

Лана Божић*



ДИГИТАЛНА ПРИВАТНОСТ У СРБИЈИ: КОЛИКО НАС ЗАКОН ЗАИСТА ШТИТИ

Клик. Пост. Шер. Лајк. Колико смо свесни шта све пуштамо у етар и колико је компромитована наша приватност? Насупрот интими коју сами делимо са интернет „пријатељима“, колико има ситуација за које не знамо да се користе наши лични подаци? Живимо у времену у којем свака порука, email, онлине куповина, односно локација оставља дигитални траг. Памти се где смо били, коју смо страницу последњи пут гледали у претраживачу, коју храну најчешће поручујемо, које садржаје волимо. Низ иде у недоглед. И сви се ти подаци бележе, анализирају и чувају. Како је неко рекао, парафразирам, „нисмо посматрачи док скролујемо по друштвеним мрежама, него ми постајемо мета и предмет анализе, како би нам се касније на основу тога нешто продало.“

Зато је дигитална приватност постала једно од најважнијих правних питања данашњице. Намеће се логично питање, да ли закон прати технологију? И да ли се наши подаци користе на начин који је у складу са законом?

Кренимо најпре од тога: Шта су уопште „Лични подаци“?

Лични подаци су све информације које се односе на неко физичко лице, као што су име и презиме, адреса, број телефона, email адреса, пол, идентификациони бројеви (ЈМБГ и број личне карте). То су назовимо их основни подаци који се захтевају приликом куповине, аплицирања на разне садржаје (изузев идентификационих бројева који су посебно осетљиви). Међутим, лични подаци могу бити и IP адреса, фотографија, снимак са камере и сл. Ако може да те идентификује — то је лични податак.

Према Закону о заштити података о личности „податак о личности је сваки податак који се односи на физичко лице чији је идентитета одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета.“ Такође, према овом Закону, свако лице на које се подаци односе има право на законитост обраде, информисање, право на исправку или брисање података о личности, право на ограничење обраде података, као и право на приговор. У циљу заштите основних права и слобода физичких лица у вези са обрадом, за праћење примене овог Закона надлежан је Повереник за информације од јавног значаја и заштиту података о личности.

Претпостављамо да су ове законске одредбе просечном правном лаику неинтересантне, те да је једноставније објаснити да уколико сматрате да вам је повређено неко право о личности, можете се обратити Поверенику ради жалбе, тужити суду за накнаду нематеријалне штете или поднети у крајњем случају кривичну пријаву уколико постоји сумња да је неко лице злоупотребом свог положаја компромитовало ваш лични податак.

Е сад се враћамо на праксу, тј. на питање где су највећи ризици за приватност. Прва асоцијација је на горе поменуте друштвене мреже и интернет генерално. „Трагови“ које остављамо у виду података о себи се прикупљају, обрађују па чак и даље продају трећим лицима, и то често без стварне свести корисника интернета о томе. Затим су присутне камере, тј видео надзор који се налази свуда, од градских улица до тржних центара. Спорни моменат је да ли се приликом видео надзора користи систем за препознавање лица – тзв. биометријски надзор. Закон ово забрањује (осим у изузетним ситуацијама), али нисмо увек сигурни како се то у пракси реализује. Поред тога, путем електронских уређаја (компјутера, мобилних телефона, таблета) може се приступити нашој тренутној локацији, што је такође податак који би ваљало учинити мање јавним из безбедносних разлога.

Затим, све чешће смо упозорени о изменама услова коришћења апликација, па је тако новост да сад вештачка интелигенција „ради“ унутар dm-а на Instagram-у или Gmail-у. Ова опција се може онемогућити у подешавањима. Али већина људи овога није свесна и управо је у томе проблем.

Болнице, школе, општине, пореска управа — све поседују осетљиве податке. Погрешно чување може довести до цурења информација. Примера има још много, али ваља доћи до закључка.

Највећи проблем није закон — већ примена. Србија има Закон о заштити података о личности који прати принципе GDPR-а (Опште уредбе о заштити података) донете од стране Европске уније 2018. године. Међутим, многи системи су застарели или институције не спроводе адекватне контроле, а грађани не знају своја права.

Зато је најбитније како сами можемо да се заштитимо: не дајемо ЈМБГ без потребе, не остављамо идентификационе документе као „депозит“ (нпр. у хотелима), обавезно прочитамо основне услове приватности када се пријављујемо на апликацију колико год нам то било незанимљиво, искључимо праћење локације на апликацијама, ограничавамо могућност приступа приватним порукама у опцији подешавања и наравно пријављујемо када сумњамо у злоупотребу личних података.

Закључак: Да ли смо заштићени?

Да — али не довољно. Јер технологија се развија брже од закона, грађани нису довољно информисани, а контроле нису увек довољно ефикасне.

Заштита постоји само ако грађани знају своја права и ако их активно користе.

Датум објаве: 16.12.2025. године

*Текстови објављени на страници *Правне теме* на сајту Асоцијације судијских помоћника не представљају правне савете, већ личне ставове аутора, који не морају нужно одражавати ставове Асоцијације судијских помоћника.