(ЗЛО)УПОТРЕБА „ШПИЈУНСКИХ СОФТВЕРА" У ПРАКСИ СЛУЖБИ БЕЗБЕДНОСТИ: МЕТОДОЛОШКЕ СМЕРНИЦЕ ЗА АНАЛИЗУ МЕДИЈСКОГ ИЗВЕШТАВАЊА

Оригинални научни рад

DOI: 10.5937/zurbezkrim2501009M	COBISS.RS-ID 143293441	УДК 351.746.1:316.774

Саша Мијалковић[1]
Криминалистичко-полицијски универзитет, Република Србија

Апстракт: „Шпијунски софтвери" последњих генерација за приступ садржајима, надзор комуникација и функционалних операција мобилних телефона (укључивање микрофона или камере мобилног телефонског уређаја без знања корисника), попут озлоглашених *Pegasus* и *Predator*, моћно су средство које службе безбедности, али и други недржавни актери, могу да злоупотребе против политичких неистомишљеника и критичара (новинара, адвоката, активиста), политичких противника и сваке врсте конкуренције.

Начин на који поједини медији о томе извештавају директно утиче на формирање јавног мњења о односу државе и служби безбедности према грађанима и политичким актерима: једни оптужују службе безбедности за неовлашћени електронски надзор и злоупотребу политичке моћи влада; други негирају злоупотребу, правдајући употребу интересима националне безбедности; трећи „ћуте". Дакле, медији могу да буду значајан узбуњивач због могућих нерегуларности, али и промотер лажних вести које могу да шкоде угледу служби безбедности и угледу државе.

С тим у вези, циљ овог истраживања је анализа садржаја медијског извештавања о шпијунским софтверима за надзор мобилних телефона у периоду после 2015. године, у земљама у којима су такве афере имале запажени медијски третман и запажену пажњу јавности: Мађарска, Пољска, Северна Македонија, Грчка, Израел и Мексико. Такође, дате су и начелне смернице за примену методе анализе садржаја у истраживању медијских саопштења о овом истраживачком предмету и проблему.

Кључне речи: методологија научног истраживања, анализа садржаја, медијска саопштења, шпијунски софтвери, надзор мобилних телефона, службе безбедности.

1 Проф. др Саша Мијалковић је редовни професор на Криминалистичко-полицијском универзитету у Београду. Имејл: sasa.mijalkovic@kpu.edu.rs

УВОД

Технички метод у прикупљању обавештајних сазнања је све значајнији у раду полиције, обавештајних и безбедносних служби. Важан аспект техничког метода јесте и употреба савремених софтверских решења за надзор телефонских комуникација, како фиксне тако и мобилне телефоније (Мијалковић, Милошевић & Ђеранић, 2023).

„Шпијунски софтвер" за тајни надзор и контролу мобилних телефонских уређаја је жаргонски назив за специјализовани рачунарски програм који омогућава неовлашћени приступ туђим мобилним телефонима ради увида у садржаје који су складиштени у телефону, ради надгледања писане, усмене и мултимедијалне комуникације, односно, ради управљања одређеним подсистемима/функцијама апарата (микрофон, камера, ГПС локатор итд.). Правилнији назив био би *софтвер за тајни надзор комуникација, садржаја и операција мобилних телефона* (Mijalković, 2017).

Најпознатији такав софтвер је *Pegasus* израелске компаније *NSO Group*, који је развијен почетком друге декаде овога века (Share Fondacija, 2021).[2] *Pegasus* омогућава потпуну контролу над зараженим телефоном – приступ камерама, микрофону, порукама, имејловима и фајловима, без знања корисника (Udruženje novinara Srbije, 2025).

Слични софтвери су се појавили широм света. Један од познатијих је *Predator*, који је развила компанија *Cytrox* (део конзорцијума *Intellexa*), и то у Северној Македонији. Његово постојање је обелодањено откривањем афера шпијунирања новинара и политичара у Грчкој и Египту (Investigative Reporting Lab Macedonia, 2023).

Осим *Pegasus* и *Predator*, постоје и други „комерцијални" шпијунски алати попут *FinFisher* и *Hacking Team* алата, који су током претходне деценије продавани владама широм света.

Према медијским саопштењима, *Pegasus* и *Predator* се од претходних шпијунских програма издвајају по распрострањености злоупотребе од стране државних органа безбедности против сопствених грађана, новинара и политичке опозиције. Владе су правдале набавку ових алата борбом против тероризма и тешког криминала, али су истраживања медија и организација за људска права наводно тврдила супротно. Међународни конзорцијум новинара под координацијом *Forbidden Stories* и *Amnesty International* је 2021. године из базе процурелих информација наводно открио да је на мети *Pegasus*-а било више од 50.000 телефонских бројева. Међу надзиранима је било више од 180 новинара широм света (Share Fondacija, 2021). Наводни закључак је био тај да клијенти *NSO Group* (а то су владини актери, најмање 40 њих из Мађарске, Азербејџана, Бахреина, Мексика, Марока, Саудијске Арабије, Казахстана, Руанде, Индије и Уједињених Арапских Емирата) често

2 Овај софтвер је светску пажњу привукао 2016. године откривањем да је злоупотребљен против једног активисте за људска права у Уједињеним Арапским Емиратима. Видети: (Share Fondacija, 2021).

користе Pegasus за политичку шпијунажу, праћење независних новинара, активиста и адвоката, а не само против криминалаца (Marczak et al., 2022). Ово сазнање изазвало је глобални скандал који је познатији као „*Pegasus пројекат*" и покренуло је бројне истраге о злоупотребама надзорних технологија (Share Fondacija, 2021).

Ако је веровати медијима, софтвери попут *Pegasus*-а откривени су у употреби у преко 45 земаља широм света – од демократских држава до ауторитарних режима. Новинари и опозиционари у Јерменији, Египту, Индонезији, Мадагаскару, Индији, Мароку, Саудијској Арабији, Уједињеним Арапским Емиратима, Руанди, Азербејџану и многим другим земљама били су мете. Свуда је примећен сличан образац: власти негирају или ћуте, док независни медији и невладине организације разоткривају такве случајеве. У неким државама (нпр. Француска, где је откривено да је Мароко *Pegasus*-ом пратио француске званичнике, или Шпанија где је откривен Pegasus надзор над каталонским политичарима, или Пољска где је откривено да је *Pegasus* коришћен против активиста, опозиционих лидера и новинара) избијају дипломатски скандали и покрећу се расправе. Ово је подстакло и наднационалне реакције – Европска унија је формирала специјални комитет (*PEGA*) да истражи коришћење *Pegasus*-а у Европи и 2023. године је препоручила строже мере контроле и могућу забрану таквих софтвера ако се не уведу гаранције за људска права (European Parliament, 2023). Експерти Уједињених нација су позвали на забрану продаје и употребе високотехнолошког надзорног софтвера док се не успоставе адекватни механизми заштите људских права (Smalley, 2024).

Дакле, питање (зло)употребе „мобилног шпијунског софтвера" постало је глобално питање људских права и демократије, а медијско извештавање о томе игра значајну улогу у надзору и контроли примене, односно у узбуњивању надлежних истражних и правосудних органа.

Интересантно је то да је *Predator*, шпијунски софтвер сличан *Pegasus*-у, развијан нелегално у региону – наводно у Северној Македонији. Истраживачки документи показали су да је компанија *Cytrox* у Скопљу наводно развила Predator уз знање тамошњих власти, а тај софтвер је потом (опет наводно) продаван државама као што су Египат, Саудијска Арабија, Грчка па и Србија (Investigative Reporting Lab Macedonia, 2023). Ако је то истина, онда Балкан није само мета, већ и извор технологија за дигитални надзор, што додаје контекстуалну тежину причи о медијском представљању ових појава.

Иако се Србија донедавно није експлицитно спомињала међу клијентима *NSO Group*, медији су оптужили домаће службе безбедности да су имале приступ сличним или истим алатима. *Amnesty International* и *Citizen Lab* су 2023. и 2024. године изнеле податке о томе да су српске безбедносне структуре наводно користиле најмање две врсте шпијунских средстава: *Pegasus* или сродни софтвер за даљинско хаковање телефона преко интернет линкова и комбинацију израелског форензичког алата *Cellebrite* и домаћег шпијунског софтвера *NoviSpy* за физичко хаковање телефона приликом

преузимања уређаја од лица током саслушања. Српске службе безбедности су то негирале, наглашавајући да своје дужности врше искључиво у складу са законима Републике Србије (Pravda, 2024; Amnesty International, 2024).

Предмет овог истраживања биће медијско извештавање о злоупотребама шпијунских софтвера у земљама у којима су такве афере имале запажени медијски третман и пажњу јавности, а у некима од њих и запажену реакцију националног система безбедности: Мађарска, Пољска, Северна Македонија, Грчка, Израел и Мексико.

Истовремено, избор ових земаља је оправдан јер су њих и Репортери без граница у својим годишњим извештајима под називом „*Светски индекс слободе штампе*" препознали као земље у којима се крши слобода медија.[3] Према извештају из 2025. године, Србија је рангирана на 96. месту, од посматраних 180 земаља. Компарације ради, Грчка је на 89. месту, Северна Македонија на 42. месту, Пољска је на 31. месту, Мађарска је на 68. месту, Израел је на 112, а Мексико на 124. месту. Босна и Херцеговина је на 86. месту. Иако је саставни део Републике Србије, Косово је рангирано на 99. месту (Reporters Without Borders, 2025).

Ова искуства су важна и због тога што показују како медији могу да буду значајан узбуњивач – иницијатор друштвене реакције на могуће нерегуларности али, такође, и како могу да буду промотер лажних вести које могу да шкоде угледу служби безбедности и угледу државе.

ТЕОРИЈСКИ ОКВИР ИСТРАЖИВАЊА

Разумевање медијског приказивања злоупотребе шпијунских софтвера могуће је у оквирима више теоријских приступа, а пре свега кроз: фрејминг теорију, теорију надзора и критичку теорију медија.

Фрејминг теорија (теорија уоквиривања) базира се на тези да начин на који медији приказују одређену тему, значајно утиче на то како ту тему публика разуме и тумачи. Речју, медији креирају мњење и ставове публике (Tewksbury & Scheufele, 2009). Тако медији начелно имају три приступа употреби шпијунских софтвера: могу да је представе као неопходност државе у борби против најопаснијих претњи националној безбедности, чиме подстичу став јавности о оправданости употребе; могу да је представе као грубо кршење приватности и људских права, посебно над политичким неистомишљеницима и противницима, чиме креирају оквир за осуду употребе шпијунских софтвера; могу да буду без вредносних ставова и судова,

3 *Репортери без граница* (*Reporters Without Borders*) је међународна невладина организација са седиштем у Паризу, која пропагира заштиту права на слободу информација које гарантују међународни извори људских права. Има значајан консултативни статус при Уједињеним нацијама, UNESCO, Савету Европе и Међународној организацији франкофоније. Сваке године, на основу сопствене методологије и процене, Репортери без граница објављују извештај под насловом *Светски индекс слободе штампе (медија)*, где су државе рангиране на основу извесних индикатора о слободи медија. Видети: (Reporters Without Borders, 2025).

односно, да не извештавају о таквим темама, чиме подстичу „медијски мрак", тј. неинформисаност јавности.

Теорија надзора/заверe (surveillance studies) пружа оквир за разумевање значаја технолошког надзора над широм популацијом: перцепција сталног надзора наводи појединце на аутодисциплину и послушност, па лица која знају да могу да буду праћена почињу да се прилагођавају том сазнању, што може довести до самоцензуре и смањења грађанске иницијативе. Истовремено, подстиче се безбедносна култура грађана који бирају нове начине сигурне комуникације.[4] Дакле, случајеви попут Pegasus-а могу да буду део ширег механизма друштвене контроле. То подстиче и анализу и преиспитивање *легитимизације надзора* – како државе оправдавају употребу инвазивних технологија (нпр. реториком борбе против тероризма и организованог криминала, да се све ради по закону, да су оптужбе и извештаји о злоупотребама неистинити и политички мотивисани, да је то пракса коју упражњавају и друге државе итд.) и како медији о томе извештавају.[5]

Критичка теорија медија кроз призму Франкфуртске школе[6], анализира односе медија и моћи омогућавајући да се испита како медијске институције и садржаји могу да подрже или да поткопају постојеће владајуће друштвене и политичке структуре. Из аспекта употребе шпијунских софтвера значајна су питања: да ли медији функционишу као контролор/узбуњивач који разоткрива злоупотребе државе или као пропагандни механизам који брани државне интересе? У ауторитарнијим режимима, држава често настоји да контролише медије и усмери наратив у своју корист, што може да порекне, минимизира или релативизује шпијунске аферe (тзв. *провладини медији*). Насупрот томе, независни медији и истраживачке новинарске мреже могу да делују као контратежа, објављујући доказе о злоупотребама и дајући глас жртвама (тзв. *слободни – критички медији*). Стога је ова теорија значајна за разматрање квалитативних разлика у извештавању различитих медија и чији интереси се кроз то извештавање одражавају.[7]

МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

Временски оквир овог истраживања обухватио је период од 2016. године (када су први пут глобално споменути *Pegasus* случајеви) до 2025. године.

4 Иако се надзор најчешће врши под изговорима сузбијања тероризма (Kouba, 2022; Trbojević & Svirčević, 2023) у пракси су злоупотребе надзора комуникација врло честе.

5 Ослоњена на идеје аутора као што су Џереми Бентам (концепт „Паноптикона"), Џорџ Орвел („1984") и савремених истраживача надзорних студија. Упореди са: (Glasser, 2021).

6 Институт за друштвена истраживања у Франкфурту (основан 1923) био је марксиситички и емпиријски оријентисан. Међу најзначајнијим представницима су Ерих Фром, Херберт Маркузе и Теодор Адорно.

7 Тако *The Guardian* тврди да је у Мађарској већина медија под утицајем власти, што објашњава зашто је откриће о *Pegasus*-у дошло захваљујући међународном пројекту и неколико независних новинара, док су државни медији или игнорисали причу или нападали њене изворе. Видети: Walker (2021).

Просторно, предмет истраживања ограничен је на земље у којима су такве афере имале запажени медијски третман: Мађарска, Пољска, Северна Македонија, Грчка, Израел и Мексико.

Дубинско сагледавање медијског приказивања злоупотребе шпијунског софтвера захтева мултиметодски приступ. На првом месту, најбоље је комбиновати *анализу садржаја медијских извештаја и саопштења* који се односе на шпијунски софтвер Pegasus, Predator или општије на тему дигиталног надзора од стране државе са квалитативним увидима (*интервјуи*) и увидима из других извора (извештаји и документа националних и међународних владиних, међувладиних и невладиних организација).

Обухваћени су различити типови медија:

– *национални медији који условно могу да се поделе на:*
  – независне *и истраживачке портале/новине* (који су објективни и нису под контролом влада и политичких центара моћи) и
  – *провладине медије и таблоиде* (чији су објективност и интегритет компромитовани јер су под отвореном или латентном контролом влада и политичких центара моћи, који игноришу проблеме и оптужбе или преносе ставове власти која такве оптужбе негира и релативизује);
– *инострани и регионални медији (за компарацију)*, који такође могу да буду независни и истраживачки портали/новине и провладини медији и таблоиди.

За потребе овог истраживања, коришћени су превасходно садржаји следећих медија: *Direkt36* (Мађарска), *TVN24/Gazeta Wyborcza* (Пољска), *Kathimerini* или *Documento* (Грчка), *NOVA TV* (Северна Македонија) итд.;

– *светски медији*, чији је медијски утицај глобалног домашаја*: The Guardian, The New York Times, Washington Post, Al Jazeera, Le Monde* и други који су релевантни за теме *Pegasus*/*Predator*.

Поред тога, *анализирани су садржаји докумената и јавних података* (примерних извора), попут званичних саопштења, правних аката и извештаја организација: извештаји Европског парламента, *Amnesty International, Citizen Lab, Access Now, SHARE Foundation* и других који су послужили за проверу фактичких навода и за упоређивање шта од тога долази до медија.

Анализа садржаја је била *квантитативно-квалитативна*.

Квантитативно, кодирани су чланци према неколико категорија: *тон* (критички према властима, неутралан, провладини), *оквир* (нагласак на скандалу и кршењу права, или на безбедносним аспектима, или на демантијима и сумњи у налазе), *присуство/одсуство изјава жртава*, *присуство изјава званичника*, *коришћење међународних извора* и слично. Ово у неком опширнијем истраживању омогућава и да се статистички сагледа разлика у приступу теми између независних и провладиних медија.

Квалитативно, извршена је анализа дискурса одабраних карактеристичних текстова – како наративно осмишљавају причу о шпијунском софтверу, које метафоре или поређења се користе, какви се морални ставови имплицирају (да ли је нагласак на томе да је то недопустив атак на слободе

или да је можда неопходно зло ради безбедности, итд.). Посебна пажња посвећена је насловима и ударним деловима текстова, јер они обликују први утисак код публике.

До медијских садржаја о предмету истраживања који су били предмет анализе дошло се претраживањем интернета употребом вештачке интелигенције (*DeepSeek*[8]), по основу кључних речи: шпијунски софтвер, *Pegasus*, *Predator*, употреба софтвера за надзор мобилне комуникације, злоупотребе шпијунских софтвера, медијско извештавање. Добијени су значајни извори, од којих је за потребе овог истраживања селектован само један део. Извори који су се односили на Републику Србију нису анализирани, и биће предмет другог рада.

Дакле, овде је фокус на методу анализе медијских садржаја, али овај метод би у истраживању злоупотребе „шпијунских софтвера" требало комбиновати са другим методама. На првом месту, за то су погодни методи:

- *анализе садржаја* извора националног и међународног права којима су регулисани електронски надзор (закони о електронским комуникацијама, закони о службама безбедности, закони о кривичном поступку, кривични закони) како би се расветлила законитост употреба *Pegasus*/*Predator* софтвера, као и анализа садржаја полицијских и судских списа и предмета;
- *испитивања техником структурисаног и полуструктурисаног интервјуа*, првенствено: новинара који су радили на откривању случајева злоупотреба оваквих софтвера, новинара и уредника провладиних медија који су спремни да говоре о разлозима неизвештавања о случајевима злоупотреба оваквих софтвера, адвокатима који су заступали појединце који су неовлашћено надзирани, тужиоце и судије који су радили на таквим случајевима, стручњацима за информациону безбедност који поседују знања о шпијунским софтверима и жртве надзора. Посебно интересантни испитаници су стручњаци из организација које прате стање људских права у области комуникација и истражују случајеве злоупотреба надзора комукација (на примјер, *PEGA Committee, Amnesty International, Citizen Lab, SHARE Foundation, Access Now, Amnesty Security Lab* итд.), као и припадници служби безбедности и надзорних државних органа (парламентарни и владини одбори, омбудсман, повереник за заштиту података о личности, тужиоци, судије) који су спремни да објективно учествују у истраживању. У извесним ситуацијама треба проценити корисност примене тзв. *фокус-групног интервјуа*, ради суочавања ставова испитаника;

8 DeepSeek је кинески модел вештачке интелигенције. Видети: (Ng & Drenon, 2025). Интересантно је поменути то да је вештачка интелигенција, приликом избора текстова, за сваку државу изабрала по највише два извора, а било је случајева да се један извор односио на двије државе. Можда је то због тога што је коришћен основни („најјефтинији") претплатнички пакет.

– *испитивања техником анкете,* и то: грађана, ради добијања ставова и индикатора о степену развијености свести о могућим злоупотребама шпијунских софтвера; новинара, како из провладиних, тако и из слободних медија, о њиховим сазнањима и ставовима о предмету истраживања. Анкету је згодно сповести слањем електронских упитника на имејл адресе испитаника;
– *студије (вишеструког) случаја*, како оних који су имали судски или било какав епилог у виду реакције државних органа који контролишу рад служби безбедности тако и случајева чији је епилог само у реакцији одређених невладиних институција или медија. Уколико је реч о веома специфичном случају, у оквиру којег су наступиле страшне последице и који је посебно значајан из аспекта угрожавања безбедности појединца, корисно је применити тзв. *биографски метод*, за дубље сагледавање и повезивање свих чињеница и околности случаја;
– *статистички метод,* чија је примена ограничена због велике тамне бројке, али који је значајан за сагледавање тзв. *левка појаве*, тј. за праћење односа броја сумњивих случајева злоупотребе шпијунских софтвера, пријављених случајева, процесуираних (унутрашња контрола служби безбедности, приватна тужба, кривични процес) случајева и резултата процеса истраживања, што указује на однос органа формалне социјалне контроле према овој појави.

Комбиновањем наведених методских приступа у истраживању злоупотреба шпијунских софтвера, стекле би се шире и комплетније искуствене информационе евиденције, које омогућавају извођење правилнијих закључака, те давање адекватних препорука за решавање проблемских ситуација.

ПРИМЕРИ МЕДИЈСКОГ ИСТРАЖИВАЊА У ЕВРОПСКОМ РЕГИОНУ

Случајеви оптуживања власти због сумњи на злоупотребу шпијунских софтвера против новинара, опозиције и цивилног друштва последњих година приметни су у низу земаља Централне и Источне Европе, укључујући чланице Европске уније (European Parliament, 2023a). Медијско приказивање таквих афера варира у складу са политичким околностима, али се могу уочити неке заједничке црте.

Мађарска је постала један од најпознатијих европских примера злоупотребе Pegasus софтвера. У јулу 2021. године глобални „*Pegasus пројекат*" открио је да је велики број мађарских новинара, бизнисмена и опозиционих личности био на мети *Pegasus* надзора. Истраживачки портал *Direkt36* објавио је, уз техничку потврду *Amnesty International*-а, да су телефони најмање десетак новинара и активиста хаковани *Pegasus*-ом у периоду од 2018. па надаље.[9]

9 Посебно је упечатљив случај новинара Саба Пања (*Szabolcs Panyi*) из *Direkt36*: он је утврдио да се инфекција његовог телефона *Pegasus*-ом десила готово сваки пут непосредно након што

Медијска реакција у Мађарској била је подељена. Такозвани *независни медији* објавили су серију чланака и емисија о овој теми. *Direkt36*, *Telex*, *HVG* и неколико других објавили су имена особа које су биле мета и тражили одговорност власти. Међународни медији, попут *The Guardian*, посвећено су извештавали о владином надзору медија, наглашавајући да је притисак на новинаре попримио скривене облике попут шпијунирања и економског гушења слободних медија (Walker, 2022). Такозвани *провладини медији*, који су доминантни, или су игнорисали тему или су преносили минималне информације уз нагласак на званичне ставове. Тако су причу држали подаље од већине грађана. А званични став је у почетку био одсуство коментара (влада није дала јасан одговор новинарима, осим општих изјава о томе да „Мађарска увек поштује закон"). Тек када је притисак порастао, неки високи функционери су индиректно признали да је Мађарска набавила „софтвер за борбу против тероризма", али су инсистирали на томе да се он користи само против легитимних мета. Критички настројени портали су приметили да у Мађарској није спроведена ниједна независна истрага поводом *Pegasus* афере. Иако је међународни скандал био велики, у домаћој јавности у Мађарској није дошло до масовних протеста или озбиљне политичке штете за режим због овог открића – што делом може да се објасни управо медијским уоквиривањем и заташкавањем теме (Reuters, 2021; European Parliament, 2022).

Ситуација у Пољској је била другачија. Открића о *Pegasus*-у изазвала су такве политичке последице, да се око тога ломила јавна расправа уочи избора 2023. године. Током 2021. и 2022. године, откривено је (уз помоћ *Citizen Lab*-а) да је пољска конзервативна влада (Право и правда) користила Pegasus да прати најмање неколико политички значајних личности: међу њима опозиционог сенатора Кршистов Брежу (*Krzysztof Brejza*) који је водио кампању опозиције на изборима, затим тужитељку и адвоката опозиције. О овоме су опширно извештавали независни пољски медији (нпр. *Gazeta Wyborcza*, *TBH24*) и међународни (*Associated Press* је први јавио за случај сенатора Бреже). Владајућа Право и правда је месецима порицала да уопште поседује *Pegasus*. Међутим, притисак је растао – Европски парламент је покренуо расправу, а у Пољској је Сенат (у ком је опозиција имала већину) формирао истражну комисију. *Сенатска комисија* је у септембру 2022. закључила да је било „*грубог кршења уставних стандарда*" и да су избори 2019. можда били компромитовани употребом шпијунског софтвера против опозиције. Чак је препоручено покретање кривичних поступака против одговорних (Mazzini, 2025), а започете су и истраге (Walker, 2024).

Такозвани *независни медији* су ове налазе представили као „*Пољски Вотергејт*", апострофирајући опасност по демократију када влада прислушкује опозицију током изборне кампање. Такозвани *провладини медији*

би послао питања мађарској влади за неки истраживачки текст. То снажно индикује да је влада користила шпијунски софтвер да би *унапред сазнала* на чему ради и ко су му извори. Видети: (Walker, 2021).

покушали су да одбране владу тврдњама да је све рађено у оквиру закона и у интересу националне безбедности. Интересантно, сам лидер Права и правде, Јарослав Качињски (*Jarosław Kaczyński*), у интервјуу почетком 2022. признао је да је Пољска купила *Pegasus*, изјавивши чувену реченицу: „*Добро, имамо тај софтвер, па шта? Свако га има*", покушавајући да минимизује аферу. Међутим, инсистирао је на томе да је коришћен искључиво у сузбијању криминала. Ова признања, мада намењена да нормализују ситуацију, заправо су потврдила сумње и дала ветар у леђа независним медијима да наставе да истражују ко је све био мета. Уочи избора 2023. године, опозиција је обећала расветљавање афере. После победе опозиције, крајем 2023. нова власт (предвођена Доналдом Туском) објавила је да поседује документе који „*100% потврђују*" да је претходна власт илегално користила *Pegasus* и пратила најмање 600 људи, што је озбиљна оптужба. Ова тема је у пољским медијима доспела на насловнице – и као потврда ранијих новинарских открића, и као питање за правосуђе (Notes from Poland, 2024).

Дакле, у пољском контексту види се да су медији и институције деловали у спрези: независни медији и међународне организације открили су аферу; део институција (Сенат, после и нова влада) потврдио је налазе и покренуо званичне кораке. Ово је пример где медијско изношење скандала, захваљујући плурализму, није могло бити ућуткано и довело је до политичке одговорности. За разлику од Мађарске где монопол власти над медијима гуши ефекте скандала, у Пољској је постојао довољан простор да се тема одржи актуелном до промена власти.

У Грчкој је злоупотреба *Predator* софтвера одјекнула у медијима 2022. године. Грчка јавност била је шокирана откривањем да је грчка Национална обавештајна служба (*ΕΥΠ – Εθνική Υπηρεσία Πληροφοριών*) која је непосредно подређена кабинету премијера, прислушкивала телефоне више лица, укључујући новинара – Танасиса Кукакиса и лидера мање опозиционе партије – Никоса Андрулакиса. Испоставило се да су неке од тих мета „легално прислушкиване" (надзор комуникација уз судски налог), али да је паралелно покушано (а у случају Кукакиса и успело) да се шпијунски софтвер *Predator* инсталира на њихове телефоне. Скандал који је познат као „грчки Вотергејт" избио је у јулу 2022. и довео је до оставки шефа *ΕΥΠ*-а и генералног секретара премијера (који је уједно и нећак премијера Кирјакоса Мицотакиса) (Dimou, 2023).

Медији у Грчкој су у почетку били опрезни – државни и провладини медији нису сами открили аферу, већ су реаговали тек након што је опозиција изнела доказе. Независни медији (попут листа *Documento* и мреже *Reporters United*) одиграли су важну улогу, објављујући спискове потенцијалних мета *Predator*-а и истичући да је траг многих шпијунских операција водио до кругова блиских влади. Међународни медији (*Politico*, *The Guardian*) такође су пратили причу, што је повећало притисак. Премијер је у медијима дао изјаву да „*није знао*" за операцију и да би је одмах зауставио да је знао, покушавајући да се огради од скандала. Провладини грчки медији трудили су се да подрже ту верзију догађаја, па су неки дневници и ТВ програми

скандал представљали као „*изоловани пропуст*" обавештајне службе или чак као „*претерано надувану причу*" политичке опозиције. Ипак, грчки медијски простор је морао да се суочи са чињеницом да је поверљивост комуникација нарушена. Значајно је да је Грчка по индексу слободе медија (RSF) 2022. пала на најниже место у Европској унији, чак испод Мађарске, што су многи повезали управо са афером *Predator* и генерално лошом климом за независно новинарство. Грчки пример показује да чак и у земљи чланици ЕУ са формално снажним институцијама, механизми државног надзора могу бити злоупотребљени, а медијска борба да се то разоткрије може да буде тешка и ризична. Грчка је покренула парламентарну истрагу, али њени резултати су били ограничени због страначких подела. У међувремену, европски *PEGA* комитет озбиљно је разматрао и грчки случај као део ширег проблема употребе шпијунског софтвера у Европи (Mildebrath, 2022).

Северна Македонија има дуго искуство са скандалима о прислушкивању. Још 2015. године опозициони лидер, Зоран Заев, обелоданио је да су тадашње власти (режим Николе Груевског) нелегално прислушкивале преко 20.000 грађана, укључујући новинаре, судије, активисте и саме политичаре. Тај скандал довео је до велике политичке кризе и на крају до промене власти. Медији у Северној Македонији су 2015. године нашироко извештавали о прислушкивању – опозициони и независни медији свакодневно су објављивали сегменте прислушкиваних разговора, чинећи јасним обим злоупотреба од стране тајне полиције (Управа за безбедност и контраразузнавање – УБК). Провладини медији су покушавали да одбране режим тврдећи да су снимци можда фалсификовани или да је страни фактор умешан у „државни удар". Али, под притиском Европске уније, случај је истражен и добио је судски епилог годинама касније (The Geopost, 2024).

У последње време, међутим, Северна Македонија се помиње и у контексту модернијег шпијунског софтвера. Као што је већ наведено, истраживања су открила да је фирма *Cytrox* развијала *Predator* у Скопљу, и то уз знање власти (Euronews, 2021; Investigative Reporting Lab Macedonia, 2023).

Медијски извештаји (на примјер, македонски Истраживачки репортерски лаб – *IRL*, у сарадњи са грчким *Inside Story*) показали су да је држава још 2017. била информисана о томе, али да није реаговала (Investigative Reporting Lab Macedonia, 2023). Ово указује на могућу спрегу бизниса, власти и глобалне шпијунске индустрије.

Македонски медији су ово питање покренули након што су грчки и други европски медији скренули пажњу. Јавност у Северној Македонији делом је свесна да је њихова земља била база за такав пројекат, али није било јавних доказа да је сама македонска влада користила Pegasus или Predator против својих грађана након смене режима 2017. године. Ипак, ово је грађане учинило осетљивим на тему надзора, па се сва открића будно прате.

Регионални примери показују заједнички образац: *тамо где је медијска слобода сузбијена, злоупотребе надзора остају дуже скривене и некажњене*; *у државама са живљом медијском сценом и конкуренцијом различитих политичких опција долази до раскринкавања и бар делимичне одговорности*.

ПРИМЕРИ МЕДИЈСКОГ ИЗВЕШТАВАЊА У СВЕТУ

Шпијунски софтвери за мобилне телефоне су глобални феномен те је корисно сагледати медијска искуства из света. Овде ће фокус бити на Израелу као колевци ових технологија и примеру домаћег скандала, и на Мексику као једној од земаља са најдужом и најпотврђенијом историјом злоупотребе *Pegasus*-а.

Израел је „родно место" *Pegasus*-а и неколико других сличних алата. Иронично, сам Израел је доспео на насловнице 2022. године због оптужби да је *израелска полиција нелегално користила Pegasus против сопствених грађана*. Лист *Calcalist* објавио је серију текстова у јануару 2022. тврдећи да је полиција, без судских налога, прислушкивала телефоне десетина људи који нису осумњичени за злочине – укључујући градоначелнике, лидере протеста против Нетанијахуа, па чак и сина бившег премијера (Ganon, 2022). Ово откриће је изазвало огромну буру у израелској јавности и политици. Премијер је најавио хитну истрагу, а министар полиције је изразио шок (Al Jazeera, 2022).

Медијски дискурс у Израелу по том питању био је буран: сви већи медији су данима расправљали о томе, постављана су питања у скупштини, а цивилни сектор (*ACRI – Association for Civil Rights in Israel* – Удружење за грађанска права) захтевао је да *полиција одмах обустави употребу Pegasus-а* (Maanit, 2023).

У року од месец дана, Министарство правде је изашло са првим налазима истраге, наводећи да, иако је полиција користила *Pegasus*, „*нема доказа да је то рађено противзаконито*". Закључак да није било незаконитости образложен је тиме да је у случајевима који су проверени или постојао судски налог или је покушај хаковања био неуспешан, те да нису пронађени докази масовног прислушкивања без одобрења. Овакав исход изазвао је сумњичавост код дела јавности и новинара – *Calcalist* је стајао иза својих тврдњи, а многи су сматрали да је истрага била преуско фокусирана и да су власти пожуриле да заштите институције од скандала. Ово је био први пут да је израелска влада *јавно потврдила* да је *Pegasus* уопште коришћен против израелских држављана (McKernan, 2022).

Израелски случај је значајан из више разлога:

– показује да чак и у земљи која је извозник надзорних алата, постоји потенцијал да се они употребе *унутар* земље, што одмах покреће питања баланса између безбедности и грађанских слобода;
– медијско праћење тог скандала било је интензивно – Израел има релативно снажне медије и цивилно друштво, и иако је и тамо власт покушала да контролише наратив, постојала је отворена јавна дебата;
– израелска влада се после међународних притисака (*Pegasus пројекта*) одлучила на одређене кораке да ограничи извоз ове технологије – крајем 2021. смањен је број земаља којима израелско

Министарство одбране дозвољава куповину таквих алата. Тако је, бар декларативно, ускратила лиценце неким режимима са лошим стањем људских права. То је последица лошег публицитета *NSO Group*-а и дипломатских притисака (САД су у новембру 2021. ставиле *NSO Group* на „црну листу"). У израелским медијима се о томе расправљало кроз призму економских интереса (јер је, с једне стране, *NSO* успешна извозна фирма, а, с друге стране, доносила је негативан публицитет држави) (Al Jazeera, 2024).

Укратко, Израел у овој причи има двојаку улогу: као творац технологије који сада мора да ублажава њене злоупотребе и као држава у којој је разоткривено да ни њене институције нису имуне на искушење недозвољеног надзора.

Мексико је био један од првих и највећих клијената *NSO Group*: још 2011–2012. године, мексичке федералне власти купиле су *Pegasus* наводно за борбу против нарко-картела. Међутим, процурела тајна документа и истраживања организације *Citizen Lab* и мексичке невладине организације *R3D* открили су невероватне размере злоупотребе: мета *Pegasus* напада током мандата председника Енрике Пења Нијета (*Enrique Peña Nieto*) (2012–2018) били су новинари, активисти за људска права, адвокати па чак и међународни истражитељи. Скандал је кулминирао 2017. године када су *New York Times* и *Citizen Lab* објавили да је *Pegasus* коришћен против новинара који су истраживали корупцију, против адвоката који су заступали породице несталих студената, па чак и против детета једног од мета (у циљу праћења његових родитеља) (Kitroeff & Bergman, 2023).

Ови налази су шокирали мексичку јавност. Независни медији као што су *Aristegui Noticias* и *Proceso* дали су велики простор жртвама да испричају своја искуства, док су већи национални ТВ канали под утицајем владе у почетку извештавали опрезно, често преносећи и одбрану владе да „нема доказа" или да „то раде приватни/недржавни актери" (Aristegui Noticias, 2025).

Под притиском, 2017. године мексичко тужилаштво је отворило истрагу. Међутим, истрага годинама није имала помака и на крају је практично заташкана током претходне власти. Политичка промена долази 2018. године када је за председника изабран Андрес Мануел Лопез Обрадор (Andrés Manuel López Obrador – *AMLO*), левичар који је обећао прекид праксе шпијунирања грађана. Он је јавно рекао да његова влада неће користити *Pegasus* и да ће раскинути везе са таквим методама. И једно време тема је спласнула. Међутим, у шокантном обрту, 2022. године појављује се извештај да је чак и под Андресовом администрацијом мексичка војска наставила да користи *Pegasus*: група *R3D* и *Citizen Lab* објавили су да су најмање три особе – двојица новинара и један активиста – имале *Pegasus* инфекције телефона у периоду 2019–2021 (Solomon, 2022).

Испоставило се да су све троје истраживали наводе о кршењу људских права од стране војске у борби против дроге. То је изазвало сумњу да је мексичка војска, можда аутономно од цивилних власти, наставила да користи

софтвер. Ово откриће објављено је у октобру 2022. године (извештај *R3D* под називом *„Ejército Espía"*), а медији су поново брујали о томе како „*Pegasus и даље живи у Мексику*". Андрес је био суочен са незгодним питањима; његови представници су тврдили да влада није склопила нове уговоре, али нису директно демантовали могућност да је војска користила стари софтвер (Ejército Espía, n.d.; Solomon, 2022).

Такође, познато је да је мексичка војска раније куповала *Pegasus*, па је вероватно могла да га користи на своју руку. Ово индикује да у неким државама институције попут војске или безбедносних служби имају „тврда језгра" и сопствене агенде које одолевају променама политичке гарнитуре.

Мексички случај је медијски изузетно добро документован и анализиран у светским оквирима, и пружа јасан пример *могућности злоупотребе савремених софтверских алата за неовлашћени надзор лица, уз велику вероватноћу избегавања одговорности за учињене злоупотребе*. Упркос мноштву доказа и великој домаћој, иностраној и међународној медијској пажњи, упркос бројним насловницама, извештајима организација попут *Amnesty International* и *Human Rights Watch*, па чак и упркос препорукама специјалног извештача Уједињених нација о потреби контроле над софтверима, мексички институционални одговор је изостао и у Мексику *нико није озбиљно санкционисан* за злоупотребе *Pegasus*-а. Ово указује на културу некажњивости: медији могу обелоданити истину, али ако правосуђе и политичка воља затаје, жртве неће добити правду (Article 19, 2024).

ЗАКЉУЧАК

Медији имају важну улогу у разоткривању случајева злоупотреба надзора комуникација, у едуковању грађана о њиховим слободама и правима и начинима заштите, и у притиску на државу да расветли такве случајеве и санкционише одговорне.

Компаративна анализа медијског извештавања о случајевима злоупотребе софтвера за надзор мобилне телефонске комуникације указује на то да је оваква пракса присутна чак и у земљама Европске уније: у случајевима Мађарске и Грчке, то је угрозило углед власти и рангирање тих земаља у погледу слободе медија; у случају Пољске, јасно је да до политичких промена и односа према злоупотреби надзора комуникација може доћи, али тек након промене режима на власти. Супротно, у неким државама (Израел, Мексико) откривене афере нису имале епилог у виду кривичноправне реакције државних надзорних механизама.

Државни и провладини медији су по правилу преносили саопштења званичних државних органа, а нису саопштавали резултате независних истраживачких новинара. С друге стране, неизвештавањем о шпијунским софтверима, део јавности који прати медије са националном фреквенцијом (провладине медије) остајао је неинформисан, односно, могао је да стекне перцепцију о томе да никакве злоупотребе заправо нема.

Провладини медији тему често скрећу и на апстрактнији терен, представљајући је као део хибридног ратовања и кампање непријатељских организација против државе или њених служби безбедности. Истовремено, објављиване су и вести о сличним случајевима *у другим државама*, али на начин који релативизује домаћу причу: „сви то раде" (па и демократске државе) „па ни ми нисмо изузетак".

Уочљив је *и приступ игнорисања личности жртава*. Док тзв. независни медији објављују изјаве новинара и активиста који су били мета, тзв. провладине новине ретко спомињу имена конкретних мета надзора. На тај начин, прича остаје на нивоу апстракције и делује као поговарање.

Медијско извештавање о злоупотребама „шпијунских софтвера" може резултирати *ефектом страха грађана*, посебно политичких активиста и независних медија, код којих ће се подстаћи безбедносна култура. Они ће минимизирати комуницију мобилном телефонијом или ће користити заштићене комуникационе апликације, односно, друге видове комуницирања (уживо, фиксном телефонијом, имејловима итд.) када говоре о поверљивим темама. То доводи до *ефекта „хлађења" слободе говора*, па и до *ефекта параноје*, као последице страха од надзора и од санкције због изговорених речи.

Супротно, није немогућ ни *ефекат предаје/прегоревања*, када грађани једноставно доживе немоћ и надзирање прихвате као нешто од чега нема заштите или (не дај боже) као меру која је корисна за безбедност државе и друштва.

Исто тако, могуће је да протестовање против неовлашћеног надзора комуникација постане део агенде грађанских протеста и нереда на јавним окупљањима.

Најзад, медијско извештавање о злоупотребама „шпијунских софтвера" може резултирати ерозијом поверења у државне институције, пре свега, у службе безбедности, у полицију, у правосудне органе и у тела која су надлежна за контролу рада служби безбедности. Ово посебно уколико се у медијским саопштењима изнесу непобитни докази о неовлашћеном надзору. Уколико се таква „прашина" подигне на међународни ниво, може доћи и до реакције међународних организација, од осуђујућих, преко стопирања процеса међународних интеграција, до санкционишућих.

Али, ако су такве вести лажне, долази до неоснованог нарушавања угледа службе безбедности и владе.

ЛИТЕРАТУРА

Al Jazeera. (2022, February 8). *What you need to know about Israeli spyware Pegasus.* Retrieved June 23, 2025, from https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus

Al Jazeera. (2024, February 1). *Journalists, activists targeted in Jordan with Israeli-made Pegasus spyware.* Retrieved June 23, 2025, from https://www.aljazeera.com/news/2024/2/1/journalists-activists-targeted-in-jordan-with-israeli-made-pegasus-spyware

Amnesty International Security Lab. (2024, December). *Srbija: Vlasti koriste špijunske softvere i forenzičke alate kompanije Cellebrite za hakovanje novinara i aktivista.* Retrieved June 15, 2025, from https://securitylab.amnesty.org/latest/2024/12/srbija-vlasti-koriste-spijunske-softvere-i-forenzicke-alate-kompanije-cellebrite-za-hakovanje-novinara-i-aktivista/

Article 19. (2024, January 15). *Mexico: Investigations into the use of Pegasus spyware must continue.* ARTICLE 19. Retrieved June 23, 2025, from https://www.article19.org/resources/mexico-investigations-into-the-use-of-pegasus-spyware-must-continue/

Aristegui Noticias. (n. d.). *Pegasus.* Retrieved June 23, 2025, from https://aristeguinoticias.com/tag/pegasus/

Dimou, E. (2025, May). *Greek Watergate: Behind the Pegasus spyware scandal.* Green European Journal. Retrieved June 23, 2025, from https://www.greeneuropeanjournal.eu/greek-watergate-behind-the-pegasus-spyware-scandal/

Ejército Espía. (n. d.). *Ejército Espía.* Retrieved June 23, 2025, from https://ejercitoespia.r3d.mx/

Euronews Srbija. (2021, December 20). *Predator protiv Pegaza: Kako radi špijunski softver iz Severne Makedonije koji je pronađen i u Srbiji.* Retrieved June 23, 2025, from https://www.euronews.rs/magazin/tehnologija/29848/predator-protiv-pegaza-kako-radi-spijunski-softver-iz-severne-makedonije-koji-je-pronaden-i-u-srbiji/vest

European Parliament. (2022, October). *Briefing for the PEGA Committee: PEGA Committee – Mission to Cyprus and Greece (PE 738.330).* Retrieved June 23, 2025, from https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738330/IPOL_BRI(2022)738330_EN.pdf

European Parliament. (2023). *Spyware as a threat to fundamental rights and democracy in the EU.* Retrieved June 23, 2025, from https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

European Parliament. (2023a). *Investigation of the use of Pegasus and equivalent surveillance spyware: Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus*

and equivalent surveillance spyware (2023/2500(RSP)), P9_TA(2023)0244. Retrieved June 23, 2025, from https://eur-lex.europa.eu/eli/C/2024/494/oj/eng

Ganon, T. (2022, January 18). Israel police uses NSO's Pegasus to spy on citizens. *Calcalist Tech.* Retrieved June 23, 2025, from https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.htm

Glasser, W. (2021). *Teorija nadzora: Kako vzpostaviti učinkovit nadzor nad svojim življenjem.* Ljubljana: Chiara.

Investigative Reporting Lab Macedonia. (2023, April 12). *Israeli company developed spyware in Skopje, local officials looked the other way.* Retrieved June 23, 2025, from https://irl.mk/israeli-company-developed-spyware-in-skopje-local-officials-looked-the-other-way/

Kitroeff, N., & Bergman, R. (2023, April 18). How Mexico became the biggest user of the world's most notorious spy tool. *The New York Times.* Retrieved June 23, 2025, from https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html

Kouba, T. (2022). Online radicalization: Twitter privatization as a threat to the modern society. *Politika nacionalne bezbednosti, 13* Special Issue, 101–110.

Maanit, C. (2023, July 20). Israel to investigate police use of NGO's Pegasus spyware. *Haaretz.* Retrieved June 23, 2025, from https://www.haaretz.com/israel-news/2023-07-20/ty-article/.premium/israel-to-investigate-police-use-of-ngos-pegasus-spyware/00000189-74c0-d09f-a3a9-f7e921120000

Marczak, B., Scott-Railton, J., Razzak, B. A., Aljizawi, N., Anstis, S., Berdan, K., & Deibert, R. (2022). Pegasus vs. Predator: Dissident's doubly-infected iPhone reveals Cytrox mercenary spyware. *The Citizen Lab.* Retrieved June 23, 2025, from https://citizenlab.ca/2022/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Mazzini, M. (2025, February 25). Pegasus in Poland: A flight for justice that never took off. *Balkan Insight.* Retrieved June 23, 2025, from https://balkaninsight.com/2025/02/25/pegasus-in-poland-a-flight-for-justice-that-never-took-off/

McKernan, B. (2022, February 22). Police use of Pegasus malware not illegal, Israeli inquiry finds. *The Guardian.* Retrieved June 23, 2025, from https://www.theguardian.com/world/2022/feb/22/police-use-of-pegasus-malware-not-israeli-inquiry-finds

Mijalković, S. (2017). Contribution to differentiation of the term „intelligence operation" from „espionage". In *Archibald Reiss Days – Thematic Conference Proceedings of International Significance* (Vol. 1, pp. 219–228). Academy of Criminalistic and Police Studies.

Мијалковић, С., Милошевић, М. & Ћеранић, П. (2023). *Обавјештајне и безбједносне службе – организација и методика обавјештајног, безбједносног и субверзивног дјеловања.* Бања Лука: Факултет безбједносних наука Универзитета у Бањој Луци.

Mildebrath, H. A. (2022, September 8). Greece's Predatorgate: The latest chapter

in Europe's spyware scandal?, *European Parliament*, Retrieved June 15, 2025, from https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)733637.

Ng, K., & Drenon, B. (2025, January 28). DeepSeek: Kineska četbot aplikacija o kojoj priča svet. *BBC News na srpskom.* Retrieved June 16, 2025, from https://www.bbc.com/serbian/articles/cp8kwger1x8o/lat

Notes from Poland. (2024, April 16). *Almost 600 people targeted with Pegasus spyware under former Polish government.* Retrieved June 23, 2025, from https://notesfrompoland.com/2024/04/16/almost-600-people-targeted-with-pegasus-spyware-under-former-polish-government

Pravda.rs. (2024, December 16). *Србија као „полицијска држава": БИА, МУП и Амнести Интернатионал „у клинчу" – неко овде дебело измишља и лаже!* Retrieved June 15, 2025, from https://pravda.rs/index.php?id=1&L=992%252522%252529%252520AND%2525205224&tx_news_pi1[news]=194215&tx_news_pi1[controller]=News&tx_news_pi1[action]=detail&tx_news_pi1[day]=16&tx_news_pi1[month]=12&tx_news_pi1[year]=2024&cHash=a2dac9eb2cae3069b9861c789c8c959f

Reporters Without Borders. (2025, May 3). *RSF World Press Freedom Index 2025: Economic fragility a leading threat to press freedom.* Retrieved June 23, 2025, from https://rsf.org/en/rsf-world-press-freedom-index-2025-economic-fragility-leading-threat-press-freedom

Reuters. (2021, July 27). *Hungarians protest against alleged illegal surveillance with Pegasus spyware.* Reuters. Retrieved June 23, 2025, from https://www.reuters.com/world/europe/hungarians-protest-against-alleged-illegal-surveillance-with-pegasus-spyware-2021-07-26/

Share Fondacija. (2021, July 21). *The Pegasus Project: what happened and how to protect yourself.* Retrieved June 15, 2025, from https://sharefoundation.info/en/the-pegasus-project-what-happened-and-how-to-protect-yourself/

Smalley, S. (2024, April 25). Polish PM says previous ruling party used Pegasus spyware against 'very long' list of victims*. The Record.* Retrieved June 15, 2025, from https://therecord.media/polish-pm-says-previous-ruling-party-used-pegasus-spyware-on-long-list-of-victims

Solomon, D. B. (2022, October 3). Pegasus spyware attacks in Mexico continued under Lopez Obrador – report. *Reuters.* Retrieved June 23, 2025, from https://www.reuters.com/world/americas/pegasus-spyware-attacks-mexico-continued-under-lopez-obrador-report-2022-10-03/

Tewksbury, D. & Scheufele, D. (2009). News framing theory and research. In J. Bryant & M. B. Oliver (Eds.), *Media effects: Advances in theory and research* (pp. 17–33). Routledge.

The Geopost. (2024, June 12). *Notorious spyware 'Predator' that had spied on journalists, businessmen and politicians was developed in North Macedonia*. Retrieved June 23, 2025, from https://thegeopost.com/en/security/notorious-

spyware-predator-that-had-spied-on-journalists-businessmen-and-politicians-was-developed-in-north-macedonia/

Trbojević, M., & Svirčević, B. (2023). Methods of intelligence services in the fight against terrorism. *Politika nacionalne bezbednosti, 25*(14), 157–181.

Udruženje novinara Srbije. (2025, March 27). *Dve novinarke BIRN-a na meti špijunskog softvera: Napadači koristili lažnu N1 stranicu.* Retrieved June 15, 2025, from https://uns.org.rs/desk/vesti-iz-medija/171797/dve-novinarke-birn-a-na-meti-spijunskog-softvera-napadaci-koristili-laznu-n1-stranicu.html#:~:text=Две%20новинарке%20БИРН,поруками%2C%20мејловима%20и%20фајловима

Walker, S. (2021, July 18). Viktor Orbán using NSO spyware in assault on media, data suggests. *The Guardian.* Retrieved June 15, 2025, from https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests

Walker, S. (2022, January 28). Hungarian journalists targeted with Pegasus spyware to sue state. *The Guardian.* Retrieved June 15, 2025, from https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state

Walker, S. (2024, April 1). Poland launches inquiry into previous government's spyware use. *The Guardian.* Retrieved June 15, 2025, from https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use

Рад примљен: 11. 7. 2025.
Рад одобрен: 1. 10. 2025.