knowledge with the ability to think critically and act responsibly. Within the courses and workshops, participants explored how SMART City tools can be applied, while also debating the broader challenges facing Slovakia and the European Union.

"It is not only about helping students pass exams. The real goal is to prepare responsible citizens and future leaders who are able to design meaningful policies and strengthen democracy," explained the module's academic coordinator.

Connecting the Classroom with Real-World Practice

One of the most valuable aspects of the module was its openness to cooperation with practitioners. Political leaders, public officials, managers, and civil society representatives contributed to lectures, discussions, and even a summer school. For students, this meant the chance to confront their knowledge with real-life dilemmas. Debates on sustainability, digitalization, and civic engagement not only enriched the learning process but also laid the groundwork for a forthcoming monograph that captures the project's key findings.

An Interdisciplinary and European Outlook

The LEADER module was built on an interdisciplinary foundation, drawing from public administration, economics, environmental studies, and civic participation. Equally important

was its European dimension. Faculty members collaborated with colleagues from abroad in designing course content and disseminating results. This collaboration raised the quality of teaching while reinforcing the European perspective of the project, encouraging exchange and mutual learning in civic and European education.

A Lasting Contribution to the University and Society

The project left a clear legacy–not only for students, but also for the faculty and the wider community in Trnava. By engaging young people in summer schools and public debates, it fostered active citizenship and highlighted the importance of leadership at both local and national levels. If Slovak cities and regions are to grow in a sustainable and intelligent way, they will need young professionals ready to take on responsibility. In this sense, the LEADER module was an important step forward.

Ultimately, the project showed that the university can serve as an incubator for new generations of leaders - people who are able to combine innovation, participation, and European values as they face the challenges of the SMART era.

Acknowledgement: This article was supported by the Erasmus+ Programme under the Grant No.101085569 Erasmus+ Jean Monnet Modul LEADER.

O ČASOPISU

Základní charakteristika

Časopis Auspicia je nezávislým recenzovaným vědeckým časopisem pro otázky společenských a humanitních věd. Obsah časopisu prezentuje původní vědecké příspěvky, které jsou orientované na stěžejní obory zaměření periodika a rovněž v současnosti významné a řešené problémy. Mnohé z nich podávají formou přehledových studií návrh na reálné řešení konkrétních problémů, polemik ve smyslu akademické plurality názorů.
Historicky je založen na 5 základních a respektovaných principech:

- řádné a přísné recenzní řízení;
- mezinárodnost;
- otevřenost;
- výběrovost;
- kontinuální zvyšování kvality.

Historie

Časopis Auspicia je vydáván od r. 2004 Vysokou školou evropských a regionálních studií (VŠERS) a Vysokou školou technickou a ekonomickou (VŠTE) dvakrát ročně, pouze elektronicky. V dosavadních 41 číslech bylo otištěno zhruba 860 příspěvků a recenzí.

Rada pro výzkum, vývoj a inovace jako odborný a poradní orgán vlády ČR zařadila časopis Auspicia (ISSN 1214-4967) pro léta 2008–2013 a znovu pro rok 2015 (http://www.vyzkum.cz/FrontClanek.aspx?idsekce=733439) mezi recenzované neimpaktované časopisy, které uvedla v oborech Národního referenčního rámce excelence (NRRE).

V roce 2016 byl recenzovaný vědecký časopis Auspicia zařazen do mezinárodní databáze ERIH PLUS a od roku 2024 do online knihovny pro střední a východní Evropu – CEEOL.

Tematické sekce

Na základě úspěšného recenzního řízení jsou jednotlivé vědecké příspěvky řazeny do sekcí:

1. Společenské vědy
2. Bezpečnost
3. Veřejná správa, řízení
4. Recenze

<u>Základní pokyny autorům</u>

Jazyk vědeckého příspěvku: angličtina, čeština; **recenze**: angličtina, čeština, Články mohou být psány v angličtině nebo češtině, ale vzhledem k mezinárodnímu rozměru časopisu jsou preferovány anglické články.

Požadovaný rozsah v sekcích 1–3: max.8 normostran (1NS – 1800 znaků včetně mezer).

Data uzávěrek: 1. číslo – 1. 2. • 2. číslo – 1. 8.

Použitá literatura: 25 % zdrojů indexovaných v databázích Web of Science a/nebo Scopus.

Recenzní řízení: oboustranně anonymní, nezávislé, objektivní.

Data vydání: 1. číslo – 1. 6. • 2. číslo – 1. 12.

Podrobný zdroj: https://vsers.cz/auspicia/
Jak citovat vědecký příspěvek: In.: Pro autora. Šablona článku – https://vsers.cz/auspicia/

Autorský poplatek: Za výdaje spojené s uveřejněním vědeckého příspěvku v českém jazyce (příspěvky v angličtině jsou do odvolání dočasně bezplatné) v délce **max. 8 normostran** v sekcích 1–3 hradí autor částku **1 000,- CZK** *(popř. částku zvýšenou o 200, - Kč za každou další normostranu)*, nebo příslušnou částku v EUR dle aktuálního přepočtu, a to nejpozději do uzávěrky příslušného čísla (tj. před recenzním řízením) převodem na účet vydavatele (VŠERS) u Fio banky, a. s. (pobočka České Budějovice) č. 2101783605/2010, účet EUR/IBAN: CZ71 2010 0000 0024 0178 3607, BIC kód: FIOBCZPPXXX (zahraniční plátci si poplatek za převod hradí sami), nebo v hotovosti na ekonomickém oddělení VŠERS. Variabilním symbolem je IČO autorova pracoviště a specifickým symbolem číselný kód 12342022. Do zprávy pro příjemce se uvede jméno autora / autorů a pracoviště.

Kontaktní adresa:
Vysoká škola evropských a regionálních studií, z. ú.
Žižkova tř. 1632/5b
370 01 České Budějovice
doc. PhDr. Miroslav Sapík, Ph.D.
Telefon: +420 386 116 839
E-mail: sapik@vsers.cz, https://vsers.cz/auspicia/

ABOUT THE JOURNAL

General description

Auspicia is an independent, peer-reviewed scientific journal on the social sciences and humanities. The journal presents original scientific contributions on core areas of its field of focus, as well as currently significant and solved problems. In the form of overview studies, many of them constitute proposals for a real solution to specific problems, polemics in the sense of academic plurality of opinions.

The journal is based on five respected principles:
- proper and rigorous review procedures;
- internationality;
- openness;
- selectivity;
- continuous improvement in quality.

History

Auspicia has been published since 2004 by the College of European and Regional Studies (VŠERS) and the Institute of Technology and Business (VŠTE) twice a year, in electronic form only. So far, 860 scientific contributions and reviews have been published in 42 issues.
The Innovation Council, being a professional and advisory board of the government of the Czech Republic, included *Auspicia* (ISSN 1214-4967) among reviewed, non-impact scholarly journals involved in the topics of the National Reference Framework of Excellence (NRRE) in 2008–2013, and it was included there again in 2015 (http://www.vyzkum.cz/FrontClanek.aspx?idsekce=733439).

In 2016 *Auspicia* was listed in the international database ERIH PLUS and since 2024, it has been listed in the Central and Eastern Europe Online Library – CEEOL.

Thematic sections

After individual scientific papers successfully pass review, they are allocated towards one of the following sections:

1. Social Sciences
2. Safety
3. Public Administration, Management
4. Reviews

Basic instructions for authors

Language of the scientific paper: English, Czech; **reviews**: English, Czech. Articles can be submitted in either English or Czech, but English articles are preferred due to the international dimension of the journal.

Required range in sections 1–3: maximum 8 standard pages (1 standard page – 1800 characters including spaces).

Deadlines: 1st issue – 1 February; 2nd issue – 1 August.

Bibliography: 25% of resources indexed in Web of Science and/or Scopus databases.

Review process: double-blind, independent, objective.

Publishing dates: 1st issue – 1 June; 2nd issue – 1 December.

Detailed source: https://vsers.cz/recenzovany-vedecky-casopis-auspicia

How to cite a scientific paper: In: For the author. Article template -

https://vsers.cz/vedecky-casopis-auspicia/

Author's fee. Authors of the papers (contributions) are to pay the amount of CZK 1,000 for the expenses connected with publishing the scholarly contributions in the Czech language (contributions in English are temporary free of charge until further notice) of a maximum of 8 standard pages (or that amount plus CZK 200 per each subsequent standard page), or the appropriate amount in EUR in accordance with the current exchange rate in sections 1–3. This must be done by the closing date of the relevant volume (i.e., before the review process) either by means of bank transfer to the publisher's bank account No. 2101783605/2010**,** at Fio Banka, a. s. (České Budějovice branch), account EUR/IBAN code: CZ71 2010 0000 0024 0178 3607, BIC code: FIOBCZPPXXX (foreign payors pay the transfer charge by themselves), or they may pay it in cash at the Department of Economics of the College of European and Regional Studies. Registration numbers of authors' workplaces are variable symbols, the specific symbol is a code with the following digits: 12342022. The information regarding the payee should include the name of the author/authors and their workplace.

Contact address:
The College of European and Regional Studies
Žižkova tř. 1632/5b
370 01 České Budějovice
doc. PhDr. Miroslav Sapík, Ph.D., editor-in-chief
Telephone number: +420 386 116 839
E-mail: sapik@vsers.cz, https://vsers.cz/auspicia/