

ВОВЕД ВО ДИГИТАЛНИТЕ ПРАВА



Содржина:

ВОВЕД	2
Заштита на личните податоци	3
Заштита на личните податоци во дигиталниот простор	4
Примери на повреда на личните податоци	4
Последици за поединецот и општеството	5
Заштитни механизми:	5
ДИГИТАЛНА БЕЗБЕДНОСТ	7
Безбедност во дигиталниот простор	8
Примери на повреди	8
Последици за поединецот и општеството	9
Механизми за заштита	10
СЛОБОДА НА ГОВОР	11
Слобода на изразување во дигиталниот простор	12
Примери на повреди	12
Последици на поединците и на друштвото	13
Механизми за заштита	13
ДИГИТАЛНИТЕ ПРАВА ВО РЕГИОНОТ	15

ВОВЕД

Човековите права еднакво важат и на интернет, како и во физичкиот простор.

Дигиталните технологии отворија многу нови и интересни начини за истражување на идеи, размена на информации, здружување, протести и други активности на слободните граѓани, кои се наоѓаат под универзална заштита како основни права на сите луѓе без разлика на потеклото, статусот и останатите разлики.

Истовремено, дигитализацијата на секојдневните активности и комуникации овозможи и развој на средства за злоупотреба и прекршување на правата. Свесно или од незнаење, водени од комерцијални интереси, или со намера да воспостават контрола, различни актери како што се: државите, корпорациите, политичките и другите организации често се виновни за цензурата на интернетот, нарушувањето на приватноста на граѓаните и дискриминацијата по различни основи.

И покрај тоа што поголемиот број на корисници имаат познавање од областа на интернетот, начините на преземање на содржини од интернет и објавување на содржини на онлајн платформите, не им е секогаш до крај јасно што од тие активности спаѓа во доменот на заштита, ни во кои случаи може да се зборува за прекршување на правата. Дали се лајкот на Твитер, споделувањето на Фејсбук или метаподатоците за пребарување на Гугл лични податоци? Кога ограничувањето на пристапот на некоја веб страна прераснува во цензура? Кои човекови права се загрозени во процесот на масовна обработка на биометриски податоци во паметните системи? Дали може да има дискриминација во процесот на автоматизираното алгоритамското одлучување?

За да можат граѓаните и граѓанските организации да одговорат на овие и многу други прашања кои ќе се наметнат со широката примена на се посложените технологии, потребни им се знаења за дигиталните права-човекови права во дигиталната околина. Во овој прирачник, претставени се некои од основните поими од оваа област и илустрирани со практични примери од регионот на Западен Балкан.



ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Поимот заштита на личните податоци произлегува од основното човеково право- правото на приватност. Право на приватен избор подразбира контрола над информациите за нас, односно контрола на тоа дали било кој може да знае каде се движиме, што купуваме, каде живееме и со кого се допишуваме. Приватноста е од несомнена важност за автономниот живот за секоја индивидуа, а со доаѓањето на интернетот, нејзината ранливост станува се по очигледна.

ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ДИГИТАЛНИОТ ПРОСТОР

Со развојот на технологијата дојде до поголем проток на податоци, а најголемиот дел од овие податоци се лични податоци, односно податоци што се однесуваат на конкретна личност, што може да се идентификува. Заштитата на податоците се однесува токму на регулирањето на обработката на податоците (т.е. нивното собирање, користење и складирање) во служба на заштита на приватноста на поединците во дигиталниот простор. Денес, на личните податоци им се пристапува како на вреден ресурс врз основа на тоа кога компаниите остваруваат профит, а државите вршат контрола врз граѓаните. Поради тоа, одржувањето на приватноста во дигиталната ера се соочува со дополнителни предизвици. Нашата приватност е загрозувана во случај кога податоците не се соодветно заштитени, или ако се протечени или злоупотребени.

ПРИМЕРИ НА ПОВРЕДА НА ЛИЧНИТЕ ПОДАТОЦИ

- На социјалните мрежи почна да кружи фајл со лични податоци на над 5 милиони граѓани на една земја. Процесот на надзор утврди дека фајлот со податоци првично бил јавно достапен на веб-страницата на државната агенција од која е преземена, а таа агенција се бранела тврдејќи дека дошло преку неовластен пристап до нивниот сервер.
- Податоците како што се: имиња, телефонски броеви и локации на над половина милијарда сметки од една социјална мрежа протекоа на хакерски форум. Сепак, се дозна дека ова протекување не е причината за грешката, туку овие податоци намерно биле извлечени со помош на специјален софтвер, што е овозможено поради дефект на системот на социјалната мрежа.
- Меѓународната организација за човекови права добила списоци со повеќе од 50.000 мобилни телефони за кои постои сомневање дека се цел на потенцијална шпионажа, софтвер кој го компромитира телефонот, ги извлекува сите податоци и активира микрофон за снимање разговори.
- Десетици илјади мажи од регионот разменија интимни содржини преку апликацијата Телеграм, односно слики, видеа и фотографии

на жени, меѓу кои и малолетнички. Членовите на групите или лично ја добивале содржината во минатото од своите партнери или едноставно ја „симнувале“ од социјалните мрежи и ја испраќале до групите, често со откривање на личните податоци на личноста чија содржина ја споделуваат.

- Медиумите во една земја објавија детали за голема база на податоци што содржи лични податоци на повеќе од 910.000 гласачи. На списокот имало и новинари, активисти и други познати личности. Наводно, овие податоци ѝ биле дадени на една политичка партија за да ги користи за време на изборната кампања.

ПОСЛЕДИЦИ ЗА ПОЕДИНЕЦОТ И ОПШТЕСТВОТО

Справувањето со заштитата на податоците е од суштинско значење за да се спречат или барем соодветно да се санкционираат прекршувањата како што се протекување податоци, незаконски надзор на комуникациите или неовластена обработка на податоци. Доколку ситуациите како кражба на броеви на банкарски картички или следење на нашите разговори на социјалните мрежи беа нерегулирани, јасно е дека би живееле во свет во кој би владеел стравот и во кој сите би биле помалку слободни. Дополнително, најмаргинализираните меѓу нас дополнително би биле загрозуени, на пр. доколку компаниите имаа право непречено да обработуваат чувствителни податоци како раса или пол, тие податоци би можеле да се користат за дискриминаторски цели.

ЗАШТИТНИ МЕХАНИЗМИ:

- Право на информации - компаниите и организациите се должни да објаснат какви податоци обработуваат, односно имаме право да знаеме кои податоци за нас се собираат и како се користат.
- Право на пристап - организациите се обврзани да издадат копија од информациите што ги имаат за нас.
- Право на корекција и дополнување - имаме право да коригираме неточни податоци или да дополнуваме нецелосни.
- Правото на бришење, т.е. право на заборав - ова право може да се оствари во различни случаи како што е незаконска обработка на

податоци или кога целта за нивна обработка повеќе не постои.

- Доколку некоја компанија или организација сака да обработи податоци кои не се неопходни за обезбедување на одредена услуга или не се потребни со закон, таа мора да добие наша согласност за обработка, а ние секогаш можеме да ја повлечеме таа согласност.

На овој [линк](#) можете да пристапите до нашето кратко видео за заштита на податоците.



ДИГИТАЛНА БЕЗБЕДНОСТ

Можеме да ѝ пристапиме на безбедноста како исклучително важен аспект во животот на поединците, бидејќи таа е форма на отпор кон некој настан или однесување на другите што може да биде заканувачко. Односно, тоа претставува одредена заштита од работи кои можат да ни наштетат. Покрај тоа што може да се разговара во индивидуален контекст, на пример, дали припадниците на сексуалното малцинство можат слободно да одат на улица без страв од физичко насилство, за безбедноста може да се разговара и на ниво на организација или држава.

БЕЗБЕДНОСТ ВО ДИГИТАЛНИОТ ПРОСТОР

Сајбер нападите и сајбер криминалот стануваат се поприсутни, со веројатност нивниот број и софистицираност само да растат во иднина. Ова бара справување со безбедноста во дигитален контекст, односно постојано е потребно да се работи на градење на отпорност на информациските системи и отпорност на потенцијални напади и штети. Многу основни активности на држави и компании се прелеаја во сајбер просторот. Ако видиме дека цели сектори како транспорт, енергетика, здравство итн. се зависни од дигиталните технологии, јасно е дека тоа на еден начин ги прави покревки - односно целото општество и економија се изложени на напади кои сега можат да бидат од дигитална природа. Мета на сајбер напади може да бидат и поединци, на пр. ако ни биде одбиен пристапот до сметките на различни платформи, тоа може да биде знак дека нашата приватност и пристапот до личните податоци се загрозени или дека некој ги поседува нашите лозинки. Интернетот исто така може да не изложи како поединци на потенцијално вознемирување или следење, што може да се случи преку лажни или анонимни профили.

ПРИМЕРИ НА ПОВРЕДИ

- Неколку часови по објавувањето на докторската дисертација на еден државен функционер, која беше плагијат, веб страната која ја објави таа информација беше хакирана. Нападите на веб страната продолжија во текот на следната недела, а администраторите на веб страната изјавија дека трпат напади со години заради своите политичко несоодветни содржини.
- Една општина издаде соопштение дека нивната архива била нападната од вирус кој ги заклучува документите, односно го оневозможува пристапот до нив. Вирусот е наведен како причина зошто не беше возможно да им се издадат никакви документи на граѓаните, а проблемот беше решен во рок од неколку дена, меѓутоа не е јасно дали базата на тие податоци беше украдена во меѓувреме.
- Веб страната на изборната комисија на една држава беше мета на хакерски напад три часа, еден ден после одржаните избори. Нападот не предизвика поголема системска штета, но ја одложи објавата на резултатите од изборите.

- Неколку заразени компјутери ги нападнаа серверите на кои се наоѓаа порталите кои ја објавија веста за привилегиите на ќерката на гувернерката на Народната банка на една држава. Страниците на кои беше објавена веста покажуваа 404 Not Found грешка, која укажува на барана содржина која не постои на дадена адреса.
- Анонимна личност регистрираше профил на една социјална мрежа со името и презимето на еден професор кој е познат и ценет во својата заедница. Потоа, преку овој профил беа барани финансиски донации. Откако професорот укажа на тоа дека некој му го украде идентитетот на оваа социјална мрежа, профилот беше суспендиран.
- Градоначалник на еден град со денови не можел да пристапи на својот профил на една социјална мрежа, па ја известил корисничката поддршка за можен хакерски напад.
- Измамници ги користеа името и сликата на директорот на една голема банка за да промовираат услуги во врска со криптовалути, препишувајќи му реченици кои никогаш не изговорил.

ПОСЛЕДИЦИ ЗА ПОЕДИНЕЦОТ И ОПШТЕСТВОТО

Ако не се работи на зајакнување на дигиталната безбедност, како на индивидуално, така и на организационо ниво, ефектите на малициозните напади можат да предизвикаат се поголема штета за поединци и за цели друштва. Затоа што многу процеси кои се случуваат во сајберпросторот се однесуваат на голем број на луѓе, последиците од ваквите напади се потенцијално големи. Со зголемувањето на бројот на сајбер напади, се доаѓа и до нивна поголема софистицираност, па затоа е потребно константно да се работи на дигиталната безбедност. Иако од сајбер напади можеме да бидеме загрозувани сите, кога станува збор за сајбер односно, дигиталната безбедност, исто како и кога станува збор за безбедност во физичкиот простор, некои припадници на општеството се позагрозувани од други. Припадниците на посебни категории- на пример новинарите кои раководаат со осетливи информации, се честа мета на сајбер напади. Со нападите према нив и одстранувањето на содржината или крадењето на различни податоци, хакерите не влијаат само на представниците на овие групи, туку и на целото друштво за чија информираност работат.

МЕХАНИЗМИ ЗА ЗАШТИТА

- За да се заштитите од малициозен софтвер, видови софтвер што може да украдат или заклучуваат податоци, покрај инсталирањето софтвер за нивно идентификување, клучно е да не се отвораат мејлови од сомнителни адреси, да не се инсталираат непроверени програми и да не се верува на несигурни сајтови.
- За секоја корисничка сметка потребно е да се има различна лозинка, а таа треба да биде долга и да се состои од различни симболи и знаци.
- Двостепената автентикација за сметките е двојна потврда на идентитетот и е дополнителна бариера за хакерите.
- Треба да се користат доверливи апликации и редовно да се ажурираат.

На овој [линк](#) можете да пристапите до нашето кратко видео за дигитална безбедност.

За повеќе алатки кои можат да ја зајакнат дигиталната безбедност можете да го посетите следниов [сајт](#).



СЛОБОДА НА ГОВОР

Слободата на говор подразбира слобода да се искажуваат различни мислења без страв или пречки, но вклучува и слободен пристап до информации без мешање на државата или на други ентитети. Меѓутоа, ова право не треба да се сфати како апсолутно, бидејќи со себе носи должности и одговорности и е предмет на ограничувања како што е забраната на говор на омраза.

СЛОБОДА НА ИЗРАЗУВАЊЕ ВО ДИГИТАЛНИОТ ПРОСТОР

Со појавата на интернетот комуникацијата помеѓу луѓето е зголемена посебно, земајќи во увид дека можеме да комуницираме со повеќе луѓе истовремено, а тие можат да бидат на различни континенти. Покрај тоа, интернетот ни овозможува извесна анонимност, можат да се креираат профили кои нема да го издадат вашиот идентитет, па многу корисници комуницираат послободно во сајберпросторот, сметајќи дека последиците од однесувањето на интернет не мораат да бидат исти како во физичкиот свет. Озбилен проблем представува и цензурата преку филтрирање и блокирање на содржината на која прибегнуваат различни држави и корпорации, бидејќи нè спречува слободно да пристапиме до информации, кои исто така спаѓаат во слободата на изразување. Од друга страна, содржините можат да бидат уредувани не само преку цензура, туку преку неговото пласирање, односно алгоритмите можат да одлучат до кој вид на содржини ќе пристапи секој корисник. Како што се ствараат нови начини на комуникација, а и бројот на нивните рестрикции исто така се зголемува, заштитата на слободата на говор во дигитален контекст може да биде посебно предизвикувачка.

ПРИМЕРИ НА ПОВРЕДИ

- Новинарка од еден медијум е уапсена во сопствениот дом поради текст во кој пишуваше за лошите работни услови и недостатокот на заштита опрема за медицински работници за време на COVID-19 пандемијата. Беше задржана во притвор 48 саати, а болницата објави дека новинарката шири лажни информации и ја вознемирува јавноста.
- Казнени со парична казна се администраторите на една Фејсбук група во која беше поставена слика од стадо овци со наслов „Општински советници,,“ откако судот одреди дека оваа објава е увредлива и понижувачка.
- Пратеникот на една држава со сексистички и вулгарни пораки на Твитер навредувал одредени политичарки, повикувал на силување на функционерките и им се заканувал дека ќе пука во неговите политички противници.
- Откако една активистка за човекови права застапа во заштита на личност која била изложена на шовинистички напади, и сама стана

жртва на закани и напади преку социјалните мрежи. Затоа што чувствувала дека е загрозена, поднела неколку кривични пријави, меѓутоа не добила никаква реакција од надлежните органи, и продолжила да добива закани.

- Една социјална мрежа објави дека избришала илјадници лажни т.н. „бот налози“ кои се користеле за промовирање на владеачките партии во неколку држави.
- Неколку онлајн медиуми биле украдени и копирани со правње на веб страни со скоро идентичен домен и дизајн, а потоа биле користени за промоција на работата на владеачката партија и за да ги збунат редовните читатели на тие медиуми.

ПОСЛЕДИЦИ НА ПОЕДИНЦИТЕ И НА ДРУШТВОТО

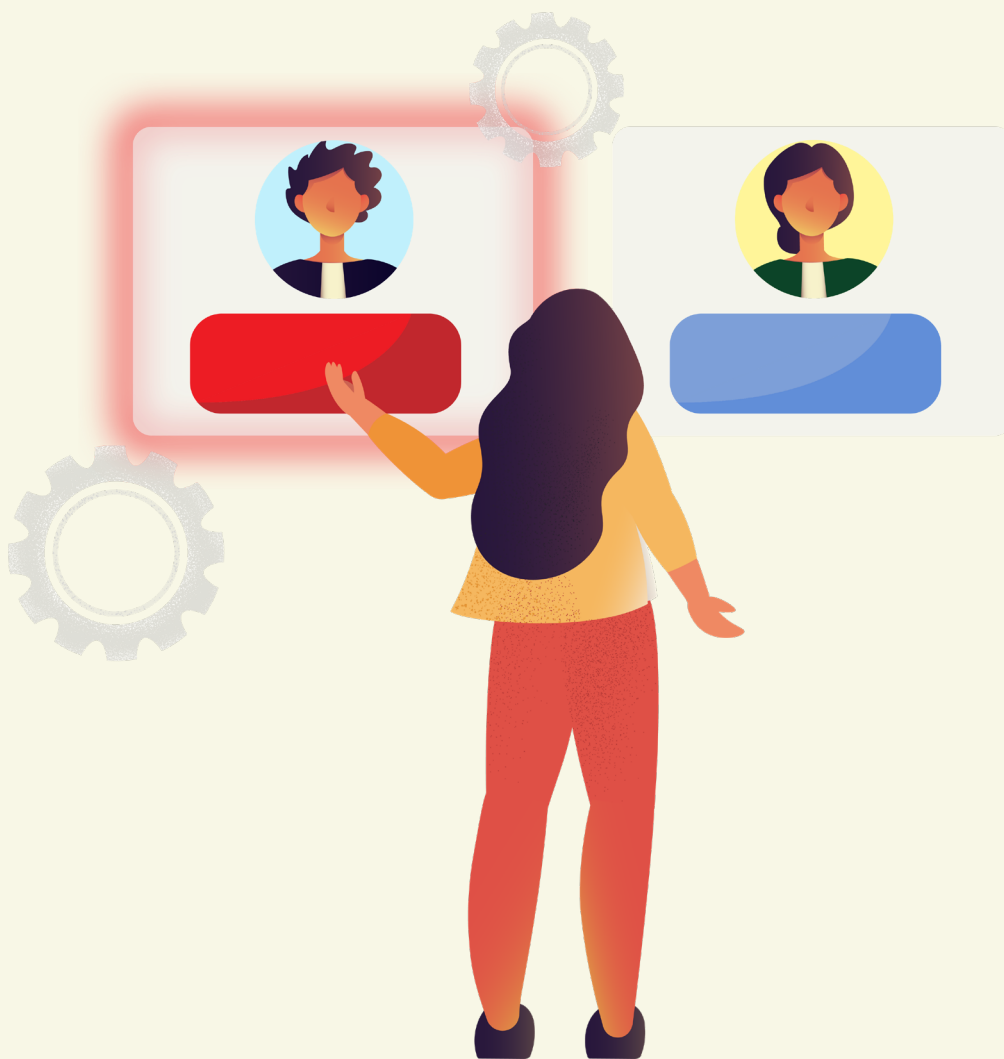
Недостатокот на слободата на говор му штети на целото друштво бидејќи му оневозможува пристап на разновидни идеји или информации кои можат да бидат од значење за јавноста т.е. кои можат да доведат до прогрес или укажување на одредени друштвени проблеми. Од друга страна, слободата на говор опфаќа и регулација на потенцијална манипулација и ширење на лажни информации. Ограничувањето на слободата на говор во вид на борба против говорот на омраза, закани, омаловажувања итн. може да го предизвика или да го зголеми бројот на насилни напади или дискриминација, да го наруши угледот и достоинството или чувството на слобода и безбедност на поединецот, може да ги замолчи малцинските групи и да ја намали кохезијата на целото друштво.

МЕХАНИЗМИ ЗА ЗАШТИТА

- Интернетот ни овозможува да бидеме не само корисници, туку и да продуцираме содржини, па тоа треба да се има во предвид кога во нашето друштво се случуваат работи кои можат да бидат цензурирани, како на пример протести.
- Доколку постојат недостапни содржини во државата во која живееме, до нив можеме да пристапиме преку на пр. Тор претражувачот, кој ни овозможува анонимност и слободен пристап до интернет.

- Доколку сметаме дека одредени веб страни ќе бидат недостапни или избришани, можеме да ги зачуваме со помош на алатки како што е the Wayback Machine. Овој алат беше овозможен од страна на Internet Archive, дигитална библиотека, која има за цел да обезбеди универзален пристап на целото знаење.
- Ако некој не навреди, ни се заканува или ги загрозува нашите лични права на друг начин, потребно е да го известиме своето опкружување и да ја блокираме и пријавиме преку друштвената мрежа личноста која не загрозува. Доколку нападите продолжат, треба да се обратиме на надлежните органи и да инсистираме на правна помош и заштита.
- Еден од начините на кои може да се реагира на замолчувањето е додатно зборување. Ако сме замолчувани заради некои критики или несогласувања, запознавањето на јавноста со дадениот проблем може да ни го врати чувството на контрола над ситуацијата.
- Ако сме жртва на говор на омраза, односно на вербален напад на основа на расна, верска, национална, сексуална, политичка, синдикална или некоја друга припадност или лично својство, потребно е да се обратиме кај некои од институциите, како полиција или кај Комесарот за заштита на рамноправноста.

На овој [линк](#) можете да пристапите до нашето кратко видео за слобода на изразување.



ДИГИТАЛНИТЕ ПРАВА ВО РЕГИОНОТ

Фондацијата SHARE воспостави постојан мониторинг на правата и слободите во дигиталното окружување и објавува редовни годишни извештаи за своите наоди. Овој процес на следење и документирање на прекршувањата на дигиталните права SHARE го започна во Србија во 2014 година, а во 2019 година се проширува во регионот во соработка со БИРН, моментално во Босна и Херцеговина, Хрватска, Унгарија, Романија и Северна Македонија. Покрај следењето на прекршувањето на правата и слободите на Интернет, мониторингот ни овозможува да ја предупредуваме и мобилизираме јавноста, исто така ни овозможува активно да учествуваме во застапувањето нова и критичка анализа на постојната легислатива за регулирање на животот на поединците, што сега се одвива и во физичкиот и во дигиталниот простор.

Можете да пристапите до базата на податоци за кршење на дигиталните права во овие 6 земји на овој [линк](#).

На овој [линк](#) можете да најдете студија за регулативата од трите области покриени во шест држави од регионот: Албанија, Босна и Херцеговина, Косово, Црна Гора, Северна Македонија и Србија.

Мислењата претставени во оваа публикација не нужно ги представуваат мислењата на Балканскиот фонд за демократија, на Германскиот маршалов фонд на САД, УСАИД или мислењата на владата на САД.



USAID
ОД АМЕРИКАНСКИОТ НАРОД

B | T | D

The Balkan Trust
for Democracy

A PROJECT OF THE GERMAN MARSHALL FUND