Финансирано од Европска Унија

ЕУ со ТЕБЕ

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

МЗМП

ДОКУМЕНТ ЗА ЈАВНИ ПОЛИТИКИ

ЗАШТИТА НА ПРИВАТНОСТА И ЛИЧНИТЕ ПОДАТОЦИ НА СОЦИЈАЛНИТЕ МРЕЖИ И НА ИНТЕРНЕТ-СТРАНИЦИТЕ

ЗАШТИТА НА ПРИВАТНОСТА И ЛИЧНИТЕ ПОДАТОЦИ НА СОЦИЈАЛНИТЕ МРЕЖИ И НА ИНТЕРНЕТ-СТРАНИЦИТЕ

Издавач:
Македонско здружение на млади правници
Центар за правни истражувања и анализи

За издавачот:
Бојана Божиновска Силјановска, Претседателка на МЗМП
Лидија Стојкова Зафировска, Претседателка на ЦПИА

Автор:
Арбен Гудачи
Мартина Дранговска Мартинова

Редакција:
Милена Јосифовска, ЦПИА
Сара Марковска, ЦПИА
Маја Атанасова, МЗМП

Лектура:
Дејан Василевски

Графички дизајн:
Релатив

Оваа публикација е изработена во рамките на проектот „**Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн-просторот**“, финансиран од Европската унија. Содржината на публикацијата е единствена одговорност на авторите и на никаков начин не може да се смета дека ги одразува гледиштата на Европската унија.

СОДРЖИНА

ПРЕДГОВОР 4

ВОВЕД 5

1. МЕЃУНАРОДНА И ДОМАШНА ПРАВНА ЗАШТИТА 7

   1.1. ПРАВО НА ПОЧИТУВАЊЕ НА ПРИВАТНИОТ И СЕМЕЈНИОТ ЖИВОТ 7

2. ИНСТИТУЦИОНАЛНА РАМКА ЗА ЗАШТИТА 10

3. ПОВРЕДА НА ПРАВОТО НА ПРИВАТНОСТ И ЗЛОУПОТРЕБА НА ЛИЧНИТЕ ПОДАТОЦИ НА ИНТЕРНЕТ 12

4. ВИДОВИ ПОВРЕДИ НА ПРАВОТО НА ПРИВАТНОСТ НА СОЦИЈАЛНИТЕ МРЕЖИ 13

   4.1. Креирање на лажни профили 13

   4.2. Неовластен пристап до профили 13

   4.3. Неовластено објавување на туѓи лични податоци 14

5. ПРЕГЛЕД НА СУДСКАТА ПРАКТИКА 15

6. ЗАКЛУЧОЦИ И ПРЕПОРАКИ 18

РЕЗИМЕ НА ПРЕПОРАКИ 20

ПРЕДГОВОР

Овој документ за јавни политики е подготвен во рамките на проектот: „Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн просторот“, финансиран од Европската унија и имплементиран од Центарот за правни истражувања и анализи (ЦПИА) и Македонско здружение на млади правници (МЗМП). Цел на проектот е да се зајакнат капацитетите на судството и јавното обвинителство во ефикасна заштита на приватноста на граѓаните, како и другите права и основни слободи засегнати од новите технологии во онлајн просторот во согласност со правото и стандардите на ЕУ.

Целта на овој документ за јавни политики е да обезбеди сеопфатен и стратешки пристап за решавање на клучните предизвици за Заштита на приватноста и личните податоци на социјалните мрежи и на интернет-страниците. Преку овој документ, се настојува да се идентификуваат и анализираат главните проблеми кои бараат интервенција, да се дефинираат приоритетите и да се предложат конкретни решенија кои ќе придонесат за Заштита на приватноста и личните податоци на социјалните мрежи и на интернет-страниците. Посебен акцент се става на инклузивноста во пристапот, каде што заклучоците и препораките ќе бидат заеднички потврдени преку активна дебата со претставници на сите засегнати институции. Ова ќе осигури дека различните перспективи и интереси се земени предвид, создавајќи сеопфатни и балансирани политики.

Со имплементација на предложените мерки, се очекува да се постигне значителен напредок во справувањето со идентификуваните проблеми и да се создадат услови за континуирано подобрување на јавните политики и услуги во областа на Заштита на приватноста и личните податоци на социјалните мрежи и на интернет-страниците.

ВОВЕД

Приватноста и заштитата на личните податоци се неразделно поврзани концепти што заеднички го обезбедуваат правото на поединецот да одреди кога, како и до кој степен неговите лични податоци ќе бидат споделени со другите.[1] Приватноста се однесува на поширокиот концепт на лична и информациска автономија, додека личните податоци претставуваат конкретни информации што идентификуваат или можат да идентификуваат поединец.

Во денешниот дигитален свет, каде што огромни количества на лични податоци се собираат, обработуваат и споделуваат преку интернет, заштитата на личните податоци е клучна за одржување на приватноста. Без ефективни механизми за заштита на личните податоци, приватноста на поединецот може да биде повредена, што може да доведе до злоупотреба на личните податоци, нарушување на дигиталната безбедност и сериозни последици за личната и професионалната репутација.

Темата за повреда на приватноста и злоупотреба на личните податоци на интернет, особено на социјалните мрежи и интернет-страниците, е од исклучителна релевантност и актуелност во Република Северна Македонија. Со брзиот раст на користењето на дигиталните технологии и интернетот, се зголемува и изложеноста на ризиците од нарушување на приватноста. Социјалните мрежи, како „Фејсбук“, „Инстаграм“ и „Тикток“, играат значајна улога во секојдневниот живот на луѓето, овозможувајќи им да комуницираат, споделуваат информации и одржуваат социјални врски. Оваа масовна употреба носи и потенцијални опасности, како што се неовластено објавување на лични податоци, креирање на лажни профили и неовластен пристап до профили, што може да доведе до сериозни последици за индивидуалната приватност и дигиталната безбедност.

Во последните години, Агенцијата за заштита на личните податоци забележува значителен пораст на претставките од граѓаните за нарушување на приватноста на интернет, особено на социјалните мрежи. Статистичките податоци покажуваат дека процентот на претставки што се однесуваат на социјалните медиуми е во постојан пораст, што укажува на зголемена свест меѓу граѓаните за овие проблеми, но и на потребата за поефикасна заштита.

Дополнително, судската практика во Република Северна Македонија исто така покажува зголемен број случаи поврзани со злоупотреба на личните податоци на интернет. Од анализираните пресуди на основните судови, голем дел се однесуваат на дела сторени на социјалните мрежи и интернет-страниците. Овие трендови укажуваат на тоа дека прашањето за заштита на приватноста и личните податоци е итно и бара зголемена внимателност и акција од страна на правосудните органи.

Целта на овој документ е да обезбеди сеопфатен увид во најчестите случаи на повреда на приватноста и злоупотреба на личните податоци на интернет, релевантни за државата, како и да обезбеди насоки и препораки за нивна поефикасна заштита. Документот се заснова на претходна анализа на правната и институционалната рамка во државата, на статистички податоци добиени преку алатката за пристап до информации од јавен карактер, како и на разгледување и анализа на конкретни пресуди на основните судови од оваа област. Сето тоа е надополнето со преглед на релевантна литература и судската практика на Европскиот суд за заштита на човековите права.

1 Westin AF. Privacy and freedom. New York: Atheneum, 1967.

Документот првенствено ќе најде примена помеѓу правосудните органи, на кои ќе им овозможи подобар увид во најчестите случаи во државата, како и целосен преглед на правната и институционалната рамка. Вклучени ќе бидат и најдобрите практики и стандарди што треба да се применуваат за подобрена заштита на правото на приватност на интернет.

Оттука, покрај правосудните органи за кои документот е првенствено наменет, документот ќе биде корисен и за креаторите на политики на кои ќе им помогне да развијат поефикасни стратегии и рамки за заштита на приватноста и личните податоци, следејќи ги современите европски стандарди и најдобрите практики. Ова ќе овозможи подобро справување со предизвиците што произлегуваат од повредата на приватноста на интернет, особено на социјалните мрежи и интернет-страниците и ќе придонесе за создавање на побезбедна дигитална средина за граѓаните на Република Северна Македонија.

1. МЕЃУНАРОДНА И ДОМАШНА ПРАВНА ЗАШТИТА

Многу важен чекор во правната заштита на приватноста е создавањето на модерниот поим за приватност во 1890 година, од страна на Луис Брандис и Семјуел Ворен, кои го дефинираа правото на приватност како „право да се биде оставен на мир“ (*right to be let alone*). Оттогаш, правото на приватност стана широкопознато и признаено, почна да се развива и стана основно човеково право во западните општества. И покрај фактот што правните системи обезбедуваат заштита на приватноста, не постои консензус за прашањето: „Што точно треба да се заштити и што е приватност?“

Одговор на ова прашање може да се бара во меѓународните инструменти за човекови права. На врвот е Универзалната декларација за човекови права од 1948 година, која во член 12 експлицитно наведува дека никој не смее да биде подложен на произволно мешање во неговата приватност, семејство, дом или кореспонденција, ниту на напади врз неговата чест и углед. Секој има право на правна заштита против такво мешање или напади. Слично, член 17 од Меѓународниот пакт за граѓански и политички права (МПГПП) ги огледува овие заштити, потврдувајќи дека никој не смее да биде подложен на произволно или незаконско мешање во неговата приватност, семејство, дом или кореспонденција, ниту на незаконски напади врз неговата чест и углед. Понатаму, тој го гарантира правото на секој на правна заштита против такво мешање или напади. Овие одредби го истакнуваат глобалниот консензус за важноста на заштитата на приватноста како основно човеково право.

Со оглед на тоа што горенаведените одредби се врамени во суштината во смисла на забрана за „мешање во приватноста“, еквивалентните одредби од член 8 од Европската конвенција за заштита на човековите права (ЕКЧП) од 1950 година се врамени во смисла на право на „почитување на приватниот и семејниот живот“:

1.1. ПРАВО НА ПОЧИТУВАЊЕ НА ПРИВАТНИОТ И СЕМЕЈНИОТ ЖИВОТ

1. Секој човек има право на почитување на неговиот приватен и семеен живот, домот и преписката.
2. Јавната власт не смее да се меша во остварувањето на ова право, освен ако тоа мешање е предвидено со закон и ако претставува мерка што е во интерес на државната и јавната безбедност, економската благосостојба на земјата, заштитата на поредокот и спречувањето на кривични дела, заштитата на здравјето и моралот или заштитата на правата и слободите на другите, во едно демократско општество.

На национално ниво, правната рамка за заштита на приватноста на интернет е втемелена во Уставот, Законот за заштита на личните податоци, Законот за електронски комуникации, Законот за следење на комуникациите и, се разбира, Кривичниот законик.

Уставната заштита е една од виталните заштитни мерки за заштита на правото на приватност. Иако Уставот на Република Северна Македонија не го дефинира правото на приватност на експлицитен начин, тоа го прави преку гаранција на правата и слободите преку кои се остварува тоа право, односно – гарантира слобода и тајност на писмата и сите други облици на општење (член 17 од Уставот), приватност на личниот и семејниот живот, почитување и заштита на приватноста, достоинството и угледот на секој граѓанин (член 25 од Уставот) и неповредливост на домот (член 26 од Уставот). Кога станува збор за заштитата на личните податоци, Уставот во член 18 експлицитно предвидува посебни гаранции:

> ***„Се гарантираат сигурноста и тајноста на личните податоци. На граѓаните им се гарантира заштита од повреда на личниот интегритет што произлегува од регистрирањето информации за нив преку обработка на податоците“.***

Понатамошното регулирање на ова право Уставот го препушта на одделните закони. Законот за заштита на личните податоци, во своите 11 поглавја, ги утврдува правата на субјектите на податоци, начелата на обработка, улогата на контролорите и обработувачите, како и механизмите за супервизија и одговорност во случај на нарушувања. Законот за електронски комуникации преку своите одредби за безбедност и интегритет на мрежите и услугите ги засилува мерките за заштита на личните податоци на социјалните мрежи и интернет-страниците. Законот за следење на комуникациите предвидува рамка за спроведување на истражни мерки и следење на комуникациите, што има значење за заштитата на приватноста преку интернет и предизвиците поврзани со неправилно користење на личните податоци.

Кривичниот законик во оваа смисла е релевантен преку инкриминацијата „Злоупотреба на лични податоци“ во член 149, како дел од кривичните дела против слободите и правата на човекот и граѓанинот:

> ***„Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.***
>
> ***Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера користејќи ги за себе или за друг да оствари некаква корист или на друг да му нанесе некаква штета“.***

На 24 октомври 2023 година, официјалната работна група го објави финалниот текст на новиот кривичен предлог-законик, кој вклучува две нови кривични дела важни за заштита на приватноста на интернет:

i. неовластено пренесување на фотографски, филмски и видеоснимки од полова природа (член 255), и

ii. повреда на приватноста на детето (член 267). Иако овој предлог-закон сè уште не е усвоен од Собранието, новите инкриминации се значајни и заслужуваат внимание.

Неовластеното пренесување на приватни фотографии или видеоснимки од полова природа е предвидено да се казнува со парична казна или затвор до три години, а доколку делото е сторено кон дете, казната ќе биде од една до пет години затвор.

Повредата на приватноста на детето, освен неовластено објавување фотографии или видеоматеријали на детето или лични податоци поврзани со идентитетот на детето, вклучува и изнесување информации од личниот или семејниот живот на детето. Клучно за ова дело е предизвикувањето вознемиреност, изложеност на потсмев или на друг начин загрозување на приватноста или интересите на детето. Казната е парична или затвор до една година, но ако делото се изврши преку медиуми или на начин што го прави пристапно за поголем број лица, сторителот ќе се казни со парична казна или затвор до три години.

Досега овие дела беа (делумно) опфатени во член 149, кој ги санкционираше со парична казна и затвор до една година. Со новиот кривичен предлог-законик, овие дела се инкриминираат одделно и се пропишуваат построги казни, што е од исклучителна важност. Оваа промена ја нагласува сериозноста на дејствата како неовластено пренесување фотографии и видеоснимки од полова природа и повреда на приватноста на детето. Со тоа, правниот систем испраќа силна порака дека овие форми на злоупотреба не се толерираат и дека сторителите ќе се соочат со значително построги санкции. Поголемите казни имаат превентивен ефект, зголемувајќи ја свеста за сериозноста на овие дела и нивното влијание врз жртвите, особено кога станува збор за деца. Дополнително, овие построги казни ја рефлектираат општествената важност на заштитата на приватноста во дигиталниот свет, обезбедувајќи подобра заштита на индивидуалните права и достоинство на луѓето.

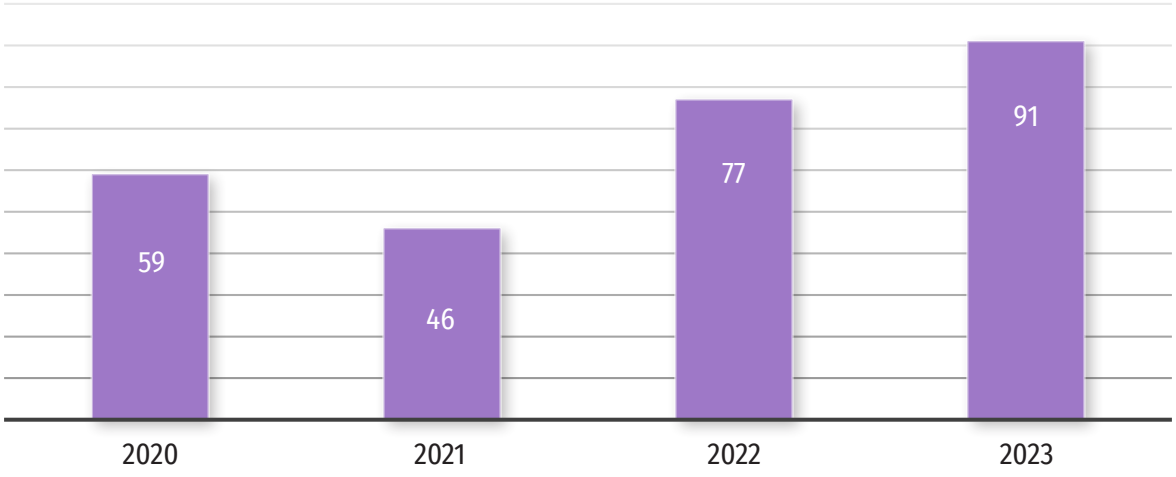
2. ИНСТИТУЦИОНАЛНА РАМКА ЗА ЗАШТИТА

Ефикасната заштита на приватноста и личните податоци на интернет зависи од соработката и координацијата меѓу повеќе институции. Главните институции што учествуваат во овој процес во Република Северна Македонија се Агенцијата за заштита на личните податоци (АЗЛП), Министерството за внатрешни работи (МВР), јавните обвинителства и надлежните судови.

АЗЛП е самостоен и независен државен орган, надлежен да врши надзор над законитоста на преземените активности при обработката на личните податоци на територијата на Република Северна Македонија, како и заштита на темелните права и слободи на физичките лица во однос на обработката на нивните лични податоци. Процесот почнува со поднесување барање од страна на граѓанинот за утврдување повреда. АЗЛП спроведува вонредна супервизија за да утврди дали има повреда на правото и, ако утврди повреда, може да изрече мерки за отстранување на неправилностите и заштита на личните податоци. АЗЛП исто така информира за можноста за судска заштита против своите одлуки.

Постапувањето по претставки од страна на Агенцијата за заштита на личните податоци во најголем дел се однесува на претставки од граѓаните за нарушување на нивната приватност на интернет, поконкретно на социјалните мрежи. Исто така, забележлив е тренд на зголемување на претставките што се однесуваат на социјалните мрежи од 2019 година наваму. Така, ако во 2020 и 2021 година околу 59%, односно 46% од претставките се однесувале на социјалните медиуми, последните две години овој процент е зголемен за 77% (2022 г.) и 91% (2023 г.). Најголем дел од претставките што се однесуваат на социјални мрежи се поднесени заради креирање на лажни профили, неовластено објавување фотографии и видеоснимки и неовластен пристап до профили (пробивање).

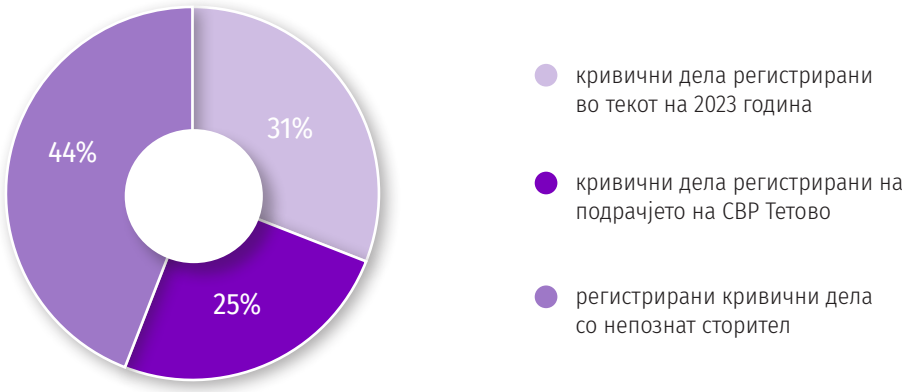
Претставки од граѓани за нарушување на нивната приватност на социјалните мрежи



Преку Секторот за компјутерски криминал и дигитална форензика, МВР е одговорно за спроведување истраги и поднесување кривични пријави за злоупотреба на личните податоци. Секторот соработува со основните јавни обвинителства за подготвување и поднесување обвинениja за кривични дела поврзани со злоупотребата на личните податоци.

Податоците од МВР укажуваат на вкупно 558 кривични дела „злоупотреба на лични податоци“ во истиот период, од кои најмногу се регистрирани во текот на 2023 година, вкупно 181 кривично дело. Најголем дел од кривичните дела се регистрирани на подрачјето на СВР Тетово (146). Забележливо е и дека од вкупниот број на регистрирани дела, речиси половина, односно 258 се со непознат сторител.

Спецификација на вкупниот број кривични дела кои се однесуваат
на злоупотреба на лични податоци (2020-2023)



Кривичните судови се надлежни за процесирање и донесување пресуди за кривичното дело злоупотреба на личните податоци. Судот постапува по обвинението поднесени од јавните обвинителства и одлучува за казните за сторителите. Понатаму, жртвите на злоупотреба на лични податоци можат да поднесат тужби пред граѓанските судови за надоместок на материјална и нематеријална штета.

Кога станува збор за злоупотреба на личните податоци низ судската практика, за потребите на овој документ беа анализирани вкупно 62 анализирани пресуди на основните судови ширум државата. Од нив, може да се заклучи дека кривичните постапки за злоупотреба на лични податоци исто така во голем дел се однесуваат на дела сторени на социјалните мрежи и интернет-страниците (вкупно 46). Најголем дел од нив се однесуваат на неовластено објавување фотографии и видеоснимки, креирање на лажни профили и објава на лични податоци.

Како надлежни органи во спроведувањето на одредбите од Законот за електронски комуникации и со тоа обезбедување на комуникациите се Министерството за информатичко општество и администрација и Агенцијата за електронски комуникации. Со член 26-а од Законот за електронските комуникации, во состав на Агенцијата за електронски комуникации се формира посебна организациона единица – Национален центар за одговор на компјутерски инциденти (МКД-ЦИРТ), која ќе претставува официјална национална точка за контакт и координација во справувањето со безбедносните инциденти кај мрежите и информациските системи и кој ќе идентификува и ќе обезбедува одговор на безбедносни инциденти и ризици.

На интернет-страницата на МКД-ЦИРТ има образец за пријавување на компјутерски инциденти. Оваа институција има превентивна улога и методи за пресретнување на компјутерски напади и инциденти, вмрежена е со исти вакви институции на меѓународно ниво и има брз проток и дојава на информации за можни закани.

3. ПОВРЕДА НА ПРАВОТО НА ПРИВАТНОСТ И ЗЛОУПОТРЕБА НА ЛИЧНИТЕ ПОДАТОЦИ НА ИНТЕРНЕТ

Социјалните мрежи и интернет-страниците играат клучна улога во секојдневниот живот на луѓето, овозможувајќи комуникација, споделување информации и социјална интеракција на глобално ниво. Сепак, овој развој на дигиталната сфера носи значителни предизвици, особено во контекст на заштита на приватноста и личните податоци на корисниците. Повредата на правото на приватност и злоупотребата на личните податоци се однесуваат на инциденти каде што личните податоци се собираат, обработуваат или се споделуваат без согласност. Овие инциденти предизвикуваат сериозна загриженост за приватноста на корисниците и потенцијалната злоупотреба на сензитивни податоци.

Согласноста е од клучно значење за обработката на личните податоци. Согласно законот, согласноста треба да биде слободно дадена, конкретна и информирана. Тоа значи дека корисниците мораат да бидат целосно запознаени со целите на обработката на нивните податоци и да ја дадат својата согласност без никаква принуда. Во практиката, корисниците често се доведуваат до заблуда при креирањето на кориснички сметки, бидејќи за да ги користат услугите на платформите, мораат да дадат согласност за обработка на нивните податоци. Ова е спротивно на принципот на слободно дадена согласност и дополнително ги нарушува заложбите за отворен интернет за сите. Новиот тренд да се понуди опција за плаќање за избегнување на обработката на личните податоци создава дискриминација, каде што заштитата на приватноста станува луксуз достапен само за оние што можат да си го дозволат тоа.

Согласно Законот за заштита на личните податоци, контролорот е правно или физичко лице или орган на државната власт кој самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци. Во практиката, ова значи дека секој што одлучува за обработката на личните податоци, без разлика дали е индивидуален корисник, компанија или државна институција, се смета за контролор.

На пример, лица и медиуми кои споделуваат лични податоци на социјалните мрежи без соодветна основа можат да се сметаат за контролори и да одговараат согласно законот. Ова вклучува не само големи платформи како „Фејсбук“ и „Твитер“ туку и мали бизниси и индивидуални блогери кои ги утврдуваат целите за обработка на личните податоци и интернет-страниците што исто така собираат лични податоци преку нивните контакт-форми и на други начини. Контролорите имаат обврска да ги почитуваат правилата за заштита на личните податоци, вклучувајќи обезбедување на информирана и слободно дадена согласност од корисниците.

4. ВИДОВИ ПОВРЕДИ НА ПРАВОТО НА ПРИВАТНОСТ НА СОЦИЈАЛНИТЕ МРЕЖИ

За да комуницираат преку социјалните мрежи и интернет-страниците, корисниците мораат да креираат онлајн-идентитети и од нив се бара да откријат лични податоци што неретко се и сензитивни (единствен матичен број, броеви на банкарски картички итн.). И во текот на комуникацијата преку интернет со другите корисници, поединците често споделуваат лични податоци со другите, слично како и во физичкиот свет. Впрочем, можностите на интернет обезбедуваат побрзо и полесно споделување податоци од кога било.

Постојат различни форми на повреди на приватноста, но во овој дел ќе стане збор само за најактуелните кај нас.

4.1. КРЕИРАЊЕ НА ЛАЖНИ ПРОФИЛИ

Креирањето профил на социјалните мрежи е многу едноставно. Сè што е потребно е функционална електронска пошта на која автоматски ќе биде испратена порака за потврда при регистрација. Откако ќе се потврди адресата, профилот е креиран. Притоа, не постои механизам за проверка на веродостојноста на личните податоци што се внесуваат на профилот.

Злонамерните актери кои злоупотребуваат лични податоци на други за да креираат профил, најчесто имаат цел да дојдат до лични податоци на корисниците кои се видливи само за нивните пријатели. Друга можна цел е да се наштети на угледот на корисникот чиј идентитет се „позајмува“ преку споделување на чувствителни лични податоци со другите (на пример, интимни фотографии) или ширење на лажни информации. Потоа, нивната цел може да биде да вршат различни измами и злоупотреби кон пријателите на лицето.

Дополнително, ваквите лажни профили можат да се користат за извршување на разни криминални активности, како што се кибер-вознемирување, изнуда или злоупотреба на доверливи информации. Лицата кои стојат зад овие профили често ги користат за да ги манипулираат и да ги искористуваат другите корисници, особено оние што имаат помалку искуство во користење на социјалните мрежи и се помалку свесни за потенцијалните закани.

4.2 НЕОВЛАСТЕН ПРИСТАП ДО ПРОФИЛИ

Вообичаено е профилите на социјалните мрежи да содржат голем број на лични податоци. Иако корисниците имаат опција да не споделат одредени лични податоци, тие често доброволно го прават тоа од причини на социјално вмрежување. Оттука, јасно е дека постојат закани по личните податоци споделени на социјалните мрежи и можности за различни злоупотреби. Неовластениот пристап до профилите и личните податоци што ги содржат претставува сериозна закана по приватноста на корисниците.

Целите на злонамерните актери кои остварile неовластен пристап до профил на социјална мрежа на друг, најчесто се исти како на оние што креираат лажни профили. Сепак, можностите за злоупотреби и измами овде можат да се зголемат значително, со оглед на тоа што хакерите преку пристапот до профилот добиваат пристап до сите лични податоци што се наоѓаат на профилот, дури и оние што претходно биле ограничени само на корисникот. Истовремено, добиваат пристап и до лични податоци на неговите пријатели. Можностите за измами исто така имаат поголема веројатност за успешен исход, со оглед на тоа што тие настапуваат како корисникот и немаат потреба да ги убедуваат пријателите на корисникот дека се работи за истото лице. Ова може да доведе до финансиски загуби, бидејќи хакерите можат да ги искористат добиените информации за да извршат финансиски измами. Тие исто така можат да го злоупотребат пристапот за да добијат доверливи деловни информации или за да извршат шпионажа.

4.3 НЕОВЛАСТЕНО ОБЈАВУВАЊЕ НА ТУЃИ ЛИЧНИ ПОДАТОЦИ

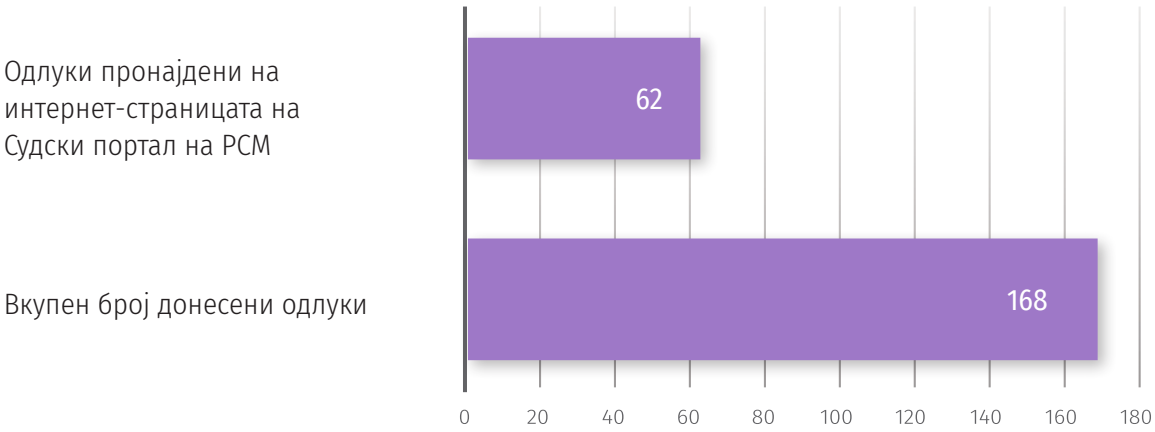
Неовластено објавување на туѓи лични податоци е сериозен проблем на социјалните мрежи. Ова се случува кога лични податоци на поединци се објавуваат на туѓи или лажни профили без нивна согласност, што претставува грубо нарушување на приватноста и може да има сериозни последици за погодените лица. Неовластеното објавување може да вклучува информации како што се име и презиме, адреса на живеење, телефонски број, електронска пошта, банкарски податоци, фотографии и видеа, како и други сензитивни информации. Овие податоци можат да бидат објавени од разни причини, вклучувајќи одмазда, малтретирање, изнуда или, едноставно, недостаток на почит кон приватноста на другиот.

Последиците од неовластеното објавување на лични податоци можат да бидат значителни. На индивидуално ниво, ова може да доведе до сериозни нарушувања на личната и професионалната репутација, финансиска штета, емоционален и психолошки стрес и безбедносни ризици. Личните податоци објавени без согласност можат да се злоупотребат за кражба на идентитет, финансиски измами или да предизвикаат физички закани и вознемирувања. Погодените лица често доживуваат значителен стрес, анксиозност и други ментални здравствени проблеми.

5. ПРЕГЛЕД НА СУДСКАТА ПРАКТИКА

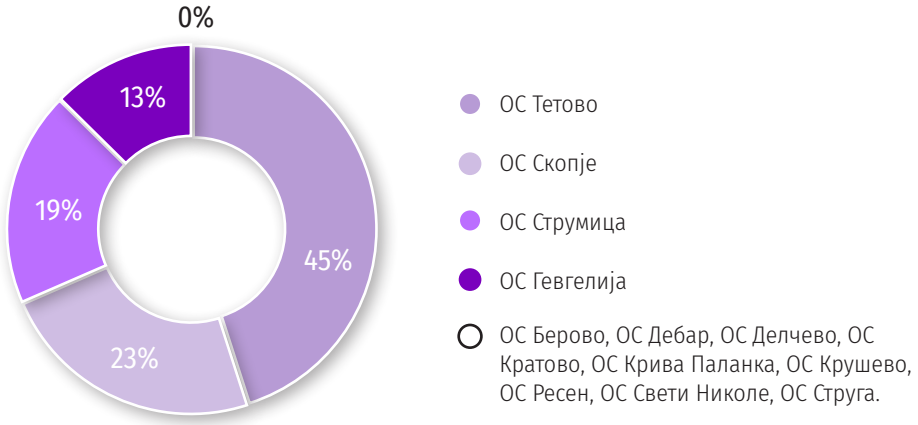
За целите на овој документ за јавни политики беа прибирани податоци од основните судови во државата за бројот на обвиненија, предмети, одлуки и осудени лица по член 149 од Кривичниот законик во периодот од 2020 до 2023 година.

Сите 26 суда одговорија на барањата за информации од јавен карактер во законски утврдениот рок. Согласно одговорите, вкупно 168 одлуки по член 149 од КЗ биле донесени во наведениот четири годишен период. Сите тие одлуки беа побарани на интернет-страницата на Судски портал на Република Северна Македонија, но само 62 пресуди (38%) беа успешно пронајдени. Ова укажува на недостаток на транспарентност и потреба од подобрување на достапноста на судските одлуки за јавноста.

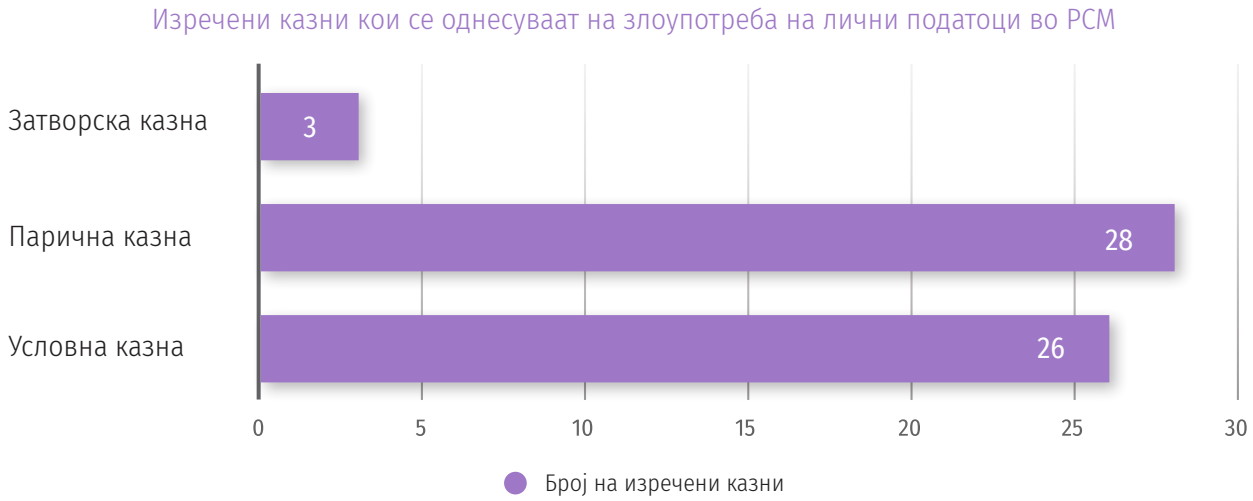


Согласно судската практика, најголем дел од случаите на злоупотреба на лични податоци се на подрачјето на ОС Тетово (вкупно 50), потоа на подрачјето на ОС Скопје (26), ОС Струмица (21) и ОС Гевгелија (14). Додека, пак, на подрачјето на основните судови во Берово, Дебар, Делчево, Кратово, Крива Паланка, Крушево, Ресен, Свети Николе и Струга нема донесени одлуки по член 149 од КЗ во наведениот период. Ова може да укажува на различни фактори, како што се бројот на население, степенот на дигитална писменост и свест за правото на приватност и заштита на личните податоци, како и ефикасноста на локалните правосудни органи.

Застапеност на случаи според подрачја на основни судови



Анализата на пресудите за злоупотреба на лични податоци во Република Северна Македонија покажува дека доминантни се условните и паричните казни, додека затворските казни се многу ретки. Вкупно 26 пресуди изрекуваат условна казна, додека 28 пресуди изрекуваат парична казна. Од анализираните пресуди, само во три случаи е изречена затворска казна.



Притоа, највисоката условна казна изречена во овие случаи е условна казна во траење од една година, која нема да се изврши доколку сторителот во временскиот период од три години не стори ново кривично дело. Од друга страна, најблагата условна казна е во траење од два месеца, која нема да се изврши доколку сторителот во временскиот период од една година не стори ново кривично дело.

Паричните казни исто така вариираат во значителна мера. Највисоката изречена парична казна е сто дневни глоби, односно 61.500 денари, а најниската е десет дневни глоби, односно износ од 6.150 денари.

Што се однесува до затворските казни, од трите затворски казни изречени во анализираните случаи, една е за траење од седум месеци, додека преостанатите две се само по три месеци. Овие податоци укажуваат на фактот дека затворските казни за злоупотреба на лични податоци се изрекуваат многу ретко и генерално се под законскиот максимум за ова дело.

Високата бројка на условни и парични казни сугерира дека судовите не ги третираат овие дела со доволна сериозност. Еден типичен пример за ова е пресудата на Основниот суд во Струмица. Во оваа пресуда, судот го прифатил предлогот на јавниот обвинител да му изрече алтернативна мерка на обвинетиот – условна осуда на утврдена казна затвор во траење од три месеци, која нема да се изврши доколку обвинетиот во временскиот период од една година по правосилноста на пресудата не стори ново кривично дело.

Се работи за случај во кој обвинетиот без согласност на оштетениот ги искористил неговите лични податоци. Користејќи копија од личната карта што му била дадена заради вадење на бугарска патна исправа, обвинетиот склучил договор за засновање претплатнички однос за пристап и користење на јавна комуникациска мрежа и јавно достапни електронски услуги за електронски комуникации. Со тоа добил претплатнички број на име на оштетениот.

Во пресудата, судот истакнува дека ги ценел олеснителните и отежителните околности на случајот. Од отежителните околности, судот ја ценел тежината на стореното кривично дело, последиците од тоа и степенот на кривичната одговорност на обвинетиот, како и зачестеноста на ова кривично дело на територијата на овој суд. Од олеснителните околности, судот го зема предвид фактот дека обвинетиот е досега неосудуван и релативно возрасен човек. Судот сметал дека и со една алтернативна мерка ќе се постигне целта на казнувањето на планот на генералната и специјалната превенција и дека ќе се влијае врз обвинетиот во иднина да се воздржува од сторување на други кривични дела, како и врз другите да не вршат кривични дела.

Оваа пресуда го отсликува начинот на кој судовите ги третираат делата за злоупотреба на лични податоци, потенцирајќи го фокусот на условни и парични казни како примарни мерки за казнување.

Еден особено загрижувачки случај е на подрачјето на Основниот суд во Гостивар во кој обвинетиот во соизвршителство со малолетно лице преку социјалната мрежа „Ватсап“ испраќал фотографии од дете со непримерна содржина на повеќе лица. И покрај сериозноста на случајот, каде што се работи за злоупотреба на фотографии од интимна природа што му припаѓаат на дете, судот изрекол условна казна во траење од три месеци, која нема да се изврши доколку обвинетиот во временскиот период од една година по правосилноста на пресудата не стори ново кривично дело.

Овој случај истакнува сериозен проблем во казнената политика. Дури и кога оштетеното е дете и се работи за интимни фотографии, казните остануваат преблаги. Условната казна од три месеци е несоодветна во однос на тежината на делото и не обезбедува адекватна заштита и правда за жртвите.

Забележливо е и дека меѓу оштетените има четиринаесет жени кои се соочиле со злоупотреба на лични податоци од поранешните интимни партнери. Меѓу нив се и десет случаи каде што биле споделени интимни фотографии и видеа без согласност. И покрај сериозноста на ваквите дела, нема разлика во висината и сериозноста на казната. Ова укажува на фактот дека жените се поранливи на злоупотреба на интимни фотографии и видеа без согласност, што ја истакнува потребата за поостри законски мерки и специјализирана поддршка за жените-жртви.

Анализата на пресудите за злоупотреба на лични податоци во Република Северна Македонија открива дека злоупотребата на интернет, особено на социјалните мрежи и интернет-страниците, е сè поактуелна и позастапена. Од вкупно 62 пресуди, 46 се однесуваат на злоупотреба на лични податоци на интернет. Ова го потврдува фактот дека дигиталниот простор станува сè поризичен во однос на заштитата на личните податоци. Најголемиот дел на делата злоупотреба на лични податоци во судската практика се однесуваат на објавување лични податоци без согласност.

ЗАКЛУЧОЦИ И ПРЕПОРАКИ

Анализата укажува на значителни регионални диспропорции во бројот на случаи на злоупотреба на личните податоци, што укажува на различни нивоа на свест и ефикасност на локалните правосудни органи. Ова е очигледно во одредени региони каде што недостатокот на одлуки укажува на нееднаква примена на законот и недоволно пријавување и процесирање на случаите. Со цел да се надмине оваа ситуација, неопходно е спроведување на обемни кампањи за зголемување на свеста за правата на приватност, особено во регионите каде што нема донесени одлуки. Овие кампањи треба да бидат насочени кон информирање на јавноста за важноста на пријавувањето на случаите и нивно процесирање, како и за правата што ги имаат во контекст на заштитата на личните податоци.

Покрај тоа, важно е да се организираат обуки за вработените од секторите за внатрешни работи што работат директно на терен, за да се осигури дека тие се запознаени со законските регулативи и практиките за заштита на личните податоци. Ова ќе придонесе за подобра примена на законот и зголемување на ефикасноста на правосудните органи во процесирањето на случаите. Исто така, формирање на специјализирани служби за поддршка на жртвите на злоупотреба на лични податоци е неопходно, со цел да им се помогне во процесот на пријавување и во текот на судските постапки.

Обуки за законските решенија и меѓународната практика се неопходни и за судиите и јавните обвинители. Потребна е специјализирана обука за заштита на личните податоци и правото на приватност во дигиталниот простор и постапување во предмети каде овие права се повредени. Организирање на продлабочена обука за заштита на лични податоци и правото на приватност за секоја генерација на слушатели на Академијата за судии и јавни обвинители е од клучно значење. Дополнително, континуирани обуки треба да се организираат на секои две години, со акцент на новите технолошки предизвици и дигиталниот простор.

Брзиот развој на нови технологии создава нови предизвици за заштитата на личните податоци и приватноста. Потребна е подобрена соработка и споделување на знаење меѓу јавните обвинителства, судовите и Секторот за дигитална форензика и компјутерски криминал при Министерството за внатрешни работи (МВР). Следење на развојот на нови технологии и нивното влијание на приватноста е од клучно значење за навремено ажурирање на законодавството и практиките за заштита на личните податоци.

Ниските казни не ги спречуваат сторителите од повторно сторување на делата, што укажува на зачестеност на овие дела. Затоа, потребно е ревидирање на казнената политика за злоупотреба на лични податоци, со фокус на изрекување на повисоки казни што ќе имаат превентивно дејство. Исто така, делото „Злоупотреба на лични податоци“ не одговара на постојната состојба во која сè поактуелни стануваат сериозни злоупотреби. Оттука, потребно е инкриминациите што се содржани во новиот кривичен предлог-законик: „Неовластено пренесување на приватни фотографии или видеоснимки од полова природа“ и „Повредата на приватноста на детето“ да бидат итно усвоени.

Судиите и обвинителите треба да ја следат и да ја применуваат практиката на Европскиот суд за човекови права во случаи на злоупотреба на личните податоци. Обезбедувањето транспарентност на судските одлуки е клучно за подобра анализа и следење на правосудните постапки. Ова може да се постигне преку осигурување дека сите судски одлуки се достапни на судскиот портал, што ќе овозможи подобра анализа и следење на правосудните постапки.

Обвинителите треба да бидат проактивни во обезбедување, заштита и презентирање на електронските докази. Потребна е подобра меѓународна соработка за брзо обезбедување на електронски докази. Организирање на специјализирани обуки за обвинителите за да се подобри нивната проактивност во обезбедувањето и заштитата на електронските докази е од суштинско значење. Подобрување на меѓународната соработка преку споделување на добри практики и унапредување на механизмите за брза и ефикасна размена на информации и докази ќе придонесе за поуспешна борба против злоупотребата на личните податоци и заштита на правото на приватност.

РЕЗИМЕ НА ПРЕПОРАКИ

» Навремено пријавување и точност на пријавите: Потребно е зголемување на свеста кај граѓаните за важноста од навремено и точно пријавување на инциденти поврзани со злоупотреба на лични податоци. При секое пријавување, граѓаните треба да достават прецизни информации, како што се УРЛ, деталите за социјалната мрежа и релевантни податоци за сторителот.

» Јакнење на капацитетите на Министерството за внатрешни работи (МВР): Потребно е значително зголемување на кадарот во Секторот за компјутерски криминал и дигитална форензика, со цел побрзо постапување по случаи и поефикасна обработка на податоци добиени од социјалните мрежи.

» Организирање обуки за вработените во СВР кои работат директно на терен за да се осигури дека се запознаени со законските регулативи и практиките за заштита на личните податоци.

» Подолг период за задржување на податоци: Потребни се законски измени кои ќе овозможат подолг период за задржување на IP адресите и логовите од интернет провајдерите и платформите, со јасно дефинирани критериуми за нивно чување според сериозноста на делото. Ова ќе овозможи поефикасни истраги, особено кога пријавите се доцни.

» Подобрување на меѓународната правна помош: Неопходно е подобрување на механизмите за меѓународна правна помош за брза размена на податоци и електронски докази. Мора да се олесни соработката со социјалните платформи, вклучувајќи развој на директни канали за комуникација со платформите како Телеграм, особено за полесни кривични дела.

» Промени во законодавството: Потребни се законски измени кои ќе ги усогласат домашните закони со препораките на Советот на Европа, особено во однос на продолжување на роковите за чување на електронски комуникации. Исто така, треба да се вметне ново кривично дело – неовластено споделување интимни и сексуални слики, кое ќе се гони по службена должност, наместо по приватна тужба.

» Организирање континуирани обуки на секои две години во рамките на континуираната обука за судии и јавни обвинители, со фокус на новите технолошки предизвици и дигиталниот простор, како и за правилна примена на практиката на Европскиот суд за човекови права, особено во случаи на злоупотреба на лични податоци.

» Обезбедување специјализирани обуки за судиите и обвинителите: Потребни се континуирани и специјализирани обуки за правилна примена на законите за заштита на приватноста и личните податоци. Овие обуки треба да бидат насочени кон точна примена на член 149 од Кривичниот законик и новите предизвици кои произлегуваат од дигиталниот простор, со посебен акцент на маргинализираните групи и продолжените кривични дела.

» Организирање на специјализирани обуки за обвинителите за да се подобри нивната проактивност во обезбедувањето и заштитата на електронските докази.

» Поголема координација меѓу институциите: Неопходно е да се зајакне координацијата меѓу МВР, Обвинителството и судовите, особено за унифицирано толкување на законот, со цел избегнување на различни толкувања и подобрување на правната квалификација на делата. Ова би се постигнало преку заеднички обуки и работни групи.

» Подигнување на свеста кај жртвите: Спроведување кампањи кои ќе ги информираат граѓаните и жртвите за процедурата на пријавување дигитални кривични дела, со достапни темплејти на барања на веб-страниците на релевантните институции, како што е веб-страницата на МВР.

» Спроведување на обемни кампањи за зголемување на свеста за правата на приватност во регионите каде што нема донесени одлуки, со акцент на важноста на пријавувањето и процесирањето на случаите.

» Зголемување на казните за злоупотреба на лични податоци: Потребно е ревидирање на казнената политика за злоупотреба на лични податоци и воведување на повисоки казни, со цел да се спречат идни прекршоци и да се обезбеди соодветна заштита на жртвите.

» Формирање специјализирани служби за поддршка на жртвите: Потребно е да се формираат специјализирани служби кои ќе обезбедат поддршка за жртвите на дигитални кривични дела, вклучувајќи правна и психолошка помош, особено за маргинализираните групи.

» Транспарентност на судските одлуки: Потребно е сите судски одлуки поврзани со заштитата на лични податоци да бидат достапни на јавниот Судски портал, со цел да се овозможи подобра анализа на правосудните процеси и да се обезбеди транспарентност.

» Транспонирање на Е-директивата во македонското законодавство: Потребно е целосно транспонирање на Е-директивата во македонското законодавство, со цел да се усогласат домашните прописи со европските стандарди за заштита на електронските комуникации и чување на податоци.

» Консултации со Агенцијата за заштита на личните податоци (АЗЛП): При секоја измена или донесување на закони кои се поврзани со обработка на лични податоци и заштита на приватноста, задолжително е да се консултира АЗЛП за да се обезбедат професионални насоки и да се почитуваат најдобрите практики.

» Постојано следење на развојот на нови технологии и нивното влијание на приватноста, со цел навремено ажурирање на законодавството и практиките.