# Не ризикуј, заштити податке- информатор о дигиталној безбедности новинара

*Ауторка: Александра Ничић, Удружење новинара Србије (УНС)*

*УНС се захваљује Радету Драговићу и Бојану Перовићу из Института за стандарде и технологије и адвокату Урошу Недељковићу на помоћи у изради информатора.*

**Садржај**

## Увод

Експанзија интернета у 21. веку пренела је већ постојеће претње медијским професионалцима на онлајн простор, али је истовремено изнедрила и нове безбедносне ризике. Главна мета злоупотреба које су специфчне за онлајн сферу постали су лични подаци, а њихово разоткривање различитим центрима моћи претворило се у својеврстан вид опасности за новинаре. Како је све више података који се претражују, чувају, обрађују и преносе, поверљивост и тајност никада није било лакше угрозити.

„Само у 2019. години „процурело“ је 1,76 милијарди записа, а имајући у виду велики део света који не користи интернет, то значи да је нека информација сваког од нас те године била откривена“, рекао је Раде Драговић из Института за стандарде и технологије. Ови подаци нису охрабрујући ни за једног корисника, а посебно не за новинаре који се, у тежњи да информишу јавност и интерпретирају важне друштвене теме, суочавају са бројним притисцима и злоупотребама.

Како би што већи део јавности приступио садржају који су креирали, новинари и медијске куће линкове ка својим текстовима, видео и аудио записима свакодневно деле путем профила или страница на друштвеним мрежама. Социјалне платформе, на основу података које је корисник несвесно „добровољно дао“, креирају алгоритме од којих зависи које ће им се информације пласирати приликом скроловања. Приступ локацији, микрофону, лајкови, шерови, претрага и лични подаци које смо дали приликом прављења налога или преузимања апликације неки су од индикатора на основу којих ове компаније креирају алгоритме.

"Ако је нешто бесплатно, ти си производ", каже Друштвена дилема, документарни филм у коме IT стручњаци који су радили у најутицајним компанијама данашњице указују на опасности „бинарног света“.

Вођени мишљу да је приватност на интернету немогуће заштитити и да великим компанијама није битан садржај који креирају, медијски професионалци су бригу о дигиталној безбедности свели на минимум. Попут већине корисника, приликом преузимања апликација, новинари некритички дају дозволе за приступ подацима и без читања прихватају политику приватности и услове коришћења различитих плафторми.

Ипак, треба имати у виду да битка за заштиту приватности није унапред изгубљена. Начини на које се може осигурати дигитална безбедност сежу од институционалних решења попут креирања политика и покретања Центра за превенцију безбедносних ризика (ЦЕРТ) до индивидуалних свакодневних помака у које се убраја подизање свести о томе на које све начине приватност може бити угрожена.

„Свест о ризицима, активно коришћење механизама заштите, познавање окружења у којем се остварује интеракција, упознавање са политикама приватности и условима коришћења, само су неки од захтева који се стављају пред савременог корисника интернет услуга“ , сматра доц. др Марта Митровић (Митровић, 2020: 9). Од испуњавања ових и сличних стандарда зависи дигитална безбедност сваког медијског посленика, без обзира на то са којег дела планете информише јавност или интерпретира значајне друштвене феномене.

## Потенцијални ризици са којима се новинари суочавају када прикупљају информације за текстове

Узнемиравање путем интернета један је од најучесталијих видова угрожавања безбедности медијских професионалаца у Србији, наводи се у извештају платформе „Слобода медија брз одговор“ (MFRR) који су сачинили Европска федерација новинара (EFJ), Међународни институт за штампу (IPI) и Европски центар за слободу медија (ECPMF).

У Европи су, према овом извештају, поред вербалних, сајбер напади најбројнији. „Број напада који се дешавају на мрежи порастао је са 14,7% у 2021. на 22,8% у 2022. години, а интернет је постао простор на коме су новинари најчешће нападнути […] У оквиру 71 забележеног инцидента, нападнуто је 126 новинара. Ови напади укључују застрашивање и претње у већини случајева (40 инцидената), дискредитовање и клевета (10 инцидената), увреде (10 инцидената), хаковање (8 инцидената) или надзор (4 инцидента)“ (Mapping Media Freedom, 2022: 16).

Новинари који раде на важним истраживачким причама дигитално су угрожени и у фази прикупљања података. Потенцијална могућност да власти држава у којима раде имају увид у податке које прикупљају код новинара може изазвати већи страх и тежњу ка самоцензури од могућности да моћне светске компаније свакодневно приступају

њиховим подацима. Осим што је важан фактор за релевантност вести, близина представља значајан елемент и у интересовању за дигиталну безбедност. Медијски професионалци су неретко става да им злоупотреба личних и информација које су прикупили од стране моћних светских компанија неће нанети непосредну штету, а да им угрожавање приватности од стране државних институција може променити живот. Због тога, вођени страхом, одустају од објављивања информација које су месецима, а некад и годинама прикупљали.

Дигитални надзор, хаковање, напади на веб локације, присвајање новинаревог ауторског дела и рачунарске системе попут , тзв. "phishing-a" (чија је сврха крађа идентитета) и MITM напада (базирог на пресретању комуникације) само су неки од начина да се угрози дигитална безбедност новинара приликом прикупљања " (Building digital safety for journalists, 2015: 20-21).

Ваља нагласити да информација представља потатак или скуп података у одређеном контесту, те се због тога означава као резултат обраде података. Насумично поређане цифре, слова или знаци представљају податак, али постају информација тек када заједно чине нечије име, матични број, датум рођења и слично.

Данас се информације најлакше претражују путем интернета, на коме су доступне многобројне архиве, базе, али и текстови са различитих портала, неретко пласирани на друштвеним мрежама. Прикупљајући информације, новинари информације „дају“ и тзв. "трећој страни“, а њу чине многе фирме које зарађују од препродаје наших података, и то најчешће у маркетиншке сврхе, каже Бојан Перовић из Института за стандарде и технологије.

На пример, како тврди адвокат Урош Недељковић, информације о томе на који начин смо трошили новац трећим лицима неретко продају такозване картичарске компаније.

„Основни приход картичарских компанија је продавање података трећим лицима. Банке немају право да продају податке, али картичарске компаније су фирме као и сваке друге. Стога се немојте зачудити уколико идете да купите тепих и након годину дана крену да вам излазе рекламе тепиха. Логика је: можда му се излизао тепих, ево рекламе“, рекао је Недељковић.

Значајан метод за прикупљање података је и интервју, који се неретко обавља путем интернета, бележи уређајима или модификује уз помоћ дигиталних алата. Као такав, са собом носи ризике да важне информације пошаље „у погрешне руке“. Мислећи да „трећу страну“ подаци неће интересовати у мери да пресреће телефонске разговоре или приступа микрофону њихових телефона, новинари свакодневно користе мобилне телефоне за снимање интервјуа у току којих некада добијају врло поверљиве информације. Да лични подаци појединаца нису тако небитни посебно потврђују информације које је изнео Едвард Сноуден, према којима Америчка агенција за безбедност (NSA) врши надзор над становништвом.

Др Катарина Јонев је у разговору за УНС истакла да чињеница да су том приликом процуреле преписке са преко 250 хиљада налога људи које нису јавне личности показује да сваки корисник треба да води рачуна о дигиталној безбедности.

"Приватне информације о нама и информације које смо прикупили обично завршавају код "треће стране", а она је значајна за прављење архива које ће завршти на даркнету, односно мрачној страни интернета. Тада неко може злоупотребити наше податке израдом фалсификата личних карата и пасоша, како би се представљао као ми. Са друге стране, информације се продају маркетиншким компанијама", објаснила је Јонев.

У истраживању UNESCO-а о дигиталној безбедности новинара наводи се да је тешко утврдити који ентитет или субјекти надзиру наше активности на интернету или на сличан начин угрожавају нашу приватост. „Специјалиста за дигиталну безбедност би могао да открије име компаније која је направила софтвер за надзор, али је теже утврдити ко је наручио или применио напад“, оцењују из UNESCO-а. (Building digital safety for journalists, 2015: 22).

**Новинари се са ризицима суочавају и након обајвљивања информација**

Многи новинари приликом дистрибуције информација подлежу аутоцензури, јер су свесни да њихово објављивање није крај већ почетак борбе са различитим притисцима. Неке од претњи са којима се медијски професионалци суочавају су из офлајн света пренети у онлајн сферу у којој им је због брзине дисеминације информација појачан интензитет. Протон мејл показао се као један од начина да се редакцијама и појединцима шаљу претње, а пошиљаоци се могу открити тек када се активирају све надлежне

институције. Ово потврђује недавни пример претњи које су стигле у редакцију дневног листа Данас.

Ваља нагласити да је ова Протон мејл потпуно легална платформа и сматра се једним од уобичајених начина заштите идентитета пошиљаоца. Ипак, попут многих корисних ствари, и овај начин енкрипције добио је своју негативну сврху оличену у претњама разним корисницима.

Да онлајн претње новинарима нису безазлене, показује UNESCO-ово истраживање о дигиталној безбедности новинара, из 2015. године, у коме се наводи да је у периоду од 2011. до 2013. године већина убијених новинара користила дигиталне алате за свакодневни рад, те да постоји могућност да су убијени јер су њихови подаци били изложени убицама (Building digital safety for journalists, 2015: 14) . Ова информација указује на то да дигиталним опасностима нису изложени само новинари који пишу за онлајн издања већ и медијски професионалци који раде за традиционалне медије, јер су и за њих архиве и базе података на интернету битан извор информација.

Организације за људска права често не располажу са довољно ресурса да са сигурношћу утврде ко стоји иза сваке претње медијском раднику, као и колико често се на тај начин угрожава слобода изражавања. Важан задатак је стога идентификовати врсте претњи и одговарајуће заштите за оне који се сматрају дигитално угроженима, наводе у истраживању UNESCO-a (Building digital safety for journalists, 2015: 14).

## Шта све новинар може учинити да се заштити

На основу процене могућих ризика за дигиталну безбедност новинара, издвојене су препоруке које би помогле медијским професионалцима да се заштите од могућих злоупотреба на интернету. Дате смернице могле би помоћи новинарима да очувају своју приватност, али и кредибилитет приликом обављања свакодневних новинарских задатака.

**Новинар мора водити рачуна о идентитету особе са којом комуницира.** Када се каже „заштита телефона“, обично се најпре помисли заштиту од вируса који би могли оштетити уређај. Ипак, у новинарској професији битнија је заштита од штетне комуникације. Новинар не би требало да преко мејла или СМС-а прихвата ништа што

није у оквирима њему познатог комуникационог поља. Погрешан лого организације, сумњиво време слања, језик некарактеристичан за пошиљаоца, изостављен наслов, Гмаил или Yahoo налог којим се представља значајна институција или компанија само су неки од аларма који сигнализирају новинару да не преузима документ и не отвара линк који је тим путем примио. Одбијањем да преузме такав документ, новинар превенира многобројне облике угрожавања дигиталне безбедности – од Ransomware напада до крађе личних података.

Ransomware напад дешава се када одређена група прође вашем систему и закључа га, након чега тражи откуп. Ове групе, како објашњава Раде Драговић из Института за стандарде и технологије, процењују колико су појединац или институција спремни да плате да би откључали податке. Стога Ransomware напад можемо спречити водећи рачуна о томе шта отварамо на рачунару, јер нам путем мејла могу пристићи документи или ликнови чије отварање нам онемогућава даљи приступ нашим фајловима.

Највећа мета напада је, сматра Драговић, оно што најчешће користимо, те су најугроженији Мајкрософт фајлови (doc, docx), као и pdf који није Мајкрософтов али се чита кроз Мајкрософт алате.

**Вишеструка провера информација добијених на интернету.** У јеку технолошког напретка све је више начина на који новинар може доћи до информација, али и све више шанси да упадне у замку објављивања полуинформација и дезинформација. Данас, када свако може доћи до различитих подтаака, новинара од других издваја управо способност да објави тачну и проверену информацију.

Медијска присменост је за дигиталну писменост постала conditio sine qua non. Медијски професионалац нипошто не може закључити да је безбедан у дигиталном окружењу уколико наивно приступа информацијама са сваког портала. Да би се заштитио од дезинформација и злоупотреба, новинар чувено 5Ws правило може применити и за проверу поузданости интернет извора информација.

За процену кредибилности онлајн извора, како сматра професор др Веселин Кљајић, неопходно је проверити „ауторитет, тачност, објективност, ажурирање и покривање“. Неопходно је, дакле, одговорити на питања: „Ко је поставио сајт? Шта сајт обухвата? Где

пронаћи податке који вам требају? Када је update-ован и са колико актуелних података располаже? Како пронаћи жељене информације?“ (Кљајић, 2009: 118).

Осим тога, новинарима путем интернета свакодневно пристижу информације од грађана, до редакција је никад лакше доћи, а све ово интензивира двосмерну комуникацију новинара и саговорника. Поузданост новинара у онлајн партиципацији грађана је све важнија. Како доц. др Марко Недељковић наводи у Приручнику за предузетничко новинарство, „то значи да он проверава и верификује информације добијене од корисника, чини их кредибилним, и тек након тога их инкорпорира у медијски садржај који креира“ (Недељковић ет. ал, 2014 : 20).

**Директан приступ медијима.** Негативна последица алгоритама на друштвеним мрежама је једноличан медијски садржај који се пласира на почетним странама сваког корисника. Уколико кориснику на друштвеним мрежама излази искључиво медијски садржај који му је идеолошки близак и уврштава се у категорију оног што свакодневно прати, могућност да реципијент чује другу страну сведена је на минимум. Због тога је за новинара који жели да буде квалитетно информисан важно да се приликом информисања не ослања на садржај који му се пласира на почетним странама друштвених мрежа, већ да прати различите портале улазећи на њих директно. Да је ова пракса уобичајена за медијске професионалце показује Гугл аналитика сајта специјализованог за новинарство – uns.org.rs, према којој највише корисника на сајт долази директно, а не путем друштвених мрежа.

**Избегавање снимања поверљивих интервјуа мобилним телефоном.** Када услове коришћења апликације, корисник даје дозволу компанији да његови подаци, у које се убраја и звук, буду обрађивани. Осим ових апликација, како каже Раде Драговић, постоје и други центри моћи који могу приступити значајним информацијама када радимо истраживачке приче које угрожавају интересе појединаца. Тако "трећа страна" сигурно може чути интервју који је новинар уснимио чак и пре њега самог. Уколико новинар обавља поверљиве разговоре изворима информација који би му били водиља за истраживачку причу али их притом не би објавио, снимање диктафином је најбољи начин да те информације не процуре.

**Подизање свести о томе да се на „паметним телефонима“ све обради и пре него што видимо.** Уколико корисник уђе на свој Гугл налог и на претраживачу на апликацији

"Гугл слике" укуца на пример реч „пас“ или дог, изаћи ће фотографије свих паса које је икада фотографисао, што значи да паметни телефони добро препознају садржај и сврху фотографија. Новинар на ово посебно треба да обрати пажњу када ради неку важну истраживачку причу са поверљивим информацијама добијеним од извора.

**Подешавање дупле аутентификације.** Дупла аутентификација (двостепена ауторизација) представља механизам који спречава да било ко осим самог корисника приступи његовом налогу на друштвеним мрежама. С обзиром на то да се показало да лозинке, посебно слабе или средње, не штите довољно од злонамерног пријављивања на профиле, компаније су утврдиле да је корисницима потребан „додатни слој заштите“. Када корисник на подешавањима активира дуплу ауторизацију, он стопира процес пријављивања како би се утврдило да ли се заиста пријављује корисник који стоји иза одређеног профила. То се чини тако што апликација шаље код за пријаву на број телефона или имејл адресу корисника које је новинар доставио приликом прављења налога. Све што је потребно је да новинар унесе овај код у поље које му се након уношења лозинке појави на екрану.

Уколико новинар покушава да се пријави на свој имејл налог, шифра за пријављивање стићи ће на имејл адресу коју је пријавио као алтернативну.

Ипак, треба имати у виду да ни дупла аутентификација не представља стопроцентну заштиту већ само доприноси заштити података. С обзиром на то да тај SMS у коме корисник добија код стиже не стиже у криптованом обилку, за хакера није тешко да до тих података дође пре корисника. Из тог разлога, Бојан Перовић из Института за стандарде и технологије сматра да је двостепена аутентификација самостално недовољно јака и новинарима као решење предлаже договоре са операторима како би код који шаљу апликације заштитили од пресретања и различитих видова злоупотреба.

**Избегавање прикључивања на јавне WiFi мреже.** Многи новинари прикључују се на јавне WiFi мреже у кафићима, библиотекама или другим јавним местима како би објавили текстове или их шеровали на друштвеним мрежама. Објављивање ауторских дела и важних истраживачких прича, као и обављање новчаних трансакција и других активности у оквиру којих се деле поверљиви подаци сваки новинар треба избегавати када је повезан на отворену вајрлес мрежу. Стручњаци за дигиталну безбедност неретко истичу да су отворене WiFi мреже најчешћа мета хакерских напада. Иако су многе

отворене мреже безбедне, радње у којима се деле поверљиви подаци не треба обављати на уређају који је прикључен на јавну мрежу.

**Коришћење јаких лозинки и њихова честа промена.** Јака лозинка подразумева лозинку са више од десет карактера које обавезно чине мала слова и бар по једно велико слово, број и знак. Непрепоручљиво је да шифре садрже име или презиме корисника. За сваку платформу на којој има профил новинар би требало да осмисли другачију лозинку.

Лозинке треба често мењати, како би се могућност да се неко улогује на наш профил свела на минимум. Кенет Олмстед и Ерон Смит сматрају да је најпрепоручљивије користити софтвере за формирање лозинки јер је такав вид заштите најтеже "разбити" (Olmstead & Smith, 2017: 14).

Иако су се софтвери за креирање лозинки показали као делотворни, они који служе за тестирање њихове ефикасности су заправо и сами извор опасности. Раде Драговић истиче да је основни циљ ових софтвера управо прикупљање лозинки које је корисник осмислио, како би се приступило његовим налозима и злоупотребили његови приватни подаци.

Драговић сугерише новинарима да лозинке пишу као да их је дете изговорило, јер су хакери најлакше приступају лозинкама са изразима који постоје у светским речницима.

**Често ажурирање апликација и целокупног софтвера.** Новије верзије апликација и софтвера подразумевају унапређенију заштиту и нови низ мера за безбедније коришћење. „Стручњаци за безбедност подстичу кориснике да редовно и правовремено инсталирају ажурирања за своје апликације и оперативни систем, пошто ова ажурирања често садрже важне безбедносне слојеве“, наводе Олместед и Смит (Olmstead & Smith, 2017: 20).

Међутим, ажуриране верзије неретко изискују неколико десетина мегабајта меморије више, за шта многи уређаји немају капацитета. Из тог разлога, корисници одбијају предлоге за ажурирање софтвера како не би били принуђени да ослобађају простор са својих телефона.

**Информисање о томе чему „колачићи“ служе.** Веб-сајтови претраживачу корисника шаљу фајлове у виду текста које претраживачи чувају, и на тај начин памте се детаљи о

посети корисника. Подаци се даље користе за анализу преференција корсника, које служе за унапређивање сајта или имају маркетиншку сврху.

Маркетиншки колачићи, према публикацији о дигиталној безбедности коју су радили Балканска истраживачка мрежа Србије (BIRN) и SHARE фондација, користе се „за прикупљање различитих информација о вашој посети нашем сајту, као што су информације о садржају који сте прегледали, везама које сте пратили, вашем претраживачу, уређају или IP адреси“, док аналитички колачићи „омогућавају да прикупљамо податке о вашем коришћењу интернет странице у циљу побољшања њеног учинка и дизајна“ (Политике и протоколи за медије – заштита података о личности и дигитална безбедност, 2022: 7–8).

**Новинар мора пазити шта преузима.** Уколико новинар који ради у великим системима на рачунару на послу преузме звук, фотографију, видео-снимак или било који други фајл са вирусом, то може узроковати пад система. Није исто преузети датотеку са вирусом на личном рачунару, јер ће узроковати мању штету него на рачунару медијске куће.

**Не инсталирати апликације које потражују превише личних података и давати само неопходне дозволе.** Могућности уређивања и дистрибуирања онлајн садржаја су све веће, са њима расте и али недостатак информисаности о могућем угрожавању приватности коју доноси инсталирање одређених платформи. Корисник не треба да даје дозволе које нису неопходне да би апликација функционисала. Многи софтвери су креирани тако да им је основна сврха прикупљање података корисника. Због тога апликације овог типа не треба инсталирати. Пример злоупотребе података су неке апликације за препознавање песама, јер је основна дозвола коју траже стални приступ микрофону са телефона корисника. Такве платформе Бојан Перовић назива „апликацијама трећих страна“, због чега препоручује само инсталирање општепознатих апликација, а изузетак су мање релевантне апликације које не траже сагласност за приступ важним личним информацијама.

Тренутак у којем се од корисника тражи сагласност за приступ подацима за сваки оперативни систем је специфичан. Код паметних уређаја са оперативним системом Андроид, дозволе за приступ подацима дају се непосредно након инсталирања како би се уопште могло приступити апликацији. Тада новинари нису у стању да уоче предности

апликације пре него што дозволе да приступи њиховим личним подацима, јер су иницијално условљени да дају сагласност.

За кориснике iOS интерфејса ситуација је другачија, јер апликације инсталиране на I-phone-у, I-pad-у и другим уређајима са овим оперативним системом шаљу упит за дозволу тек када корисник приступи апликацији. Напретком се може сматрати и опција да дамо дозволу апликацији да приступа одређеним подацима само док је користимо, а то значи само док је апликација укључена.

Корисницима се препоручује да се информишу о компанији чију апликацију преузимају, пажљиво прочитају услове коришћења и образложење компаније у коме се наводи због чега им потражује сагласност за приступ личним подацима. Ваља истаћи да кориснику након прихватања ових услова коришћења неће бити познато колико учестало се прикупљају његови подаци.

Раде Драговић као могуће решење препоручује новинарима и да искључе дозволе у подешавањима након обављања неопходне радње на апликацији или да апликацију деинсталирају и инсталирају је поново када им буде неопходна.

**Куповина оперативних система.** Инсталирање крекованих софтвера је непрепоручљиво јер са собом носи безбедносни ризик. Ови софтвери представљају иманентну опасност да личне информације корисника буду откривене. Новинари, који неретко располажу важним информацијама, морају бити свесни тога да у дигиталном свету није бесплатно.

**Уколико се суочи са угрожавањем безбедности, новинар о томе треба обавестити струку и институције.** Информисањем новинарских удружења, медијских кућа и међународних владниних и невладиних организација о томе са којим се ризицима суочава, новинар може предупредити сличне случајеве у будућности. Због тога из UNESCO-а препоручују да се новинар у току и након суочавања са безбедносним ризицима на интернету обрати телима Уједињених нација, међународнним и регионалним организацијама (владине и невладине), влади, корпорацијама, новинским организацијама, образовним установама за новинаре, новинарским удружењима, колегама и свим другим особама или институцијама које доприносе новинарству (Building digital safety for journalists, 2015: 50)

**Развој дигиталне писмености.** Дигитална писменост представаља „сет знања, вештина и ставова неопходних за критичко, безбедно и креативно коришћење дигиталне технологије" (Кузмановић према Гроздић, 2021: 29). Ове компетенције стога не подразумевају само практична знања о коришћењу различитих интернет платформи већ и свест о опасностима које дигитални свет са собом носи.

Многа истраживања базирана на анкетама као основној методи показала су да корисници не размишљају о безбедносним ризицима на интернету.

Интернет анкета од 308 корисника Андроида и лабораторијска студија од 25 корисника Андроида открили су да је само 17% обраћало пажњу на дозволе (укључујући оне које апликацији дају приступ подацима који су осетљиви на приватност) приликом инсталирања апликације. Такође су открили да је само 3% испитаника интернет анкете показало потпуно разумевање екрана са дозволама [9] (Poter Felt et. al, 2012: 4)

**Новинар треба испитати на који начин му законска регулатива може помоћи да осигура дигиталну безбедност.** GDPR или Општа уредба заштити података је уредба Европске уније односи се на права која сваки појединац има када неко прикупља или обрађује његове личне податке. У Србији GDPR није директно на снази али је Закон о заштити података о личности усклађен са европском законском регулативом везаном за очување приватности података на интернету. У податке о личности се убрајају генетски, биометријски и подаци о здрављу, наводи се на сајту WTS Србија[1].

Према овом Закону, подаци о личности се морају прикупљати у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама („ограничење у односу на сврху обраде“); Надлежни органи приватне податке могу прикупљати и обрађивати искључиво ако постоји јасна сврха за ову радњу. Подаци о личности који су прикупљени од стране надлежних органа у посебне сврхе не могу се обрађивати у сврху која је различита од сврхе за коју су подаци прикупљени, осим ако је та даља обрада прописана законом, наводи се у Закону о заштити података о личности.

https://www.wtsserbia.com/blog/gdpr-srbija/ (posećen: 28. novembra u 02:10 časova)

Такође, Устав Републике Србије гарантује тајност писама и других средстава комуницирања, док Закон о информационој безбедности садржи скуп мера за заштиту подФопреаатака.

Наш лик је податак, као што је и фотографија. Из тог разлога, није дозвољено неовлашћено фотографисати, односно, објављивати фотографије које су настале као производ неовлашћеног фотографисања.

Када се обављају телефонски позиви за које је неопходно законско пресретање, надлежни државни орган који врши ову радњу, дужан је да води евиденцију о пресретнутим комуникацијама. Уколико постоји наредба да се позив пресретне, мора се видети на основу чега је заведена, а прикупљени подаци морају остати приватни, рекао је адвокат Урош Недељковић.

Оператер је дужан да задржи податке о одлазним и долазним позивима - почетку, завршетку, трајању и врсти комуникације. Како Урош Недељковић истиче, евиденција обухвата и позиве на које се неко није одговорио, али не обухвата позиве чије успостављање није успело (уколико смо звали, а било је заузето).

Забрањено је задржавање података који откривају садржај комуникације, односно, оно о чему смо разговарали са неким.

Нико нема право да пресреће разговоре телефона, без обзира на то да ли је у питању комуникација путем мобилне мреже, фиксне мреже или интеренета. Законско пресретање, по одлуци суда, могу вршити само безбедносне службе које имају право да прислушкују због криминалног дела, каже Бојан Перовић. Оператери немају право да чувају садржај разговора, осим уколико је суд наложио да садржај сачувају.

***Уколико новинар сматра да му је угрожена дигитална безбедност имејл може послати на адресу Удружења новинара Србије (УНС) unsinfo1@uns.org.rs. Ово удружење биће канал комуникације са стручњацима из Института за стандарде и технологије, који ће им дати савете како да их реше.***

## Препоруке за медијске куће

**Сарадња са професионалцима за дигиталну безбедност.** За новинаре је неопходно повезивање са стручњацима који би спровели различите механизме за заштиту сваког новинара и корисника. Ангажовање стручњака за дигиталну безбедност који би сугерисао новинарима које платформе нису конципиране на начин да угрожавају његову дигиталну безбедност. Осим што би новинаре упознали са безбедносним ризицима, ови стурчњаци би водили рачуна о томе на који начин функционише целокупан систем. На тај начин би спречили DoS, phishing, MITM и друге нападе, али и заштитили кориснике који приступају порталима ових медијских кућа.

**Формирање ЦЕРТ-а.** Иако постоји национални Центар за безбедност информационо-комуникационих система односно Центар за превенцију безбедносних ризика (ЦЕРТ), препорука Радета Драговића је да медијске куће и новинарска удружења формирају свој заједнчки ЦЕРТ, који би, по угледу на ЦЕРТ-ове других бранши, имао директну везу са националним ЦЕРТ-ом. На овај начин медијски професионалци би омогућили експедитивно и делотворно реаговање на безбедносне инциденте, али и анализирали могуће ризике и спречили наредне нападе на свој информационо-комуникациони систем.

**Политике за очување дигиталне безбедности.** Свака медијска кућа требало би да има адекватну политику безбедности која ће се састојати од низа мера које ће обезбедити нормално функционисање редакција приликом дигиталних напада. Ове политике би требало да буду интерне за сваки медиј.

„У зависности од капацитета и ресурса организације, у креирању интерних безбедносних политика се подразумева учешће менаџмента, уредништва, чланова тима задужених за IT, као и новинара и других запослених који поседују напредније техничке вештине које могу пренети другима. Обука и едукација запослених су значајне како би се процедуре и политике примењивале а да се притом редовни процеси рада не ремете“ (Политике и протоколи за медије – заштита података о личности и дигитална безбедност, 2022: 10).

# Izvori:

## Literatura:


- BIRN & SHARE fondacija (2022). Politike i protokoli za medije – zaštita podataka o ličnosti i digitalna bezbednost, Beograd
- Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012, July). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-14).
- Grozdić, V. B. (2021). Digitalna pismenost-potencijalni odgovor na izazove kriza. *Život u kriznim vremenima-andragoški pogledi*, 27-41.
- Henrichsen, J. R., Betz, M., & Lisosky, J. M. (2015). *Building digital safety for journalism: A survey of selected issues*. UNESCO Publishing.
- Kljajić, Veselin (2009). Intervju u štampi, onlajn magazinima, na internetu, Čigoja štampa, Beograd
- Media Freedom Rapid Response – EFJ – IPI – ECPMF (2022). *Mapping media freedom*.
- Mitrović, M. (2020). Sloboda izražavanja i zaštita podataka o ličnosti na internetu: Perspektiva internet korisnika u Srbiji. *CM: Communication and Media*, *15* (47).
- Nedeljković, Marko (2014). Osnove veb novinarstva. U: Marko Nedeljković (ur), Priručnik za preduzetničko novinarstvo (str. 9-16), Beograd: Konrad-Adenauer-Stiftung.


## Zakoni:


- Zakon o zaštiti podataka o ličnosti
- Zakon o informacionoj bezbednosti


## Onlajn izvori:


*www.wtsserbia.com*